EDITORIAL ESDEG

Revista
Ciberespacio, Tecnología e Innovación
Volumen 2, número 4, julio-diciembre 2023
Bogotá, D.C, Colombia
ISSN: 2955-0270 • eISSN: 3028-3310
Página web: https://esdegrevistas.edu.co/index.php/rcit

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

John Alexander Villarraga Gamboa

CITACIÓN APA:

Villarraga Gamboa, J. A. (2023). Competencias digitales del mando militar en el marco DigComp 2.2: caso Escuela Militar de Cadetes "General José María Córdova". *Ciberespacio, Tecnología e Innovación, 2*(4), 107-146.
https://doi.org/10.25062/2955-0270.4810

Publicado en línea: **Diciembre 30 de 2023**

Enviar un artículo a la Revista

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.

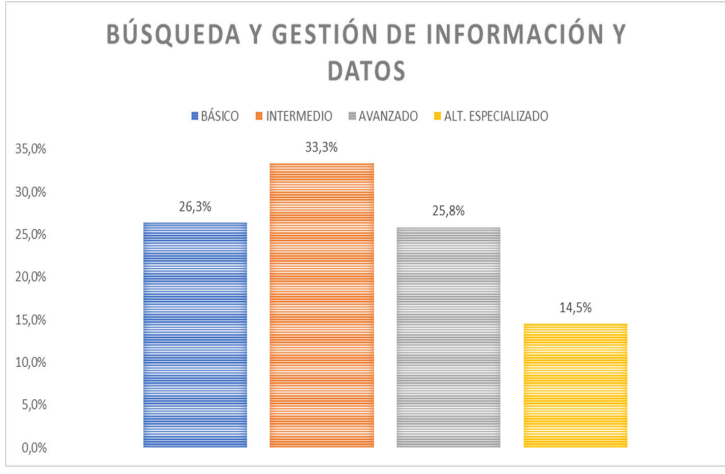
Competencias digitales de Alféreces de la ESMIC de acuerdo al marco de competencias digitales DigComp 2.2

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.

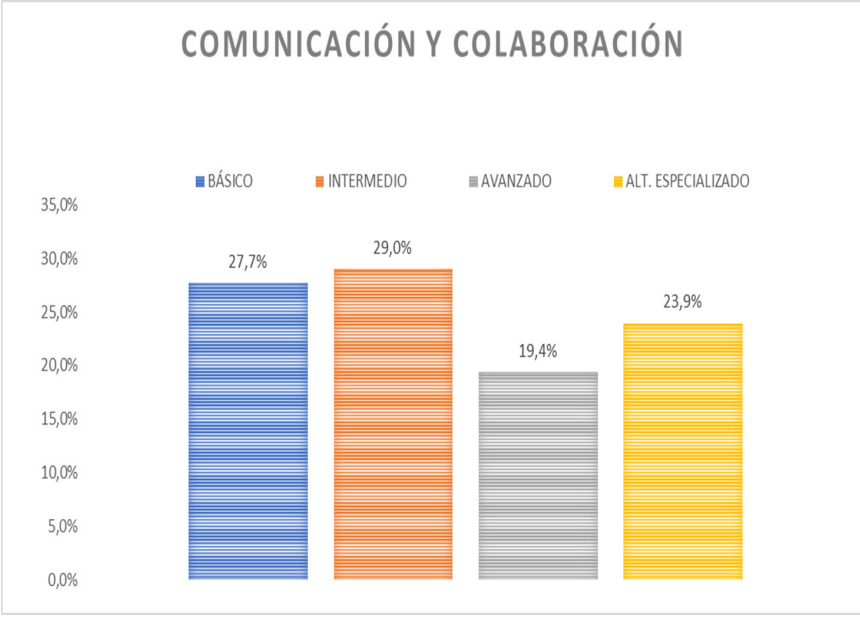


Fuente: Elaboración propia, 2023

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.

