4

ISSN: 2955-0270
eISSN: 3028-3310

Revista Ciberespacio, Tecnología e Innovación

Volumen 2 - Número 4
2023 (julio-diciembre)
Bogotá., Colombia

Revista **Ciberespacio, Tecnología e Innovación**

Volumen 2, número 4 julio-diciembre 2023
ISSN: 2955-0270 • eISSN: 3028-3310
Bogotá, D.C., Colombia

Indexada en:

Google Scholar

ESCUELA SUPERIOR
DE GUERRA
"General Rafael Reyes Prieto"
Colombia

EDITORIAL **ESDEG**

Esta página queda intencionalmente en blanco

Revista **Ciberespacio, Tecnología e Innovación**

Volumen 2, número 4 julio-diciembre 2023
ISSN: 2955-0270 • eISSN: 3028-3310
Bogotá, D.C, Colombia

La **RCIT** es una publicación académica de acceso abierto, revisada por pares y editada semestralmente por la **Escuela Superior de Guerra "General Rafael Reyes Prieto"** (**ESDEG**), principal centro de pensamiento conjunto del **Comando General de las Fuerzas Militares de Colombia**, a través de su **Sello Editorial ESDEG**.

2023, Escuela Superior de Guerra "General Rafael Reyes Prieto"
Vicedirección de Investigación - Sello Editorial ESDEG
Carrera 11 No. 102-50. Bogotá, D. C., Colombia
Página web: https://esdegrevistas.edu.co/index.php/rcit
Correo electrónico: esdegrevistas@esdeg.edu.co

Revista Ciberespacio, Tecnología e Innovación

1. ENFOQUE Y ALCANCE

La **Revista Ciberespacio, Tecnología e Innovación** (RCIT). La RCIT es una publicación académica de acceso abierto, revisada por pares y editada semestralmente por la Escuela Superior de Guerra "General Rafael Reyes Prieto" (ESDEG), principal centro de pensamiento conjunto de las Fuerzas Militares de Colombia, a través de su Sello Editorial ESDEG.

La **RCIT** es una revista interdisciplinaria, con un enfoque en las Ciencias Sociales (Clase 5I01, OCDE / UNESCO), abierta a la discusión y difusión de trabajos teóricos e investigaciones sobre el ciberespacio identificado como quinto dominio, en donde la ciberseguridad, la ciberdefensa y la innovación son ejes para el análisis de este ámbito. Su finalidad es abordar ejes temáticos sobre la seguridad digital, la información, las tecnologías disruptivas, las ciberamenazas, las guerras cibernéticas, entre otros temas, reconociendo la necesidad de generar desarrollo tecnológico de innovación en relación con un quinto dominio de la guerra que afecta desde lo digital a los dominios físicos como la infraestructura crítica de un Estado.

2. ORGANIZACIÓN TEMÁTICA Y PÚBLICO OBJETIVO

Cada número de la **Revista Ciberespacio, Tecnología e Innovación** cuenta con cuatro secciones:

a) **Debates:** artículos de investigación científica y tecnológica.

b) **Coyuntura:** artículos de reflexión o revisión.

c) **Perspectivas:** entrevistas a académicos o tomadores de decisión.

d) **Enfoques:** reseñas de libros.

La **RCIT** está dirigida a un amplio público que incluye decisores políticos, miembros de las Fuerzas Armadas, servidores públicos, profesionales, docentes, investigadores y estudiantes de ciencias sociales y de otras áreas del conocimiento, interesados en la seguridad y la defensa.

3. TIPOLOGÍA E IDIOMA DE LOS ARTÍCULOS

La **RCIT** publica artículos en español e inglés en tres categorías:

a) **Investigación científica y tecnológica:** documento que presenta de manera detallada los resultados originales derivados de proyectos de investigación y/o desarrollo tecnológico finalizados.

b) **Reflexión:** documento que ofrece resultados de investigación desde una perspectiva analítica, interpretativa y crítica del autor, sobre un tema específico, recurriendo a fuentes originales.

c) **Revisión:** documento que organiza, analiza y se integran los resultados de investigaciones publicadas o no publicadas sobre un campo en ciencia o tecnología, con el fin de dar cuenta de los avances y las tendencias de desarrollo.

4. PERIODICIDAD

La **RCIT** es editada semestralmente (enero-junio y julio-diciembre) en formato en formato digital (eISSN: 3028-3310) e impreso (ISSN: 2955-0270). La versión en línea y la versión impresa aparecen publicadas el penúltimo día del último mes del periodo de cada número, esto es, 30 de junio para el número enero-junio y 30 de diciembre para el número julio-diciembre. Cada uno de los artículos de la **RCIT** tiene un DOI (Digital Object Identifier) asignado para su identificación y referenciación.

5. FINANCIAMIENTO

La **Revista Ciberespacio, Tecnología e Innovación** es una publicación académica de la Escuela Superior de Guerra "General Rafael Reyes Prieto" (ESDEG), perteneciente, a su vez, al Comando General de las Fuerzas Militares de Colombia que, como entidad pública, se financia con los recursos asignados por el gobierno nacional. Con el fin de mantener su carácter crítico e independiente, la **RCIT** no acepta financiamiento ajeno a la ESDEG para su funcionamiento. Así las cosas, todo el proceso de publicación de la revista está completamente libre de costo para los autores; tampoco se realizan cobros por el envío, procesamiento y publicación de artículos (*no article submission or processing charge*).

6. ACCESO ABIERTO, DERECHOS DE AUTOR Y LICENCIA PARA PUBLICACIÓN

7. POLÍTICA CROSSMARK

La **RCIT** utiliza Crossmark para mantener informados a sus lectores sobre cualquier cambio que tengan los artículos publicados. CrossMark es una iniciativa de CrossRef para proporcionar una forma normalizada de localizar la versión oficial de un documento. La **RCIT** reconoce la importancia de mantener la integridad de los registros académicos para investigadores y bibliotecas, razón por la cual garantiza que su archivo electrónico siempre cuenta con un contenido confiable.

Al hacer clic en el icono CrossMark se informa al lector sobre el estado actual del documento así como información adicional sobre el historial de publicación de este. Los contenidos que muestran el ícono de CrossMark son aquellos contenidos publicados en la página web de la **RCIT**, actuales o futuros.

8. ARCHIVO DE LOS CONTENIDOS

La **RCIT** utiliza la plataforma Portico para el archivo digital de los contenidos publicados. Así mismo, la **RCIT** permite que los autores puedan autoarchivar en repositorios institucionales, temáticos o páginas webs personales su artículo en la versión final publicada en línea.

9. RESPONSABILIDAD DE CONTENIDOS

La responsabilidad por el contenido de los artículos publicados por la **RCIT** corresponde exclusivamente a los autores. Las posturas y aseveraciones presentadas son resultado de un ejercicio académico e investigativo que no representa la posición oficial ni institucional de la Escuela Superior de Guerra "General Rafael Reyes Prieto", el Comando General de las Fuerzas Militares de Colombia o el Ministerio de Defensa Nacional.

10. INDEXACIÓN

La **Revista Ciberespacio, Tecnología e Innovación** se encuentra incluida en los siguientes Sistemas de Indexación y Resumen (SIR):

Google Scholar

Tabla de Contenido

Esta página queda intencionalmente en blanco

Editorial

Editorial

Esta página queda intencionalmente en blanco

Revista Ciberespacio, Tecnología e Innovación
Volumen 2, número 4, julio-diciembre 2023 (pp. 103-104)
Bogotá, D.C, Colombia

EDITORIAL ESDEG

Editorial. La innovación en la ciberseguridad y ciberdefensa en escenarios complejos

Editorial. Innovation in cybersecurity and cyberdefense in complex scenarios

DOI: https://doi.org/10.25062/2955-0270.4819

Tania Lucia Fonseca Ortiz
Editora en Jefe de la Revista Ciberespacio, Tecnología e Innovación

La Escuela Superior de Guerra "General Rafael Reyes Prieto", hace pública la cuarta edición de la revista Ciberespacio, Tecnología e Innovación, correspondiente al Volumen 2 y Número 4 del segundo semestre del 2023. Esta edición titulada *La innovación en la ciberseguridad y ciberdefensa en escenarios complejos*, es una recopilación de productos resultado de investigación que tiene como objetivo dar a conocer a la comunidad académica sobre las oportunidades para el desarrollo de propuestas de innovación que aporten a la seguridad y defensa, reconociendo que el ciberespacio se ha convertido en un escenario complejo que impulsa a las instituciones y a los Estados a que generen propuestas de emprendimiento tecnológico. Por lo anterior, se presenta la edición organizada en diferentes secciones: debates, contexto, perspectivas y enfoques.

Para la *Sección Debates* se presentan tres artículos resultados de investigación:

El primero titulado *Competencias digitales del mando militar en el marco DigComp 2.2: caso Escuela Militar de Cadetes "General José María Córdova"*, una investigación descriptiva que aborda la necesidad de fortalecer las competencias conforme a los niveles establecidos en el manual de competencias digitales de Europa. En este documento, y a manera de propuesta, se realizan recomendaciones para que los cadetes de la escuela de oficiales del Ejército Nacional de Colombia desarrollen una serie de competencias mínimas que tendrán que emplear como futuros líderes y en función a normativas europeas. Como resultado, se establece la importancia de proyectar el conocimiento y competencias básicas en áreas de la ciberseguridad como parte de su formación como líder que tendrá que afrontar escenarios complejos generados en el ciberespacio.

El segundo artículo, titulado *Propuesta de capacitación virtual para promover la cibercultura en el Ejército Nacional de Colombia,* es el resultado de un análisis de necesidades en materia de la formación de miembros del Ejército Nacional de Colombia en temas relacionados con la cibercultura. A raíz del complejo contexto en seguridad y defensa de la información, el autor realiza una propuesta orientada a capacitar a oficiales, suboficiales y civiles para salvaguardar la información institucional ante ciberincidentes. Como resultado, se plantea una propuesta de capacitación que permita a largo plazo fomentar la cibercultura a nivel organizacional.

El tercer artículo, qué tiene como nombre *Uso de satélites artificiales para la integración de las plataformas estratégicas de las Fuerzas Militares*, es un análisis descriptivo sobre la importancia de integrar las plataformas estratégicas relacionadas con la comunicación en las Fuerzas Militares Colombianas mediante la tecnología satelital. El autor realiza una descripción del contexto de las comunicaciones en ámbitos operacionales militares y resalta la necesidad de articular las comunicaciones dado los nuevos escenarios tecnológicos. Esta investigación abre el debate sobre el uso de tecnologías y la necesidad de innovar como parte del fortalecimiento de las fuerzas.

Para *Sección Debates, Una aproximación del Metaverso a los sistemas de comando y control en las Fuerzas Militares de Colombia,* se presenta un artículo corto de reflexión y análisis sobre los sistemas de comando y control que pueden ser impulsadas por tecnologías como el metaverso. En este análisis, el autor propone la creación de un metaverso para la toma de decisiones con el objetivo de fortalecer el direccionamiento a nivel estratégico de las Fuerzas Militares.

Sección Perspectivas, se presenta la entrevista titulada *Importancia de la ciberseguridad y seguridad de la información en la política Colombia: Entrevista David Luna Sánchez,* se aborda una importante apreciación sobre la ciberseguridad de la información en el ámbito político. En esta interesante entrevista se reconoce la existencia de riesgos, peligros y amenazas que pueden afectar al sistema político, y al mismo tiempo, se reconoce la necesidad de considerar la ciberdefensa como un aspecto importante en el escenario social colombiano.

Finalmente, en la *Sección Enfoques,* se presenta el libro recomendado titulado *Ciberseguridad, una estrategia informático/militar,* en este escrito se realiza un breve resumen y descripción de una lectura que resulta ser recomendada para las personas interesadas en profundizar, de manera conceptual y técnica, en temas relacionados con la ciberseguridad y la ciberdefensa.

Esperamos que esta edición motive a los académicos, investigadores y estudiantes interesados en la ciberseguridad y ciberdefensa, a compartir sus propuestas resultado de investigación para que sean compartidas a nivel nacional e internacional, y de esta manera, permita la generación de una ciberconciencia y cibercultura en temas importantes que se encuentran determinados por el empleo tecnológico.

Debates

Debates

Esta página queda intencionalmente en blanco

Revista Ciberespacio, Tecnología e Innovación
Volumen 2, número 4, julio-diciembre 2023 (pp. 107-146)
Bogotá, D.C, Colombia

EDITORIAL ESDEG

Competencias digitales del mando militar en el marco DigComp 2.2: caso Escuela Militar de Cadetes "General José María Córdova"

Digital competencies of the military leadership within the framework of DigComp 2.2: case of the "General José María Córdova" Military Cadet School

DOI: https://doi.org/10.25062/2955-0270.4810

John Alexander Villarraga Gamboa
Escuela Superior de Guerra "General Rafael Reyes Prieto", Bogotá D. C., Colombia

Resumen

La brecha de competencias digitales se ha constituido en un problema creciente para quienes requieren interactuar con las nuevas tecnologías de la información y de las comunicaciones, mucho más en países en vía de desarrollo como lo es Colombia. Esta brecha se refiere a la diferencia en el nivel de habilidades tecnológicas entre aquellos que tienen acceso a la tecnología y aquellos que no lo tienen, y es precisamente este enfoque el determinado como punto de atención en el desarrollo del presente trabajo. En contexto, para el Ejército Nacional este problema no es ajeno, y es que, a pesar de ser actores activos de las tecnologías, los alféreces de la Escuela Militar carecen de las habilidades requeridas para desenvolverse de manera efectiva y segura en los entornos digitales como los futuros promotores, generadores y ejecutantes de políticas e iniciativas de seguridad y defensa en el ciberespacio.

Palabras Clave: Competencias digitales; tecnologías; ciberseguridad; brecha digital.

Abstract

The digital skills gap has become a growing problem for those who need to interact with new information and communication technologies, especially in developing countries like Colombia. This gap refers to the difference in the level of technological skills between those who have access to technology and those who do not, and it is precisely this focus that is determined as the point of attention in the development of this work. In this context, for the National Army, this problem is not unfamiliar. Despite being active players in technology, the cadets of the Military School lack the required skills to effectively and safely navigate digital environments as future promoters, creators, and implementers of cybersecurity policies and initiatives.

Key words: Digital competencies; technologies; cybersecurity; digital gap.

Artículo de reflexión
Recibido: 28 de noviembre de 2023 • **Aceptado:** 18 de diciembre de 2023
Contacto: John Alexander Villarraga Gamboa villarragaj@esdeg.edu.co

Introducción

El tema de competencias digitales ha sido ampliamente abordado por autores y organizaciones alrededor del mundo por considerarse un factor determinante para la inclusión de los ciudadanos en la sociedad de la información (González *et al.,* 2016) y por los desafíos que suponen los procesos de transformación digital, "[…] las tecnologías emergentes, como la inteligencia artificial, la realidad virtual y aumentada, la robotización, el internet de las cosas, la "dataficiación" o nuevos fenómenos como la información errónea y desinformación […]" (Vuorikari, *et al.,* 2022, p.1). Todas estas, han llevado a nuevas exigencias de alfabetización digital, que se vieron acentuadas a partir de la pandemia del COVID-19, que obligó a los profesionales en todos los campos a establecer interacciones a través de canales y medios informáticos, supeditados tanto a las facilidades, los riesgos propios del ciberespacio, "[…] la solidaridad, el aprendizaje autónomo, el cuidado propio y de otros, las competencias socioemocionales, la salud y la resiliencia, entre otros." (CEPAL-UNESCO, 2020, p.4).

En Colombia, desde el año 2006 se han actualizado varias iniciativas en materia de política pública en medio de un entorno de constante transformación digital. Es así como, con el documento *Estándares básicos de competencias en tecnología e informática* del Ministerio de Educación Nacional (2006) se especificaron las competencias a desarrollar en áreas puntuales de la educación formal, especialmente en tecnología e informática, siendo este el punto de partida donde se evidencia que existe una brecha entre las competencias que se deben adquirir y las capacidades individuales que aún se encuentran por desarrollar.

Por su parte, el Departamento Nacional de Planeación (2022), a partir del año 2011, y en los años siguientes, expidió y actualizó los documentos CONPES que han contribuido al desarrollo de estrategias de alcance nacional, dada la inexistencia de estas y las debilidades del Estado frente a la gestión de amenazas para la ciberseguridad y la ciberdefensa, que, en algunos casos, como lo expone la ENISA[1] (2016), se debe a que solo se desarrolla cuando existe una necesidad apremiante de cumplir.

El Ejército Nacional, como parte de las entidades del Estado, no ha sido ajeno a los planteamientos de interacción en el ciberespacio, máxime cuando es este uno de los pilares en el mantenimiento de la seguridad y defensa nacional, estableciendo y ejecutando conjuntamente con otras entidades, políticas y estrategias que impactan el sector público y privado en el orden nacional. Por tal razón, atendiendo dicho rol para dar cumplimiento a las disposiciones del CONPES 3995 del 2020 *Política Nacional de Confianza y Seguridad Digital,* la Fuerza requiere de capacidades, enfocadas en el talento humano,

1 European Union Agency For Network and Information Security

cuyos esfuerzos sean dirigidos al desarrollo de competencias profesionales de los tomadores de decisiones.

En este sentido, este artículo investigación se desarrolló bajo el marco teórico propuesto por Van Dijk (2005), denominado *Teoría de los recursos y de la apropiación,* analizando las barreras en la apropiación de una nueva tecnología basada en el "acceso diferencial" (Pick y Sarkar, 2016, p.3.895) a través de los cuatro tipos de acceso presentados por el autor, e identificadas en el estudio realizado a los alféreces de la Escuela Militar de Cadetes "José María Córdova" (en adelante, ESMIC) como futuros oficiales al mando de unidades militares, en el entendido final que las brechas digitales, en mayor o menor medida, son generadas por barreras en el acceso y por consiguiente en la apropiación de las tecnologías de información y comunicaciones. (Gómez *et al.,* 2018).

Para hacer un análisis de la estrategia propicia de cierre de las brechas y barreras identificadas, se estableció como referencia el Marco de Competencias Digitales para la Ciudadanía de la Comisión Europea (DigComp 2.2.), por su orientación hacia el manejo de habilidades y la formación digital de los individuos, y por la estructuración articulada de este con otras organizaciones globales como la Organización Internacional del Trabajo (OIT), la Organización de las Naciones Unidas para la Cultura, las Ciencias y la Educación (UNESCO) y el Banco Mundial (Vuorikari, *et al.,* 2022) . El modelo de referencia conceptual del DigComp evalúa cada una de las competencias necesarias a partir de áreas que van desde la búsqueda y gestión de información y datos, la comunicación y colaboración, pasando por la creación de contenidos y la seguridad, sin dejar de lado a la resolución de problemas (Vuorikari, *et al.,* 2022), de ahí que fue pertinente tomar este documento como base conceptual en la investigación.

Por último, el artículo respondió a la siguiente pregunta de investigación: ¿De qué manera fortalecer las competencias digitales de los Alféreces de la Escuela Militar José María Córdova del Ejército Nacional de Colombia, de acuerdo al marco de competencias digitales DigComp 2.2. de la Unión Europea y teniendo en cuenta el cumplimiento del CONPES 3995 del 2020?, orientándose hacia el objetivo general de proponer una estrategia para fortalecer las competencias digitales de los alféreces de la ESMIC, de acuerdo al marco de competencias digitales DigComp 2.2 y teniendo en cuenta el cumplimiento del CONPES 3995 del 2020.

Así mismo, a través de los objetivos específicos desarrollados en el siguiente orden: primero, se describió el marco de competencias digitales DigComp 2.2 y su relación frente a lo dispuesto por el CONPES 3995 de 2020; segundo, se identificó el estado actual en competencias digitales de los alféreces para lograr establecer las competencias digitales requeridas por estos; y tercero, se diseñó la estrategia buscada, en el marco de los documentos referenciados previamente.

De esta forma, se defendió la tesis sobre la carencia del personal en habilidades, conocimientos y actitudes digitales para la orientación, liderazgo y gestión de acciones frente a los objetivos y responsabilidades definidos por el CONPES 3995 de 2020 para el Ministerio de Defensa Nacional - EJC, y lograr superar las brechas existentes.

Con ello, se propuso una estrategia que además de los cinco dominios del marco DigComp 2.2., logró la implementación de un sexto, que trata de las competencias para afianzar o fortalecer el concepto de defensa en el entorno digital de gobierno y Estado, por su importancia como riesgo global (World Economic Forum, 2023a), y porque en cabeza del Ejército Nacional, y particularmente en su personal al mando, está la dirección, administración y ejecución de las medidas para preservar y defender los intereses nacionales en el ciberespacio.

Metodología

Se desarrolla con un enfoque cualitativo y de alcance descriptivo que permitirá la generación de la estrategia propuesta como objetivo general. Teniendo en cuenta lo anterior, el diseño planeado para la investigación es diseño no experimental (transeccional descriptivo), orientado a las competencias digitales, las tecnologías digitales, y la seguridad digital como categorías de análisis. La población universo de estudio será sobre el total de los alféreces disponibles en la Escuela Militar, al momento de la implementación de la herramienta de recolección de información, teniendo como mínimo de base de estudio 50 alféreces.

Atendiendo al tipo de estudio, las fuentes serán primarias, apoyadas conceptual y teóricamente con fuentes académicas como SciELO y Redalyc, además de las publicaciones de política pública y documentos generados por entidades estatales. Los datos recolectados se analizarán mediante métricas que indiquen los resultados y sobre los cuales de manera cualitativa se expresen reflexiones tendientes a facilitar el diseño de la estrategia propuesta.

Competencias digitales DigComp 2.2 de la Unión Europea y su relación frente a lo dispuesto por el CONPES 3995 de 2020

En el contexto de la revolución digital y cuarta revolución industrial, que según Cujabante ***et al.*** (2020) es también una revolución cultural, la disposición hacia el uso de tecnologías de la información y las comunicaciones TIC´S, determinan los niveles de desarrollo y progreso de un estado.

Es así como para Colombia, fomentar las capacidades en este campo ha sido una labor paulatina e incremental, partiendo desde la puesta en marcha a nivel nacional de la evaluación de la educación por competencias, definidas estas por Ríos y Herrera (2017)

como los "saberes combinados que integran el ser, el saber hacer y el saber estar" (p. 1076) frente a condiciones que requieran "usar el conocimiento para aplicarlo a la solución de situaciones nuevas o imprevistas, fuera del aula, en contextos diferentes, y para desempeñarse de manera eficiente en la vida personal, intelectual, social, ciudadana y laboral". (Ministerio de Educación Nacional, 2006, p. 5).

En este sentido, el Ministerio de Educación Nacional (2017) definió como una competencia laboral general a la competencia tecnológica, la que resalta procedimientos de innovación, uso de herramientas informáticas, y apropiación y creación de tecnologías. (Ministerio de Educación Nacional, 2017, p. 9), pudiendo definirse entonces como una *competencia digital,* esto en concordancia con lo expuesto por la recomendación del Consejo de la Unión Europea a los Estados miembros sobre las competencias clave necesarias para el aprendizaje permanente, que estableció la competencia digital como aquella que "[…] implica el uso seguro, crítico y responsable de las tecnologías digitales para el aprendizaje, en el trabajo y para la participación en la sociedad, así como la interacción con estas." (Vuorikari, *et al.,* 2022, p.3).

Ahora bien, como soporte a la línea de esfuerzo de generación de competencias personales desde la educación en el ámbito de la tecnología (competencia digital), el Gobierno Nacional, como otros gobiernos, consiente que para lograr una verdadera transición hacia una sociedad digital, requiere definir estrategias que motiven a intermediarios e individuos a aprovechar los recursos existentes o a innovar de acuerdo a las necesidades (Carretero, 2021), a través de los documentos del Consejo Nacional de Política Económica y Social (CONPES), ha formulado políticas frente al fortalecimiento de estrategias que mediante el uso de las TIC han buscado alcanzar una mayor productividad, inclusión, eficiencia, prosperidad y bienestar social (Departamento Nacional de Planeación, 2019).

La evolución de las políticas en el ámbito digital, desde los primeros lineamientos para una política nacional e informática en 1997, llevó a la construcción en el 2020 del CONPES 3995 denominado *Política Nacional de Confianza y Seguridad Digital*, con el argumento de robustecer y generar condiciones para promover la confianza digital, a través de gobernabilidad, inclusión, competencia y seguridad (Departamento Nacional de Planeación, 2020), basado en la "creciente participación de ciudadanos en el entorno digital, la alta dependencia de la infraestructura digital y el aumento en el uso y adopción de nuevas Tecnologías de la Información y las Comunicaciones (TIC) traen consigo una serie de riesgos e incertidumbres" (Departamento Nacional de Planeación, 2020, p. 3), relacionados con la seguridad en los entornos digitales.

Frente a tales desafíos, el Gobierno Nacional ha priorizado también que el país desarrolle y disponga de capacidades para la gestión acertada frente a las amenazas, los ataques o los incidentes, que cada día son más sofisticados y complejos, y que implican impactos graves en la sociedad (Departamento Nacional de Planeación, 2020), atañendo

esta prioridad tanto al sector privado como, en un mayor nivel de responsabilidad, al sector público, y en detalle, al Ministerio de Defensa Nacional, en cabeza de las fuerzas del Estado encargadas de garantizar la seguridad y defensa nacional en el ciberespacio. Así mismo, orientando a este a la adopción de modelos y estándares con "énfasis en nuevas tecnologías para preparar al país a los desafíos de la 4RI" (Departamento Nacional de Planeación, 2020, p. 27), que proporcionen un lenguaje de capacidades común, práctico e idóneo para ciudadanos y funcionarios.

Competencias digitales DigComp 2.2

A partir de la recomendación sobre las competencias clave y definidas como "aquéllas que todas las personas precisan para su realización y desarrollo personal, así como para la ciudadanía activa, la inclusión social y el empleo" (Consejo de la Unión Europea, 2006, p.13) por parte del consejo de la Unión Europea, el 18 de diciembre de 2006, que hizo referencia a fomentar y desarrollar la oferta de las competencias clave en sus estrategias de aprendizaje, además de utilizar como marco de referencia el documento *Competencias clave para el aprendizaje permanente — un marco de referencia europeo* (Consejo de la Unión Europea, 2006), estableció entre otras a la comunicación en lenguas extranjeras, la competencia digital, y a las competencias sociales y cívicas, como parte de las 8 competencias a aplicar. Estas competencias se actualizarían posteriormente, culminando en la relación presentada en la figura 1.

Figura 1. Competencias clave

Fuente: Documento DigCom 2.2 pág. 5

Conocida la recomendación de 2006, los trabajos para diseñar e implementar la competencia digital finalizaron en una primera etapa en el 2013, con la publicación del primer marco de referencia denominado DigCom, el que luego de ser actualizado en 2017 (DigCom 2.0), y 2020 (DigCom 2.1), presenta actualmente su versión 2022 con el DigCom 2.2, que realciona la competencia digital como un compendio de 21 competencias divididas en cinco grupos o áreas de competencia, como se muestra en la figura 2.

Figura 2. Taxonomía de competencias.

Fuente: Documento DigCom 2.2 pág.4.

Así las cosas, las áreas de competencia corresponden a:

1. Área de búsqueda y gestión de información y datos, en la que se ejecutan actividades de navegación en entornos digitales, búsqueda de datos, recopilación de información, evaluar las fuentes y gestionar contenidos.
2. Área de comunicación y colaboración, que contiene competencias para la participación activa en la sociedad a través de los recursos digitales.
3. Área de creación de contenidos, que permite la generación de contenidos digitales, la observancia del derecho de autor y mejorar e integrar la información.

4. Área de seguridad, que promueve la protección física y mental de los ciudadanos digitales, sus dispositivos, contenidos y la garantía de entornos seguros.
5. Área de resolución de problemas, en la que se es competente para identificar situaciones, problema en el entorno digital y hacer uso de herramientas para mejorar procesos.

Cabe destacar, que las áreas de seguridad y de resolución de problemas, son de carácter transversal, ya que se sobreentiende que se deben aplicar en todo momento y condición.

En cuanto al nivel de aptitud en la competencia, la evaluación propuesta por el marco de referencia establece como niveles generales al nivel básico, el nivel intermedio, el nivel avanzado y un cuarto nivel denominado altamente especializado. A su vez, estos cuatro niveles se subdividen cada uno en dos niveles más (niveles granulares) que permiten detallar el estado de la competencia para el desarrollo de la tarea particular.

Ahora bien, el nivel de progresión de las competencias se evalúa a través de las variables de "complejidad de la tarea, la autonomía y la necesidad de orientación para llevarlas a cabo, y el dominio cognitivo indicado por el uso de los verbos de acción según la taxonomía de Bloom" (Vuorikari, *et al.*, 2022, p. 70).

Par entender el nivel de aptitud y progresión de la competencia, resulta pertinente resumir los conceptos con la figura 3.

Figura 3. Descripción de aptitud y profesión.

4 NIVELES GENERALES	Básico		Intermedio		Avanzado		Áltamente especializado	
8 NIVELES GRANULARES	1	2	3	4	5	6	7	8
COMPLEJIDAD DE LAS TAREAS	Tarea sencilla	Tarea sencilla	Tareas bien definidas y rutinarias, y problemas sencillos	Tareas, y bien definidas y problemas no rutinarios	Diferentes tareas y problemas	Tareas más adecuadas	Resolver problemas complejos con soluciones limitadas	Resolver problemas complejos con muchos factores que interactúan
AUTONOMÍA	Con orientación	Autonomía y con orientación cuando sea necesario	Sin ayuda	Independiente y según mis necesidades	Guiar a los demás	Es capaz de adaptarse a los demás en un contexto complejo	Integrarse para contribuir a la práctica profesional y orientar a los demás	Proponer nuevas ideas y procesos al sector
DOMINIO COGNITIVO	Recordando	Recordando	Entendiendo	Entendiendo	Aplicando	Evaluación de	Creación de	Creación de

Fuente: Documento DigCom 2.2 pag.71.

Por último, el marco de referencia DigCom 2.2, expone ejemplos de los conocimientos, habilidades y actitudes para el desempeño de la competencia. Tal es el caso de la competencia 1.1 navegar, buscar y filtrar datos, información y contenidos digitales, que en cuanto a conocimientos se ejemplifica, entre otros, con: sabe que algunos de los contenidos en línea que aparecen en los resultados de la búsqueda pueden no ser de acceso

libre o gratuito y pueden requerir el pago de una cuota o la suscripción a un servicio para poder acceder a ellos (Vuorikari, *et al.,* 2022, p. 86).

En relación a las habilidades de esta misma competencia, el ejemplo es el de "puede elegir el motor de búsqueda que más se ajuste a sus necesidades de información ya que distintos motores de búsqueda pueden ofrecer resultados diferentes incluso para la misma consulta" (Vuorikari, *et al.*, 2022, p. 86).

Finalmente, al hablar de actitudes, se tiene, por ejemplo: "evita intencionadamente las distracciones y pretende evitar la sobrecarga de información al acceder y navegar por la información, los datos y los contenidos" (Vuorikari, *et al.*, 2022, p. 86), mejorando así el uso, entendimiento e interpretación de este marco de referencia.

CONPES 3995 de 2020

Como se expuso en la parte introductoria de este objetivo, el CONPES 3995 de 2020 (01 de julio), fue estructurado como "Política Nacional de Confianza y Seguridad Digital" (Departamento Nacional de Planeación, 2011, p.1), por parte del Departamento Nacional de Planeación, el Ministerio de Tecnologías de la Información y las Comunicaciones, y el Departamento Administrativo de la Presidencia de la República, para establecer acciones hacia el fortalecimiento de la confianza digital y la mejora de la seguridad, consiguiendo con esto un presente y futuro más competitivo para el país.

Es de anotar que la intención de un entorno digital nacional más seguro se vio materializada a nivel de CONPES con el documento 3701 de 2011, enfocado a presentar lineamientos de política en ciberseguridad y ciberdefensa, especialmente para entes gubernamentales (Departamento Nacional de Planeación, 2011), creando "[…] las máximas instancias de coordinación y orientación superior en torno a la Seguridad Digital en el gobierno […]" (Baldomero, 2019, p.117), y robusteciendo las condiciones y las capacidades específicas de cara a las amenazas en el ciberespacio con la puesta en marcha del "Grupo de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT), el Centro Cibernético Policial, CECIP y el Comando Conjunto Cibernético CCOCI, bajo un modelo de coordinación intersectorial". (Departamento de Planeación Nacional, *et al.,* 2020, p.10).