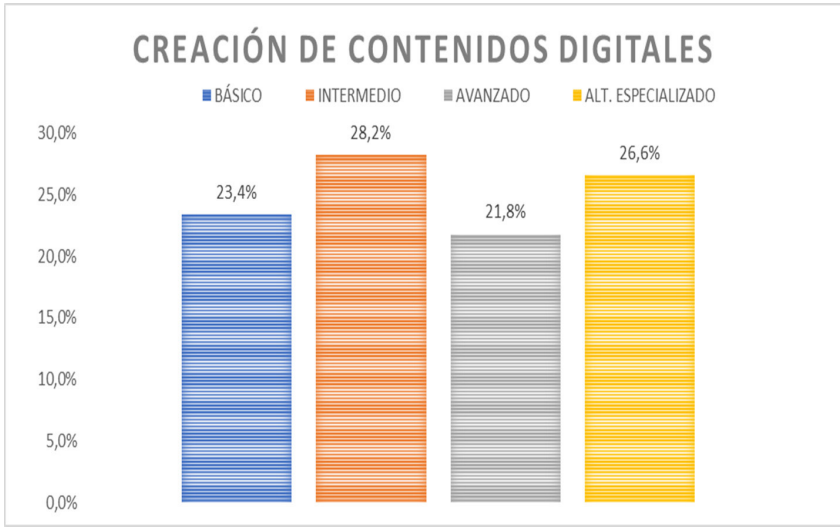
Gráfico 2. Área comunicac*ión y colaboración.*



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.

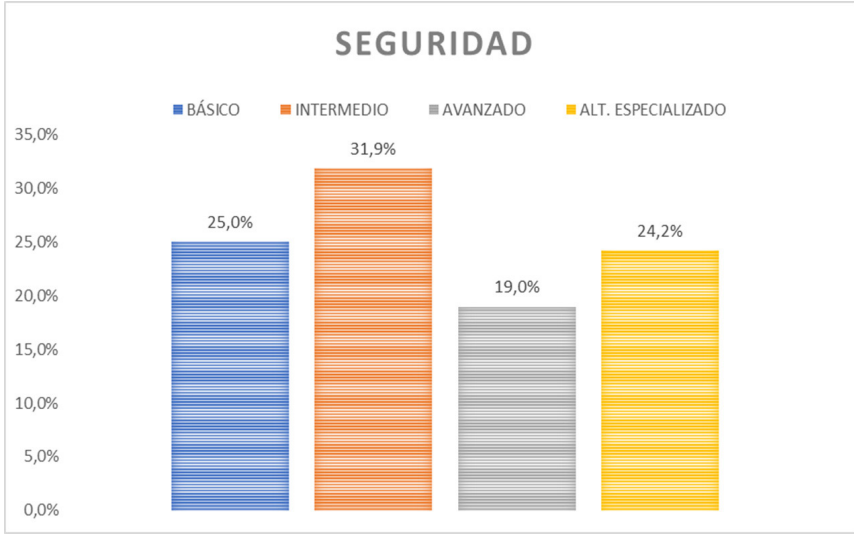
Gráfico 3. Área creación de contenidos digitales.



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.

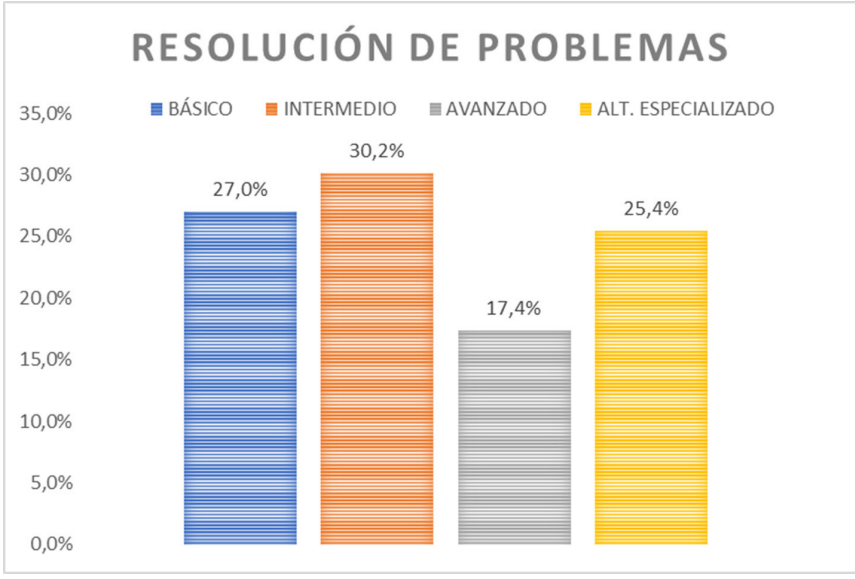
Gráfico 4. Área seguridad.