En 2016, el CONPES 3854 *Política Nacional de Seguridad Digital,* fortaleció las capacidades en seguridad digital, hacia la gestión de riesgos, promoviendo estrategias dirigidas a la prevención más que a la reacción ante las amenazas. (Departamento Nacional de Planeación, 2016).

En lo corrido del 2018, con el Decreto 1008, el esfuerzo fue dirigido hacía fortalecer las políticas de seguridad de la información. Se expide además el *Manual de Gobierno Digital* del Ministerio de las Tecnolgias de la Información y las Comunicaciones - MINTIC

y se da línea de aplicación del *Modelo de Seguridad y Privacidad de la Información* (MSPI), modelo enfocado hacia "[…] preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos" (Ministerio de las Tecnolgias de la Información y las Comunicaciones, 2021, párr.2) por parte de los usuarios de la infraestructura informática, que en gran medida corresponden al eslabón más débil de la seguridad de la misma (Cuevas y Da Silva, 2022).

Para el 2019, y con posterioridad a la Ley 1955 que planteó el plan Nacional de Desarrollo 2018-2022, y en él las estrategias para desarrollar el "Pacto por la transformación digital de Colombia: Gobierno, empresas y hogares conectados con la era del conocimiento" (Congreso de la República, 2019, p.1), el Ministerio de Defensa Nacional generó la *Política de Defensa y Seguridad para la legalidad, el emprendimiento y la equidad de Colombia* con estrategias de fortalecimiento militar para defensa en el ciberespacio. De la misma forma, para este año se expide el CONPES 3795 *Política Nacional para la Transformación Digital e Inteligencia Artificial,* cuyo objetivo fue "aumentar la generación de valor social y económico a través de la transformación digital del sector público y del sector privado" (Departamento Nacional de Planeación, 2019, p.38), ampliando la confianza digital hacia la ciudadanía en los diferentes sectores del país.

Todo lo anterior, en resumen, se establece como los antecedentes de política sobre confianza y seguridad digital en el país, y dan cuenta de la evolución de estas a la par de las necesidades crecientes de cara a las nuevas tecnologías, las cuales, si bien presentan falencias complejas como se verán más adelante, también han llevado a que, como lo publica el DQ Institute (2022) en su índice de seguridad infantil, el país se sitúe en el puesto doce a nivel global, después de Estados Unidos (puesto 10) y del Reino Unido en el puesto número uno, en desarrollo de actividades de protección de la infancia en el ciberespacio.

Ahora bien, tras el análisis diagnóstico realizado en el CONPES 3995, se determinaron las siguientes vulnerabilidades y debilidades en el país:

1. **Debilidades en las capacidades en seguridad digital de los ciudadanos, del sector público y del sector privado.** En este primer punto se concluye que en "Colombia hay deficiencias en todo el conjunto de las capacidades relacionadas con la seguridad digital, por parte de los ciudadanos, del sector público y del sector privado […]" (Departamento de Planeación Nacional, *et al.*, 2020, p.23).
2. **El marco de gobernanza en materia de seguridad digital no ha alcanzado un grado de desarrollo adecuado.** Esta debilidad determinó que en el país no hay la suficiente interacción entre las entidades, demostrando baja cohesión y coordinación de medidas robustas frente a la seguridad digital del orden nacional.
3. **Se requiere la adopción de modelos, estándares y marcos de trabajo en materia de seguridad digital con énfasis en nuevas tecnologías.** Se concluye la

> necesidad de fortalecer las capacidades de gestión ante las amenazas de las nuevas tecnologías, por cuanto el país no cuenta con modelos actualizados en seguridad digital. (Departamento Nacional de Planeación, 2019, pp.18 - 26),

Así pues, el CONPES 3995, para hacer frente al contexto negativo visualizado en el diagnóstico, planteó los siguientes objetivos específicos:

1. Fortalecer las capacidades en seguridad digital de los ciudadanos, del sector público y del sector privado para aumentar la confianza digital en el país […] 2) Actualizar el marco de gobernanza en materia de seguridad digital para aumentar su grado de desarrollo y mejorar el avance en seguridad digital del país […] 3) Analizar la adopción de modelos, estándares y marcos de trabajo en materia de seguridad digital, con énfasis en nuevas tecnologías para preparar al país a los desafíos de la 4RI. (Departamento Nacional de Planeación, 2020, pág. 27)

Para desarrollar lo anterior, se estableció un plan de acción con medidas particulares a cada objetivo, a continuación, se referencia de modo general las definidas para el Ministerio de Defensa Nacional y sus instituciones:

Objetivo 1. *Fortalecer las capacidades en seguridad digital de los ciudadanos, del sector público y del sector privado para aumentar la confianza digital en el país.*

El compromiso del MDN en este objetivo, se enfoca en trabajar de manera conjunta con entidades como el DAPRE[2], el MINTIC, la SIC[3], el SENA[4], el DAFP[5], el Ministerio de Justicia y la Fiscalía General de la Nación, y la DNI[6] para el diseño de estrategias de generación de capacidades en seguridad digital para ciudadanos y funcionarios públicos, el diagnóstico y desarrollo de normatividad, el diseño e implementación de acciones de mejoramiento interno del talento humano, y la implementación de redes de colaboración y gestión frente a incidentes (Departamento Nacional de Planeación, *et al.*, 2020).

Objetivo 2. *Actualizar el marco de gobernanza en materia de seguridad digital para aumentar su grado de desarrollo y mejorar el avance en seguridad digital del país.*

Para este caso, el compromiso del MDN se centra en trabajar con el MINTIC para crear un sistema de nivel nacional para gestionar los incidentes de carácter cibernético, así como, generar y poner a disposición un mecanismo de gestión de información entre

2 Departamento Administrativo de la Presidencia de la República.

3 Superintendencia de Industria y Comercio.

4 Servicio Nacional de Aprendizaje.

5 Departamento Administrativo de la Función Pública

6 Dirección Nacional de Inteligencia.

los actores críticos del país, generando reportes de seguimiento de avances institucionales (Departamento Nacional de Planeación, *et al.,* 2020).

Objetivo 3. *Analizar la adopción de modelos, estándares y marcos de trabajo en materia de seguridad digital, con énfasis en nuevas tecnologías para preparar al país a los desafíos de la 4RI.*

Sobre este último, se invita al MDN a participar, en conjunto con el MINTIC y la DNI, para generar "guías metodológicas para la identificación y gestión de riesgos de seguridad digital en la adopción que las entidades del sector público hagan de tecnologías de la 4RI, tales como, IoT, blockchain, big data, computación en la nube e inteligencia artificial" (Departamento de Planeación Nacional, ***et al.,*** 2020, p.37).

Como se puede observar, el CONPES 3995, delegó al MDN una serie de responsabilidades, tareas y acciones a cumplir frente al fortalecimiento de la seguridad y en pro de coadyuvar a mejorar la confianza de los ciudadanos, sectores económicos y demás actores del entorno digital nacional, teniendo entonces la labor de proyectar capacidades propias de su talento humano para el cabal logro de los objetivos de esta y las demás políticas vigentes.

Relación del DigComp 2.2 y el CONPES 3995 de 2020

En general, la relación que guardan los documentos DigComp 2.2. y el CONPES 3995 de 2020 es que ambos, como referente de política pública, buscan otorgar lineamientos para sentar las bases de los elementos educativos, tecnológicos e institucionales para la formación de competencias digitales ciudadanas. Lo anterior, partiendo de reconocer que el avance de la tecnología y la digitalización acelerada para todos los procesos ha reformulado la relación de los estados con sus ciudadanos, sin que esto determine, como lo describe Almenara *et al.* (2020) "[…] que al estar sumergidos en una sociedad digital asegura las mismas oportunidades para toda la ciudadanía en cuanto a su acceso y uso […]" (p.46). Haciendo así, imprescindible crear una gobernanza nacional que permita fomentar y estimular el crecimiento de la arquitectura digital existente.

En conclusión, cada una de las responsabilidades dispuestas en el CONPES 3995 de 2020 para el MDN y cada una de sus instituciones, en especial el Ejército Nacional, requieren de un recurso humano altamente calificado y competente, conocedor en la teoría y en la práctica sobre la doctrina, seguimiento y control, análisis de riesgos, vulnerabilidades, identificación de amenazas y todos aquellos conocimientos y habilidades técnicas, "destreza manual y el uso de métodos, materiales, herramientas e instrumentos" (Vuorikari, *et al.,* 2022, p. 3), necesarios para una correcta y acertada gestión de la seguridad y la defensa en el ciberespacio.

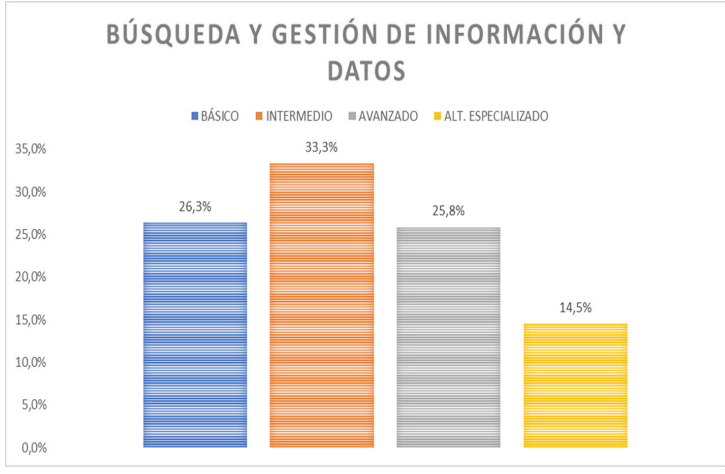
Competencias digitales de Alféreces de la ESMIC de acuerdo al marco de competencias digitales DigComp 2.2

Como se expuso en el segmento anterior, la clave en el cumplimiento de las responsabilidades previstas para el MDN a través de sus instituciones es la capacidad plena de sus funcionarios para hacer frente a los retos de proyección / formulación, ejecución y asesoría en acciones dispuestas para la seguridad y defensa en el ciberespacio; En tal razón, como técnica de recolección de información sobre el estado actual de las competencias, se utilizó una encuesta de autoría propia, en formato de cuestionario de ***google forms (online),*** relacionando las cinco áreas de competencia del Digcomp 2.2, y la sexta área denominada "defensa en el ciberespacio", con una pregunta cerrada en cada una de las competencias, y cuatro respuestas (una por cada nivel de aptitud) de acuerdo a la capacidad y conocimiento frente a la pregunta formulada. Tras la tabulación de resultados, y su correspondiente análisis estadístico, se registra lo siguiente:

Estado de las competencias de los Alféreces de la ESMIC

En el área de competencia de búsqueda y gestión de información y datos, se obtuvo en promedio valores entre el 14,5% y el 33,3% (ver gráfico 1). El primero, correspondiente a los encuestados que se consideran estar en el nivel altamente especializado, y para el segundo, aquellos que se sitúan en un nivel de aptitud intermedio. De manera particular por competencias, es de anotar que los valores más altos son compartidos entre la competencia de navegar, buscar y filtrar datos y, evaluar datos, información y contenidos digitales, situando en cada una de ellas un 38,7% de los alféreces en niveles básico e intermedio respectivamente.

Gráfico 1. Área búsqueda y gestión de información y datos.

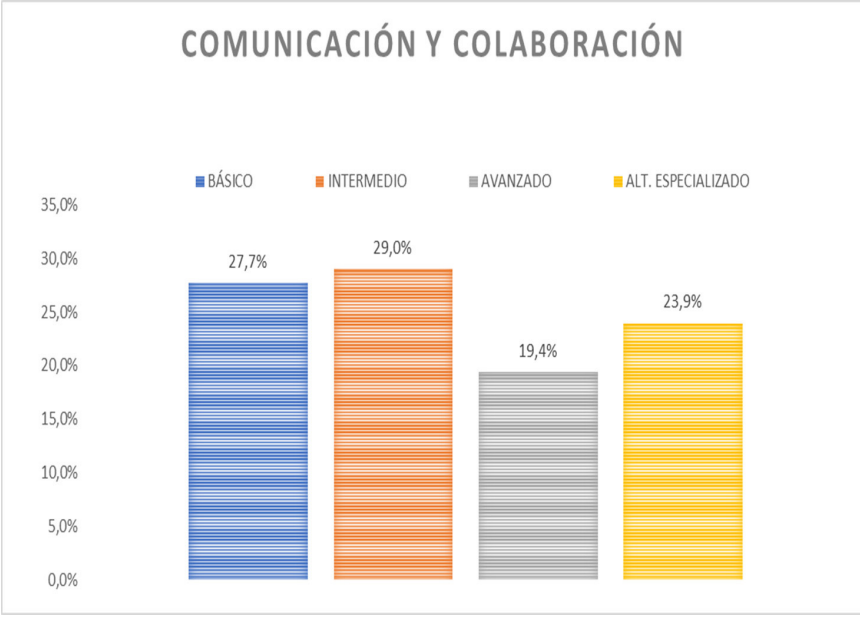


Fuente: Elaboración propia, 2023

En lo que corresponde al área de competencia de comunicación y colaboración, se obtuvo en promedio que solo un 19,4% de los alféreces se sitúa en el nivel avanzado, mientras que el 29% de ellos se establecen en el nivel intermedio, siendo este el porcentaje más alto en promedio de la medición (ver gráfico 2).

En el análisis particular por competencias, resalta como en valores iguales de 32,3%, los encuestados se sitúan respectivamente en el nivel básico e intermedio de las competencias: interactuar a través de tecnologías digitales y, comportamiento en la red. Así mismo, se destaca positivamente que un 35,5% del personal se sitúa en el nivel de aptitud altamente especializado de la competencia de gestión de la identidad digital.

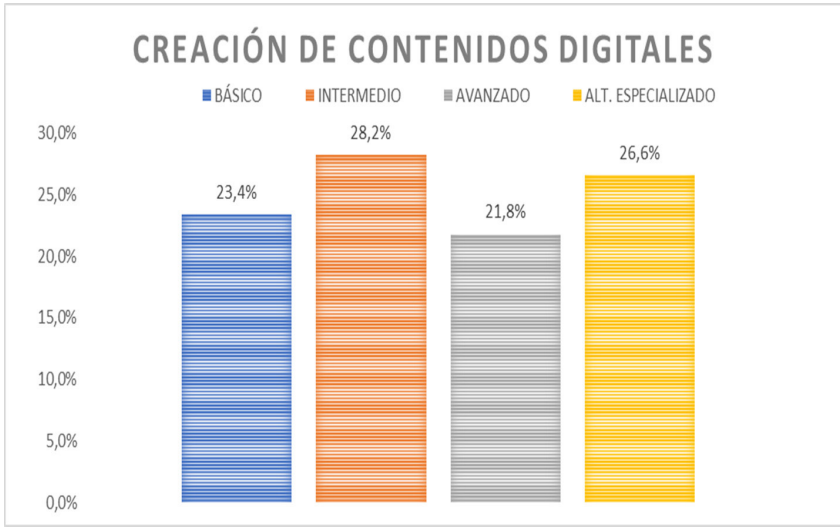
Gráfico 2. Área comunicac*ión y colaboración.*



Fuente: Elaboración propia, 2023

Respecto al área de competencia de creación de contenidos digitales, se obtuvo en promedio un valor mínimo de 21,8% y un máximo de 28,2%, en donde ese valor máximo corresponde a los encuestados que se situaron en un nivel intermedio, mientras que el valor mínimo corresponde a aquellos que se consideran en el nivel avanzado (ver gráfico 3). En esta evaluación se destaca el resultado particular por competencia más alto (33,9%) correspondiente a la competencia de integración y reelaboración de contenido digital, en todo caso, situado en el nivel intermedio.

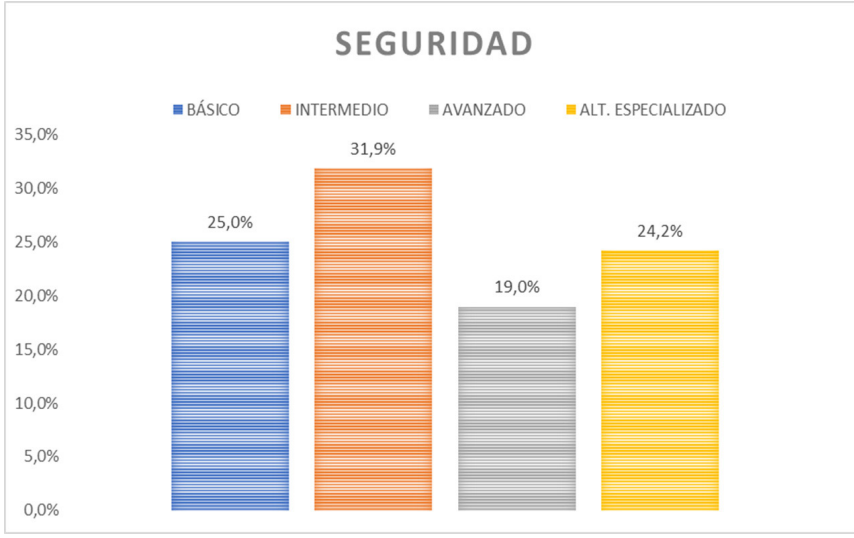
Gráfico 3. Área creación de contenidos digitales.



Fuente: Elaboración propia, 2023

Por su parte, en el área de competencia de seguridad, resultó en promedio con el más alto valor porcentual, el nivel intermedio, con un 31,9% de los alféreces. En contraste, el mínimo porcentaje de alféreces se situó en el nivel avanzado, con un 19%. (gráfico 4). En el detalle particular por competencias, se destaca que el 35,5% de los encuestados se sitúan en el nivel intermedio en las competencias de protección de dispositivos y protección de datos personales y privacidad.

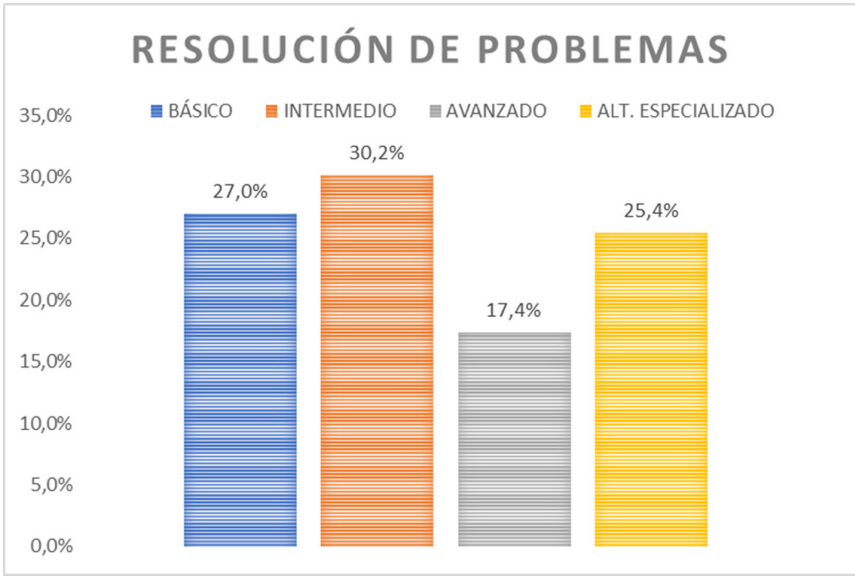
Gráfico 4. Área seguridad.



Fuente: Elaboración propia, 2023

Finalmente, en el área de competencia de resolución de problemas, se obtuvo como resultado en promedio que, del total de los encuestados, el 30,2% se considera en el nivel intermedio, y, así como en el área de competencia anterior, solo el 17% del personal se sitúa en un nivel avanzado. (ver gráfico 5). El análisis detallado de las competencias mostró como el 32,3% de los encuestados en la competencia de identificar lagunas en las competencias digitales, se ubicó en el nivel intermedio, corroborando con esto los resultados generales de nivel de aptitud para el área de competencia total.

Gráfico 5. Área resolución de problemas.



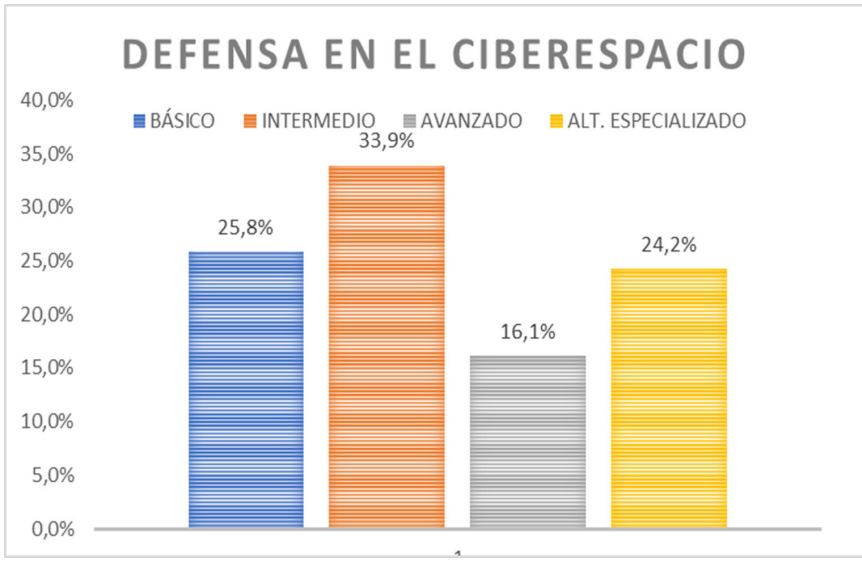
Fuente: Elaboración propia, 2023

Ahora bien, con el ánimo de ahondar en las competencias de los alféreces en cuanto a sus capacidades y conocimientos en ciberdefensa, se les planteó en la misma encuesta, una pregunta encaminada a la gestión de acciones de defensa en el ciberespacio, en la que se obtuvo como resultado que un 33,9% del personal se considera en el nivel intermedio, siendo este porcentaje el más alto de toda la competencia. (ver gráfico 6).

En conclusión, y según lo obtenido en cada una de las áreas de competencia evaluadas, se registra con claridad que todo el personal encuestado, en promedio, se considera e identifica en el nivel de competencia intermedio, asociando este nivel a sus habilidades, conocimiento y actitudes para:

1. Exponer sus necesidades de información, organizar estrategias de búsqueda de datos e información en entornos digitales, y describir cómo acceder a ellos;

Gráfico 6. Área defensa en el ciberespacio



Fuente: Elaboración propia, 2023

realizar análisis, comparaciones, interpretaciones y evaluaciones de fuentes, datos e información digitales. Además, poder organizar la información, datos y contenidos de manera que puedan ser almacenados y recuperados de entornos estructurados.

2. Utilizar tecnologías digitales y medios de comunicación adecuados para compartir datos e información, actuando como intermediario; seleccionar servicios digitales para participar en la sociedad y discutir argumentativamente sobre las tecnologías adecuadas para capacitarse y participar como ciudadano digital. De igual manera, discutir sobre normas de comportamiento y conocimientos técnicos en entornos digitales, adaptándose a diversos públicos y considerando aspectos culturales y generacionales. Además, comprender cómo proteger su reputación en línea y manipular datos utilizando herramientas, entornos y servicios digitales.
3. Crear y editar contenidos en diferentes formatos, expresándose a través de medios digitales; discutir y argumentar sobre la modificación, perfeccionamiento, mejora e integración de contenidos e información para crear nuevos y originales. Además, comprender las reglas de derechos de autor y licencias aplicables a información y contenidos digitales. Por último, identificar y enumerar instrucciones para que un sistema informático resuelva problemas específicos o realice tareas determinadas.

4. Proteger sus dispositivos y contenidos, identificar riesgos y amenazas en entornos digitales, seleccionar medidas de seguridad y considerar la fiabilidad y privacidad. También, discutir argumentativamente sobre la protección de datos personales y privacidad, así como el uso seguro de información personal identificable en servicios digitales. Además, abordar cómo evitar amenazas a la salud física y psicológica relacionadas con el uso de tecnología, protegerse y proteger a otros de peligros, y debatir sobre las tecnologías digitales para el bienestar y la inclusión social. Por último, discutir con argumentos sobre la protección del medio ambiente frente al impacto de las tecnologías digitales y su uso.
5. Evaluar y resolver problemas técnicos en entornos digitales y con dispositivos aplicando diversas soluciones. También explicar y seleccionar herramientas y respuestas tecnológicas para satisfacer necesidades específicas, ajustando y personalizando los entornos digitales según sus necesidades. Además, diferenciar herramientas y tecnologías digitales para crear conocimiento e innovar procesos y productos, participando tanto individual como colectivamente en la comprensión y solución de problemas en entornos digitales. Por último, discutir argumentativamente sobre cómo mejorar su competencia digital, apoyar a otros en su desarrollo, y buscar oportunidades de autodesarrollo y actualización.
6. Diferenciar y seleccionar las herramientas y técnicas adecuadas para detectar, analizar y mitigar ataques cibernéticos en entornos digitales (Vuorikari, *et al.*, 2022).

Competencias necesarias del ejercicio del mando en entornos digitales

Basado en el estado actual de las competencias, tal como se mostró con los resultados, ninguno de los promedios generales máximos se situó en el nivel altamente especializado, por consiguiente, no se puede descartar o minimizar la importancia sobre la necesidad de lograr una mejora en todas las competencias digitales tratadas, para los alféreces de la ESMIC. Así las cosas, las 21 competencias siguen siendo parte física en lo proyectado como propuesta de estrategia, salvo con la consideración de, someter estás a los criterios del nivel avanzado, como paso lógico y subsecuente, agregándole valor a su profesión y haciéndolo altamente competitivo (Segrera *et al.,* 2020) ante el enfoque de orientación y liderazgo en contextos complejos, propios de este nivel de competencia, el cual además, se alinea conceptualmente frente al rol de mando de los oficiales, y en particular a su capacidad de realizar valoraciones acertadas, y la aplicación, adaptación y toma de decisiones de impacto colectivo (Escuela Militar de Cadetes, 2023).

De acuerdo a lo anterior, se describen a continuación las habilidades, conocimientos y actitudes de referencia en las áreas de competencia en un nivel avanzado:

1. Valorar y comprender las necesidades de información propias y de otros, aplicando diversas estrategias de búsqueda para encontrar datos, informaciones y contenidos adecuados, y explicando cómo acceder y navegar por ellos; ejercer un juicio crítico sobre la fiabilidad y seriedad de fuentes digitales, datos e información relevante para tomar decisiones informadas y, adaptar la gestión de información, datos y contenidos a entornos estructurados más apropiados para la organización, procesamiento, almacenamiento y recuperación en la resolución de problemas complejos.
2. Adaptar una variedad de tecnologías digitales y medios de comunicación según las necesidades particulares y las de otros, para una interacción adecuada en el contexto específico; evaluar las tecnologías más adecuadas para compartir información y contenidos, siendo un intermediario flexible y variando las prácticas de referencia y atribución según corresponda. También, utilizar servicios digitales y tecnologías apropiadas para participar y capacitarse en la sociedad, seleccionando herramientas adecuadas para colaborar, co-construir y co-crear datos, recursos y conocimientos con otros; adaptar normas de comportamiento, conocimientos técnicos y estrategias de comunicación para interactuar en entornos digitales, considerando la audiencia y aspectos de diversidad cultural y generacional. Además, proteger su propia reputación en línea y ajusta los datos producidos empleando diversas herramientas, entornos y servicios.
3. Adaptar el contenido digital utilizando formatos adecuados y generar medios digitales apropiados para expresarse; evaluar formas de modificar, perfeccionar e integrar información para crear contenido nuevo y original. Asimismo, seleccionar normas adecuadas sobre derechos de autor y licencias para datos e información digital. Además, determinar las instrucciones más apropiadas para que un sistema informático resuelva problemas y realice tareas específicas.
4. Elegir la protección más adecuada para dispositivos y contenidos digitales, identificando riesgos y amenazas; seleccionar medidas de seguridad apropiadas y valora la fiabilidad y privacidad. También, evaluar formas adecuadas de proteger datos personales y privacidad, y de utilizar y compartir información personal identificable con precaución. En cuanto a la salud y el bienestar, identificar formas apropiadas de evitar riesgos físicos y psicológicos al usar tecnologías digitales; protegerse a sí mismo y a otros de peligros y, variar el uso de tecnologías para fomentar el bienestar y la inclusión social. Finalmente, elegir soluciones adecuadas para proteger el medio ambiente del impacto de las tecnologías digitales y su uso.
5. Identificar y resolver problemas técnicos al utilizar dispositivos y tecnologías digitales, adaptando soluciones adecuadas; evaluar y seleccionar herramientas digitales para satisfacer necesidades propias y de otros, personalizando entornos digitales según requerimientos; Adaptar herramientas para la creación de

conocimiento e innovación, resolviendo problemas conceptuales en entornos digitales individual y colectivamente. Además, tomar decisiones sobre mejorar la propia competencia digital, evaluar la de otros y buscar oportunidades de autodesarrollo para mantenerse actualizado.

6. Diseñar y aplicar estrategias de defensa cibernética, integrando herramientas y tecnologías avanzadas, con el objetivo de prevenir, detectar y responder eficazmente a incidentes de seguridad informática (Vuorikari, *et al.,* 2022).

Así las cosas, y conocidos los resultados, para este punto de la investigación se pudo comprobar la tesis base del problema de investigación, frente a la teoría de los recursos y de la apropiación con los siguientes argumentos:

1. En cuanto al acceso a la motivación, el resultado (nivel intermedio) permitió evidenciar que el personal encuestado tiene el deseo y la voluntad de interactuar en ambientes de tecnología digital, siendo que "El gusto por el uso de tecnologías digitales ha sido una característica propia de las generaciones más jóvenes, que ven internet, en general, y las redes sociales y las tecnologías móviles, en particular, como su hábitat natural de actuación" (Osuna, 2022. párr.3).
2. Respecto al acceso físico o material, el personal de alféreces cuenta con dispositivos tecnológicos necesarios para el desenvolvimiento en ambientes digitales. Además, la ESMIC les brinda la infraestructura necesaria para tal fin. Este acceso es permitido entre otras a las exigencias mínimas de equipo y material exigido a los estudiantes para su ingreso a la escuela militar.
3. En contraste, en el acceso a las competencias y el acceso para el uso, el resultado permite observar las falencias en los niveles de competencia digitales, en particular, en lo concerniente a la poca capacidad de adoptar roles de liderazgo frente a escenarios complejos; ahora bien, como dinamizador de la falta de competencias, se destaca la limitación de espacios académicos de fortalecimiento teórico práctico en temáticas afines a las tecnologías y al ciberespacio. Esto teniendo en cuenta el análisis realizado a los programas académicos (militar y complementarios) en donde escasamente se encuentra un saber denominado *ofimática* con 48 horas de trabajo, de las cuales 32 son trabajo sincrónico / modalidad virtual y 16 de trabajo asincrónico en modalidad virtual, desarrollado bajo contenidos temáticos de corto alcance, que no permiten el dominio y la generación de mejores prácticas educativas que posibiliten en general la construcción de nuevo conocimiento a través de las tecnologías (Arras *et al.*, 2021), e imposibilitan la correspondencia efectiva (pertinencia) entre el perfil profesional y el perfil laboral (Jaramillo, 2015) esperado del egresado de la ESMIC, contenidos listados a continuación:
    - Definición sobre la seguridad informática y sus características.
    - Implementación de mecanismos de control.

- Bases de datos estructuradas y no estructuradas.
- Introducción al Excel (cinta de opciones inicio, datos, vista, funciones matemáticas; formato; funciones matemáticas y estadísticas, formulas; funciones lógicas, tablas dinámicas, gráficos dinámicos).
- Elaboración de un documento escrito, interrelación word – Excel. (ESMIC, 2023)

Propuesta de estrategia para el fortalecimiento de las competencias digitales del mando militar de acuerdo al DigComp 2.2 y el CONPES 3995 del 2020.