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.



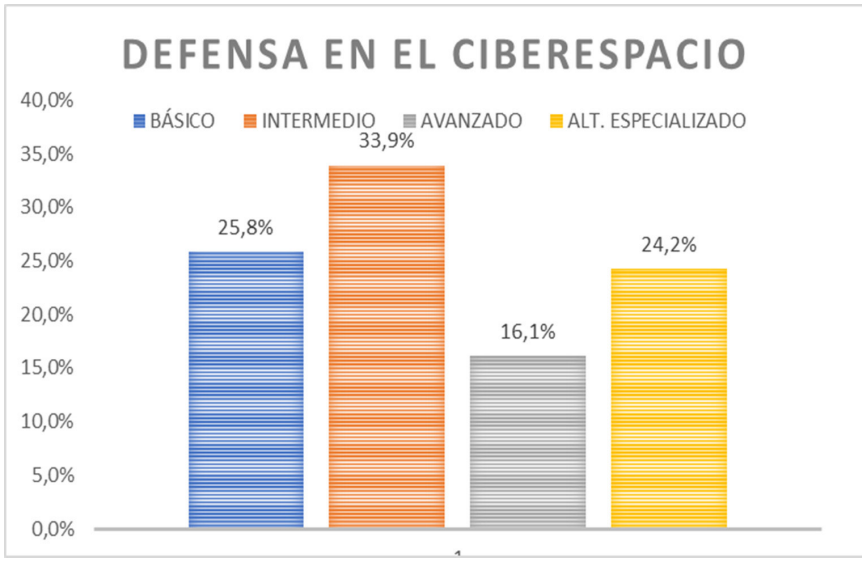
Fuente: Elaboración propia, 2023

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: **Ciberseguridad y Ciberdefensa**	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.
	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

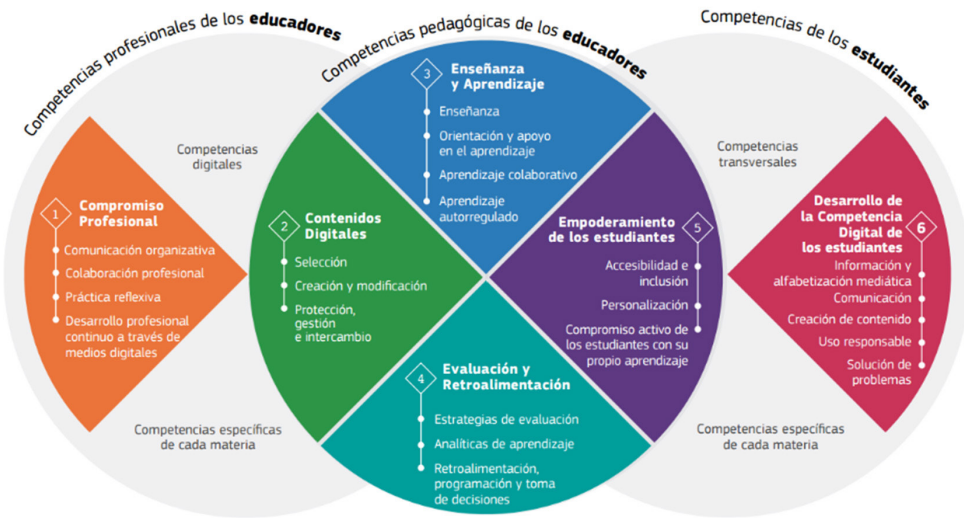
digitales, para coadyubar a fortalecer las competencias particulares de los estudiantes, en especial en los alféreces. Como se podrá observar en las áreas de actividad del educador, planteados en el marco DigCompEdu.

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