De acuerdo a lo expuesto como resultado, y su análisis frente al marco teórico, la propuesta de estrategia se desarrolla como a continuación:

Objetivo general

Proponer una estrategia para el fortalecimiento de competencias digitales de los alféreces, a través de la aplicación de actividades concretas de índole académica en la ESMIC, para dar cumplimiento efectivo de las responsabilidades acogidas por el MDN y sus instituciones con el CONPES 3995 de 2020.

Objetivos específicos

Presentar una propuesta de portafolio de programas para la disminución de la brecha de competencias digitales entre el nivel básico al nivel avanzado en el personal de alféreces, de acuerdo al DIGCOMP 2.2.

Presentar un marco de orientación para el afianzamiento de competencias digitales de la planta docente.

Medios de la estrategia

Los medios para el desarrollo de la estrategia se determinan por cada una de las líneas de acción proyectadas, así pues, se consideran los siguientes:

Educación Informal (Formación y educación continua): "bajo la premisa de que las competencias no son estáticas, sino que se construyen y desarrollan a través de la práctica, en un proceso permanente de aprendizaje para obtener niveles de desempeño cada vez más altos" (Ministerio de Educación Nacional, 2023, párr.1), la educación continua permitiendo la formación, actualización y perfeccionamiento en una disciplina y la generación y fortalecimiento de competencias profesionales, y se constituye, como lo resalta el World Economic Forum (2022) como una de las soluciones de fortalecimiento de fuerza laboral

ante las necesidades de habilidades cibernéticas. De esta forma, en lo concerniente a la primera línea de acción propuesta, la disminución de la brecha de competencias digitales se desarrollará a través de cursos, diplomados, y seminarios taller, elaborados a partir de las áreas de competencia y competencias particulares del DigComp 2.2.

Finalmente, se ha estipulado una estructura guía en cada una de las propuestas en donde se registra inicialmente una denominación del módulo correspondiente al área de competencia, seguido de unos temas particulares, y cerrando con el objetivo general en cada caso. Esto permitirá de forma didáctica, correlacionar la información con el propósito de aplicación de la actividad de formación.

Aplicación de marcos comunes internacionales: a fin de lograr adquirir las competencias digitales requeridas, y en cumplimiento al objetivo específico No3 del CONPES 3995, la adopción de la experiencia internacional a través de buenas prácticas y modelos de referencia probados se convierte en una herramienta pertinente y de gran valor. Por tanto, la adopción de estos marcos comunes permite generar y asumir criterios propios y adaptados a las necesidades específicas de individuos u organizaciones.

Al aplicar marcos usuales internacionales, se facilita la integración y cooperación al adoptar estándares reconocidos y aceptados internacionalmente; se aceleran los procesos de aprendizaje al acceder a prácticas y enfoques exitosos; se tiene eficiencia de esfuerzos y recursos en la consecución de los objetivos y, se amplía el campo de competencias más allá de lo local.

En este sentido, la orientación de afianzamiento de competencia digitales en la segunda línea de acción se llevará a cabo con la implementación del Marco Europeo para la Competencia Digital de los Educadores – DigCompEdu, el cual, en palabras de Redecker (2017) proporciona una base sólida que puede guiar las políticas educativas en todos los niveles; un modelo que permite a las partes interesadas locales pasar rápidamente a desarrollar un instrumento concreto, adaptado a sus necesidades, sin tener que desarrollar una base conceptual para este trabajo; un lenguaje y una lógica común que pueden ayudar al debate y al intercambio de las mejores prácticas entre países; y, finalmente, un punto de referencia para validar la integridad y el enfoque de sus propias herramientas y marcos, tanto actuales como futuros. (p.13).

Modos de la estrategia

La propuesta de estrategia está configurada por las siguientes líneas de esfuerzo:

1. Participación de los estudiantes en actividades de fortalecimiento de competencias digitales.
2. Fomento de las competencias digitales de la planta docente.

Desarrollo de la estrategia

Línea de acción No1.

Propósito: Promover la participación de los estudiantes en actividades de fortalecimiento de competencias digitales, a través de programas y actividades de educación continuada (seminarios, diplomados, cursos, etc) que permitan la actualización constante de conocimientos, y el cierre de brechas en los niveles de competencia.

En esta línea de acción, se proponen las siguientes actividades:

Diseño e implementación de un diplomado en competencias digitales acorde al marco DigComp 2.2, que contenga como mínimo la siguiente estructura:

Tabla 1. Diseño e implementación de un diplomado

Módulo	Temas Particulares	Objetivos
Módulo 1: Cultura Digital	Generalidades del entorno digital	Identificar los conceptos básicos del entorno digital.
	Conocimiento de herramientas ofimáticas	Relacionar las herramientas ofimáticas a las necesidades.
	Fundamentos de seguridad digital	Conocer prácticas generales de seguridad en línea.
	Principios éticos y normativos de la tecnología digital	Establecer principios éticos y normativos aplicados en entornos digitales.
Módulo 2: Búsqueda y gestión de información y datos	Procedimientos de consulta de información en buscadores	Desarrollar herramientas individuales para el uso avanzado de motores de búsqueda.
	Análisis de las fuentes de información	Analizar y seleccionar información de calidad en internet
	Valoración y consolidación de la información disponible	Establecer criterios para valorar y consolidar información de internet
	Plataformas educativas para la educación virtual	Emplear plataformas en línea para mejorar la educación individual
	Principios éticos, morales y legales en la información on line	Considerar la relevancia de mantener estándares éticos para el uso y difusión de la información.
Módulo 3: Comunicación y Colaboración Digital	Contexto de la comunicación on line	Conocer el contexto de la comunicación on line.
	Herramientas de construcción colaborativa en línea	Articular esfuerzos con otros usuarios para colaboración en línea en proyectos específicos
	Uso de plataformas digitales (Redes sociales)	Identificar la importancia del uso de las redes sociales y su impacto
	Comunicación en situaciones complejas	Plantear comunicación efectiva como respuesta en momentos complejos
	La ética en las comunicaciones digitales	Considerar la necesidad de plantear comunicaciones éticas en entornos digitales.

Continúa tabla...

Módulo	Temas Particulares	Objetivos
Módulo 4. Creación de contenidos digitales	Generalidades de los contenidos digitales	Conocer desde su generalidad, los contenidos digitales existentes, tipos y formas de almacenamiento
	Uso y combinación de herramientas y técnicas para la creación de contenidos digitales accesibles	Emplear las herramientas disponibles para diseñar, desarrollar y poner en funcionamiento contenidos digitales para su organización
	Modificación y mejoras a contenidos digitales	Usar aplicaciones de software para crear e incorporar contenidos digitales o una modificación de ellos a fin de integrarlos entre sí
	Aspectos legales y propiedad intelectual	Conoce cómo usar, compartir, combinar y crear contenidos digitales de forma legal, respetando los derechos de propiedad intelectual de los desarrolladores
	Programación	Desarrolla contenidos digitales a partir del uso y programación de algoritmos, lenguajes de programación, bloques de programa
Módulo 4: Seguridad	Seguridad en herramientas digitales y dispositivos vinculados	Emplear herramientas de protección de los dispositivos y herramientas en línea frente a amenazas externas
	Derecho a la privacidad y protección de datos	Aumentar los estándares de seguridad a partir de la configuración y protección de datos en internet
	Protección personal en entornos digitales	Reflexionar sobre los riesgos por el uso excesivo de entornos digitales y su impacto en la salud y el bienestar
	Componente medioambiental	Reflexionar sobre la importancia del uso de prácticas sostenibles en el uso de sistemas y tecnologías digitales en general
Módulo 5: Resolución de problemas	Funcionamiento y conectividad de dispositivos digitales	Resolver problemas técnicos, de conectividad y de interconexión de equipos, sistemas y/o dispositivos
	Identificación de necesidades y respuestas tecnológicas	Emplear herramientas de accesibilidad para la gestión de tecnologías digitales
	Creatividad e innovación digital	Colaborar en la solución de problemas inherentes a las tecnologías digitales, a través de métodos innovadores y soluciones creativas
	Soluciones técnicas a problemas específicos	Responder efectivamente a soluciones digitales empleando las técnicas apropiadas

Continúa tabla...

Módulo	Temas Particulares	Objetivos
Módulo 6: Ciberdefensa y Ciberseguridad	Actualidad y principios generales sobre la ciberseguridad y ciberdefensa	Entender los principios básicos y el contexto actual en materia de ciberseguridad y ciberdefensa
	Desafíos cibernéticos en el mundo contemporáneo	Profundizar acerca de las amenazas cibernéticas y sus consecuencias para los países, sociedades e individuos
	Protección en redes y sistemas de información de carácter militar	Comprender la importancia de mantener y mejorar la seguridad en sistemas, plataformas y redes de uso militar para fines de seguridad y defensa
	Seguridad cibernética y estrategias de respuesta ante ataques cibernéticos	Detectar y proponer respuestas adecuadas frente a amenazas y ataques en el ciberespacio
	Legislación y normatividad en ciberdefensa	Conocer y actualizarse frente a las leyes y regulaciones relacionadas con la ciberdefensa
Módulo 7: Transformación digital	Conceptualización de ecosistemas digitales y transformación digital	Aprender y relacionar conceptos fundamentales para la innovación digital
	Retos y desafíos en el desarrollo y los avances de la tecnología y su impacto	Profundizar sobre los avances tecnológicos recientes y posibles impactos (Big Data y la inteligencia artificial)
	Procesos de transformación digital	Identificar y plantear soluciones digitales en pro de la transformación digital.
	Internet de las cosas	Actualizarse frente al desarrollo e innovación de sistemas inteligentes que se integran y se conectan a través de las redes de internet
	Principios éticos, morales y legales de la innovación en la tecnología digital	Conocer los aspectos éticos y legales a considerar en desarrollo de mejoras e innovación digital

Fuente: Elaboración propia a partir del Syllabus materia ofimática programa ciencias militares ESMIC 2023; Diplomado en ciberseguridad y ciberdefensa ESDEG 2023 y Diplomado en transformación digital Universidad Javeriana 2023.

Diseño e implementación de un seminario - taller en competencias digitales acorde al marco DigCom 2.2, que contenga como mínimo la siguiente estructura:

Tabla 2. Diseño e implementación de un seminario

Módulo	Temas Particulares	Objetivo
Módulo 1: Alfabetización digital - Búsqueda y gestión de la información y datos	Inducción a la alfabetización en el entorno digital y la gestión de información en línea.	Enseñar cómo generar la búsqueda y evaluación de información en línea.
	Motores de búsqueda, fuentes y evaluación de información confiable.	
	La información respecto a los derechos de autor	
	Compartir información en plataformas digitales (redes sociales).	
Módulo 2: Comunicación y colaboración	Inducción a la comunicación y colaboración.	Enseñar a comunicarse, colaborar y participar en comunidades en línea, de forma efectiva.
	Herramientas de comunicación en la red.	
	Plataformas digitales: perfiles en redes sociales, etiqueta en línea, privacidad y seguridad.	
	Herramientas de colaboración y trabajo en equipo.	
Módulo 3: Creación de contenido digital	Inducción a la creación de contenido.	Enseñar a crear y editar contenido utilizando herramientas digitales.
	Procesadores de texto, formatos y estilos.	
	Editores de imágenes, formatos y resolución.	
	Editores de video, formatos y efectos.	
Módulo 4: Seguridad	Inducción a la seguridad en línea.	Identificar cómo protegerse en línea, reconociendo las vulnerabilidades, amenazas y riesgos digitales y las correspondientes medidas de prevención.
	Seguridad de la información: contraseñas y otros tipos de autenticación.	
	Seguridad de dispositivos electrónicos: antivirus y otras medidas de protección.	
	Seguridad en plataformas digitales (spam, malware y suplantaciones de identidad.	
Módulo 5: Ciberdefensa	Actualidad y principios generales sobre la ciberseguridad y ciberdefensa	Enseñar el contexto y los fundamentos generales de la ciberdefensa, asi como los desafíos presentes y futuros en el ciberespacio.
	Desafíos cibernéticos en el mundo contemporáneo	
	Protección en redes y sistemas de información de carácter militar	
	Seguridad cibernética y estrategias de respuesta ante ataques cibernéticos	
	Legislación y normatividad en ciberdefensa	

Fuente: Elaboración propia a partir del documento DIGCOMP 2.2 y el Diplomado en Ciberseguridad y Ciberdefensa ESDEG 2023

Diseño e implementación de cursos de profundización por áreas de competencia digital acorde al marco DigComp 2.2, que contengan como mínimo las siguientes estructuras:

Tabla 3. Diseño e implementación de un seminario en Búsqueda y Gestión de la Información y Datos

CURSO DE PROFUNDIZACIÓN EN BÚSQUEDA Y GESTIÓN DE LA INFORMACIÓN Y DATOS		
Módulo	**Temas Particulares**	**Objetivo**
Módulo 1: Inducción a la búsqueda (navegación y filtro) y gestión de la información y datos	Inducción a la búsqueda y gestión de la información y los datos en red.	Entender la importancia de una acertada búsqueda y gestión de información y datos, conociendo los conceptos y herramientas para concretar las tareas.
	Conceptualización básica: las fuentes de información y datos, los metadatos, las etiquetas y taxonomías.	
	Herramientas y plataformas de búsqueda: motores, base de datos, bibliotecas virtuales.	
	Estrategias de optimización de búsqueda: las palabras claves, los operadores booleanos y los filtros.	
Módulo 2: **Evaluación de fuentes, datos, información y contenidos digitales**	Análisis y evaluación de las fuentes de información: fiabilidad, precisión, autoridad, actualidad, relevancia y pertinencia.	Comprender los criterios de calidad en la evaluación de información y datos, de manera crítica pero efectiva.
	Evaluación y análisis de la información, datos y contenidos digitales: criterios y variables de calidad.	
	Prevención de la desinformación y la información errónea.	
Módulo 3: Gestión de datos, información y contenidos digitales.	Organización de la información y los datos a través de la taxonomía, las etiquetas y categorías.	Conocer cómo organizar y almacenar la información y los datos de manera efectiva y de fácil acceso, a través de herramientas digitales.
	Almacenamiento de información y datos a través de nubes, discos y servidores.	
	Herramientas para organizar y almacenar en entornos estructurados a través de gestores de referencias bibliográficas y gestores de archivos y contraseñas.	

Continúa tabla...

CURSO DE PROFUNDIZACIÓN EN COMUNICACIÓN Y COLABORACIÓN		
Módulo	**Temas Particulares**	**Objetivo**
Módulo 1: Inducción a la comunicación y la colaboración	Inducción a la comunicación y colaboración.	Entender la comunicación y la colaboración en el entorno digital.
	Fundamentos básicos en correo electrónico, servicios de mensajería instantánea, herramientas de videoconferencia y las redes sociales.	
Módulo 2: Interacción a través de tecnologías digitales	Comunicación y colaboración con Gmail, WhatsApp, Zoom y Facebook.	Identificar cómo utilizar redes sociales como herramientas de comunicación y colaboración.
	Estrategias de comunicación y de colaboración a través de etiquetas en línea, netiquetas y trabajo en equipo.	
	Fundamentos básicos en redes sociales: el perfil, las publicaciones, los seguidores, los hashtags.	
	Redes sociales como herramientas (Facebook, Twitter, Instagram, etc.)	
	Estrategias para comunicarse y colaborar con redes sociales (creación de contenido, interacción con la audiencia, trabajo en equipo).	
Módulo 3: Herramientas de colaboración y gestión	Inducción a las herramientas de colaboración en entono virtual.	Entender la colaboración en línea como herramienta de trabajo efectiva y eficiente
	Gestión de proyectos con Trello, Asana y Basecamp.	
	Edición de documentos con Google Docs y Microsoft Office 365.	
	Comunicación en equipo a través de Slack y Microsoft Teams.	
Modulo 4: Participación ciudadana a través de las tecnologías digitales	Participación ciudadana de control y fiscalización.	Reconocer la importancia de la participación a través de las tecnologías digitales
	Identificación de servicios virtuales de gobierno (plataformas, redes, buzones).	
	La ética y la moral de la participación en medios digitales.	
Modulo 5: Comportamiento en la red	Diversidad cultural y generacional en la red.	Identificar los factores de multi-culturalidad y de generación en la adopción de buenas prácticas de comportamiento en la red.
	Normas de comportamiento (públicas y privadas)	
Modulo 6. Gestión de la identidad digital	Creación y gestión de perfiles en entornos digitales (comercio electrónico, redes sociales, participación ciudadana).	Identificar la relevancia de la correcta gestión de identidades digitales en los espacios de interacción digital.
	La huella digital y la gestión de datos propios en línea.	
	Gestión y administración de actividades en internet (navegación privada, gestión de cookies, consentimientos).	

Fuente: Elaboración propia a partir del documento DigComp 2.2, área de competencia: Búsqueda y gestión de información y datos.

Tabla 4. Curso de profundización en Creación de Contenidos Digitales

CURSO DE PROFUNDIZACIÓN EN CREACIÓN DE CONTENIDOS DIGITALES		
Módulo	**Temas Particulares**	**Objetivo**
Módulo 1: Introducción al desarrollo de contenidos digitales	Inducción al desarrollo de contenidos.	Conocer la importancia de la creación de contenidos digitales.
	Conceptos básicos en formatos de archivo, derechos de autor y propiedad, y licencias Creative Commons.	
	Plataforma Canva, Adobe Spark y GIMP, como herramientas de creación de contenidos.	
	Estrategias de creación storytelling, diseño gráfico y edición de video.	
Módulo 2: Integración y reelaboración de contenidos digitales con herramientas avanzadas	Inducción a las herramientas avanzadas de creación de contenidos.	Utilizar herramientas de creación de contenidos digitales complejos y sofisticados.
	Herramientas para edición de video (Adobe Premiere y Final Cut Pro).	
	Herramientas para diseño gráfico avanzado (Adobe Photoshop e Illustrator).	
	Animación, efectos especiales y diseño de interfaces como estrategias de creación de contenidos avanzados.	
Módulo 3: Derechos de autor (copyright) y licencias de propiedad intelectual	Fundamentos de la propiedad intelectual y los derechos de autor en línea	Concienciar sobre la importancia del cumplimiento de la normativa en propiedad intelectual y derechos de autor.
	Normativa nacional en propiedad intelectual aplicado en la red	
	Licencias y códigos (abiertos/cerrados)	
	Ética en la publicación de contenidos y prevención del deterioro moral. La ética y la moral frente a la propiedad intelectual	
Módulo 4: Publicación y difusión de contenidos digitales	Inducción a la publicación de contenidos.	Aprender a publicar y difundir contenidos digitales de manera efectiva
	Publicación en redes sociales, blogs y sitios web.	
	Estrategias de difusión a través marketing de contenidos y publicidad en línea.	
	Ética en la publicación de contenidos y prevención del deterioro moral.	

Fuente: Elaboración propia a partir del documento DigComp 2.2, área de competencia: Creación de contenidos digitales.

Tabla 5. Curso de profundización en curso de Profundización en Seguridad Digital

CURSO DE PROFUNDIZACIÓN EN SEGURIDAD DIGITAL		
Módulo	**Temas Particulares**	**Objetivo**
Módulo 1: Protección de dispositivos	Descripción de los principales riesgos y amenazas en entornos digitales.	Describir los principales riesgos y amenazas virtuales, así como las acciones de prevención y protección.
	Análisis de casos de estudio (estadísticas).	
	Desarrollo de acciones para prevenir y proteger (ciber higiene, acciones de contención)	
Módulo 2: Protección de datos personales y privacidad	Principales riesgos y amenazas a la privacidad.	Identificar y gestionar riesgos y amenazas a la privacidad personal en línea.
	Gestión adecuada de datos personales en línea (lo público y lo privado)	
	Medidas de seguridad básicas en la interacción con el comercio electrónico y otros.	
	Estrategias de protección de la privacidad de contenidos en línea.	
Módulo 3: Protección de la salud y el bienestar	Principales riesgos y amenazas a la salud física y mental con el uso de tecnologías digitales.	Identificar los riesgos y amenazas a la salud física y mental en entornos digitales.
	Estrategias de control y de limitación del uso de tecnologías digitales.	
	Estrategias contra técnicas de manipulación, acoso y pérdida de control de decisión en línea.	
Módulo 4: Protección medio ambiental.	Principales desafíos de la protección medioambiental por el uso de tecnologías digitales.	Identificar el impacto en el medio ambiente con el uso de tecnologías y la falta de acciones de protección al respecto.
	Estudio de casos de afectación medioambiental por el uso de tecnologías digitales	

Fuente: Elaboración propia a partir del documento DigComp 2.2, área de competencia: Seguridad.

Tabla 6. Curso de profundización en Resolución de Problemas

CURSO DE PROFUNDIZACIÓN EN RESOLUCIÓN DE PROBLEMAS		
Módulo	**Temas Particulares**	**Objetivo**
Módulo 1: Fundamentos de la resolución de problemas	Fundamentos del proceso de resolución de problemas.	Comprender los principios esenciales de la resolución de problemas y generar habilidades para abordarlos de manera estructurada
	Describir, identificar y definir problemas (pensamiento crítico y analítico).	
	Generación de soluciones creativas en equipo.	
	Evaluación de opciones y toma de decisiones.	
Módulo 2: Uso creativo de la tecnología en la resolución de problemas	Identificación de problemas en la tecnología y la web.	Aprender a abordar problemas que surgen en entornos digitales y en línea de manera efectiva.
	Uso de herramientas digitales para el diagnóstico y análisis de problemas.	
	Las tecnologías como herramienta de innovación de procesos y productos.	
	Herramientas de trabajo colaborativo	
Módulo 3: Identificación de falencias en las competencias digitales	Identificación de falencias en las competencias digitales (herramientas de diagnóstico y pruebas de habilidad).	Identificar las falencias en las competencias digitales y cómo lograr su fortalecimiento a través de la aplicación de marcos de competencia.
	Estrategias de fortalecimiento de competencias digitales (autoaprendizaje, otros).	
	Marcos de competencias (DigComp 2.2 e ISTE.	

Fuente: Elaboración propia a partir del documento DigComp 2.2, área de competencia: Resolución de problemas.

En cuanto a la profundización en el área de ciberdefensa, se plantea la participación de los estudiantes en el Diplomado en Ciberseguridad y Ciberdefensa de la Escuela Superior de Guerra. Mencionado diplomado se detalla a continuación:

Tabla 7. Diplomado en Ciberseguridad y Ciberdefensa

Módulo	Temas Particulares	Objetivo
Módulo general:	Amenazas cibernéticas contemporáneas	Contextualizar y concientizar a miembros de la academia y organizaciones públicas y privadas sobre los factores de riesgo, amenazas, oportunidades y dinámicas estratégicas del ciberespacio, desde una perspectiva multidisciplinaria, que permita la profundización de conocimientos y fortalecimiento de habilidades analíticas y de toma de decisiones.
Ciberseguridad y Ciberdefensa	Contexto en ciberseguridad y ciberdefensa	
	Gobernanza de la ciberdefensa	
	Seguridad y defensa en el ciberespacio	
	Técnicas de inteligencia artificial en ciberseguridad	
	Ciberdiplomacia y cooperación en el ciberespacio	
	Regulaciones en ciberseguridad	

Fuente: Diplomado en Ciberseguridad y Ciberdefensa de la Escuela Superior de Guerra 2023.

Línea de acción No 2.

Propósito: Fomentar los conocimientos, habilidades y actitudes en los entornos digitales, de la planta docente con el fin de poder aprovechar el potencial de las tecnologías digitales para mejorar e innovar en educación (Redecker, 2017), y su posterior impacto positivo en los estudiantes a través de la inmersión, el manejo adecuado y oportuno, la reflexión, y la conciencia de seguridad digital.

En esta línea de acción, se propone la siguiente actividad:

Aplicación del Marco Europeo para la Competencia Digital de los Educadores – DigCompEdu en la ESMIC.

Ser personal docente e investigador en el siglo XXI requiere, entre otras cosas, ser competente digitalmente. La adquisición y entrenamiento de un conjunto de habilidades, conocimientos y actitudes que se incluyen en la competencia digital deberían facilitar la funcionalidad y operatividad de las actuaciones del docente (Martín *et al.,* 2020, p.5).

Apoyado en la interrelación de los marcos de competencia digital europeos, y entendiendo los retos y desafíos que al mando militar le corresponde en su función de seguridad y defensa en el dominio ciber espacial, el personal docente de la ESMIC debe tener las competencias digitales afines a la integración e interacción con las herramientas TIC (Gutiérrez y Leguizamón, 2021), que les permita estar a la par de las innovaciones metodológicas en educación, motivar activamente los cambios, aprovechar los beneficios tecnológicos (González *et al.,* 2019), y asimilar la presencia masiva de dispositivos

digitales, para coadyubar a fortalecer las competencias particulares de los estudiantes, en especial en los alféreces. Como se podrá observar en las áreas de actividad del educador, planteados en el marco DigCompEdu.

El DigCompEdu, es el marco común de referencia de la Unión Europea para fomentar la competencia digital de los educadores, ofreciendo un lenguaje y una lógica compartida, (Redecker, 2017), para la medición, promoción y certificación de la competencia digital.

Según el DigCompEdu, el marco se centra en tres marcos de competencia: competencias profesionales de los educadores, competencias pedagógicas y competencias de los estudiantes, que demuestran entre otros, como el aprendizaje del docente para utilizar la tecnología y preparar las sesiones de clase se refleja en el uso de esta por los estudiantes, configurándose una sinergia entre el docente, la tecnología para el aprendizaje y el alumno (Bolo *et al.*, 2023).

Las seis áreas de la actividad profesional del docente y las competencias digitales detalladas se presentan a continuación en la figura 4.

Figura 4. Modelo general del DigCompEdu.

Fuente: Documento DigComEdu pag.19

A continuación, se presenta de manera general un cuadro resumen con las actividades que son cubiertas al afianzar las competencias presentadas en la figura 4. Estas actividades exponen la idea central y un alcance (no limitado) de la competencia en particular.

Tabla 7. Áreas de competencias, competencia y actividad general

Área de competencia	Competencia	Actividad general
Compromiso profesional	Comunicación organizativa	Permite mejorar la comunicación y la colaboración en la comunidad académica.
	Colaboración profesional	Permite emplear en una red de colaboración conjunta para compartir, intercambiar e innovar en las prácticas pedagógicas.
	Práctica reflexiva	Promueve la reflexión individual y colectiva sobre la práctica pedagógica.
	Desarrollo profesional digital continuo	Promueve el desarrollo profesional continuo y progresivo.
Contenidos Digitales	Selección de competencias digitales	Permite la búsqueda, evaluación y selección de recursos digitales para apoyar y mejorar el proceso de enseñanza / aprendizaje.
	Creación y modificación de recursos digitales	Permite la adaptación o creación (individual o en colaboración) de los recursos de acuerdo a las licencias abiertas existentes.
	Protección, gestión e intercambio de contenidos digitales.	Permite organizar los contenidos para la comunidad académica, respetando y aplicando la normativa sobre privacidad y propiedad intelectual.
Enseñanza y aprendizaje.	Enseñanza	Permite gestionar, programar y poner en funcionamiento recursos digitales (conocidos o novedosos) en el proceso de enseñanza.
	Orientación y apoyo en el aprendizaje	Permite utilizar las tecnologías y servicios digitales para ofrecer orientación y apoyo dentro y fuera de las sesiones lectivas.
	Aprendizaje colaborativo.	Facilita utilizar las tecnologías para la creación conjunta de conocimiento.
	Aprendizaje autorregulado	Fomenta el uso de las tecnologías para reflexionar y formular soluciones creativas sobre el propio aprendizaje.
Evaluación y retroalimentación.	Estrategias de evaluación	Permite utilizar las tecnologías para la evaluación formativa y sumativa.
	Analíticas de aprendizaje	Permite analizar e interpretar de forma crítica las estadísticas digitales de progreso del alumnado.
	Retroalimentación, programación y toma de decisiones	Permite utilizar las tecnologías para proporcionar retroalimentaciones selectivas y oportunas.
Empoderamiento de los estudiantes.	Accesibilidad e inclusión	Permite garantizar la accesibilidad de todos los estudiantes a los recursos y actividades de aprendizaje.
	Personalización	Permite utilizar las tecnologías para atender las necesidades particulares de aprendizaje de los estudiantes.
	Compromiso activo de los estudiantes con su propio aprendizaje	Permite utilizar las tecnologías para promover el compromiso activo, el pensamiento crítico y la expresión creativa de los estudiantes.

Continúa tabla...

Área de competencia	Competencia	Actividad general
Desarrollo de la competencia digital de los estudiantes	Información y alfabetización mediática	Permite incorporar actividades para localizar información y recursos en entornos digitales.
	Comunicación y colaboración digital	Permite incorporar actividades académicas que requieran que los estudiantes utilicen de las tecnologías digitales.
	Creación de contenido digital	Permite incluir actividades académicas que requieran a los alumnos expresarse a través de medios digitales.
	Uso responsable	Permite tomar medidas para garantizar el bienestar físico, psicológico y social de los estudiantes al utilizar las tecnologías digitales.
	Resolución de problemas digitales	Permite incorporar académicas que requieran que los estudiantes identifiquen y resuelvan problemas técnicos.

Fuente: Elaboración propia a partir del documento DigCompEdu.

En cuanto a los niveles de actitud frente a cada una de las competencias, el marco los caracteriza en los siguientes:

1. Novel (A1): Este nivel describe a quienes requieren orientación y estimulo en el uso de tecnologías.
2. Explorador (A2): Los exploradores son aquellos que están interesados en la exploración de tecnologías digitales.
3. Integrador (B1): Los integradores llevan el uso de las tecnologías a su entorno profesional y personal, aplicándolos con facilidad y creatividad en sus prácticas pedagógicas.
4. Experto (B2): Este nivel está apartado a quienes utilizan con confianza variadas tecnologías en su labor profesional.
5. Líder (C1): El líder es aquel que tiene un manejo consistente e integral de las tecnologías en sus labores.
6. Pionero (C2): En este nivel se sitúan quienes están en la capacidad de desarrollar novedosas metodologías a través de tecnologías de alta y compleja innovación.

Ahora bien, como ejercicio inicial para la aplicación del DigComEdu, se hace necesario hacer un diagnóstico de las competencias de la planta docente, para esto, a continuación, se presenta la propuesta de estructura básica para la herramienta de diagnóstico (encuesta) de las competencias digitales, para el correspondiente abordaje posterior de las acciones de mejora. Es de anotar que cada una de las respuestas corresponde a un nivel de actitud, por lo cual, al final de la encuesta se obtendrá con facilidad el nivel del educador en cada una de las competencias, así:

Tabla 8. Áreas de competencias, competencia y actividad general

PROPUESTA DE ESTRUCTURA HERRAMIENTA DE DIAGNOSTICO (ENCUESTA)	
Marco de competencia:	competencias profesionales de los educadores.
Área de competencia:	compromiso profesional
Competencia:	comunicación organizativa
Permite mejorar la comunicación y la colaboración en la comunidad académica.	
¿Cuál afirmación considera que se adapta a sus conocimientos y capacidades en cuanto a la competencia de comunicación organizativa?: 1. Casi nunca uso tecnologías digitales en mi comunicación como educador. 2. Hago uso de las tecnologías digitales para comunicarme con estudiantes, compañeros o personal de apoyo y administrativo. 3. Utilizo diferentes canales y herramientas de comunicación digital dependiendo del propósito y del contexto de la comunicación, haciéndolo de forma responsable y ética, respetando la netiqueta y las políticas de uso. 4. Selecciono y puedo adaptar estrategias de comunicación, así como los canales, formatos y estilos más adecuados para un determinado propósito, contexto y destinatarios específicos. 5. Evalúo, reflexiono y debato con mi comunidad educativa sobre cómo utilizar eficazmente las tecnologías digitales para la comunicación organizativa e individual. 6. Contribuyo a desarrollar estrategias coherentes a las condiciones de mi organización, sobre el uso eficaz y responsable de las tecnologías digitales para la comunicación.	

Fuente: Elaboración propia.

Finalmente, una vez obtenido el resultado de nivel de actitud individual de los docentes en cada una de las competencias, se podrá realizar un seguimiento a la progresión de cada uno, partiendo desde la base de acumulación en cada uno de los niveles, es decir, si en determinada competencia un docente se sitúa en el nivel experto (B2), es porque ya ha tenido la capacidad, el conocimiento y la actitud para desarrollar las actividades de los niveles inferiores Novel (A1), Explorador (A2) e Integrador (B1). Así las cosas, la progresión en el marco DigCompEdu se facilitará con la generación individual y/o colectiva de actividades que promuevan fortalezas y desempeño de roles desafiantes en los educadores, a través, sobre todo, de los retos y la motivación hacia el avance profesional.

Conclusiones

El desarrollo de la investigación permitió reconocer que el Estado colombiano requiere del trabajo integrado y conjunto del sector público con el sector privado y la academia para fortalecer la seguridad y confianza digital en el país, aplicando marcos comunes de referencia con reconocimiento y aprobación internacional.

Por su parte, el Ejército no es ajeno a reconocer que el uso masivo de tecnologías de información y comunicaciones tiene enormes beneficios, no obstante, siempre será

un desafío mantener más y mejores contramedidas para la protección de activos de seguridad en entornos digitales.

El fortalecimiento de las competencias digitales del mando militar, iniciando desde la formación en la ESMIC, permitirá la interacción efectiva y el cumplimiento de las políticas de seguridad y defensa en el ciberespacio, y en particular, con lo establecido en el CONPES 3995 de 2020.

El marco de competencias DIGCOMP 2.2 y DIGCOMPEDU son modelos de aplicación prioritaria en la ESMIC para la generación o fortalecimiento de capacidades digitales del personal de oficiales.

En cuanto al DIGCOMP 2.2, las competencias del personal de alféreces deben ser fortalecidas con el ánimo de escalar del nivel intermedio a un nivel avanzado en el que se refleje el liderazgo y la orientación del mando militar en entornos colectivos y complejos, y que sean, como lo expone Ospina y Sanabria (2020), profesionales competentes en la generación de un criterio propio que sustente su acción frente a las normativas en la lucha contra las ciberamenazas.

Para mantener la iniciativa, la ESMIC debe generar modelos objetivos de evaluación y seguimiento de competencias digitales que permitan medir acertadamente el nivel de cada uno de los estudiantes, y con esto proveer herramientas particulares de acuerdo a los resultados (Silva y Lázaro, 2020).

De cara a las condiciones actuales del país, en la que se busca robustecer la preparación y la resiliencia de las entidades estatales frente a las amenazas y riesgos en el ciberespacio (Departamento Nacional de Planeación, 2022), se hace necesario que desde la ESMIC se promueva la participación y el liderazgo de sus egresados en el desarrollo de políticas e iniciativas de gobierno respecto a la seguridad digital de corto y mediano plazo, como las establecidas a través del Plan Nacional de Desarrollo 2022 – 2026.

En contraposición a lo que se pueda pensar sobre estudiantes y docentes y su interacción diaria con múltiples dispositivos y un uso masivo de internet, esto no supone un desarrollo intuitivo y espontáneo de competencias en los entornos digitales (Zorrilla *et al.,* 2023). Por lo tanto, la constante inmersión y apropiación de tecnologías pertinente deben ser un pilar fundamental de la formación militar. Lo anterior, permitirá establecer modelos y marcos de trabajo eficientes en el desarrollo de las funciones y la optimización del personal en los diferentes cargos que los alféreces de la ESMIC desarrollen a lo largo de su carrera militar.

Por último, se logró determinar la necesidad que la ESMIC revise la pertinencia de incorporar contenidos temáticos más acordes a la actualidad de los temas de competencias digitales, fortaleciendo las mallas curriculares en los programas de ciencias militares y programas de educación complementaria.

Recomendaciones

Primero, se recomienda que la Escuela Militar aplique la propuesta de estrategia planteada o desarrolle una propuesta propia para fortalecer las competencias digitales de sus estudiantes, de preferencia bajo el marco del DIGCOMP 2.2., sin dejar de lado el componente temático de la ciberdefensa.

Como segundo elemento, se recomienda que la Escuela Militar promueva el seguimiento y control a la estrategia planteada, con el ánimo de mantener el esfuerzo de mejora a largo plazo.

Tercero, re recomienda generar desde la Escuela Militar las competencias digitales necesarias para que el personal de oficiales logre hacer frente a los desafíos y amenazas en el ciberespacio, como líderes y gestores de políticas y como parte de equipos de trabajo interdisciplinarios.

Finalmente, se recomienda incorporar contenidos temáticos más acordes a la actualidad, de los temas de competencias digitales, en las mallas curriculares, en los programas de ciencias militares y programas de educación complementaria.

Declaración de divulgación

El autor declara que no existe ningún potencial conflicto de interés relacionado con el artículo.

Autor

John Alexander Villarraga Gamboa. Mayor del Ejército Nacional de Colombia. Magíster en Seguridad y Ciberdefensa, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Magíster en Gestión de Proyectos, Université du Québec à Chicoutimi, Canadá. Profesional en Ciencias Militares, Escuela Militar de Cadetes "General José María Córdova", Colombia.

Orcid: https://orcid.org/0009-0005-4007-0948 Contacto: villarragaj@esdeg.edu.co

Referencias

Almenara, J., Osuna, J.,Gutiérrez Castillo, J., y Palacios-Rodríguez, A. (2020). Validación del cuestionario de competencia digital para futuros maestros mediante ecuaciones estructurales. Bordón *Revista de Pedagogía*. 72 (2), 45-63. DOI:10.13042/Bordon.2020.73436

Arras-Vota, A. M., Bordas-Beltrán, J. L., Porras-Flores, D. A., & Gómez-Ramírez, J. I. (2021). Competencias en tecnologías de información y comunicación. Estudios de caso: Universidad Santo Tomas (Colombia) y Universidad Autónoma de Chihuahua (México). *Formación Universitaria, 14*(1), 135-146. http://dx.doi.org/10.4067/S0718-50062021000100135

Baldomero, A. (2019). Gestión de riesgo en seguridad digital en el sector privado y mixto - contexto general. En G. Medina (Ed.), *La seguridad en el ciberespacio: un desafío para Colombia* (pp. 169-199). Escuela Superior de Guerra «General Rafael Reyes Prieto». https://doi.org/10.25062/9789585216549.05

Bolo-Romero, K. M., Córdova-Berona, H. A., & Gutiérrez-Velasco, F. (2023*). Relationship Between Digital Competencies and Critical Thinking - A Review of the Scientific Literature From 2015 To 2022.* SciELO Preprints.

Carretero Gómez, S. (2021). Banco Interamericano de Desarrollo. (IDB, Ed.) https://clic-habilidades.iadb.org/es/habilidades-digital

CEPAL & UNESCO. (2020). *La educación en tiempos de la pandemia de COVID-19*. https://www.cepal.org/es/publicaciones/45904-la-educacion-tiempos-la-pandemia-covid-19

Congreso de la República. (25 de Mayo de 2019). *Ley 1955. por el cual se expide el plan nacional de desarrollo 2018-2022 pacto por Colombia, pacto por la equidad*. Congreso de la República.

Consejo de la Unión Europea. (2006). *Recomendación del Parlamento Europeo y del Consejo de 18 de diciembre de 2006 sobre las competencias clave para el aprendizaje permanente*. Diario Oficial de la Unión Europea.

Cujabante Villamil, X. A., Bahamón Jara, M. L., Prieto Venegas, J. C., & Quiroga Aguilar, J. A. (2020). Ciberseguridad y ciberdefensa en Colombia: un posible modelo a seguir en las relaciones cívico-militares. *Revista Científica General José María Córdova, 18*(30), 357- 377. http://dx.doi.org/10.21830/19006586.588

Cuevas, A. & da Silva França, F. (2023). *Competencias digitales para el uso didáctico del smartphone en el aula y la seguridad digital: aplicaciones móviles.* II Jornada «Aprendizaje Eficaz con TIC en la UCM» (pp. 191-201). Ediciones Complutense.

Departamento Nacional de Planeación. (2011, 14 de julio). *Lineamientos de Política para la Ciberseguridad y Ciberdefensa CONPES 7101*. Departamento Nacional de Planeación. https://bit.ly/2UhnzYC

Departamento Nacional de Planeación. (2016, 11 de abril). *Política Nacional de Seguridad Digital CONPES 3854*. Departamento. Nacional de Planeación. https://bit.ly/3brazVR

Departamento Nacional de Planeación. (2020, 01 de julio). Política Nacional de Confianza y Seguridad Digital. CONPES 3995. Bogotá. https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf

Departamento Nacional de Planeación. (2022). *Bases del Plan nacional de Desarrollo 2022-2026*. Departamento Nacional de Planeación.

Departamento Nacional de Planeación. (8 de Noviembre de 2019). *Política Nacional para la Transformación Digital e Inteligencia Artificial CONPES 3975*. Política Nacional para la Transformación Digital e Inteligencia Artificial.

DQ Institute. (2022). ***Child Online Safety Index***. https://www.dqinstitute.org/child-online-safety-index/

Escuela Militar de Cadetes -ESMIC-. (2023). *Proyecto Educativo del Programa Ciencias Militares.* Escuela Militar de Cadetes "General José María Córdova".

Escuela Militar de Cadetes -ESMIC-. (2023). *Sillabus Ofimática*. Escuela Militar de Cadetes "General José María Córdova".

European Union Agency for Network and Information Security (ENISA). (2016). *Cyber Hygiene practices.* https://www.enisa.europa.eu/publications/cyber-hygiene/at_download/fullReport

Gómez, A., Alvarado, R., Martínez, M., & Diaz de León, C. (2018). La brecha digital: una revisión conceptual y aportaciones metodológicas para su estudio en México. *Entreciencias: diálogos en la Sociedad del Conocimiento, 6*(16), 47-62. https://doi.org/https://doi.org/10.22201/enesl.20078064e.2018.16.62611

González, C., Galvis E., González M.,(2016). Estudio exploratorio sobre competencias digitales y uso de e-servicios. Caso estudiantes de una Facultad de Salud de Norte de Santander - Colombia. *Entramado, 12*(2), 276-288, http://dx.doi.org/10.18041/entramado.2016v12n2.24224

González, F., Tarango, J., & Villanueva A. (2019). Hacia una propuesta para medir capacidades digitales en usuarios de internet. *Revista Interamericana de Bibliotecología, 42*(3), 197-212. https://doi.org/10.17533/udea.rib.v42n3a01

Gutiérrez, F., & Leguizamón, M. (2021). Alfabetización Informacional: una vía de acceso a la información confiable. *Revista Historia de la Educación Latinoamericana, 23*(36), 161-181. Epub October 22, 2021.https://doi.org/10.19053/01227238.11620

Jaramillo, O. (2015). Pertinencia del perfil de los profesionales de la información con las demandas del mercado laboral. *Revista Interamericana de Bibliotecología, 38*(2), 111-120. https://doi.org/10.17533/udea.rib.v38n2a03

Martín, M., Pérez, L., & Jordano de la Torre, M. (2020). Las competencias digitales docentes en entornos universitarios basados en el Digcomp. *Educar em Revista*, 36, 1-21. https://doi.org/10.1590/0104-4060.75866

Ministerio de Educación Nacional. (2006). *República de Colombia. Estándares básicos de competencias en tecnología e informática* [online]. Ministerio de Educación Nacional. http://www.semmonteria.gov.co/download/estandares-basicos-tecnologia-informatica-version15.pdf

Ministerio de las Tecnologías de la Información y las Comunicaciones. (2021). *Manual de Gobierno Digital.* https://gobiernodigital.mintic.gov.co/692/channels-594_manual_gd.pdf

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

Pick, J., & Sarkar, A. (2016). *Theories of the Digital Divide: Critical Comparison. 2016 49th Hawaii International Conference on System Sciences* (HICSS)(16), 3888–3897. https://doi.org/https://doi.org/10.1109/HICSS.2016.484

Redecker, C. (2017). *Marco Europeo para la Competencia Digital de los Educadores: DigCompEdu. Centro Común de Investigación de la Comisión Europea.* https://doi.org/ doi:10.2760/159770

Ríos Muñoz, D., & Herrera Araya, D. (2017). Los desafíos de la evaluación por competencias en el ámbito educativo. *Educação e Pesquisa, 43*(4), 1073-1086. https://doi.org/http://dx.doi.org/10.1590/S1678-4634201706164230

Segrera, J., Páez H., Polo A. (2020) Competencias digitales de los futuros profesionales en tiempos de pandemia. *Utopía y Praxis Latinoamericana, 25*(11), 222-232. ISSN: 1315-5216. https://www.redalyc.org/articulo.oa?id=27964922015

Silva Quiroz, J. E., & Lázaro-Cantabrana, J. L. (2020). La competencia digital de la ciudadanía, una necesidad creciente en una sociedad digitalizada. Edutec. *Revista Electrónica De Tecnología Educativa,* (73), 37-50. https://doi.org/10.21556/edutec.2020.73.1743

Vuorikari, R., Kluzer, S., Punie, Y. (2022). DigComp 2.2, *The Digital Competence framework for citizens: with new examples of knowledge, skills and attitudes, Publications Office of the European Union.* https://data.europa.eu/doi/10.2760/115376

World Economic Forum - WEF. (2023). *Global Cybersecurity Outlook 2023.* https://www.weforum.org/reports/global-cybersecurity-outlook-2023

World Economic Forum - WEF. (2023a). *The Global Risks Report 2023.* https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf

Revista Ciberespacio, Tecnología e Innovación
Volumen 2, número 4, julio-diciembre 2023 (pp. 147-167)
Bogotá, D.C, Colombia

EDITORIAL ESDEG

Propuesta de capacitación virtual para promover la cibercultura en el Ejército Nacional de Colombia

Virtual training proposal to promote cyberculture in the Colombian National Army

DOI: https://doi.org/10.25062/2955-0270.4811

Manuel Eduardo Oviedo Sierra
Escuela Superior de Guerra "General Rafael Reyes Prieto", Bogotá D. C., Colombia

Resumen

La Cibercultura es un tema que se encuentra en consolidación debido a su importancia en el contexto tecnológico, pero que ha tenido una gran relevancia en el ámbito educativo y no solamente al interior de las Fuerzas Armadas, sino a nivel global. A través de este artículo, se establece una propuesta de capacitación virtual al personal militar para fomentar el uso responsable de estas tecnológicas emergentes. Uno de los métodos que se utilizó, fue la recopilación de documentos académicos y científicos que permitieron comprender el fenómeno de estudio. Uno de los resultados encontrados, es que, la capacitación en Cibercultura está al alcance de todo el personal militar y, por ende, debe fomentarse en el corto, mediano y largo plazo. En conclusión, la Cibercultura es un tema estratégico que permite fomentar el uso responsable de todo tipo de tecnologías en el mundo global.

Palabras Clave: Cibercultura, capacitación, virtualidad, tecnologías, formación.

Abstract

Cyberculture is an issue that is booming due to its importance in the technological context, but it has had a great relevance in the educational field and not only within the Armed Forces, but globally. This article establishes a virtual training proposal for military personnel to promote the responsible use of these emerging technologies. One of the methods used was the compilation of academic and scientific documents that allowed us to understand the phenomenon of study. One of the results found is that cyberculture training is available to all military personnel and should therefore be promoted in the short, medium and long term. In conclusion, Cyberculture is a strategic issue that allows promoting the responsible use of all types of technologies in the global world.

Key words: Cyberculture, training, virtuality, technologies, training.

Artículo de reflexión
Recibido: 23 de noviembre de 2023 • **Aceptado:** 18 de enero de 2023
Contacto: Manuel Eduardo Oviedo Sierra manuel.oviedo@buzonejercito.mil.co

Introducción

Colombia, a lo largo de su historia, ha tenido que atravesar por distintos tipos de conflictos los cuales se han dado en el contexto social, económico, político y cultural llevando a que la violencia se encuentre arraigada en las zonas más apartadas del territorio nacional. Con el surgimiento de las guerrillas a partir del año de 1960 y del narcotráfico en la década de los 70, el país se encontraba sumergido en un escenario de crimen organizado a manos de los grupos al margen de la ley y de las redes del narcotráfico (Fajardo, 2014).

No obstante, para hacer frente a este tipo de amenazas el Estado colombiano ha tenido a su disposición unas Fuerzas Militares (FF.MM), para hacer frente a los grupos armados y delincuenciales, y así, salvaguardar y proteger los intereses tanto de la misma nación como de los ciudadanos (Congreso de la República, 1991). En relación con esto, el Ejército Nacional de Colombia, es la Fuerza más antigua en el contexto militar, ya que, ha tenido que afrontar los conflictos más violentos del país, sobresaliendo a través del tiempo, en la medida que ha demostrado su capacidad de resiliencia y adaptación al contexto en que se encuentre el país en materia de defensa y seguridad.

Para lograr esto, el Ejército a lo largo de su historia ha venido efectuando diferentes procesos de adaptación de acuerdo con el comportamiento de las amenazas que se encuentren en el territorio nacional. Por ejemplo, para el año 2002 los cultivos ilícitos y el poder delictivo de los grupos al margen de la ley, se habían convertido en la mayor preocupación para el gobierno nacional, por esto el Sector Defensa a través del Plan Colombia, inició la modernización y actualización de sus capacidades para hacer frente a los grupos armados y organizaciones del crimen organizado, y así, afectar significativamente las redes de criminalidad y narcotráfico en el país (Guevara Latorre, 2009).

Para el año 2010, el gobierno nacional a través de su política de Defensa y Seguridad, había logrado afectar en su mayoría las estructuras de los grupos guerrilleros, como fue el caso de las Fuerzas Armadas Revolucionarias de Colombia, Ejército del Pueblo (FARC-EP), donde la Fuerza Pública logró recuperar territorios y zonas que habían sido controladas durante décadas por parte de este grupo al margen de la ley, al mismo tiempo se generó inversión social y se brindó seguridad en zonas donde el Estado no había logrado hacer presencia en años atrás (Ministerio de Defensa Nacional, 2010).

Al igual que el crimen organizado se iba transformando, de la misma forma lo comenzaban a hacer los medios para la guerra, por ejemplo, el aumento de las amenazas en el Ciberespacio se comenzaron a ver, sobre todo con ataques como el Phising, Ransware, Business Email, entre otros, los cuales buscaban vulnerar la seguridad informática de las redes digitales; tanto a nivel Estatal como privado, de tal forma, que se tuviera una afectación directa, los principales medios informáticos donde se almacenaba datos relevantes de las Entidades públicas del Estado colombiano, y es allí, donde el Ciberespacio comenzó a convertirse en un nuevo escenario en términos de amenazas (Centro de Investigación Internacional, 2019).

Para el año 2010, ya las amenazas territoriales a manos de las guerrillas habían cambiado, en la medida que el Crimen Organizado Transnacional (COT) se había tornado en Colombia, debido a la gestación de nuevas organizaciones sin ideología de lucha, pero sí buscaban afectar la seguridad del país a través de las redes del narcotráfico. Por esto, el Ministerio de Defensa Nacional realizó la proyección que debía tener el Ejército Nacional, para hacer frente a estas nuevas amenazas emergentes en el marco de la defensa y seguridad del país, atendiendo los nuevos desafíos que esto podría representar (Ministerio de Defensa Nacional, 2012).

Desde las últimas décadas y hasta la actualidad, el Ejército Nacional de Colombia ha venido adaptando la estrategia militar para hacer frente a las nuevas amenazas que surgen en el territorio nacional, y durante este proceso, se han venido implementando tecnologías que han permitido el uso de información necesaria, para así, obtener datos en tiempo real que permitan el desarrollo de operaciones militares a lo largo y ancho del territorio nacional (Gaitán, 2021).

En relación con esto, el problema raíz que se ha visto al interior de la Fuerza es la falta de una adopción de cultura en términos de Ciberseguridad, debido a los nuevos escenarios de la guerra electrónica o digital, si bien es cierto, el Ejército Nacional ha venido cumpliendo su mandato Constitucional, en relación con la desarticulación de las distintas amenazas que se han presentado en el territorio nacional, el Ciberespacio se ha convertido en un escenario que requiere de personal militar capacitado en áreas inmersas de la Ciberseguridad, para así, afrontar este tipo de amenazas que puedan colocar en riesgo la defensa y seguridad de la nación.

Es importante tener en cuenta, que, durante todos estos cambios y transformaciones de las capacidades del Ejército Nacional, la Fuerza cuenta con el sistema de educación militar el cual ha sido el encargado de rediseñar estrategias asociadas al proceso de formación y capacitación de los oficiales, suboficiales y soldados profesionales que hacen parte de la Institución, en la medida que esto, garantiza que el personal militar se adapte a los distintos cambios que tiene el país en temas de defensa y seguridad (Ministerio de Defensa Nacional, 2021).

Uno de los componentes que se han venido fomentando y promoviendo en la formación del personal militar, ha sido el uso de las Tecnologías de la Información y Comunicación (TIC's). Sin embargo, y ante el cambio constante de las tecnologías, el uso apropiado de las redes informáticas se ha convertido en una prioridad en el contexto académico, y no solo en las FF.MM, sino en el mundo global. Hay que señalar, que el Ejército Nacional ha venido diseñando nuevos planes de estudio, los cuales se ajustan al contexto militar y a la política del Sector Defensa, pero se observa que no hay un acercamiento profundo con la Cibercultura.

Para el desarrollo de esta investigación se planteó como pregunta ¿De qué manera se puede promover la cibercultura en el Ejército Nacional de Colombia a través de la capacitación virtual del talento humano?

Como tesis se resalta la idea de hacer un buen uso de las tecnologías que se encuentran a disposición del personal militar resulta ser un eje esencial, ya que, de esta forma, se puede prevenir que se utilice algún tipo de tecnología o información que pueda afectar las actividades que se llevan a cabo al interior del Ejército Nacional en diferentes ámbitos. También le permite a la Fuerza, comprender diferentes ámbitos y contextos que hacen parte del ciberespacio y de los ciberciudadanos.

La importancia de esta investigación es que, a partir de este estudio, sea el Comando de Educación y Doctrina (CEDOC), del Ejército, quien inicie un plan piloto para certificar al personal militar en el ámbito de la cibercultura, convirtiéndose en uno de los pioneros en fomentar el buen uso de las redes informáticas a nivel nacional y en el Sector Defensa. También se espera, que, a partir de este artículo, se desarrollen otras líneas educativas enfocadas al ciberespacio, el ciberciudadano y demás temas emergentes.

Metodología

Para el desarrollo de este artículo de investigación, se utilizó el método cualitativo a través de un estudio documental sobre el fenómeno determinado, en este caso la Cibercultura en el Ejército Nacional, y a partir de esto, se analizaron los resultados encontrados. Por otra parte, y como técnica de recolección de información, se empleó el análisis de documentos académicos que dieron soporte para el desarrollo de los objetivos específico a lo largo de la investigación.

Cibercultura y sus aportes al fortalecimiento de la educación virtual y del talento humano en prevención de ciberataques

En este primer apartado se describen las generalidades del concepto de la *cibercultura* y cómo esta aporta para fortalecer los procesos de la enseñanza en la educación virtual, y al mismo tiempo, permite prevenir ciberataques en diferentes contextos. A continuación, se detallan los aportes de la *cibercultura* al fortalecimiento de la educación virtual y del talento humano en prevención de ciberataques:

Importancia de la cibercultura

El siglo XXI ha traído consigo, un sin número de cambios sociales, culturales, políticos y militares, sin embargo, el que más cambios constantes y dinámicos ha traído, ha sido el tecnológico, en la medida que, hoy en día en la mayoría de los países y de los territorios, cuentan con acceso a teléfonos inteligentes, computadores, cámaras y demás medios de tecnología informática, esto ha permitido conectar al mundo de un lado a otro sin importar la distancia (Moya & Vásquez, 2010).

Debido a esto, surge el término de cibercultura y para comprenderlo, primero, hay que abordar el concepto de Cultura el cual ha sido definido como:

La Cultura ha sido vista como un conjunto de comportamientos, tradiciones y hábitos que son realizados de forma frecuente por cierto tipo de población. Es decir, en sí, el concepto tiene relación con el medio en que se desarrolla una sociedad en determinado lugar o territorio específico, ahora, no puede verse esto como una serie de comportamientos que se realizan a nivel general (Barrera, 2013).

Con base a lo anterior, es importante tener en cuenta que, lo que se antepone a la Cultura es lo anticultural, y es ahí, donde este concepto toma relevancia. Por ejemplo, en América Latina existen comportamientos o acciones que no son bien vistos en cambio en otra parte del mundo esto es algo normal (Cultural). En este sentido, se genera un choque entre las distintas costumbres y comportamientos que tienen las sociedades a nivel mundial, y cabe señalar, que la diferencia de culturas ha sido un escenario que también ha generado distintos tipos de conflictos (Ron, S.f).

Entendiendo esto, la Cibercultura es vista como:

Un conjunto de hábitos, costumbres y formas de comportarse que adoptan las personas en determinado campo de la sociedad. Allí, convergen distintos tipos de Culturas, lo que hace la diferencia, es que, este tipo de Culturas se materializan a través del uso y empleo del Internet y las Tecnologías de la Información y la Comunicación (TIC). Es decir, que, en sí, la Cibercultura está relacionada directamente con el uso de internet y herramientas informáticas en el contexto actual (Lévy, 2007).

En el campo de la cibercultura se manejan 3 áreas de vital importancia, las cuales son:

Hipertextualidad

Es un conjunto de enlaces que se crean a través de elementos tecnológicos; tales como nodos y anclajes, los cuales permiten difundir información de determinado tema o área de estudio de forma masiva y rápida, esto es lo que caracteriza a la hipertextualidad en el marco de la cibercultura. Es importante, tener en cuenta que este tipo de enlaces son utilizados por los distintos usuarios que se encuentran en las redes sociales (De forma digital) quienes también son llamados como los nativos digitales (Caro & Arbeláez, 2009).

También hace referencia a la forma que tienen las personas para relacionarse con los distintos dispositivos móviles que se encuentran a su alcance y de la comunidad en general, como, por ejemplo, un celular, Smartphone, computador portátil, tabletas, etc., allí, se crean los contenidos digitales, y es que esto resulta ser atractivo, debido a que, los usuarios tienen la opción de seleccionar y elegir qué tipo de programas o redes sociales quieren interactuar en determinado contexto (Meritxell, 2002).

Para comprender la relación entre cibercultura y la hipertextualidad, Herrera y Capacho (2019) hacen referencia, a que la primera, es la forma en que se adopta un conocimiento específico en un área determinada, mientras tanto, el segundo, es el escenario y medio en que se genera un nuevo conocimiento para las personas que se encuentran inmersas en un área específica del aprendizaje. Con base en esto, al mismo tiempo la hipertextualidad se convierte en un escenario de vulnerabilidad, debido a su uso en medios tecnológicos y digitales, dando paso al incremento de los ciberataques; tanto en el ámbito público y privado.

Por otra parte, la hipertextualidad se relaciona con el talento humano y los ciberataques, debido a que quienes se encuentran inmersos en este tipo de escenarios digitales deben contar con conocimientos específicos para el manejo de la información y los datos que allí se generan, de lo contrario se tendrá una vulnerabilidad o debilidad en lo que se refiere al manejo o administración de dispositivos móviles, lo cual abre la puerta, para que grupos delictivos puedan extraer datos esenciales en el entorno digital (Caro & Arbeláez, 2009).

Sin embargo, hay que reconocer que la hipertexualidad tiene un aporte significativo en el marco de la educación virtual, ya que, y como lo menciona Tabares (2008), esta temática se ha convertido en una herramienta esencial para el desarrollo de aprendizajes virtuales; tanto sincrónicos como asincrónicos, permitiendo el desarrollo de ambientes virtuales de enseñanza, a través de un elemento principal, como es el hipertexto, sin embargo, son temas que no han sido estudiados o dados a conocer a la comunidad educativa en general, sobre su uso e importancia en el campo de la enseñanza.

Multimedialidad

Es el escenario donde se integran los distintos formatos de hipertexto, los cuales están asociados a gráficos, medios audiovisuales, dibujos animados, entre otros. Es decir, la Multimedialidad hace relación a la combinación de dos o más medios donde lo que se busca es generar un espacio interactivo donde las personas exploran y adquieren nuevos conocimientos en determinada área o rama de la educación. Es importante tener en cuenta que a partir del año 2008 esto tomó relevancia en gran medida al auge de la educación virtual en distintas áreas del conocimiento (Lapuente, S.f).

Con base en esto, la Multimedialidad se relaciona con el talento humano, debido a que, quienes operen estos espacios virtuales de aprendizaje deben poseer habilidades de manejo de herramientas digitales tales como la generación de ilustraciones, figuras en 3D, mapas interactivos, animaciones, videos, entre otras, y es allí, donde el personal que se encargue de generar este tipo de contenido debe poseer las habilidades y competencias necesarias para interactuar en estos espacios virtuales de aprendizaje (Díaz & García, 2022). De esta forma, también se relaciona con la ciberseguridad, ya que, quienes

tengan la competencia para desarrollar contenidos en el contexto de la Multimedialidad, deberán conocer los métodos más efectivos de seguridad en estos escenarios virtuales de aprendizaje, es decir, que todo esto se encuentra relacionado como un todo y no puede entenderse como temáticas separadas en el marco de la ciberseguridad.

En segundo lugar, la Multimedialidad también tiene una relación directa con las vulnerabilidades informáticas, ya que, es una temática que se encuentra en constante evolución, sobre todo en el marco educativo y de la misma forma las amenazas informáticas se han ido incrementando con el pasar del tiempo. Por ejemplo, el Malware, Ataques de Denegación de Servicio Distribuido (DDoS), extracción de contraseñas, etc., se convierten en retos y desafíos en el marco de la ciberseguridad en los entornos digitales (Ambit20 Year, 2020).

En cuanto al relacionamiento de la Multimedialidad con la educación virtual, Salcedo (2010) dio a conocer un modelo pedagógico realizado bajo esta temática, allí resalta que la dimensión tecnológica utilizada y empleada fue fundamental para lograr generar contenido virtual en diferentes áreas del conocimiento, también hace énfasis en el papel que juega el buen uso y empleo de las herramientas virtuales dispuestas en el entorno educativo. Por otra parte, resalta que la Multimedialidad es un factor clave para generar un conjunto de acciones y agrupación de medios electrónicos, para la creación de contenido virtual, es decir, que, en sí, son elementos que permiten avanzar en la formación en línea en diferentes partes del mundo.

Aporte de la cibercultura y la educación virtual

Tabla (2020), explica que la educación virtual ha permitido que un sin número de personas a nivel mundial logren estudiar sin tener que desplazarse a determinado lugar, pero al mismo tiempo, es un escenario donde la cibercultura ha jugado un papel esencial en la medida, que hoy en día, los estudios de educación superior se ven en un alto grado de combinación de culturas a nivel global y esto se da en gran medida gracias a los 3 principios de la cibercultura como lo son: la interconexión, las comunidades virtuales e integración colectiva de sus usuarios, permitiendo que se avance hacia la generación de nuevo conocimiento.

Pesce (2011), explica que la cibercultura ha sido uno de los principales elementos que han llevado a que se genere el aprendizaje en línea, ya que, en el momento que se logra desarrollar la interactividad, lleva a que se genere una vinculación e interconexión entre los distintos tipos de culturas a nivel nacional, regional y mundial, lo cual tiene un impacto más representativo, en la medida que, se conocen otras perspectivas que se tienen sobre determinado tema y permite adquirir nuevos conocimientos en determinada área y con distintos usuarios.

Tomando lo dicho por los autores, en sí, la correlación directa entre la educación virtual y la Cibercultura es la convergencia que existe a través del uso y empleo de las TIC y los programas informáticos para generar el aprendizaje en línea. No obstante, lo que se debe resaltar, es que, este escenario ha permitido que exista un intercambio de ideas, costumbres y demás factores de comportamiento de distintas sociedades, conllevando, a que generen diferentes mundos virtuales conformados a partir de distintos tipos de Culturas (Bastidas & Sequera, 2018).

Principales aportes:

- Conectividad.
- Manejo de la información en tiempo real.
- Comunicación efectiva.
- Construcción del conocimiento a través de la cultura.
- Eliminación de barreras (Lenguaje-espacio).
- Entre otras.

Ciberespacio

Es el entorno o espacio donde se desarrollan distintos tipos de herramientas informáticas, es decir, no es un lugar físico, sino por el contrario, es un sitio totalmente digital donde los computadores u ordenadores emplean para estructurar nuevos medios tecnológicos o mejorar otras herramientas ya existentes en el marco de la era digital. Hoy en día, el ciberespacio está asociado directamente con el uso del Internet en la medida que todo se realiza a través de las páginas web, sistemas de correos electrónicos, redes informáticas y sociales, etc., es decir, que todo se resume al uso de los servidores y su manipulación por los usuarios (Pérez, 2013).

Para comprender con mayor claridad qué es el ciberespacio, hay que tener en cuenta dos variantes: la primera, el límite que existe entre lo digital y lo físico, es decir, que lo virtual representa el espacio donde interactúan varias personas o una comunidad específica, a través de, la utilización de distintos Software, para emplear distintos servicios de Internet tales como el correo electrónico, transacciones, consultas, etc. La segunda, es el lugar virtual que se crea, ya que, todo lo dicho anteriormente, funciona gracias al respaldo informático que existe, para la protección de los datos y la información de las personas, y es allí, donde se crea el Ciberespacio (Conislla, 2019).

Ciberespacio y Ciberataques

Si bien es cierto, hoy en día los sistemas informáticos se encuentran expuesto, mayormente, a ataques por diferentes grupos de criminalidad que buscan extraer información; tanto de empresas públicas como privadas y sobre todo de organismos de seguridad, con el fin de causar un daño inmediato. Y es que, como lo menciona Abad (2020), este

tipo de amenazas se han convertido en un verdadero desafío en el Ciberespacio, ya que, y debido al gran avance tecnológico que se ha tenido durante los últimos 20 años, esto ha sido de vital importancia para el mundo a nivel general, sin embargo, también ha traído consigo mismo una serie de peligros en el ámbito del ciberespacio, debido a que, cada día se crean nuevas redes que buscan afectar los sistemas informáticos y por ende se crean nuevos mecanismos de defensa digital.

Como se han mencionado en los apartados anteriores, la cibercultura es aquella, que permite el intercambio de culturas a través del uso y empleo de las TIC y redes informáticas y al mismo tiempo, juega un papel esencial en la prevención de ataques, ya que, debido a los avances que ha tenido la educación virtual, no solamente en Colombia, sino a nivel global, los controles y mecanismos de prevención que se han tenido que desarrollar; tanto para la protección de la información académica como de las mismas redes digitales, ha conllevado que los ciberataques se vean reducidos en una gran proporción, convirtiendo esto en un aspecto principal en el contexto digital.

A modo de conclusión de este primer capítulo, se detalla que la cibercultura ha sido un espacio propicio para el intercambio de ideas, pensamientos, costumbres, etc., convirtiéndose así en uno de los ejes principales para avanzar en la educación virtual a nivel mundial. Por otra parte, la cibercultura ha permitido que se entrelace de forma directa con lo que tiene que ver con el ciberespacio, dándole una representación esencial en el nuevo contexto digital y llevando a la prevención de ciberataques.

Vulnerabilidades de la Ciberseguridad en el EJC de Colombia

En este segundo capítulo, se darán a conocer los hechos más relevantes que han estado relacionados con la vulnerabilidad y amenazas a las que se ha encontrado expuesto el Ejército Nacional de Colombia en el marco de la ciberseguridad, con el propósito, de entender cuáles son los desafíos que se deben abarcar en el marco de la cibercultura como se mencionó en el primer capítulo.

Contexto de la Ciberseguridad

Antes de adentrarse en las principales amenazas que se enfrentan en temas de ciberseguridad en el Ejército Nacional de Colombia, es importante, primero, precisar una serie de conceptos de tal forma que se entienda el contexto de análisis desde el marco internacional y nacional como se muestra a continuación:

Ciberseguridad

Todo se remonta a la década de los años 50, cuando los desarrollos de las redes informáticas se encontraban en auge en la medida, que buscaba tener una mayor conexión con los equipos de cómputo a nivel internacional (Jarava, 2013). A partir de este contexto, la

ciberseguridad comenzó a tomar relevancia, lo cual se dio en dos momentos; el primero, antes del surgimiento del Internet, debido a que, los ataques eran de forma física a las redes informáticas, el segundo, se da con la puesta en marcha del internet a mediados de 1960, ya que, surge el ciberespacio y con él los ataques pasan a ser de forma cibernética (Ardissom de Souza, 2018).

Debido a las nuevas amenazas en el ciberespacio, es en la década de los años 70 cuando se pone en marcha la Seguridad Informática (SI), y debido a estos avances, en 1980 surge el antivirus como una medida para identificar posibles ataques o daños a las redes informáticas y protección de los equipos de cómputo, sin duda alguna, este tipo de Software fueron y continúan siendo una de las mayores apuestas en el campo de la informática (Ficarra|, 2002).

No obstante, es en el año 2002 cuando los ciberataques a las redes informáticas se convierten en una verdadera amenaza a nivel internacional, ya que, surgen organizaciones criminales que se dedican a generar ataques en el ciberespacio, colocan en riesgo la SI sobre todo a las entidades públicas, y con el pasar del tiempo, el sector privado también se convirtió en objetivo para este tipo de organizaciones ilegales (Jiménez, 2022). Es a partir del siglo XXI que la ciberseguridad toma gran relevancia en ambos sectores (Estatales y privados) ya que se comienzan a desarrollar mecanismos y herramientas digitales para hacer frente a estos retos en el marco de la SI.

Ciberseguridad en América Latina

El Banco Interamericano de Desarrollo - BID (2016), publicó un informe donde detalla que, debido a los avances e importantes desarrollos tecnológicos informáticos que se han dado durante los últimos 15 años, se ha logrado avanzar de forma significativa, lo cual ha llevado a que el mundo se encuentre de más hiperconectado cada día en diferentes sectores. Sin embargo, esto también ha generado que cada día las amenazas en el ciberespacio tomen mayor importancia, y es allí, donde el BID hace énfasis en que los países deben desarrollar mecanismos efectivos para hacer frente a estos retos en el marco de la ciberseguridad.

A su vez, el Observatorio de la Ciberseguridad en América Latina y el Caribe, organismo del BID, ha venido publicando informes de seguimiento a las amenazas que convergen en el ciberespacio de la región, también ha estudiado con detenimiento los casos en que este tipo de ciberdelincuentes han logrado vulnerar los servicios informáticos tanto; en el sector público como privado. Debido a esto, ha creado un portal de libre acceso para efectuar diferentes comparaciones en ataques provenientes por organizaciones cibernéticas, con el fin de que los países fomenten alianzas y mecanismos de protección a las redes de información.

De acuerdo con Latam Business School (2020), los países que más sufren de ciberataques en América Latina son Brasil, México, Colombia, Perú, Argentina y Chile, sin embargo, quienes tienen mayor debilidad en términos de ciberseguridad es el gobierno argentino, ya que, carecen de desarrollo informático para la protección de las redes cibernéticas. Ante esto, el organismo señala que el mayor peligro en el ciberespacio de la región es el Phishing, el cual actúa de forma ilegal para acceder a los datos que se encuentran en los centros digitales, tanto de entidades públicas como privadas.

Ciberseguridad en Colombia

En el caso nacional, el país ha tenido que afrontar diversos hechos en materia de ciberdelincuencia a manos de grupos delictivos que han buscado vulnerar la SI de distintos sectores; tanto públicos como privados. Por ejemplo, a finales del año 2022 un grupo llamado RansomHouse se atribuyó haber accedido a la base de datos de una de las Empresas Prestadoras de Salud (EPS) llamada "Sanitas" lo cual conllevó que la Entidad tuviera que suspender la plataforma a través de la cual se llevaban a cabo los respectivos trámites de servicios de salud, generando caos y pérdida de millones de datos que allí se encontraban (Osorio, 2022).

Otro caso que generó especulaciones fue en el año 2021, cuando el grupo llamado Anonymous logró deshabilitar la página del Senado de la República y al mismo tiempo, dejó sin servicio los correos electrónicos de los Congresistas del Congreso. Sin duda alguna, estos hechos se han convertido en una amenaza en materia de defensa y seguridad, ya que coloca en peligro la información de los ciudadanos; tanto en el ámbito público y privado. Cabe resaltar que el país ha generado la normatividad necesaria con el liderazgo del Ministerio de las Tecnologías de la Comunicación y la Información (MinTIC).

Hechos de Ciberataques al Ejército Nacional

El Ejército Nacional de Colombia ha ido avanzando en materia de ciberseguridad, ya que, cuenta con Unidades Militares especializadas para hacer frente a este tipo de amenazas diariamente, lo cual ha permitido salvaguardar y proteger la SI de la Institución. Por ejemplo:

El día 04 de mayo del 2021, el grupo llamado Anonymous se atribuyó haber extraído una cantidad de correos electrónicos y contraseñas del personal militar. Ante esto, el grupo especializado en materia de ciberseguridad dio a conocer que se trataban de cuentas que ya habían sido deshabilitadas en el año 2018, las cuentas no contaban con información sensible, sino por el contrario, solamente tenían datos de archivo en general. No obstante, esto se convirtió en una alerta de prevención para mejorar y fortalecer los mecanismos de SI en todos los sistemas tecnológicos de la Fuerza.

En julio del 2021, se conoció que agencias externas habían intentado acceder a archivos secretos en materia de Inteligencia Militar del Ejército Nacional de Colombia, lo cual provocó y generó grandes especulaciones sobre la seguridad de los SI de la Fuerza. Sin embargo, esto fue aclarado por parte de la Institución donde se da a conocer que se han implementado controles y mecanismos efectivos para evitar este tipo de Ciberataques por parte de organizaciones delincuenciales.

En octubre de este mismo año, otro grupo llamado Guacamaya dio a conocer que habían logrado extraer información confidencial de la página Web del Ejército Nacional de Colombia, hechos que fueron aclarados por parte del grupo de Ciberseguridad de la Fuerza. Ante esto, lo primero que se hizo, fue revisar los controles que se tienen para el manejo de la SI en sitios Web y allí, se precisó que la información que se encuentra publicada es precisamente, para el público en general. Es decir, que puede ser consultada por parte de la ciudadanía, sin embargo, este hecho también se convierte en alertas para continuar con el fortalecimiento de la seguridad en los sistemas cibernéticos.

Debido a estos eventos relacionados con la ciberseguridad, Mozo & Ardila (2022) explican que debido a los avances en materia tecnológica e informática que se han dado tanto a nivel nacional como internacional, esto ha permitido que se tenga una sociedad más hiperconectada, sin embargo, también esto ha incrementado los riesgos y amenazas en materia de seguridad tecnológica, en la medida que las amenazas cada día son más emergentes y silenciosas, lo cual hace que los retos y desafíos sean cada día mayores y se deban aplicar controles efectivos en materia de ciberseguridad. En este artículo, se resalta el modelo de riesgos y mitigación de amenazas que se ha adoptado al interior de la Institución, para así, reducir en su máxima expresión los ataques por parte de organizaciones u personas delincuenciales.

Capacitación Virtual para el Fortalecimiento de la Ciberseguridad en el Ejército Nacional de Colombia

En este tercer y último capítulo, se dará a conocer una propuesta de capacitación virtual para el personal militar del Ejército Nacional en lo que tiene que ver con la cibercultura en el campo de la ciberseguridad, con el fin de que esta temática sea tenida en cuenta en los planes de estudio de las escuelas de Capacitación, ya que, es un área educativa que permite fortalecer los conceptos en el marco de la ciberseguridad, enfocado a los procesos que lleva a cabo el personal militar en las distintas Unidades Militares, así:

Educación Virtual (EV)

La Educación Virtual (EV) o también conocida la educación en línea, es el método que se utiliza para llevar a cabo cierto tipo de enseñanza de forma digital donde se emplean

medios tecnológicos e informáticos para colocar a disposición del alumno todas las herramientas para adquirir nuevo conocimiento (Chirinos et al, 2010). En relación con esto, y a través del tiempo, la comunidad educativa a nivel global ha ido avanzando para generar una oferta amplia sobre cursos especializados, técnicos, tecnológicos y profesionales de forma virtual, lo cual se aumentó, con la llegada de la pandemia del Sars-Cov2-(Covid-19) en el año 2020, donde la EV tomó gran relevancia en el campo educativo (uTn, 2021).

Una de las principales características de la EV, es que permite conectar a un sin número de personas en tiempo real, sin importar la distancia o el lugar en que se encuentren conllevando al intercambio de culturas y distintos pensamientos en determinadas áreas del conocimiento, un modelo que resulta propicio para el Ejército Nacional, en lo que tiene que ver con el fortalecimiento del aprendizaje de la Ciberseguridad en cumplimiento de su labor en las distintas Unidades Militares.

Estrategias Pedagógicas en el Curso de Ciberseguridad en el EJC

La Educación Militar en el Ejército Nacional ha sido fundamental para formar, capacitar y entrenar a los Oficiales, Suboficiales y Soldados que hacen parte de la Fuerza y así dotarlos de conocimientos y habilidades específicas para atender los desafíos en materia de Defensa y Seguridad. Sin embargo, para el desarrollo del curso de ciberseguridad de modalidad virtual se requiere de la aplicación de estrategias pedagógicas mediadas por TIC, como se muestra a continuación:

Habilidades de los Docentes en materia de uso de las TIC

Lo que se busca es que los docentes tengan la capacidad de utilizar y emplear de la mejor manera los recursos tecnológicos para así alcanzar los objetivos propuestos desde el ámbito curricular. Por ejemplo:

Gamificación. Es una metodología que permite desarrollar la adquisición de conocimiento a través de distintos tipos de juegos educativos, conllevando que el aula tenga un enfoque lúdico y dinámico en materia de aprendizaje. Al mismo tiempo, genera una participación de todos los alumnos que se encuentran en modalidad virtual, ya que, su participación se da, de acuerdo con el conocimiento que se ha adquirido durante el desarrollo del saber y convirtiendo esto, en un punto de partida para el docente (Borrás, 2015).

Aula invertida. Es una técnica que rompe de forma directa los métodos tradicionales de la enseñanza, ya que, tiene como principal elemento intercambiar el rol que juega el docente y el alumno. Es decir, el profesor toma la posición de acompañar la construcción del conocimiento a través de actividades de pensamiento y análisis crítico con actividades como debates, foros, charlas, etc., en el caso de los estudiantes, son quienes interactúan en la clase a través de preguntas y cuestionamientos del tema que se está

estudiando con esto se logra atender las principales necesidades u vacíos de conocimiento que presentan los estudiantes (Vidal et al, 2016).

Herramientas a Emplear en el Aula Virtual del Curso de Cibserseguridad

Pizarras electrónicas. Estas han tomado gran relevancia en la EV, ya que, permite la generación de contenido; dinámico y efectivo, para la apropiación del conocimiento, al mismo tiempo conlleva a que se desarrollen ejercicios de forma paralela y grupal generando una ruptura positiva en los métodos de enseñanza virtual tradicionales, y a su vez, permite desarrollar diversos tipos de actividades propuestas para el aula de clases (Innovate Learning Solutions, 2023).

Aplicaciones educativas. Llevar a cabo procesos de Gamificación en el aula se ha convertido en algo novedoso y dinámico, en la medida que, esto permite la participación de todos los alumnos en el aula de modalidad virtual, todo esto, debido a la gran oferta que existe en el mercado educativo virtual, ya que, se pueden emplear un sin número de aplicaciones para la comprobación del conocimiento, como, por ejemplo, las aplicaciones de evaluaciones, cuestionarios, foros, diagramas, etc., actividades de las cuales se extraen resultados en tiempo real (Vargas, 2019).

Material digital. Las lecturas en formato Portable Document Format (PDF) han sido fundamentales para la adquisición de nuevo conocimiento en las distintas áreas de la educación virtual. Sin embargo, en un área de estudio como es la ciberseguridad, los Ebooks han tomado mayor relevancia debido a que busca tener la mayor similitud a un libro físico, permitiendo mayor comodidad en términos de aprendizaje, por esto, debe ser una herramienta fundamental en el marco de la EV (E-Learning Specialist, 2022).

Ambientes para el Desarrollo de la EV en Ciberseguridad

Un ambiente de desarrollo para la EV, es el espacio en el medio tecnológico en el que se crea un Ambiente Virtual de Aprendizaje (AVA) para generar la adquisición de nuevo conocimiento en determinada área y propiciar el intercambio de ideas grupales académicas. En una AVA se desarrollan los contenidos digitales en relación con actividades, simulaciones, tareas, entre otros, que se encuentran a disposición de los alumnos y profesores de forma virtual (Romero, 2020).

Ava de Ciberseguridad

Lo que se busca, es que, se tenga un curso de ciberseguridad que esté al alcance de todo el personal de oficiales y suboficiales del Ejército Nacional de forma virtual, con el fin de fortalecer la Cibercultura y el manejo de la información en las Unidades Militares, el cual deberá estar conformado de los siguientes módulos de aprendizaje, a continuación, se dan a conocer los respectivos Objetivos de Aprendizaje (OVA):

Propuesta de Módulos de Ciberseguridad en el Ámbito Militar

En este apartado, se darán a conocer los módulos de estudio que se aplicarán de forma virtual para el aprendizaje de la Ciberseguridad en el contexto militar por parte del personal de oficiales y suboficiales del Ejército Nacional, de tal forma, que se genere una cibercultura, así:

Fundamentación de la Ciberseguridad

En este módulo de aprendizaje, lo que se busca es que el alumno adquiera la fundamentación teórica y conceptual sobre la ciberseguridad en el campo general, comprendiendo su importancia en el contexto actual. Por ejemplo, se deben explorar los escenarios en qué se forjó la ciberseguridad desde el campo internacional hasta llegar al contexto nacional, desde el componente académico e investigativo y de esta forma, el estudiante entenderá la procedencia de esta temática en diferentes ámbitos de aplicación.

La Seguridad en Diferentes Ambientes y Escenarios

En esta área de estudio, el alumno tendrá a su disposición una serie de casos y eventos que se han dado en el campo de la Ciberseguridad a nivel mundial y nacional, abarcando esto desde diferentes contextos. Por ejemplo, lo empresarial, económico, político, la seguridad y defensa nacional, para que, de esta forma, el estudiante comprenda la importancia que tiene la Ciberseguridad en diferentes ambientes y escenarios; tanto en la vida personal como en su rol como militar al interior del Ejército Nacional de Colombia.

La Ciberseguridad en el Ambiente Militar

Este módulo será de tipo específico, en la medida que el alumno conocerá y adoptará la importancia de la ciberseguridad en el ambiente militar, ya que, se le dotará de temas específicos en esta área de estudio, tales como: uso de servidores, herramientas de software, utilización de cuentas electrónicas, seguridad informática (uso de contraseñas), virus, amenazas, riesgos, etc., en este módulo, el alumno estará en la capacidad de aplicar la cibercultura dentro de su rol como militar en las diferentes Unidades del Ejército Nacional.

La Ciberdefensa

En este objeto de aprendizaje, lo que se busca es que, el alumno esté en la capacidad de identificar los principales elementos que hacen parte de la ciberseguridad en el ciberespacio enmarcado en la defensa y seguridad nacional. En este OVA, el estudiante aprenderá a analizar datos sensibles que se encuentren relacionados con los ciberataques a organizaciones; tanto públicas como privadas, en relación con las amenazas existentes. Para esto, en el aula virtual se dispondrán de casos de estudio, con el propósito de desarrollar en el estudiante la competencia de análisis e interpretación de datos relacionados con el contexto nacional e internacional.

Vulnerabilidades de la Ciberseguridad

En este módulo de aprendizaje, el alumno conocerá las principales debilidades y vulnerabilidades a las que se encuentra expuesta la seguridad informática en los distintos niveles del Estado colombiano, en temas relacionados con el ciberataque. Con esto, el estudiante entenderá la importancia de aplicar los mecanismos y métodos necesarios para salvaguardar y proteger la información que se encuentra en las redes informáticas, de tal forma, que esto conlleve a adquirir una cibercultura en las distintas Unidades Militares.

Generalidades para la Ejecución del Curso

Teniendo en cuenta la estructuración del curso en ciberseguridad para el personal militar, es importante, tener en cuenta los siguientes elementos:

Sistema tecnológico a utilizar y dirección administrativa

Teniendo en cuenta, que el curso de ciberseguridad para el personal de oficiales y suboficiales será ofertado en el sistema de educación militar, el sistema tecnológico (Plataforma académica) que se utilizará será la BlackBoard, ya que, es el sistema que se encuentra habilitado en términos de licencias educativas por parte del Ministerio de Defensa Nacional (MDN). En cuanto a la dirección de este curso, deberá impartirse desde el Centro de Educación Militar (CEMIL), debido a que es el centro que orienta la capacitación y niveles de ascenso junto con la ESACE, por lo cual, desde el CEMIL debe llevarse a cabo la parte administrativa y de certificación.

Costos de implementación

Para colocar a disposición del personal de oficiales y suboficiales el curso de ciberseguridad, se requieren de los siguientes elementos: el primero, una plataforma académica la cual ya existe en términos de funcionamiento y licenciamiento, en este caso es la BlackBoard, el segundo, el personal que debe estructurar los contenidos académicos de los módulos de ciberseguridad, esto se haría a través de los convenios educativos que ha suscrito el Departamento de Educación Militar (CEDE7) con universidades privadas que ofertan este tipo de cursos en ciberseguridad, el tercer elemento es, la generación de las OVA y ambientes de aprendizaje en la plataforma, esto si requiere un desarrollo de generadores de contenido digitales, procedimiento que deberá efectuarse desde la contratación de personal especializado en esta área.

Con base a lo anterior, el único proceso contractual en términos económicos que tendría que realizar sería la contratación para el desarrollo de las OVA y los ambientes virtuales de aprendizaje en la plataforma BlackBoard, esto requiere de diseñadores web en términos académicos. Un aproximado para el desarrollo de los 5 módulos de

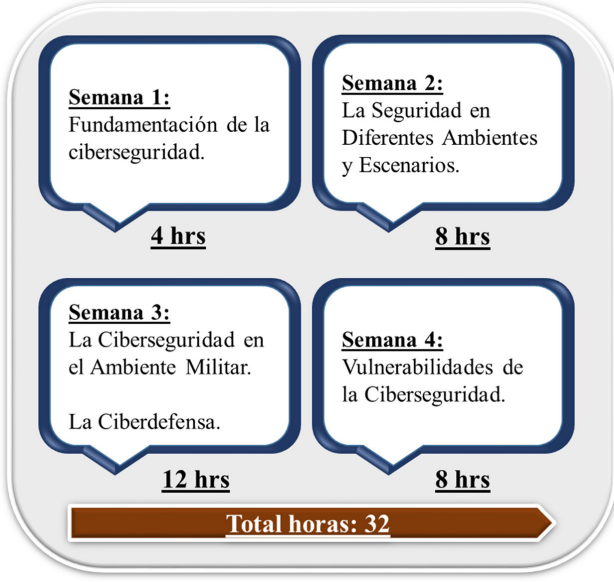
ciberseguridad, sería de $ 25.000.000 millones de pesos, cifra que se encuentra viable desde la apropiación presupuestal del sistema de educación militar.

Tiempo de desarrollo

El curso de ciberseguridad será ofertado en el programa de Educación Continuada (EC) de la directiva de cursos militares del respectivo año. A su vez, será de modalidad virtual, con el fin de que se desarrollé de forma paralela; tanto en las escuelas de Capacitación de los Oficiales y Suboficiales, como en los respectivos cursos de ascenso que se llevan a cabo en la Escuela de Armas Combinadas del Ejército Nacional (ESACE) en los diferentes niveles. Esto, con el propósito, de que, todo el personal militar que se encuentre desarrollando su ciclo de capacitación, obtenga los conocimientos específicos en el manejo de la información en el contexto de la ciberseguridad.

El curso, deberá desarrollarse en un tiempo estimado de 4 semanas distribuidas, así:

Ilustración 1. Tiempo de desarrollo curso de ciberseguridad personal militar.



Nota: Elaboración propia. Diseño curricular del curso de ciberseguridad para ser desarrollado en un lapso de 4 semanas en modalidad virtual.

En relación con el desarrollo del curso, los **módulos esenciales** serían los que se encuentran en la semana 3, ya que, en este punto el oficial o suboficial tendría conocimientos básicos sobre lo que es la ciberseguridad en distintos ámbitos y escenarios, en esta semana afianzaría y entendería su papel dentro del contexto militar en lo que tiene que ver con el manejo de la información y los sistemas tecnológicos, aplicado a la ciberseguridad.

Población objetivo del curso

El personal que hará parte del curso de ciberseguridad, serán los oficiales y suboficiales que se encuentren en el proceso de ascenso y capacitación en la ESACE. Es decir, quienes estén desarrollando los cursos de Intermedio, Comando, Capinte, Capavan y Pisaje, este curso estará a disposición para realizarse de forma autónoma, pero deberá ser requisito de culminación de estudios para culminar el proceso de capacitación y de esta forma asegurar una cultura en términos de ciberseguridad.

A modo de conclusión de este tercer y último capítulo, se específica que este curso virtual de Ciberseguridad debe convertirse en un requisito en términos académicos, el cual debe desarrollarse a través de las escuelas de capacitación, debido a que, esto conllevaría a adoptar y garantizar una cibercultura tanto a nivel personal (Oficiales, suboficiales y soldados) como Institucional, y así, prevenir Ciberataques por parte de personas u organizaciones que busquen vulnerar la seguridad informática en los distintos niveles de la Institución.

Conclusiones

La cibercultura juega un papel esencial en términos de seguridad informática, ya que, es el método por el cual se adoptan hábitos; tanto a nivel personal como social en determinado contexto. En el caso de la ciberseguridad, es una forma de lograr adquirir un alto grado de responsabilidad en lo que tiene que ver con el manejo de la información, visto desde el marco de la defensa y seguridad nacional, ya que, un manejo incorrecto de la información llevaría a la generación de ciberataques por parte de organizaciones u personas que se encuentran en la ciberdelincuencia.

En lo que concierne a los incidentes que se han registrado hacia el Ejército Nacional ante la opinión pública, cabe señalar que la Institución ha empleado mecanismos efectivos para salvaguardar y proteger la información que se encuentra a nivel interno, ya que, ha sido clasificada en diferentes niveles de consulta. Sin embargo, personas u organizaciones ajenas al Ejército han intentado acceder a las bases de datos para extraer información de alto nivel, lo cual no ha sucedido a la fecha, pero los eventos que se han registrado si han sido una alerta para que se incrementen los controles en términos de seguridad informática. En cuanto a la capacitación virtual en ciberseguridad, se convierte en un elemento prioritario en términos de competencias educativas, ya que, permitiría que todo el personal militar adopte una cibercultura en cuanto al manejo de la información en los distintos niveles de la Institución y así disminuir la probabilidad de ciberataques por parte de organizaciones u personas ajenas a la Institución, lo cual debe darse desde las Escuelas de Capacitación.

Declaración de divulgación

El autor declara que no existe ningún potencial conflicto de interés relacionado con el artículo.

Autor

Manuel Eduardo Oviedo Sierra. Mayor del Ejército Nacional de Colombia. Magíster en Seguridad y Ciberdefensa, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Profesional en Ciencias Militares, Escuela Militar de Cadetes "General José María Córdova", Administrador en Seguridad y Salud Ocupacional, "Universidad Militar Nueva Granada", Colombia.

Orcid: https://orcid.org/0009-0003-3005-8924

Contacto: manuel.oviedo@buzonejercito.mil.co

Referencias

Abad, W. (2020). *Ciberataques: Desafíos en el Ciberespacio.* Academia de Guerra.

Ambit20 Year. (2020). *Tipos de Vulnerabilidades y Amenazas informáticas.* Tipos de Vulnerabilidades y Amenazas informáticas: https://www.ambit-bst.com/blog/tipos-de-vulnerabilidades-y-amenazas-informa%C3%A1ticas

Ardissom de Souza, R. (2018). De las redes al ciberespacio. *Revista Digital Universitaria, 19* (19), 11. https://doi.org/http://doi.org/10.22201/codeic.16076079e.2018.v19n2.a2

Banco Interamericano de Desarrollo. (2016). *Ciberseguridad: ¿Estamos preparados en América Latina y el Caribe?* Seguridad informática. https://doi.org/https://publications.iadb.org/publications/spanish/viewer/Ciberseguridad-%C2%BFEstamos-preparados-en-Am%C3%A9rica-Latina-y-el-Caribe.pdf

Barrera, R. (2013). El concepto de la Cultura: definiciones, debates y usos sociales. *Digital de Historia y Ciencias Sociales,* 24. https://doi.org/file:///D:/Descargas/Dialnet-ElConceptoDeLaCultura-5173324.pdf

Bastidas, J., & Sequera, N. (2018). Cibercultura educativa: umbral entre realidad y virtualidad. *Universidad de Carabobo, 12* (1), 10. https://doi.org/http://servicio.bc.uc.edu.ve/educacion/eduweb/v12n1/art06.pdf

Borrás, O. (2015). *Fundamentos de la Gamificación.* Universidad Politécnica de Madrid. https://doi.org/https://oa.upm.es/35517/1/fundamentos%20de%20la%20gamificacion_v1_1.pdf

Caro, L., & Arbeláez, N. (2009). Hipertextualidad, literacidad y discurso académico: conceptos para la gestión del conocimiento en la red. *Universidad Católica del Norte* (28), 24. https://doi.org/https://www.redalyc.org/pdf/1942/194214468007.pdf

Centro de Investigación Internacional. (2019). *Dilemas del ciberespacio. Contención de las amenazas a la ciberseguridad.* Instituto Matías Romero. https://doi.org/file:///D:/Descargas/Dilemas_del_ciberespacio_Contencion_de_l.pdf

Chirinos, N., Hinojosa, L., & González, R. (2010). *La educación virtual como apoyo instruccional durante el proceso de aprendizaje en la educación superior de Venezuela.* Congreso Iberoamericano de Educación. https://doi.org/https://www.adeepra.org.ar/congresos/Congreso%20IBEROAMERICANO/TICEDUCACION/R1133_Hinojosa_Chirinos.pdf

Congreso de la República. (1991). *Asamblea Constituyente.* Congreso de la República. https://doi.org/http://www.secretariasenado.gov.co/senado/basedoc/constitucion_politica_1991.html

Conislla, F. (2019). ¿Qué es el Ciberespacio? ¿Qué es el Ciberespacio? https://academy.seguridadcero.com.pe/blog/que-es-el-ciberespacio

Díaz, F., & García, V. (2022). Hipertexto, multimedia e interactividad del ciberperiodismo. *Questión, 3,* (29). https://doi.org/https://perio.unlp.edu.ar/ojs/index.php/question/

E-Learning Specialist. (2022). *6 razones por las que utilizar libros digitales en centros educativos*. 6 razones por las que utilizar libros digitales en centros educativos: https://www.cae.net/es/razones-por-las-que-utilizar-libros-digitales-en-centros-educativos/#:~:text=Una%20de%20las%20grandes%20ventajas,tienden%20a%20prestar%20m%C3%A1s%20atenci%C3%B3n.

Fajardo, D. (2014). *Estudio sobre los orígenes del conflicto social armado, razones de su persistencia y sus efectos más profundos en la sociedad colombiana.* Universidad Externado de Colombia. https://doi.org/https://www.centrodememoriahistorica.gov.co/descargas/comisionPaz2015/FajardoDario.pdf

Ficarra, F. (2002). *Antivirus y seguridad informática: El nuevo.* Centro Internacional de Estudios Superiores de Comunicación para América Latina. https://doi.org/https://www.redalyc.org/pdf/160/16007913.pdf

Gaitán, L. (2021). Las amenazas híbridas: Un nuevo escenario para el Ejército Nacional. *Revistascedoc.com, 1*, 3. https://doi.org/https://revistascedoc.com/index.php/bep/article/view/529

Giroux, H. (1997). La pedagógica de frontera y la política del postmodernismo. *Revista Intringulis* (6), 96.

Guevara Latorre, J. (2009). *El Plan Colombia o el desarrollo como seguridad: un análisis documental entre la primera versión del Plan Colombia y la definitiva.* Universidad Colegio Mayor de Nuestra Señora del Rosario. https://doi.org/https://repository.urosario.edu.co/server/api/core/bitstreams/f3324def-7190-4195-882f-a220455847af/content

Herrera, E., & Capacho, A. (2019). El lenguaje hipertextual como herramienta de comunicación y de aprendizaje. *Revista Pensamiento Udecino, 3* (1), 10. https://doi.org/http://portal.amelica.org/ameli/jatsRepo/301/3011426008/html/index.html#:~:text=Es%20importante%20enfatizar%20que%20la,en%20la%20significaci%C3%B3n%20de%20los

Innovate Learning Solutions. (2023). *Importancia de las pizarras digitales interactivas en aulas virtuales. Importancia de las pizarras digitales interactivas en aulas virtuales:* https://www.cae.net/es/importancia-pizarras-digitales-interactivas-aulas-virtuales/

Jarava, S. (2013). *Historia de la administración informática.* En U. V. Mar. Corporación Universitaria del Caribe.

Jiménez, J. (2022). *Ciberdelincuencia: Evolución y relación con la actual situación de pandemia. nuevas modalidades y nuevas problemáticas.* Universidad de Salmanca. https://doi.org/https://gredos.usal.es/bitstream/handle/10366/150144/TG_Jim%C3%A9nezRozas_Ciberdelincuencia.pdf?sequence=1&isAllowed=y

Lamarca, M. (2015). *Hipertexto: El nuevo concepto de documento en la cultura de la imagen.* Hipertexto: El nuevo concepto de documento en la cultura de la imagen. http://www.hipertexto.info/documentos/multimedial.htm

Lapuente, M. (S.f). *Multimedialidad del hipertexto.* Multimedialidad del hipertexto: http://www.hipertexto.info/documentos/multimedial.htm

Latam Business School. (2020). *Ranking de Países de Latinoamérica que Sufren más Ciberataques.* Ranking de Países de Latinoamérica que Sufren más Ciberataques: https://blog.latam.university/blog/ranking-de-paises-de-latinoamerica-que-sufren-mas-ciberataques/#:~:text=Brasil%2C%20M%C3%A9xico%2C%20Colombia%20y%20Argentina,con%203.8%20millones%20de%20ataques.

Lévy, P. (2007). *Cibercultura: informe al Consejo de Europa.* Ciencia, tecnología y sociedad. https://doi.org/K10plus ISBN

Margalef, L., & Arenas, A. (2006). ¿Qué entendemos por innovación Educativa? A propósito del desarrollo curricular. *Perspectiva Educacional, 1*(47), 13-31.

Meritxell, E. (2002). Interactividad e interacción. *Revista Latinoamericana de Tecnología Educativa, Vol. 1*(Núm. 1), 10. https://doi.org/file:///D:/Descargas/Dialnet-InteractividadEInteraccion-1252603.pdf

Ministerio de Defensa Nacional. (2010). *Política de Consolidación Democrática.* Gobierno Nacional de Colombia. https://doi.org/https://pdba.georgetown.edu/Security/citizensecurity/Colombia/politicas/consolidacion.pdf

Ministerio de Defensa Nacional. (2012). *Transformación y futuro de las Fuerzas Armadas.* Gobierno Nacional. https://doi.org/https://www.mindefensa.gov.co/irj/go/km/docs/Mindefensa/Documentos/descargas/estrategia_planeacion/proyeccion/documentos/trasnformacion_futuro_FP.pdf

Ministerio de Defensa Nacional. (2021). *Política Educativa para la Fuerza Pública (PEFuP) «Hacia una educación diferencial.* Capital Humano del Ministerio de Defensa Nacional.

Moya, M., & Vasquez, J. (2010). De la Cultura a la Cibercultura: la mediatización tecnológica en la construcción de conocimiento y en las nuevas formas de sociabilidad. *Cuadernos de Antropología Social* (Núm. 31.), 22. https://doi.org/file:///D:/Descargas/Dialnet-DeLaCulturaALaCibercultura-5236551-1.pdf

Mozo, O., & Ardila, J. (2022). El fenómeno de las ciberamenazas: afectaciones a la ciberseguridad del Ejército nacional de Colombia. *Universidad Militar Nueva Granada, 14* (Núm. 23), 95. https://doi.org/http://doi.org/10.47961/2145194X.333

Osorio, C. (24 de diciembre de 2022). *La precaria ciberseguridad de Colombia*. La precaria ciberseguridad de Colombia. https://elpais.com/america-colombia/2022-12-24/la-precaria-ciberseguridad-de-colombia.html

Pérez, V. (2013). *El ciberespacio: ¿una realidad en construcción?* Universidad San Jorge.

Pesce, L. (2011). *La contribución de la Cibercultura a la educación en línea.* Universidad Católica de Sao Paulo.

Romero, D. (2020). *Descubre cómo funcionan los Ambientes Virtuales de Aprendizaje (AVA) y qué aportan a la educación.* Descubre cómo funcionan los Ambientes Virtuales de Aprendizaje (AVA) y qué aportan a la educación: https://rockcontent.com/es/blog/ambientes-virtuales-de-aprendizaje/

Ron, J. (S.f). *Sobre el concepto de cultura.* Cuadernos Culturales. https://doi.org/https://biblio.flacsoandes.edu.ec/libros/digital/48111.pdf

Roselli, N. (2011). Teoría del aprendizaje colaborativo y la teoría de la representación social: convergencias y posibles articulaciones. *Revista colombiana de Ciencias Sociales, 2*(2), 173-191.

Salcedo, A. (2010). Modelo Pedagógico Multimedial Interactivo en Educación a Distancia (tercera parte). *Revista Academia y Virtualidad, 3* (1), 23. https://doi.org/file:///D:/Descargas/Dialnet-ModeloPedagogicoMultimedialInteractivoEnEducacionA-6981085.pdf

Slavin, R. (2002). *Aprendizaje cooperativo: Teoría, investigación y práctica.* AIQUE.

Tabares, L. (2008). El hipertexto como herramienta educativa: Un recorrido conceptual. *Revista de Educación, Comunicación y Tecnología, Vol. 3*(Núm. 5), 9. https://doi.org/https://repository.upb.edu.co/bitstream/handle/20.500.11912/6550/El%20hipertexto%20como%20herramienta%20educativa.pdf?sequence=1&isAllowed=y

Tabla, E. (2020). *Cibercultura y educación virtual: Fundamentos para una interpretación pedagógica.* Universidad Distrital Francisco José de Caldas. https://doi.org/https://repository.udistrital.edu.co/bitstream/handle/11349/22972/Tesis%20final%20repositorio.pdf?sequence=1&isAllowed=y

uTn. (2021). *La educación virtual en el siglo XXI.* Centro de Formación Pedagógica y Tecnológica Educativa. https://doi.org/http://ftp.campusvirtual.utn.ac.cr/e-learning/La%20educaci%C3%B3n%20virtual%20en%20el%20siglo%20XXI.pdf

Vargas, L. (2019). *Las apps son gratis y sirven para todas las edades, además se encuentran disponibles en los sistemas Android y iOS.* Las apps son gratis y sirven para todas las edades, además se encuentran disponibles en los sistemas Android y iOS: https://www.larepublica.co/especiales/especial-educacion-septiembre-2019/siete-aplicaciones-con-las-que-puede-ensenar-o-aprender-2915330

Vidal, M., Rivera, N., Nolla, N., Morales, I., & Vialart, M. (2016). Aula invertida, nueva estrategia didáctica. *Escuela Nacional de Salud Pública (ENSAP), 30* (3), 11. https://doi.org/http://scielo.sld.cu/pdf/ems/v30n3/ems20316.pdf

Esta página queda intencionalmente en blanco

Revista Ciberespacio, Tecnología e Innovación
Volumen 2, número 4, julio-diciembre 2023 (pp. 169-191)
Bogotá, D.C, Colombia

EDITORIAL ESDEG

Uso de satélites artificiales para la integración de las plataformas estratégicas de las Fuerzas Militares

Use of artificial satellites for the integration of the strategic platforms of the Military Forces

DOI: https://doi.org/10.25062/2955-0270.4812

Darwin Alexis Joya Moreno
Escuela Superior de Guerra "General Rafael Reyes Prieto", Bogotá D. C., Colombia

Resumen

Las plataformas estratégicas de las Fuerzas Militares son activos vitales para la defensa de los intereses de cualquier Estado. Con el pasar de la historia de los conflictos armados regulares, han presentado escenarios donde la coordinación e integración entre las Fuerzas Regulares de un Estado/Nación, se ve afectada por la poca o nula integración que existe entre estas, en cada uno de los diferentes dominios. En el presente trabajo se pretende analizar la experiencia adquirida a nivel nacional, regional y global con el uso de los pico/nano-satélites tipo CUBE-SAT, en los diferentes ámbitos de la ciencia y la tecnología(-tanto civil como militar); identificar sus vulnerabilidades en ciberseguridad y proponer de una manera eficiente y sostenible, el uso de este tipo de tecnologías y poder proponer soluciones en la interoperabilidad y la conjuntez necesaria en caso de un conflicto de carácter internacional.

Palabras Clave: Pico-Satélite; Cube-Sat; Ciberseguridad, Espectro Electromagnético, Plataformas Estratégicas, Integración, Conjuntez, Maniobra.

Abstract

The strategic platforms of the Military Forces are vital assets for the defense of the interests of any State. Over the history of regular armed conflicts, there have been scenarios where the coordination and integration between the Regular Forces of a State/Nation is affected by the little or no integration that exists between them, in each of the different domains. The present work aims to analyze the experience acquired at the national, regional and global level with the use of pico/nano-satellites type CUBE-SAT, in the different areas of science and technology (both civil and military); identify their cybersecurity vulnerabilities and propose, in an efficient and sustainable way, the use of this type of technologies and be able to propose solutions in the interoperability and the necessary togetherness in the event of an international conflict.

Key words: Pico-Satellite; Cube-Sat; Cybersecurity, Electromagnetic Spectrum, Strategic Platforms, Integration, Jointness, Maneuver.

Artículo de reflexión
Recibido: 28 de noviembre de 2023 • **Aceptado:** 20 de diciembre de 2023
Contacto: Darwin Alexis Joya Moreno joyad@esdeg.edu.co

Introducción

Colombia tiene el orgullo de haber sido pionera en América en cultivar la astronomía cuando en el año de 1803 se inaugura el primer observatorio astronómico del continente. Este proyecto, que hizo parte de la real expedición botánica, (dirigido por el español José Celestino Mutis), tuvo como primer director al científico y comerciante payanés Francisco José de Caldas.

> El Observatorio Astronómico Nacional de Colombia es una de las edificaciones científicas y patrimoniales más antiguas de Bogotá, la cual se terminó de construir en 1803 como uno de los frutos de la Real Expedición Botánica del Nuevo Reino de Granada, dirigida por el español José Celestino Mutis (1732–1808) (Ochoa, 2022, p. 2)

Es así como Colombia se hace pionera en el continente en el área de la astronomía, gracias a su privilegiada ubicación *ecuatorial,* la cual le brinda ventajas con sus pares de la región. Desafortunadamente, esta ventaja geoestratégica no ha sido muy bien aprovechada por nuestro país, teniendo en cuenta la amplia brecha digital que aún persiste en las regiones más apartadas del territorio nacional.

El mundo actual gira en torno a la tecnología y a las telecomunicaciones, ya que han facilitado el paso a la globalización, y permiten la interacción en tiempo real sin importar la distancia. Las telecomunicaciones, que en su inicio operaban en un rango limitado, actualmente han generado procesos multidimensionales de transmisión de datos que sin lugar a duda representan un desafío tanto para la ciberseguridad como para la ciberdefensa de los Estados.

Los antecedentes de los proyectos espaciales en Colombia se remontan a la llegada del nuevo milenio, cuando el gobierno colombiano comenzó a mostrar interés por la tecnología espacial-satelital, como una forma estratégica de mejorar las comunicaciones y reducir mencionada *brecha digital.* Mediante la ley 1341 de 2009 se crea la Agencia Nacional del Espectro (ANE), "Como una Unidad Administrativa Especial del orden nacional, adscrita al Ministerio de Tecnologías de la Información y las Comunicaciones" (Departamento Administrativo de la Función Pública , 2011, p. 1), con el fin de regular el uso del espectro electromagnético en Colombia, y promover el desarrollo del sector de las comunicaciones en el país.

Tres años atrás se habría creado la Comisión Colombiana del Espacio (CCE), mediante el decreto ley 2442 de 2006 en su artículo N°2: "Créase la Comisión Colombiana del Espacio, como órgano intersectorial, […] con el fin de orientar la ejecución de la política nacional para el desarrollo y aplicación de las tecnologías espaciales, y coordinar la elaboración de planes, programas y proyectos en este campo" (Departamento Nacional de la Función Pública, 2006, p. 1) entre otros con la misión de diseñar y desarrollar un satélite artificial que tendría por nombre SATCOL-1, proyectado para el año 2011, con esto dar inicio a la adquisición de experiencia y autonomía en el ámbito satelital y desarrollar independencia

en el uso de este tipo de tecnología, ahorrándole al Estado importantes recursos en contratación de servicios satelitales (Fuerza Aeroespacial Colombiana, 2023, p. 1).

Pero la *academia* y más específicamente la Universidad Sergio Arboleda, ante una proeza y contra todo pronóstico el 17 de abril de 2007, le gana la *carrera aeroespacial nacional* al Estado, y logran lanzar el nano-satélite Libertad-1, satélite artificial de tan solo 5kg de masa y 10 cm cúbicos, que tan solo 35 segundos después de su puesta en órbita, emitía su primer paquete de datos. "El 17 de abril de 2007, Colombia tuvo éxito en su proyecto de poner en órbita, el primer artefacto diseñado, programado e implementado por un grupo multidisciplinario de investigadores de la Universidad Sergio Arboleda, denominado *Colombia en órbita*" (Joya, 2020, pág. 3).

> El satélite fue dejado en una órbita geoestacionaria a 693 km de altura, más alto que la de la Estación Espacial Internacional y que el telescopio espacial Hubble. Desde ahí da una vuelta al planeta cada 99 minutos, en promedio, a una velocidad de 7,5 kilómetros por segundo. El objetivo del satélite era obtener telemetría de voltaje, temperatura y corriente desde el espacio. (Morante, 2017, p. 4)

Para la fecha, la secretaria ejecutiva de la CCE era liderada por el Instituto Colombiano Agustín Codazzi, posteriormente pasaría a la Fuerza Aérea Colombiana (ahora Fuerza Aeroespacial Colombiana) FAC y bajo su tutoría, se iniciaría el proyecto FACSAT-1 el cual estaba proyectado inicialmente para el 2014 con la misión de tomar fotografías tanto del planeta, como del territorio nacional, pero varias circunstancias llevaron que este solo pudiera ser puesto en órbita 4 años después de su proyección inicial.

> En el año 2015, se realizaron pruebas de integración al modelo de vuelo, y en el año 2016 se consiguió el apoyo económico por parte de la Fuerza Aérea Colombiana para su lanzamiento, desarrollando las gestiones contractuales durante el 2017 y de esta manera ser puesto en órbita. (Fuerza Aérea Colombiana, 2023, p. 1)

En enero de 2020, una comisión del Centro de Investigación en Tecnologías Aeroespaciales de la FAC (CIATE), realizó la instalación de una antena tipo *Yagui* en la Antártida, con el fin de aprovechar la órbita polar y así recibir del FACSAT-1 una mayor cantidad de información, debido a sus características de órbita espacial.

> La elección del continente antártico como futuro centro para las comunicaciones satelitales de la FAC, está basada en las ventajas que ofrece por su ubicación geoestratégica en relación con la órbita polar que describe el FACSAT-1, por la cual se incrementa la cantidad de *pases diarios* y por consiguiente el tiempo de comunicación efectiva. (Fuerza Aérea Colombiana, 2021, p. 2).

En la actualidad, Colombia se encuentra llevando a cabo varios proyectos de ingeniería en pico y nanosatélites tipo CUBE SAT, tanto por la *academia* (universidades públicas y privadas), así como por el Estado, con el firme propósito de seguir avanzando en este ámbito científico, que le permita explorar y posteriormente explotar un infinito de capacidades que ofrece este tipo de tecnología. Es así como la Universidad Sergio

Arboleda, en coordinación con otras instituciones (público-privadas), está evaluando el proyecto Libertad-2 para que este, a través de un modelo de negocio (venta de servicios) pueda garantizar la autosostenibilidad de este tipo de proyectos a futuro.

Por otra parte, la Universidad Distrital "Francisco José de Caldas" en el marco de su programa CUBE SAT-UD Telemedicina y Telemetría (cuyo objetivo fue desarrollar un taller de diseño crítico, para el ensamble de un pico satélite con misiones de cardiología), actualmente está desarrollando un laboratorio con infraestructura de estación terrena, infraestructura de *sala limpia,* y construcción de cada uno de los módulos que compone un sistema o laboratorio de montaje para desarrollo de pico satélites a nivel nacional. (Espinel & Giraldo, 2018, p. 2)

De igual manera se desarrolló por parte del Gobierno Nacional, el Consejo Nacional de Política Económica y Social (CONPES) N°3983, el cual establece la Política de Desarrollo Espacial, que tiene como objetivo primordial generar las condiciones habilitantes y el entorno institucional para que con una visión de largo plazo el sector espacial contribuya a la productividad, diversificación y sofisticación del aparato productivo del país (Departamento Nacional de Planeación, 2020).

Como tesis, se plantea que Colombia es un país tradicionalmente consumidor de tecnología satelital y teniendo en cuenta lo expuesto anteriormente, se evidencia que el entorno nacional se encuentra en una etapa de maduración en la cual, varios sectores de investigación se encuentran altamente interesados en el desarrollo de este tipo de tecnología y en general en el campo aeroespacial. Se puede evidenciar que ya existen unas bases sólidas para que el sector defensa y en especial en la Fuerza Pública, que, de la mano con la academia, pueden llegar a impulsar el desarrollo de diferentes proyectos que brinden no solo un avance en la investigación, si no que a mediano y largo plazo le generen al Estado, un retorno a la inversión que le brinde sostenibilidad a este tipo de proyectos.

Se requiere por parte del gobierno nacional voluntad política, con el fin que se destine los recursos necesarios a instituciones como el Instituto Geográfico Agustín Codazzi, Colciencias -actualmente Minciencias- (entre otros) y que, bajo la lupa y dirección de la CCE, se fortalezca este tipo de programas y que esto a su vez, estimule al estudiantado universitario y personal profesional idóneo en la materia, desarrollar proyectos concretos que generen en un futuro un avance tecnológico y un retorno a la inversión con venta de servicios a la región andina y del caribe.

En el marco de la conjuntes, vale la pena resaltar que las plataformas estratégicas de las Fuerzas Militares, como activos de alto valor para el Estado, (al ser estos equipos considerados altamente disuasivos), demanda hondar todos esfuerzos que se requieran con el fin de integrarlos activa y eficazmente.

De igual manera, y aterrizando este trabajo a su objetivo principal, determinar si es viable implementar la tecnología satelital, para integrar las capacidades conjuntas y a su vez garantizar una ciberseguridad robusta en el desarrollo de las operaciones militares, blindando el sistema de un posible escenario negativo (espionaje) que, con la llegada de diferentes tipos de amenazas, puedan afectarla.

Teniendo en cuenta lo anterior, ¿De qué manera se puede promover el uso de los satélites artificiales para la integración de las plataformas estratégicas de las Fuerzas Militares en un posible escenario de conflicto internacional?

Metodología

Como es de amplio conocimiento, la Fuerza Pública y la academia, han dado pequeños, pero importantes pasos en el desarrollo de proyectos satelitales en el ámbito científico, con el fin de ir cerrando la brecha que existe entre el mito de que esta tecnología es de uso exclusivo de las grandes potencias y la realidad que en la actualidad es otra.

El pasado 15 de abril de 2023, fue puesto en órbita *Chiribiquete,* el tercer satélite colombiano, esta vez más con fines más operacionales que científicos, lo que demuestra que esta tecnología, aunque aún no es lo suficientemente económica, ya empieza a ser más asequible para países en vía de desarrollo, como el nuestro.

Como se mencionó anteriormente, Colombia logró llevar a cabo con éxito otros dos proyectos que han acumulado experiencia en este tipo de tecnología, y han brindado información científica valiosa para nuestro país.

Por lo anterior, para el presente trabajo se planteó usar una metodología cualitativa mediante la descripción de experiencias a nivel científico e investigativo, empleando para esto entrevistas a personal destacado en los proyectos nacionales llevados a cabo, así como documentos científicos de fuentes abiertas y material audiovisual del ámbito global. Estas entrevistas fueron realizadas a personal destacado en los proyectos satelitales (tipo CUBE-SAT) desarrollados en el país.

De igual manera, se asistió a los *seminarios de Fuerza* brindados por la Escuela Superior de Guerra, con el fin de enriquecer el conocimiento en dos temas específicos (plataformas estratégicas de la Fuerza Pública, y proyectos satelitales llevados a cabo por la FAC) para que, a través de la formulación de preguntas, generen conocimiento dentro del constructivismo que caracteriza a la Escuela Superior de Guerra, además de despertar el interés y la conciencia en la importancia de integrar estas plataformas, por parte de los asistentes. De igual manera, todo este conocimiento se afianzó con las Prácticas Geoestrategias Nacionales, donde se generó conciencia sobre la gran falencia en la integración efectiva de las plataformas y se pudo evidenciar posibles soluciones

a esta problemática planteada. Todo lo anterior se afianzó en la investigación activa en fuentes académicas abiertas con el fin de consolidar y dar una postura más sólida al trabajo de investigación.

Tecnología espacial - Nano Satélites tipo Cube-Sat

Small-Sat

Para poder entrar en materia tenemos que entender algunas definiciones propias de este tipo de tecnología. El anglicismo *smallsat* (contracción de ***small satellite***) o satélite pequeño, hace referencia a un satélite de tamaño menor y bajo peso (masa), por lo general menor de 500 kilogramos. Si bien en esta categoría pueden denominarse *pequeños,* se pueden catalogar en función de su peso. Los satélites se construyen pequeños para reducir el alto costo económico de su lanzamiento y puesta en órbita, además del costo de su diseño y construcción (Alen Space, 2022, pág. 2)

Los Small-Sat, en grandes cantidades, pueden ser más útiles para algunos designios que los de mayor tamaño, (recopilación de datos científicos, climatológicos, aerofotografías y radioenlaces, entre otros). Los retos en el diseño y construcción de este tipo de satélites incluyen la corta capacidad de almacenar suficiente energía (ya que requieren de baterías muy pequeñas) o contar con poco espacio para incluir un sistema de propulsión (para su mantenimiento en órbita).

Los satélites artificiales se subclasifican de acuerdo por su prefijo de la siguiente manera:

Clasificación de los satélites por su tamaño:

Tabla 1. Tamaño de los satélites

Denominación del grupo	Masa (kg)
Satélite grande	> 1000
Satélite mediano	500 a 1000
Minisatélite	100 a 500
Microsatélite	10 a 100
Nanosatélite	1 a 10
Picosatélite	0,1 a 1
Femtosatélite	<0.1

Fuente: Agencia Espacial Mexicana (2016)

Nano Satélite

El término *nanosatélite* o *nanosat* se aplica a un satélite artificial con una masa entre 1 a 10 kg. (Ortiz, 2021, p. 2). "Los diseños propuestos de este tipo de satélites pueden lanzarse individualmente, o pueden tener múltiples nanosatélites trabajando juntos o en formación, en cuyo caso, a veces se puede aplicar el término *enjambre de satélites* o *nave espacial fraccionada*" (SpaceWorks Enterprises, Inc, 2014, p. 5). Algunos diseños requieren de un satélite principal más grande para su interacción con la estación terrena o con otros Smallsat. Para los satélites individuales basta con una estación terrena para la recepción de datos, toda vez que la órbita de este tipo de tecnología no supera los 1.000 km de altura (en la mayoría de los casos). Más de 1.300 nanosatélites se han puesto en marcha a partir de enero de 2020. (SpaceWorks Enterprises, Inc, 2014, p. 7)

Pico Satélite

El término *picosatélite o picosat* usualmente se aplica a satélites con una masa (peso) entre 0,1 a 1 kg, aunque suele usarse para cualquiera de estos equipos que su masa esté por debajo de 1 kg.

> Mientras que la Armada y la Fuerza Aérea se han centrado en el potencial de los microsatélites, la opinión del Ejército de EE. UU. es que cuanto más pequeño, mejor. (Defense Industry Daily staff, 2011, p. 3)

El diseño CubeSat, de aproximadamente 1 kg, es un ejemplo de un gran picosatélite (o nanosat mínimo)

Cube-Sat

Por otro lado, "el termino Cube-Sat es un estándar de diseño de nano-satélites, cuya estructura es escalable en cubos de 10 cm de arista y masa inferior a 1,33 kg. Esta unidad es conocida como 1U". (California State Polytechnic University, 2012, p. 9)

Las especificaciones de los diseños tipo CubeSat buscan cumplir varios objetivos específicos.

> La simplificación de la estructura del satélite permite el diseño y manufactura de un satélite funcional de bajo costo. La encapsulación del lanzador y la interfaz de la carga útil reducen problemas burocráticos y prohibiciones, que se daban durante el acuerdo del lanzador y el desarrollador. (Romero, 2021, p. 11)

Gracias a este tipo de tecnología, muchas universidades y colegios en el mundo han podido desarrollar proyectos espaciales, con un bajo costo, logrando avances significativos para la ciencia, lo cual ha impulsado de manera exponencial el conocimiento para el ámbito académico, generando un mayor interés a las nuevas generaciones.

El término *CubeSat* es usado para denotar nanosatélites que se adhieren a los estándares descritos en el documento de especificaciones de satélites artificiales tipo CubeSats. (David, 2004, p. 3)

La universidad de California (Cal Poly) en aras de crear un estándar para la comunidad científica, publicó el estándar en un esfuerzo liderado por el profesor Robert Twiggs, en conjunto con profesor Jordi Puig-Suari.

Más recientemente, el profesor Bob Twiggs, del Departamento de Aeronáutica y Astronáutica de la universidad de Stanford, actualmente miembro de la facultad de Ciencia Espacial en la universidad Morehead State, de Kentucky, ha contribuido intensamente a la comunidad CubeSat.

> Sus esfuerzos se han enfocado en CubeSats de instituciones educativas. Estas especificaciones no aplican a otros nanosatélites de forma cúbica, como el *MEPSI,* de la NASA, poco más grande que un CubeSat. (Verenzuela, 2022, p. 3)

Pico/Nano-Satélites tipo Cub-Sat puestos en órbita por las potencias espaciales suramericanas.

Antes de hablar de las misiones espaciales nacionales, debemos hacer una breve descripción de los proyectos tipo Cub-Sat en los países referentes de la materia en la región, como lo son Argentina y Brasil, ya que estos han servido como inspiración para los proyectos locales, aún más que los mismos proyectos de las grandes potencias.

La Carrera Espacial en Suramérica

Argentina y Brasil, son las potencias y pioneros en Suramérica en investigación e innovación espacial. En el caso de Argentina, este país ya ha puesto varios satélites en órbita, obteniendo con esto una amplia experiencia con este tipo de tecnología.

La carrera espacial en este país comienza en la década de los 90 con el satélite Lusat I, el primero de su especie de fabricación argentina, que fue un proyecto impulsado por un grupo de radioaficionados. Después de 20 años en órbita, con sus baterías totalmente descargadas, (pero debido a sus condiciones de bajo peso) aún continúa orbitando.

> En 1996 siguieron los satélites profesionales, en agosto el MU-SAT, conocido también como *Víctor I,* empleó un equipo de técnicos del misil argentino Cóndor II; y en noviembre la comisión estatal CONAE inició, con el SAC B (Satélites de Aplicaciones Científicas), su serie de satélites científicos como parte de un Plan Espacial Nacional, *Argentina en el Espacio,* implementado por la Comisión Nacional de Actividades Espaciales (CONAE). También el satélite, el Pehuensat-1, diseñado y elaborado por la Universidad Nacional del Comahue y lanzado en enero de 2007, desde la India. (Agencia TAO, 2020, p. 1)

Los proyectos espaciales del sector privado argentino comenzaron en 2013, con el lanzamiento del nanosatélite tipo Cube-Sat ***Capitán Beto*** por parte de la compañía Satellogic. La siguiente en hacer un lanzamiento fue DIY Satellite, con el PocketQube DIY1 Arduiqube, en 2021.

> El DIY-1 es el primer pocketQube desarrollado en Argentina. Un demostrador tecnológico construido con fines principalmente educativos que orbitará el planeta a una altura aproximada de 600 km. (Argentina En El Espacio , 2021, p. 3)

El 16 de octubre de 2014, en el cohete Ariane 5, desde la Guayana Francesa, se realizó el lanzamiento del primer satélite geoestacionario, primero fabricado totalmente en el país, y segundo satélite de comunicaciones de Latinoamérica. Un año después, (el 30 de septiembre de 2015), se realizó con éxito el lanzamiento del ARSAT-2, con el cual, Argentina obtuvo llegada satelital a todo el continente y a toda su plataforma continental (Agencia TAO , 2020, p. 2).

El caso Brasil

Brasil, otro de los referentes en Suramérica, tiene una robusta carrera espacial liderada en su mayoría por la Agencia Espacial Brasilera (AEB), quienes desde 1993 han logrado poner con éxito más de 30 satélites (de diferente tipología y misión) de los cuales solo se relacionará los pico/nanosatélites tipo Cube-Sat, de acuerdo al siguiente cuadro, así:

Tabla 2. Proyectos satelitales de Brasil

Satélite	Año (Lanzamiento)	Vehículo	Observaciones
SACI-1	1999	Larga Marcha 4B	Plataforma multimisión, falla en el lanzamiento
SACI-2	1999	VLS-1 V2	Plataforma multimisión, falla en el lanzamiento
NanoSatC-Br 1	2014	DNEPR	Monitoreo de magnetosfera, medición de campo magnético sobre Brasil
NanoSatC-Br 2	2021	Soyuz 2	Estudio de la región de anomalías magnéticas de América del Sur
AESP 14	2021	EEI	Cubesat investigación científica
PION BR1	2022	SpaceX	PION Labs
Alfa Cruz	2022	Falcon 9	UNB/AEB
SPORT	2022	SpaceX	ITA/NASA/INPE - clima espacial orbital

Fuente: Agência Espacial Brasileira (2022).

Es importante destacar que la tecnología Cub-Sat ha permitido que países con menor capacidad financiera y tecnológica puedan acceder al espacio y desarrollar capacidades espaciales propias, como lo son Ecuador, Perú, Venezuela y por supuesto Colombia, entre otros.

El desarrollo de tecnología satelital es un proceso complejo que requiere de una inversión significativa en investigación y desarrollo, así como de la colaboración de múltiples entidades, tanto del sector privado como estatales.

Es posible que Brasil, debido a sus tempranos inicios en este tipo de tecnología, haya decidido enfocar sus esfuerzos en el desarrollo de satélites de mayor tamaño y complejidad.

> Aunque si ha desarrollado y lanzado satélites de pequeño tamaño para misiones de observación de la Tierra, como el Amazonia-1 lanzado en 2021, que si bien no son satélites tipo Cub-Sat, utilizan tecnología similar en cuanto a tamaño, configuración y costo. (Actualidad Aeroespacial, 2020, p. 3).

Los principales objetivos de este satélite son la observación terrestre, la lucha contra la deforestación ilegal, la vigilancia del mar, entre otras. Se programa una serie de satélites con al menos tres equipos de este tipo.

> Aunque no es el primer satélite brasilero, es el primero diseñado, producido y probado íntegramente en el país, siendo el tercer satélite brasileño de teledetección actualmente en operación con CBERS-4 y CBERS-4A. (Actualidad Aeroespacial, 2020, p. 2)

En cuanto a la razón por la cual Brasil no ha sido referente de tecnología satelital tipo Cub-Sat, es posible que se deba a que este país cuenta con una industria aeroespacial más robusta que los demás países de la región y en sus inicios, los proyectos satelitales son de generaciones anteriores, lo que le permitió desarrollar equipos de mayor dimensión y complejidad. La tecnología tipo CubeSat es de desarrollo más reciente (a nivel científico y académico principalmente). Es por esta razón que satélites como el Geoestacionario de Defensa y Comunicaciones Estratégicas (SGDC), cuenta con una masa de más de 5 toneladas y fue construido por la empresa brasileña *Visiona Tecnología Espacial* en colaboración con la compañía francesa *Thales Alenia Space*.

El SGDC se compone de una serie de Satélites (todos de fabricación Brasileña), operados por *TeleBras* en coordinación con la *Fuerza Aérea Brasileña* por intermedio de su *Centro de Operaciones Espaciales.* Este satélite de la serie (SGDC/1) fue lanzado desde el puerto espacial de Korou por un cohete Ariane y aún está operativo, el segundo está planeado y la intención del gobierno brasileño es tener una flota de mínimo tres satélites, lanzada en un intervalo aproximadamente de cinco años entre cada uno de estos (Fuerza Aérea del Perú, 2017, p. 2).

Falencias de integración en las plataformas estratégicas de las Fuerzas Militares

Para entender estas falencias primero tenemos que definir algunos conceptos, como lo son:

Plataformas Estratégicas

Las plataformas militares estratégicas son sistemas de guerra de alto nivel tecnológico, que son usados en el ámbito militar para fines estratégicos. Estos equipos están diseñados para tener un impacto disuasivo significativo en el teatro de la guerra y para influir en el equilibrio de poder en posible un conflicto armado. Estos constituyen un amplio espectro de sistemas y tecnologías avanzadas. Algunos ejemplos comunes incluyen:

1. **Armamento nuclear:** hace referencia a los sistemas de armas nucleares que tienen como principio físico de acción y reacción la fisión y fusión nuclear, tales como lo son los misiles balísticos intercontinentales, los cuales son lanzados desde tierra firme (normalmente de carácter subterráneo), los SLBM (submarine launched ballistic missile), más conocidos como *submarinos nucleares,* que tienen la capacidad de portar y lanzar armas nucleares de gran alcance y desde zonas avanzadas estratégicas, así como los bombarderos de largo alcance, con capacidad de lanzar misiles de crucero tanto subsónicos, como supersónicos. (Britannica , 2023, p. 2)
2. **Misiles balísticos:** Estos son misiles de largo alcance que pueden transportar cargas útiles convencionales o nucleares y que pueden ser utilizados para atacar objetivos estratégicos a grandes distancias, se caracterizan porque una parte de su trayectoria está definida por la balística que puede ser ICBM (Intercontinental Ballistic Missile) IRBM (Intermediate Range Ballistic Missile) y los SRBM (Short Range Ballistic Missile) (Britannica , 2023, p. 3).
3. **Sistemas de defensa antimisiles:** Son sistemas de defensa con capacidad para detectar misiles y cohetes dirigidos hacia un territorio, para destruirlos por impacto directo en la atmósfera antes de que alcancen su objetivo (El Mundo España, 2022, pág. 1). Estos sistemas se despliegan para proteger áreas estratégicas, como ciudades o bases militares, de ataques con misiles.
4. **Aviones de combate estratégicos:** Son aviones con capacidad de vuelo subsónico, supersónico o en algunos casos hipersónico (velocidad superior a MACH 5), de alto rendimiento, diseñados para acorde a su configuración (sus prestaciones, armamento y equipamiento) entrar en el espacio aéreo enemigo y tomar el control de este. (Ecu Red, 2022, p. 2)
5. **Sistemas de inteligencia y vigilancia:** Son sistemas y plataformas especializadas que recopilan información y datos de inteligencia para respaldar la toma de

decisiones estratégicas, monitorear actividades enemigas y detectar amenazas potenciales. Entre otras podemos destacar algunos satélites de vigilancia y aviones *plataforma* (Cortés, 2019, p. 5).

Estos equipos militares estratégicos son tecnológicamente sofisticados y requieren una inversión significativa en términos de desarrollo, adquisición y mantenimiento. Son esenciales para la capacidad de un estado para proyectar poderío militar, disuadir amenazas y proteger sus intereses estratégicos tanto en el ámbito nacional como internacional.

El Ejército Nacional

El Ejército Nacional de Colombia (EJC), cuenta con varios tipos de vehículos blindados de infantería y caballería para sus operaciones militares (Cepeda, 2023, p. 3). Algunos de los vehículos más destacados se incluyen:

1. **Blindados de transporte de personal:** Entre ellos se encuentran vehículos como el EE-11 Urutú y el GLDS LAV III, que se utilizan para transporte de tropa (infantería mecanizada).
2. **Vehículos de combate de infantería:** El Ejército de Colombia ha empleado vehículos como el M113-A2, un blindado que puede adaptarse para transportar tropa o montar ametralladoras y cañones para apoyo de fuegos.
3. **Vehículos de reconocimiento:** Para misiones de reconocimiento, se utilizan vehículos como el Humvee y otros modelos especializados con capacidades de vigilancia y comunicación.
4. **Artillería autopropulsada:** El Ejército de Colombia ha confirmado la compra de 18 piezas del sistema Obús autopropulsado ATMOS, que proporciona apoyo de fuego a las unidades en el área de operaciones (Infodefensa , 2023, p. 3).
5. **Vehículos blindados de combate:** COTECMAR ha ganado una amplia experiencia en el ensamblaje y posterior fabricación del vehículo BTR-80 y el BTR-82ª Caribe, para el Ejército Nacional y la Infantería de Marina. También se cuenta con los EE-9 *Cascabel* el cual es empleado para apoyo de fuegos, pero su principal misión es la maniobra de caballería liviana.
6. **La aviación del Ejército,** cuenta con una basta flota de aeronaves, entre los que se destacan el Sikorski UH60 y S70i *Blackhawk,* el Kazam MI-17 en sus versiones 1V-MD y V5, así como las aeronaves de la casa BELL, como lo son el UH1N *Cazador* y el UH1H Huey II *Rapaz,* así como una flota de aviones que cumplen misiones de transporte de carga/personal, reconocimiento, evacuaciones aeromédicas, plataformas de inteligencia, entre otros.

La Armada Nacional

La Armada de Colombia cuenta con varios tipos de buques que le permiten cumplir con su misión de protección de la soberanía y la lucha contra el narcotráfico, tanto como guardacostas, así como en altamar. "Actualmente está conformada por 86 buques de mar y de río, tripulados por 2026 hombres y mujeres". (Armada Nacional de Colombia, 2023, pág. 5) Algunas de las plataformas estratégicas más destacadas son:

1. **Fragatas Misileras:** Las fragatas misileras son buques de guerra generalmente diseñados para operar en aguas oceánicas (altamar) y realizar misiones de defensa y vigilancia. Colombia cuenta en servicio con fragatas misileras tipo *FS 1500* construidas en Alemania, entre las que se destacan el ARC Caldas, y el ARC Independiente, reconocidas por el litigio de Coquivacoa en 1987.
2. **Corbetas Misileras:** Las corbetas PCC778 de la clase POHANG son embarcaciones más pequeñas que las fragatas y se utilizan para misiones multipropósito, tanto guardacostas como misiones de vigilancia y defensa de la soberanía.
3. **Patrulleras:** Las patrulleras son embarcaciones livianas, veloces y versátiles que son usadas para patrullar áreas marítimas cercanas a la costa (operaciones guardacostas), así como fluviales y llevar a cabo operaciones de interdicción y control de tráfico marítimo ilícito. Colombia cuenta con varias clases de patrulleras, incluidas algunas fabricadas a nivel nacional por la empresa del Grupo Empresarial del Sector Defensa GESED-COTECMAR (Corporación de Ciencia y Tecnología para el Desarrollo de la Industria Naval Marítima y Fluvial).
4. **Buques de Desembarco Anfibio:** Estos buques se utilizan para el transporte de tropa (infantería de Marina), equipo y suministros a áreas costeras y en operaciones anfibias. Colombia a través de COTECMAR está desarrollando este tipo de embarcaciones.
5. **Buques científicos y de apoyo logístico:** Estos buques brindan apoyo logístico a la flota y pueden llevar a cabo funciones como reabastecimiento en el mar, transporte de suministros y reparaciones en alta mar. De igual manera COTECMAR logró la construcción del buque *ARC BOLÍVAR,* con el objetivo de cumplir más misiones en la Antártida y así lograr un desarrollo exponencial de su capacidad científica en esta zona estratégica global.
6. **La flota de la aviación naval,** tiene una diversidad de aeronaves que le permiten cumplir misiones SAR (búsqueda y rescate por sus siglas en ingles), operaciones de interdicción, tanto en altamar como guardacostas, entre otros.

La Fuerza Aeroespacial Colombiana

La Fuerza Aeroespacial Colombiana cuenta con aviones de superioridad aérea, entre los cuales podemos destacar los ya veteranos IAI K-FIR en su versión C10 y C12, los cuales

como es de conocimiento público, ya cumplieron su tiempo de servicio. "Las primeras aeronaves llegaron al país en 1989, desde ese momento han sido protagonistas de la historia de Colombia, salvaguardando la soberanía y participando en diferentes operaciones" (Fuerza Aeroespacial Colombiana, 2022, p. 5). Sin embargo, mientras se toma una decisión política para su remplazo por parte del Ejecutivo, en la actualidad es la plataforma estratégica con la que Colombia cuenta para su protección, en caso de una amenaza o incursión externa.

De igual manera, esta Fuerza cuenta con otros tipos de aeronaves (utilitarias) que generan las condiciones estratégicas necesarias para brindar una *disuasión externa,* tal como lo son los Embraer EMB 312 *Tucano* y los EMB 314 *Super Tucano,* los cuales, por sus características operacionales, son tácticamente mucho más versátiles, ya que en caso de así requerirse, tienen la capacidad de aterrizar y decolar en una pista mucho más corta, teniendo en cuenta que en un caso de conflicto internacional, Colombia debe activar todo su *poder aéreo* incluyendo la aviación civil.

A lo anterior se suma la ventaja estratégica con la que cuenta esta flota, al tener un sostenimiento logístico más reducido en tiempo y costos (comparado con el de la flota de superioridad aérea), lo que conlleva garantizar un nivel más alto de alistamiento en línea de vuelo para las operaciones militares conjuntas.

Las comunicaciones militares

Las comunicaciones, así como los más grandes avances tecnológicos en la historia de la humanidad, han evolucionado a medida de su necesidad. En la antigüedad, los ejércitos y las marinas de guerra se comunicaban con un código de banderas de colores, que se cifraba previamente para indicar cuando una unidad debía entrar en batalla o simplemente cuando retirarse del campo de combate (Jornet, 2023, pág. 7).

> A Cleóxenes o Demócrito se le adjudica la creación de un sistema usado en el siglo II a.C. por los ejércitos de Filipo, rey de Macedonia; y posteriormente por cartagineses y romanos. Se trata de dividir el alfabeto en cinco filas y cinco columnas […] el emisor elevará a la izquierda el número de antorchas que representan la columna, y a su derecha el número que representan la fila. (Velazco, 2017, p. 18)

Posteriormente, en Francia se adopta un código cifrado por medio de luces de colores, emitidos desde faros en tierra, (podría llamarse a este sistema la primera fibra óptica) que combinados en intervalos de tiempo podrían enviar una infinidad de mensajes que tardarían mucho tiempo en llegar mediante un mensajero a caballo (Jornet, 2023, p. 9).

Con la llegada del telégrafo (tanto óptico como eléctrico), comienzan las Naciones y sus Ejércitos a incurrir en los medios tecnológicos para suprimir los mensajes escritos, pero al siempre existir la necesidad imperiosa por parte del bando contrario, de descifrar los mensajes de sus oponentes, había que innovar para estar en la vanguardia de la seguridad en las comunicaciones.

> Entre 1753, primera fecha de referencia en la historia de la telegrafía eléctrica, y 1837, año donde se realizan las primeras patentes de telégrafos eléctricos, hubo más de cuarenta sistemas telegráficos. […] Serán dos sistemas los que se consoliden, uno en Inglaterra: el de Cooke y Wheatstone; y otro en Estados Unidos, el de Morse. (Velazco, 2017, p. 23)

Con el telégrafo y posteriormente la invención del teléfono por parte de Alexander Graham Bell, ya se podía comunicar a distancias considerables, incluso más allá de las costas (gracias a los cables submarinos punto a punto), pero su gran limitante era precisamente esta, los puntos terminales a los que llegaban estos cables. Aún quedaban incomunicados los barcos, tresnes, guarniciones militares y zonas rurales. Superar estas limitantes comenzó a ser posible gracias a una cadena de inventos.

> Lograr un medio, que sin necesidad de hilos ni postes permitiera comunicarse a distancia, pudo ser una idea o más bien casi un sueño. Un sueño que se hizo realidad cuando, en código Morse, los radiogramas cruzaron el espacio. (Velazco, 2017, p. 36)

Por esto es por lo que la radio, en sus inicios, fue llamada *Telegrafía sin Hilos*. "Los estudios de Maxwell y su formulación matemática de los efectos eléctricos y magnéticos serán el origen de la comunicación inalámbrica" (Velazco, 2017, p. 40)

Posteriormente, en 1895, Guglielmo Marconi un científico eléctrico italiano, recopila los conocimientos plasmados por Maxwel, Hertz, Branly, y por supuesto la antena de Popov, para desarrollar el gran invento que revolucionaria el mundo de las comunicaciones en el siglo XX.

La radio fue usada en muchas de las grandes y pequeñas guerras en el siglo XX, siendo este factor dominante en la inclinación de la balanza para las grandes potencias ya industrializadas, esto sumado a la segunda revolución industrial que les permitió a las mismas potencias lograr potenciar mucho más su maquinaria de guerra, que cada vez obtenía un mayor alcance.

Lograr dar a los mandos militares ese control *inmediato* mediante las comunicaciones de radio, era un factor determinante en la conducción de la guerra. Pero siempre seguía la sombra del espionaje, ya que cada día las nuevas tecnologías eran alcanzadas y se podía cifrar fácilmente estos mensajes para tomar medidas inmediatas que contrarrestaran un ataque, o debilitaran una defensa bien planeada.

Cuando los Estados Unidos entra en la segunda guerra mundial, usan los indios navajos para codificar y descifrar mensajes de radio, aprovechando su lengua nativa. Esto, debido a que el espionaje hecho por el enemigo, no le permitía surtir resultados en el frente de batalla.

> El mayor Howard Connor, de la División Quinta de la Marina declaró: "Si no hubiera sido por los navajos, los infantes de marines nunca se hubieran apoderado de Iwo Jima". (BBC Mundo, 2014, p. 2)

Esto genero una necesidad, ¿seguridad en las comunicaciones militares? La respuesta es obvia, se requería un medio de encriptación que le garantizara a los aliados poder enviar y recibir mensajes de voz *cifrados* que no fueran víctimas del espionaje enemigo, y de ahí se empiezan a desarrollar radios militares con *seguridad de voz.*

En la actualidad la Fuerza Pública, cuenta con una serie de radios de comunicaciones que le garantiza *interna e independientemente* a cada Fuerza contar un código de cifrado de voz, en el cual con el devenir del tiempo se ha venido adquiriendo de manera secuencial y periódica, pero en caso de un conflicto internacional, ¿podemos integrar en tiempo real las Fuerzas Militares?

La integración de las comunicaciones entre las FFMM.

En el marco expuesto es complejo analizar y aceptar que, en caso de un conflicto internacional, no hay una forma segura de integrar nuestras capacidades estratégicas como Fuerzas Militares, ya que individualmente cada Fuerza cuenta con una capacidad instalada, que por lógica deducción, todas ellas brindan un código de cifrado (encriptación) totalmente diferente y no compatibles entre sí. Lo anterior debido a que cada empresa cuenta con un desarrollo tecnológico distinto e independiente.

Así las cosas, vemos en el caso del EJC sistemas como el Tadiran o el Harris, en la ARC sistemas como el Rohde and Schwarz y en la FAC Bendixking o Colins. Para el caso del interior contamos con una red Trunking, también conocido como acceso troncalizado, que consiste en un sistema de radio bidireccional administrado por un controlador, (una computadora industrial capaz de gestionar diferentes canales) que permite a sus terminales *compartir* múltiples frecuencias de comunicación. Sin embargo, esta red requiere de una serie de repetidoras, las cuales son imposibles de instalar en regiones como la Orinoquia, la Amazonia, en la alta Guajira y nuestra zona marítima, principalmente en el Caribe, debido a la ausencia de obstáculos topográficos en estas áreas, y que, para la hipótesis de un conflicto internacional, son teatros de operaciones altamente expuestos y vulnerables para este ámbito.

¿Qué pasaría en caso de que en un conflicto internacional se requiera un sistema integrado de comunicación que le permita al mando garantizar unas comunicaciones cifradas, seguras y en tiempo real? ¿Qué pasaría si por urgencia extrema las Fuerzas Militares requieren coordinar sus operaciones mediante sistemas de comunicación en modo claro? ¿Cuál sería el costo para las operaciones militares? ¿Cuál sería el costo en vidas y material si el enemigo accede fácilmente a nuestras comunicaciones?

Analizando potencias aliadas, el Comando de Defensa Espacial y de Misiles del Ejército de los Estados Unidos (USASMDC/ARSTRAT) ha lanzado un programa para desarrollar nanosatélites de comunicación.

> Los nanosatélites están diseñados para servir como nodos para la comunicación en el campo de batalla. (Defense Industry Daily staff, 2011, p. 3)

El programa Space and Missile Defense Command: Operational Nanosatellite Effect (SMDC-ONE) tiene planeado desarrollar una cantidad considerable de este tipo de satélites (gracias a su bajo costo) y ponerlos en órbita baja para brindar una capacidad de comunicaciones tácticas/estratégicas según sea el escenario y la necesidad.

Empleo de satélites artificiales para la integración de las plataformas estratégicas

Como se mencionó al inicio del presente trabajo, la Fuerza Aeroespacial Colombiana, viene desarrollando interesantes avances en el ámbito satelital, y es precisamente esta fortaleza que podría llegar a explotarse teniendo en cuenta el potencial desarrollo en comunicaciones que genera esta área de la tecnología.

Teniendo en cuenta que actualmente hay una brecha en seguridad de las comunicaciones militares, ya que como se mencionó, en la hipótesis de un conflicto bélico, necesitaríamos recurrir al *modo claro* en VHF (Very Hight Frequency), para poder integrar no solo las plataformas estratégicas, sino los demás actores incluido el mando superior con sus unidades conjuntas, al no existir un estándar de equipos que me asegure la integración de estas, lo que convertiría nuestros radios militares en simples sistemas de comunicación civil sin ningún tipo de seguridad de voz.

Ciberseguridad en las comunicaciones

Teniendo en cuenta la problemática presente en la integración de los sistemas de comunicación entre las Fuerzas, y esto sumado a que en caso de un conflicto armado internacional, las plataformas estratégicas se verían en la necesidad de integrar sus comunicaciones por sistema VHF, el Ministerio de Defensa Nacional (MDN) por intermedio del Comando General de las Fuerzas Militares (CGFM), debe garantizar que estas no sean sujetas a una posible y muy viable interceptación por parte del enemigo, lo cual generaría serios fracasos operacionales que no solo tendrían costos económicos sino también en vidas.

Por lo anterior, se debe de garantizar un sistema robusto que genere un código de encriptación entre las diferentes plataformas estratégicas que no pueda ser vulnerado por la inteligencia enemiga.

La Armada Nacional, por intermedio de COTECMAR, ha iniciado un programa denominado Sistema de Enlace de Datos Tácticos (TDL-Datalink) Link-Co.

> COTECMAR desarrolló un sistema de Enlace de Datos Tácticos *LINK-CO,* el cual tiene la capacidad de integrar diferentes sensores de navegación y vigilancia de la unidad con el fin de conformar el escenario táctico, el cual puede ser transmitido a la red táctica utilizando radios de la familia Rohde & Schwarz - R&S, Tadiran, Harris, Collins, comunicaciones IP y enlace satelital. Permitiendo de esta manera a todas las unidades que participan en la Red Táctica, compartir un escenario táctico común (Cotecmar, 2021, p. 3)

Figura 1. Grafica Unidad de Distribución de Datos

Fuente: COTECMAR (2021)

En la gráfica anterior podemos detallar como el sistema data link 32 integra información de los diferentes sistemas de las plataformas tanto de la flota de superficie como la submarinista, lo que permite a los comandantes a bordo tener información de sus capacidades marítimas en tiempo real.

Pero ¿qué sucede en el escenario cuando tengamos que integrar otras plataformas al teatro de operaciones o peor aún, en el teatro de la guerra?

Este tipo de tecnología le está apuntando a integrar información en tiempo real, pero lo que se pretende no es limitarnos a transmisión de datos ya que, si bien esta información es relevante para el ambiente operacional, no es suficiente para integrar y sobre todo para coordinar la maniobra entre las plataformas estratégicas.

Se debe tener en cuenta que, para coordinar un apoyo de fuegos o una maniobra conjunta, se debe de garantizar la comunicación voz a voz entre el piloto de la aeronave, con el comandante de la fragata misilera, este a su vez con los otros posibles actores de la maniobra, como el comandante de misión en los diferentes dominios, incluso aun con el radioperador del blindado que se encuentra en tierra.

El uso de satélites artificiales en Ciberseguridad.

Con todos estos avances tecnológicos, seguimos teniendo la misma limitante, ya que no se puede integrar en tiempo real las diferentes plataformas estratégicas para coordinar la maniobra voz a voz. Ahora bien ¿Por qué no aprovechar los avances en las capacidades desarrolladas por la ARC (COTECMAR) y la FAC (CIATE) para desarrollar un código de encriptación y así poder aprovechar la capacidad instalada en comunicaciones militares?

En el mundo de la tecnología todo es posible, y teniendo en cuenta que contamos con laboratorios dedicados a este tipo de desarrollos tecnológicos, debemos orientar y coordinar sus capacidades para analizar esta problemática que, a todas vistas, parte de un solo principio, la ausencia de conjuntas entre las Fuerzas Militares.

Conclusiones

Está plenamente identificada una falencia altamente potencial, porque si bien, Colombia no se encuentra inmersa en un conflicto internacional, también hay que tener presente que existe un peligro inminente, ya que existe un tramo de frontera importante aún no definido con algunos países vecinos, de los cuales, algunos han optado posturas bélicas, con antecedentes no muy antiguos en este sentido como lo son la crisis del golfo de Coquivacoa (1987) y el actual litigio con Nicaragua en el mar Caribe.

Esto nos hace reflexionar sobre una serie de cuestionamientos para hallar la hoja de ruta a seguir, ¿Se debe seguir adquiriendo material técnico o estandarizar el ya existente a nivel CGFM?, ¿casarnos con una sola casa fabricante para todas nuestras Fuerzas Militares?, ¿Se puede invertir en tecnología e innovación y así lograr integrar algunas capacidades ya adquiridas para generar desarrollo tecnológico? ¿Se cuenta con los medios, pero, también con voluntad política? ¿Se puede seguir usando la diplomacia blanda en nuestras relaciones internacionales para la solución de los diferentes incidentes presentados en las fronteras? ¿Se podría optar una postura más rígida para darle solución a nuestros diferendos fronterizos? ¿Qué se requiere en? nuestras Fuerzas Militares para poder disuadir a nuestros pares regionales?, y si esa diplomacia falla, ¿Qué se debe hacer para defender nuestra soberanía? Este conjunto de preguntas son tema de una profunda reflexión porque simplemente en el campo de la prospectiva, cualquier hipótesis tiene que ser evaluada y analizada al detalle, y cada una de ellas cuenta un amplio espectro y complejidad en el marco de la guerra hibrida. Como miembros de las Fuerzas Militares debemos analizar todos los posibles escenarios, y más aún debemos prepararnos técnica y tecnológicamente para todos.

Colombia siempre ha tenido una postura diplomática pasiva, toda vez que como nación nuestra cultura no ha sido expansionista. Esto lleva a que algunos de nuestros pares, quieran sacar provecho y poder consolidar planes de vieja data, que a toda vista

tienen como objetivo, adherir a sus territorios zonas de amplia riqueza, no solo en recursos, sino que le generan a nuestro país, una extensión estratégica en el dominio marítimo, como ya se mencionó anteriormente, en la alta Guajira y el mar Caribe. Estas zonas geográficas las que refiere principal atención el presente trabajo, toda vez que son tal vez las más ricas en recursos naturales y minerales, ya que tanto el golfo de Coquivacoa como la zona marítima conocida como la costa de Mosquitos, en el archipiélago de San Andrés, han sido motivo de disputas tanto por Venezuela como por Nicaragua respectivamente, además de los recursos minerales que ofrecen nuestra Orinoquia y Amazonia.

Por lo anterior se concluye, que contando con unas capacidades adquiridas, y analizando el marco económico tanto nacional como global, la política monetaria y cambiaria actual del país, y el marco que define la conjuntes de nuestras Fuerzas Militares, se requiere que el CGFM ahonde sus esfuerzos en el firme propósito de integrar todas estas capacidades para generar desarrollo, que no solo queden plasmados en el ámbito académico, sino tomar todos estos esfuerzos aislados y aterrizarlos a la realidad. Se cuenta con importantes centros de investigación y desarrollo, con unas capacidades y estándares muy altos, como lo son EMAVI, COTECMAR, ESMIC, UMNG, ESCOM, INDUMIL, por mencionar algunos, que son referente a nivel regional y global.

No estamos lejos, no tenemos que arrancar de cero, ya la FAC tiene un avanzado desarrollo en tecnología satelital, la ARC por su parte cuenta con avances importantes en cifrado de datos con su sistema DATA LINK 32 de transmisión de información para su flota de superficie, por su parte el EJC con su Laboratorio de Comunicaciones Militares, cuenta con unas capacidades tanto de desarrollo tecnológico como programación de equipos de comunicación militar y de sostenimiento. Solo se requiere aplicar el concepto de conjuntez entre nuestras Fuerzas, integrar esas capacidades que nos hace referentes en la región.

Pero para lograr esta integración se requiere que el Ministerio de Defensa Militar (MDN) como ente rector entre el Grupo Social y Empresarial del sector Defensa (GSED) y el Comando General de las Fuerzas Militares (CGFM), genere unas políticas y lineamientos claros, que el Comando Conjunto Cibernético (CCOCI) como direccionador y articulador en el sector defensa (en ciberseguridad y ciberdefensa) lidere este proceso y bajo la sombrilla del MDN se logre articular estas capacidades para darle una solución tacita y real a esta problemática estratégica planteada en el presente trabajo.

Recomendaciones

- Al MDN como integrador entre el CGFM y el GESED, la generación de políticas y lineamientos para la articulación de capacidades.
- Al CGFM incluir en el plan de inversión 2024-2025 recursos necesarios, promover el desarrollo y materializar estas capacidades conjuntas.

- Al CCOCI como ente rector de la Ciberseguridad y la Ciberdefensa, generar estrategias de integración y coordinación para las Fuerzas.
- Al EJC impulsar Centro de desarrollo tecnológico, ESMIC-ESCOM para el desarrollo de capacidades, y promover investigación en sus escuelas.
- A la ARC que en su sistema de DATA LINK 32, se incluya capacidad de transmisión voz a voz ***modo seguro*** para integrar radios multiplataforma.
- A la FAC desarrollar una constelación satelital con capacidad de integración DATA LINK 32 que sirva como repetidor táctico en ultramar, así como desarrollar capacidades de autonomía energética y micropopulcion para los small sats

Declaración de divulgación

El autor declara que no existe ningún potencial conflicto de interés relacionado con el artículo.

Autor

Darwin Alexis Joya Moreno. Mayor del Ejército Nacional de Colombia. Magíster en Ciberseguridad y Ciberdefensa, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Especialista en Administración de Recursos Militares para la Defensa Nacional, Centro de Educación Militar. Especialista en Conducción y Administración de Unidades Militares, Centro de Educación Militar. Profesional en Ciencias Militares, Escuela Militar de Cadetes "General José María Córdova", Colombia.

Orcid: https://orcid.org/0009-0007-4537-9914 Contacto: joyad@esdeg.edu.co

Referencias

Actualidad Aeroespacial. (2020). *El satélite brasilero Amazonia-1*. https://actualidadaeroespacial.com/el-satelite-brasileno-amazonia-1-viajo-a-la-india-para-su-lanzamiento-en-febrero/

Agência Espacial Brasileira. (2022). *Ministério da Ciência, Tecnologia e Inovações*. Programa Nacional de Atividades Espaciais (PNAE): https://www.gov.br/aeb/pt-br/programa-espacial-brasileiro/politica-organizacoes-programa-e-projetos/programa-nacional-de-atividades-espaciais

Agencia Espacial Mexicana. (2016). *Guía de orientación regulatoria. Satélites pequeños*. Agencia Espacial Mexicana. http://smallsats.cicese.mx/wiki/index.php/Sat%C3%A9lites_peque%C3%B1os

Agencia TAO. (2020). *Argentina y el espacio: una historia con luces y sombras.* Agencia TAO. https://agenciatao.wordpress.com/2020/12/30/argentina-y-el-espacio-una-historia-con-luces-y-sombras/#:~:text=El%20primer%20lanzamiento%20de%20un,aeroespacial%20que%20tiene%20nuestro%20pa%C3%ADs.

Alen Space. (2022). *Guía básica de nanosatélites.* https://alen.space/es/guia-basica-nanosatelites/

Argentina En El Espacio. (2021). *Argentina en el Espacio.* http://argentinaenelespacio.blogspot.com/2021/01/diysatellite-pondra-en-orbita-el.html

Armada Nacional de Colombia. (2023). *Armada de Colombia conmemora 202 años de su Flota de Superficie.* Armada Nacional de Colombia. https://www.armada.mil.co/es/content/armada-colombia-conmemora-202-anos-su-flota-superficie

BBC Mundo. (2014, septiembre 14). ¿Quiénes son los navajos, la tribu que logró la mayor compensación de la historia en EE.UU.?. *BBC Mundo.* https://www.bbc.com/mundo/noticias/2014/09/140925_estados_unidos_quienes_son_navajos_bd

Britannica . (2023). *Enciclopedia Británica*. Tecnología Militar. https://www.britannica.com/technology/strategic-missile

California State Polytechnic University. (2012). *CubeSat Design Specification.* Cal Poly – San Luis Obispo, CA.

Cepeda, C. F. (2023). *Zona Militar. Desde la Sociedad por la Defensa.* Zona Militar. https://www.zona-militar.com/2023/04/07/los-vehiculos-blindados-del-ejercito-de-colombia-a-lo-largo-de-las-decadas-de-los-70-80y-90/

Cortés, P. M. (2019). Inteligencia y contrainteligencia militar frente a fallos y desafíos. El caso de Culiacán, México. *Revista Latinoamericana de Estudios de Seguridad,* (26), 37-56 https://revistas.flacsoandes.edu.ec/urvio/article/view/4225/3260

Cotecmar. (2021). *Corporación de Ciencia y Tecnología para el Desarrollo de la Industria Naval Marítima y Fluvial.* Ciencia y Tecnología. https://www.cotecmar.com/ciencia-y-tecnologia

David, L. (2004). *SPACE.COM. Cubesats: Tiny Spacecraft, Huge Payoffs.* https://www.space.com/308-cubesats-tiny-spacecraft-huge-payoffs.html

Defense Industry Daily staff. (2011). *Defense Industry Daily. Small Is Beautiful: US Military Explores Use of Microsatellites*. https://www.defenseindustrydaily.com/Small-Is-Beautiful-US-Military-Explores-Use-of-Microsatellites-06720/

Departamento Administrativo de la Función Pública. (2011). *Departamento Administrativo de la Función Pública. Decreto 4169/2011:* https://n9.cl/2h7de

Departamento Nacional de la Función Pública. (2006). *Departamento Nacional de la Función Pública*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=66645

Departamento Nacional de Planeación. (2020). Presidencia de la República. Consejo Nacional De Política Económica y Social. https://www.dnp.gov.co/conpes

Ecu Red. (2022). *Caza de Superioridad Aérea.* Ecu Red. https://www.ecured.cu/Caza_de_superioridad_a%C3%A9rea

El Mundo España. (2022). Qué es un escudo antimisiles y cómo funciona. *El Mundo de España.* https://www.elmundo.es/como/2022/10/14/63492340fc6c8315338b45e9.html

Espinel, D. F., & Giraldo, A. E. (2018). *Repositorio Institucional UD. Implementación del laboratorio de picosatélites de la Universidad Distrital Francisco José de Caldas.* Repositorio Universidad Distrital. https://repository.udistrital.edu.co/bitstream/11349/13857/1/EspinelG%C3%B3mezDiegoFernando2018.pdf

Fuerza Aérea Colombiana. (2021). *Proyectos FacSat*. Poder Espacil. https://poderespacial.fac.mil.co/es/facsat/exploracion-cientifica-antartida

Fuerza Aérea Colombiana. (2023). *Comando Fuerza Aérea Colombiana*. https://facsat1-fuerzaaereacol.hub.arcgis.com/#antecedentes

Fuerza Aérea del Perú. (2017). *Pesquisa FAP ESP. Un nuevo satélite en órbita para el sistema de comunicaciones de Brasil.* https://revistapesquisa.fapesp.br/es/un-nuevo-satelite-en-orbita-para-el-sistema-de-comunicaciones-de-brasil/

Fuerza Aeroespacial Colombiana. (2022). *Fuerza Aeroespacial Colombiana.* Galería Fotográfica : https://www.fac.mil.co/es/posters/kfir-0

Fuerza Aeroespacial Colombiana. (2023). *FACSAT Antecedentes.* https://poderespacial.fac.mil.co/es/facsat/antecedentes

Infodefensa . (2023). *Hablemos de Defensa y Seguridad*. https://n9.cl/jl0hr

Jornet, R. (2023). *Domestika.* https://www.domestika.org/es/blog/5109-una-breve-historia-del-diseno-de-banderas-maritimas

Joya, R. A. (2020). *Universidad Sergio Arboleda. Satélite Libertad 1*: https://www.usergioarboleda.edu.co/satelite-libertad-1/

Morante, A. (2017). Se cumplen 10 años del lanzamiento del satélite Libertad 1. *El Tiempo.* https://www.eltiempo.com/vida/ciencia/libertad-1-diez-anos-del-lanzamiento-del-satelite-colombiano-84636

Ochoa, A. (2022). *El Observatorio Astronómico Nacional de Colombia.* Señal Memoria. https://www.senalmemoria.co/articulos/observatorio-astronomico-colombia

Ortiz, G. (2021). Socioeconómicos. goconqr: https://www.goconqr.com/es/ficha/30657913/socioeconomicos

Romero, L. M. (2021). *Implementación de una interface de radio definida por software SDR para seguimiento de pequeños satélites.* http://hdl.handle.net/11349/29503.

SpaceWorks Enterprises, Inc. (2014***).*** *Nano / Microsatellite Market Assessment.* Engineering Economics Group. Atlanta, GA. https://web.archive.org/web/20140222211907/http://www.sei.aero/eng/papers/uploads/archive/SpaceWorks_Nano_Microsatellite_Market_Assessment_January_2014.pdf

Velazco, R. (2017). *Universidad Politécnica de Madrid.* https://oa.upm.es/49232/1/PFC_REBECA_VELASCO_LOPEZ.pdf

Verenzuela, L. (2022). *Cube Sat. Scribd.* https://es.scribd.com/document/631986685/CubeSat#

Esta página queda intencionalmente en blanco

Coyuntura

Defiances

Esta página queda intencionalmente en blanco

Revista Ciberespacio, Tecnología e Innovación
Volumen 2, número 4, julio-diciembre 2023 (pp. 195-200)
Bogotá, D.C, Colombia

EDITORIAL ESDEG

Una aproximación del Metaverso a los sistemas de comando y control en las Fuerzas Militares de Colombia

A Metaverse approach to command and control systems in the Colombian Military Forces

DOI: https://doi.org/10.25062/2955-0270.4778

Ignacio Alexander Rosero Chamorro
Escuela Superior de Guerra "General Rafael Reyes Prieto", Bogotá D. C., Colombia

Resumen

El presente artículo aborda una revisión literaria para identificar el contexto del metaverso y como esta capacidad puede mejorar la eficiencia de los sistemas de comando y control de las Fuerzas Militares de Colombia. Lo anterior ayuda al lector a entender las bondades de esta nueva y emergente capacidad y con base en las tecnologías de blockchain e inteligencia artificial, organizar las cadenas de bloques de información y dar valor a los datos para optimizar la toma de decisiones, de esta manera proponer cambios y evitar que los procesos institucionales en los próximos 10 años no queden relegados de los avances tecnológicos.

Palabras Clave: Metaverso: capacidad; tecnología

Abstract

This article addresses a literary review to identify the context of the metaverse and how this capability can improve the efficiency of the command and control systems of the Colombian Military Forces. The above helps the reader understand the benefits of this new and emerging capability. and based on blockchain and artificial intelligence technologies, organize information block chains and give value to data to optimize decision making, in this way propose changes and prevent institutional processes from being relegated in the next 10 years. of technological advances.

Key words: Metaverse: capacity; technology

Artículo de reflexión
Recibido: 19 de agosto de 2023 • **Aceptado:** 17 de noviembre de 2023
Contacto: Ignacio Alexander Rosero Chamorro roseroi@esdeg.edu.co

Aproximación del Metaverso

A principios del siglo XX, se denominó como control y dirección de las operaciones militares, conceptos que han evolucionado con adopción progresiva de las tecnologías, estas últimas han sido de gran importancia, toda vez que ha contribuido en la construcción de entornos tecnológicos sofisticados como los sistemas de comando y control, que a su vez, incluyen otras variables (bondades) como comunicaciones, computación, ciberdefensa, inteligencia y vigilancia que permiten dinamizar el campo de batalla y vencer (Segura, 2016).

El Comando y control puede ser considerado como objeto y acción, es decir autoridad y ejercicio de dicha autoridad, pero en el hemisferio el concepto como lo presentaremos a continuación tiene divergencias. Por ejemplo, en la Infantería de Marina de Estados Unidos de América el concepto de comando y control hace referencia a los sistemas y no a la autoridad, por lo que se deduce que la evolución alcanzada no solo aborda lo tecnológico, sino también lo conceptual (Segura, 2016 p.60).

Los sistemas de comando y control (C2) son arquitecturas complejas compuestos por subsistemas informáticos, electrónicos, protocolos tecnológicos y flujos de trabajo, su rol desde un enfoque técnico es garantizar los canales para el tráfico de información de manera vertical y horizontal, y con una particularidad adicional, permitir la conexión de información con otras organizaciones durante las operaciones militares (Repetto, 2010).

El Centro de investigación y desarrollo de software (CIDESO), desarrolló un sistema de simulación de Batalla virtual (BV) en donde se integran componentes de maniobra y herramientas de estado mayor. Para escalonar el rol de un sistema BV a un escenario real (sistema de comando y control (C2), se proyecta la necesidad de incorporar experiencias de interoperabilidad entre sistemas heterogéneos como la integración de datos, interacción con redes de sensores inalámbricos e integración con hardware específico para C2 (Repetto, 2010)

Para entender mejor la dinámica de la interoperabilidad en los sistemas de C2, definen capas con sus correspondientes roles, como se muestra en la siguiente tabla.

De acuerdo con la tabla anterior, se profundiza sobre la capa cuatro y cinco, toda vez que, tiene gran relación con los antecedentes del concepto de metaverso, previamente en algunos sistemas de C2 adoptaron una arquitectura de red orientada a servicios que les permitió mostrar estaciones móviles durante operaciones militares y la combinación de servicios. Otra bondad identificada es el empleo de un meta – lenguaje (Business process execution language -BPEL-) para establecer reglas de negocio sobre servicios ya existentes de manera gráfica y simple (Repetto, 2010).

Tabla 1. Interoperabilidad en los sistemas de C2

Capa	Nombre de la capa	Descripción
1	Hardware de comunicaciones	Comunicaciones físicas; como enrutadores convencionales, satelitales y radios de todas las gamas de frecuencias.
2	Enmascaramiento de enlaces físicos	Nodo de comunicaciones de datos informativos (TCP/IP)
3	Comunicaciones lógicas	Brinda servicios de enrutamiento y seguridad en autorización, autenticación y acceso (Robustez y distribución de carga)
4	Distribución del negocio	Maneja el directorio de aplicaciones del negocio.
5	Software de C2	Sistemas que exponen las capacidades por medio de servicios para ser consumidos.

Fuente: Autoría propia información obtenida de Repetto (2010)

El Departamento de Defensa de los Estados Unidos de América, desarrolló un programa de municiones explosivas en red (AV/AT Scorpion XM 1100), que consiste en un subsistema de comando y control que permita la gestión de minas antipersonales de manera remota, con características particulares de gestión como encendido, apagado, autodestrucción, auto neutralización, es reutilizable y, además, se integra al sistema de comando y control central. Con lo anterior, se percibe la capacidad del entorno tecnológico, que permite engrandecer un sistema con desarrollos que inicialmente se crean de manera independiente (Gross, 2021 p.13).

El término metaverso aparece por primera vez en 1992 en la novela Snow Crash del escritor estadounidense Neal Stephenson (Stephenson, 2003), una de las definiciones del concepto, es la articulación de la realidad virtual y realidad aumentada que se consolidan en una realidad extendida (XR). Esta última, bajo el concepto de persistencia, facilita el crecimiento de un universo virtual con bondades mejoradas y disruptivas desarrolladas de manera independiente que, posteriormente, se terminan articulando. Otro concepto relacionado con el universo virtual lo define como la combinación de tecnologías de blockchain y la Inteligencia Artificial (IA) (Sánchez, 2022).

El primer lanzamiento de aplicación del concepto de metaverso fue en el año 2003 a través de *Second life,* el cual fracaso en razón a la limitación cultural del mercado y reducidos avances tecnológicos para el funcionamiento de este universo virtual. 20 años después (2023) es posible que se haya alcanzado parcialmente la consolidación de las superficies tecnologías para su funcionamiento, pero la transición cultural para su aplicación y adopción se encuentre en una fase inicial, algunos campos de acción del metaverso serán actividades de ocio, nuevas actividades economicas sostenibles, escenarios para interacción en el trabajo, educación e inclusión (Sánchez, 2022).

Haciendo un análisis de lo ocurrido en la evolución del internet y lo que puede suceder con el metaverso en las empresas y en especial en las Fuerzas Militares de Colombia (FF.MM.), es que al igual que se adoptó el concepto construyendo una herramienta personalizada e independiente como la intranet al interior de cada empresa para que se adopte como una variante independiente el concepto de metaverso exclusivamente a nivel empresarial (FF.MM.), donde se desarrolle escenarios de interacción en el trabajo que harían equivalencia a lo que hoy denominamos sistemas de comando y control.

El concepto de blockchain, como parte de la construcción del metaverso, inicia con la adopción de la dinámica de las criptomonedas (2008), una de sus aplicaciones es la construcción de la cadena de bloques de información bajo la teoría del árbol de hash de Merkel. Cada hoja almacena información de manera independiente haciendo parte de la estructura del árbol, cada hoja superior se compone de valores de los hashes inferiores, repitiendo esta concatenación se obtiene un solo nodo denominado raíz. También se caracteriza por la marca de tiempo que identifica el instante en que fue creada la cadena, la marca de nonce (minado) y la marca de la raíz, estos valores permiten caracterizar cada hoja de manera segura (Dolader, 2017 p.36).

Haciendo una revisión del concepto de guerra de Sun Tzu, en su literatura indica *los invisibles hilos de las comunicaciones,* que permiten ganar la guerra antes de iniciar la batalla, haciendo la analogía, el comandante moderno adopta los datos como insumo para la toma de decisiones. Desde el punto de vista epistemológico, una forma de recolectar dichos datos es a través de sensores dispuestos en las capacidades de los dominios propios, del medio ambiente y del enemigo, generando valor a través de su interacción digital en tiempo real (Gómez de Ágreda, 202). Para generar valor a partir de datos, es necesario que de manera paralela se diseñe la implementación de las herramientas de minería de datos, machine learning, inteligencia artificial, y big data

Considerando la amplitud real del escenario y las capacidades de la guerra, para incorporarse dentro de un sistema de comando y control conjunto, se necesita de herramientas tecnológicas agiles y eficientes para captar comportamientos individuales y representarlos en escenarios virtuales, como lo describe Camacho, Oropeza y Lozoya (2017). "El internet de las cosas (IoT) permite una interconexión digital entre diferentes objetos cotidianos mediante internet […], gracias a esta tecnología se puede trabajar con medios donde un objeto puede dar retroalimentación a otro" (p. 141).

Conclusiones

Las Fuerzas Militares de Colombia no cuentan con un sistema de comando y control que le permita al Comandante General visualizar el contexto en tiempo real de cualquier

situación de orden nacional o regional, que le permita de manera articulada tomar decisiones con los comandantes de Fuerza.

Al igual que en los Genesis del internet, donde las empresas adoptaron el concepto para crear la intranet empresarial, se requiere que como institución se prepare cognitivamente y desarrolle exploraciones de inmersión en el nuevo escenario virtual (metaverso institucional), como herramienta para fortalecer los sistemas de comando y control.

Como método de adopción del concepto de metaverso, se recomienda que a través de procesos de investigación y desarrollo institucionales se materialicen las nuevas herramientas tecnológicas como minería de datos, machine learning, inteligencia artificial, big data y blockchain, de esta manera impulsar la transformación hacia ese nuevo escenario virtual.

El insumo inicial para que la tecnología de metaverso funcione de manera organizada desde el primer momento de implementación, se necesita partir por el proceso de reorganizar las cadenas de bloques de información, esta línea de acción se materializara solo si, el concepto de cambio se encuentra en el liderazgo y politica de los señores comandantes.

Se concluye que un posible curso de acción para fortalecer los sistemas de comando y control conjunto de las Fuerzas Militares de Colombia, es la adopción y combinación de cuatro escenarios tecnológicos como son; el metaverso, blockchain, inteligencia artificial e internet de las cosas, que permita construir un escenario virtual de interacción, fortalecer la seguridad de la informacion operacional, analizar datos de manera ágil e interconectar digitalmente los componentes del teatro de la guerra. De esta manera, consolidar un sistema tecnológico inteligente, disponible, interoperable y que facilite de manera óptima la toma de decisiones.

Declaración de divulgación

El autor declara que no existe ningún potencial conflicto de interés relacionado con el artículo.

Autor

Ignacio Alexander Rosero Chamorro. Mayor del Ejército Nacional de Colombia. Magister en Gerencia de la innovación empresarial, Universidad Externado de Colombia, Colombia. Candidato a magíster en Ciberseguridad y Ciberdefensa, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Profesional en Ciencias Militares, Escuela Militar de Cadetes "General José María Córdova", Colombia.

Orcid: https://orcid.org/0009-0001-0897-0875 Contacto: roseroi@esdeg.edu.co

Referencias

Camacho, J., Oropeza, E., & Lozoya, O. (2017). Internet de las cosas y realidad aumentada: una fusión del mundo con la tecnología. *Revista Electrónica de Computación Informativa, Biométrica y Electrónica, 6*(2007–5448), 139–150. https://www.redalyc.org/articulo.oa?id=512253717009

Dolader, C. (2017). *L021.1*. Universidad Politécnica de Catalunya.

Gómez de Ágreda, A. (2020). *Usos militares de la inteligencia artificial, la automatización y la robótica.* Estado Mayor de la Defensa.

Gross, C. (2021). *El subsistema de munición explosiva en red integrado al sistema de comando y control de la Gran Unidad de Combate.* Escuela Superior de Guerra "Tte. Grl. Luis María Campos".

Repetto, A. (2010). *Framework de Interoperabilidad para Sistemas de Comando y Control Físico 2*. XII Workshop de Investigación En Ciencias de La Computación, 577–581.

Sánchez, A. (2022). *Plan de negocio de startup con servicios en el Metaverso. Universidad Pontificia.*

Segura, E. (2016). *Comando y control en escenarios cívico-militares.* Visión Conjunta.

Perspectivas

Perspectives

Esta página queda intencionalmente en blanco

Revista **Ciberespacio, Tecnología e Innovación**
Volumen 2, número 4, julio-diciembre 2023 (pp. 203-206)
Bogotá, D.C, Colombia

EDITORIAL **ESDEG**

Entrevista David Luna Sánchez. Importancia de la ciberseguridad y seguridad de la información en la política colombiana

Interview David Luna Sánchez. Importance of cybersecurity and information security in Colombian politics

DOI: https://doi.org/10.25062/2955-0270.4813

Luis Alejandro León Alfonso
Escuela Superior de Guerra "General Rafael Reyes Prieto", Bogotá D. C., Colombia

Biografía

David Luna Sánchez

Líder político de origen liberal, nació en Bogotá en 1975. Es abogado de la Universidad del Rosario, donde también realizó una especialización en Derecho Administrativo. Adicionalmente, adelantó la maestría en Gobierno y Políticas Públicas de la Universidad Externado de Colombia.

Actualmente, es Senador de la República de Colombia. Se desempeñó como Ministro Tecnologías de la Información y las Comunicaciones, parlamentario del partido Cambio Radical, exconcejal de Bogotá y fue candidato a la alcaldía mayor de esta ciudad.

Entrevista
Recibido: 28 de noviembre de 2023 • **Aceptado**: 12 de diciembre de 2023
Contacto: Luis Alejandro León Alfonso leonlu@esdeg.edu.co

Entrevista David Luna Sánchez. **Importancia de la ciberseguridad y seguridad de la información en la política colombiana**

Las cifras sobre ciberseguridad en Colombia son desalentadoras, según Fortinet, empresa experta en el tema, en 2022 las denuncias por ciberdelitos en Colombia fueron 54.000, frente a cerca de 11.000 que se presentaron en el 2021. Casos muy mediáticos como los ciberataques en contra del grupo Keralty y las empresas Sanitas, el DANE o el INVIMA dan fe de esta realidad. ¿Considera que la Ciberseguridad es un tema que debería estar en el primer orden de la agenda nacional?

Por supuesto que sí, solo el año pasado hubo 20.000 millones de intentos de ataques en materia de ciberseguridad, eso pone en grave riesgo la historia clínica de un ciudadano, los ahorros de otro, los datos personales de cualquiera, y en ese sentido, creo que el Estado, pero también a la sociedad. Se debe tener en cuenta que este es un enemigo oculto mucho más peligroso que el narcotráfico, o incluso que los grupos al margen de la ley.

¿Por qué?

Porque tienen la capacidad de actuar de manera irregular sin ser muchas veces percibidos; y acá hay que recordar que Colombia, como Estado, ha hecho un esfuerzo desde el año 2010 creando el Comando Conjunto Cibernético, el Centro Cibernético Policial, el CSIRT gobierno, instituciones responsables de apoyar a las entidades del Estado en la adecuada gestión de los incidentes cibernéticos como el COLCER, entidad coordinadora del orden nacional en temas de seguridad informática. Pero, lastimosamente, durante los últimos años han sido abandonadas en cuanto a la destinación de personal calificado y a la debida asignación presupuestal, y las consecuencias las evidenciamos hace un par de semanas con un importante ataque que le hizo mucho daño a las entidades públicas.

Informes internacionales como el del Foro Económico Mundial sobre *Riesgos Globales,* para el año 2023, señala que *la polarización política* ha venido aumentando exponencialmente en los últimos años, y dicha polarización trae consigo que ciberdelincuentes o hacktivistas se animen a realizar ciberataques en contra de partidos políticos, particularmente a quienes consideren como opositores a sus principios ideológicos. Bajo esta premisa Doctor Luna. ¿Qué elementos o componentes deberían tener en consideración las colectividades políticas, movimientos representativos o partidos políticos para garantizar la seguridad digital en su interior?

Coincido con usted, la organización electoral está en riesgo. En el caso colombiano, la Registraduría de forma permanente ha sido objeto de ataques y el Consejo Nacional

Electoral permanente por los expedientes que tramita, pero los partidos políticos también, muchos de ellos, piensan que esto es un delito que nunca les va a llegar.

Un partido político lo afectan, pues pueden contactar a toda su militancia y, de alguna manera, la pueden mal informar, o lo que es peor, la pueden hacer equivocar. Entonces, creo que los partidos deben trabajar en estos temas a los cuales no les han dedicado lamentablemente el esfuerzo que merecen.

¿Considera usted que las organizaciones políticas en Colombia están preparadas para hacerle frente a las amenazas que trae consigo la era digital y la exposición de datos digitales?

No solamente no están preparadas, sino que son de lejos las entidades más vulnerables que puede haber en toda la cadena; un banco está mejor preparado, una EPS está mejor preparada, una entidad pública sí está preparada. Le garantizo que no hay ningún partido político en Colombia que le haya invertido dos millones de pesos a temas de control en contra de ataques cibernéticos.

En vísperas de los diferentes procesos electorales en Colombia, la actividad al interior de los partidos y movimientos políticos aumenta y, con ello, la posibilidad de presentarse vulneraciones de seguridad digital. En ese entendido, desde su perspectiva y experiencia, ¿Cómo percibe el estado actual de seguridad digital en el partido político Cambio Radical?

Yo creo que el partido político Cambio Radical es un partido muy serio, con unos estatutos muy claros, adicionalmente, con una organización administrativa muy profesional y muy calificada, y tiene como evidencia una oficina de T.I. muy valiosa, pero desconozco cuáles han sido las inversiones que han hecho recientemente en materia de ciberseguridad, en materia de protección de data y, adicionalmente, en materia de la futura protección del proceso de conteo y reconteo en los comicios electorales. Esperaría que, hayan avanzado. Insisto, no conozco hasta el momento ningún esfuerzo que todos los partidos políticos hayan hecho en este sentido, y por ende considero, que parte de los recursos que le paga el Estado a los partidos deberían ser utilizados en estas tareas de protección.

De los diferentes modelos de Gestión de Riesgos de Seguridad Digital que usted ha podido conocer, ¿Cuál le parece adecuado implementar al interior de una organización política?

Pienso que el modelo de riesgo más importante es el que hace referencia a tener presente que todos los días hay riesgos cibernéticos, y para evitarlo se necesita estar permanentemente, no solo actualizando su software, sino adicionalmente logrando identificar cuáles datos o qué información pueden ser objetos de ataques y

eso como se identifican con otro software que demuestra donde están las vulnerabilidades. Las vulnerabilidades hay que trabajarlas de la mano de expertos, eso no lo puede hacer cualquier persona, por eso hay que contratar personal experto en temas de ciberseguridad para que tengan la posibilidad de avanzar en los procesos.

Desde su experiencia como exministro de las TIC como actual parlamentario de Cambio Radical, y como líder político. ¿Qué temas, tópicos o elementos recomienda a las directivas de los partidos políticos, en general, y a los miembros del Cambio Radical, en particular, para adelantar procesos de sensibilización o capacitación para sus directivas, colaboradores y las demás partes interesadas?

El primero de ellos sería el de incluir dentro de sus planes anuales de acción la protección en materia de ciberseguridad; Lo segundo es tener presente que se debe contratar por lo menos un experto profesional en esta materia; lo tercero, lo que mencionaba anteriormente, tener permanentemente actualizados los softwares. Por ejemplo, los de bases de datos, los de conteos electorales o el de financiación de campañas, y adicionalmente, tener software para identificar donde están las vulnerabilidades en las redes de cada uno de los partidos.

Los líderes de las organizaciones realmente necesitan intensificar e implementar capacitación y concienciación a todo nivel. El 84 % de las organizaciones de EE. UU. dijeron que la capacitación en concientización sobre seguridad digital había reducido las tasas de fallas de phishing. Con este panorama. ¿Qué iniciativas y acciones debería desarrollar Cambio Radical para disminuir las vulnerabilidades de seguridad digital, particularmente frente a amenazas como el phishing?

Lo más importante de todo es mantener permanentemente procesos de formación y capacitación con la militancia de un partido, no solamente de Cambio Radical, de cualquiera. Contándole, por ejemplo, a sus candidatos y a sus militantes elegidos que el partido solo se comunica a través de determinada vía. Si mañana llega un mensaje de texto a un concejal en cualquier parte del país diciendo *que el partido le comparte un link para recibir un bono,* seguramente, el concejal ingresará y le van a robar sus datos. El partido tiene que hacer saber que su único mecanismo de comunicación es A, B, o C, y, de esa manera, evitar termas como el phishing.

Autor

Luis Alejandro León Alfonso. Suboficial del Ejercito Nacional de Colombia. Estudiante de la Maestría en Ciberseguridad y Ciberdefensa, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Profesional en Relaciones Internacionales y Estudios Políticos, Universidad Militar Nueva Granada, Colombia.

Orcid: https://orcid.org/0009-0009-1810-870X Contacto: leonlu@esdeg.edu.co

Enfoques

Insights

Esta página queda intencionalmente en blanco

Revista **Ciberespacio, Tecnología e Innovación**
Volumen 2, número 4, julio-diciembre 2023 (pp. 209-212)
Bogotá, D.C, Colombia

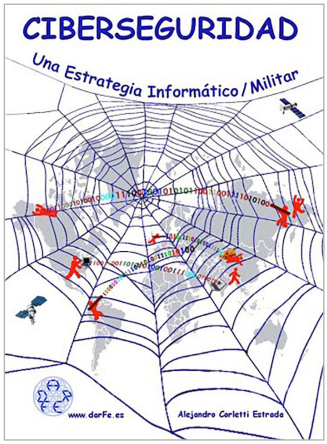
EDITORIAL ESDEG

Reseña del libro. Ciberseguridad, una estrategia informático/militar

Book review. Cybersecurity, a computer/military strategy

DOI: https://doi.org/10.25062/2955-0270.4818

Viviana Pilar Fuquen Flautero
Corporación Universitaria del Meta, Villavicencio, Colombia



Autor del libro: **Alejandro Corletti Estrada**
Editorial: DarFe Learning Consulting S.L
Año: 2017
Páginas: 245
ISBN: 978-84-697-7205-8

El libro *Ciberseguridad, una estrategia informática/militar,* es una reflexión sobre la importancia de la ciberseguridad mediante la recopilación de información y experiencias. Este trabajo se compone de 10 capítulos.

Primer capítulo, es una aproximación conceptual y de contexto sobre la ciberseguridad, en este apartado se explica las definiciones que se comprenden por ciberseguridad y ciberdefensa, reconociendo que estos dos campos resultan ser importantes para la defensa del Estado en un ambiente cibernético. La importancia es identificar que existen nuevas ciberamenazas vigentes que han explotado las ventajas tecnológicas, lo que les ha permitido abrir su accionar criminal en el ciberespacio, por ello es relevante

defenderse ante ciberataques organizados y generados desde estructuras que pueden llegar a ser mafiosas. En esta medida, se propone adoptar la resiliencia entendida como una capacidad de proceder y proteger, como parte de la estrategia para la defensa de las redes y sistemas.

Segundo capítulo, se escribe la importancia de las estrategias de seguridad en las redes, afirmando la necesidad, desde el punto de vista militar, de planear cursos de acción que permitan la relación-beneficio. En este capítulo se reconoce la existencia de emplear una buena metodología y soporte especializado con recursos tecnológicos suficientes, acompañado también de analistas para reconocer el pensamiento de las amenazas. Lo importante de este ejercicio en planeación estratégica es generar operaciones ofensivas y defensivas y desarrollar una doctrina concentrada en el desarrollo de capacidades operacionales y estratégicas en los diferentes niveles (estratégico, táctico, y operacional).

Tercero capítulo, para el autor es fundamental desarrollar una estrategia a defensa en profundidad y en altura. En este apartado y bajo esta afirmación, se establece que deben existir un orden, una misión y un desarrollo secuencial y planeado para dar cumplimiento a un objetivo final. Desde una perspectiva militar, y aplicando conceptos como la maniobra, la defensa en profundidad y deposición, la identificación de zonas claves, se establece un análisis comparado sobre lo que se debe comprender en el ciberespacio, estableciendo, por ejemplo, los espacios físicos, la gestión y servicio de las redes de comunicación.

Cuarto capítulo, en este apartado el autor aborda la importancia de los procesos en la ciberseguridad. Se establece un análisis descriptivo sobre la comprensión de los procesos tales como la de producción, gestión de cambios, gestión de accesos, configuraciones e inventario, gestión del backup, gestión de incidencias, supervisión y monitorización, gestión de logs. Bajo este análisis se establece la necesidad del registro de una auditoría que identifique las facilidades y prioridades en las plataformas, reconociendo que bajo el concepto de sistema todos tus aspectos resultan ser interdependientes y lo que permitiría a largo plazo reducir los incidentes informáticos.

Quinto capítulo, un aspecto esencial es comprender que existe un espacio virtual y uno digital, y frente al escenario físico y tangible, existen plataformas e infraestructuras de seguridad en la red, deben gestionarse, supervisarse y defenderse. Para el autor es importante establecer una secuencia, detección, prevención y mitigación.

Sexto capítulo, profundizando el análisis, establece que en el escenario mundial las redes resultan ser un eje principal para la comprensión de la ciberseguridad. En este apartado se analiza la forma en que está configurada la interconexión a nivel mundial y destacando la existencia de redes "tubos" (fibras ópticas, cables de cobre y enlaces

de radio) lo cual le permite el funcionamiento de la internet y demás actividades a nivel mundial.

Séptimo capítulo, en un aspecto técnico, se analiza el empleo de NOC (Network Operation Center) y SOC (Security Operation Center), lo cual le permite generar disponibilidad y alertas tempranas para fortalecer la ciberdefensa. La NOC, se encuentra centrada en el control de la red y se caracteriza por la convergencia de la supervisión, monitorización y alarmas de la red en infraestructuras. Lo característico de este procedimiento es que establece y prioriza las infraestructuras como a plataformas, dispositivos, redes y sistemas que serán monitorizados. La SOC se concentra en el capital humano y recursos disponibles, manteniendo como característica la monitorización, detección, análisis, prevención y seguimiento de eventos de seguridad en las redes. Según el autor, los dos diferentes enfoques a nivel estratégico generan una serie de servicios que dependiendo de la actividad desarrollada pueden generar un costo de beneficio mayor.

Octavo capítulo, en este apartado se establece la relevancia del registro de auditoría (LOGS). Mediante un análisis conceptual se establece que los registros son una serie de huellas que se pueden detectar en los diferentes procesos de los sistemas de información, lo característico de este ejercicio es reconocer dichos registros con el objetivo de categorizarlos y priorizarlos. Estos registros hacen parte del concepto de resiliencia que se caracteriza por el resguardo y la recuperación ante ciberincidentes, adicionalmente se trata de un cuidado que es estar sincronizado.

Noveno capítulo, establece y abordó un concepto militar, los juegos de guerra, esta vez relacionados con la ciberguerra. Para este apartado se establece que existir una metodología de evaluación como auditoría y acción que mejore la respuesta ante incidentes, por lo cual los juegos de guerra tienen una serie de características como las de capacitar al personal, comprobar los planes y preparar al personal para el desarrollo de capacidades. En esta medida, el autor propone que los juegos de guerra deben considerar una serie de elementos para que sean desarrollados en el ciberespacio y entre los cuales debe existir como aspecto fundamental el desarrollo de una doctrina, es decir, una normativa que regule los temas de seguridad, redes e incidentes en la organización

Décimo capítulo, finalmente en este apartado se aborda una recopilación de nuevos conceptos, metodologías y desafíos. Para el autor es importante considerar que, en dicha transformación a nivel mundial generada por el ciberespacio, las instituciones deben centrarse en tres conceptos cruciales como las redes, nodos y zonas, señalando que estos conceptos son los que se abordarán a largo plazo y de manera transversal por las diferentes dinámicas sociales en las diferentes instituciones. Adicionalmente, es relevante señalar que existen desafíos que cada vez van a ser más complejos si no se desarrollan protocolos de seguridad en la red, por lo cual la resiliencia será un concepto importante en la defensa desde el ciberespacio.

Autora

Viviana Pilar Fuquen Flautero. Ingeniera Industrial, Corporación Universitaria del Meta, Colombia. Especialista en Administración en Seguridad y Salud en el Trabajo, Corporación Universitaria del Meta, Colombia. Técnica en Asistencia, Análisis y Producción de Información Administrativa con énfasis Contable del CENACAP, Colombia. Técnica profesional en Planificación para la Creación y Gestión de Empresas, Servicio Nacional de Aprendizaje, Colombia.

Orcid: https://orcid.org/0000-0002-0714-7895

Contacto: viviana.fuquen@academia.unimeta.edu.co

Referencia

Corletti, A. (2017). *Ciberseguridad, una estrategia informático/militar.* DarFe Learning Consulting S.L.


EDITORIAL ESDEG

Revista **Ciberespacio, Tecnología e Innovación**

EDITORIAL **ESDEG**

ISNN 2955-0270

9 772955 027005