
# Ciberdefensa: Análisis en la capacitación y formación de los oficiales en la detección de brechas y vulnerabilidades en las redes informáticas del Ejército Nacional.

Mayor (EJC) Miguel David Giraldo Gaitán

Artículo para optar al título profesional:

Magister en Ciberseguridad y Ciberdefensa

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia
2025

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

| DATOS GENERALES | | |
|---|---|---|
| **Nombre del estudiante** | **:** | Mayor (EJC) Miguel David Giraldo Gaitán |
| **Identificación** | **:** | 1032372398 |
| **Programa académico** | **:** | Maestría en Ciberseguridad y Ciberdefensa |
| **Tutor metodológico** | **:** | Jairo Andrés Becerra Cuervo |
| **Tutor temático** | **:** | Jonnathan Jiménez |
| **Fecha de entrega** | **:** | 26 de agosto de 2024 |
| **Extensión** | **:** | 8.146 |

## DECLARACIÓN DE ORIGINALIDAD Y CESIÓN DE DERECHOS

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

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



## AUTORIZACIÓN DE PUBLICACIÓN

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

# Ciberdefensa: Análisis en la capacitación y formación de los Oficiales en la detección de brechas y vulnerabilidades de las redes informáticas del Ejército Nacional

## Cyberdefense: Analysis in the training and education of officers in the detection of breaches and vulnerabilities of the National Army's computer networks

Miguel David Giraldo Gaitán*
Escuela Superior de Guerra "General Rafael Reyes Prieto"

**Resumen:** las crecientes dependencias de las fuerzas militares en sistemas tecnológicos exponen al Ejército Nacional de Colombia a diversas amenazas cibernéticas que en determinado momento pueden comprometer la seguridad nacional. Sin embargo, se identifican graves deficiencias en la capacitación y formación de los oficiales para detectar y mitigar estas vulnerabilidades en las redes militares en este en este artículo se revisan fuentes académicas recientes y documentos normativos (CONPES, ISO) con el fin de analizar estas falencias. Se evidencia que persiste un bajo nivel de formación especializada y una integración insuficiente en la ciberdefensa de la estructura institucional. Basándonos hoy en los Marcos internacionales y experiencias de otros países avanzados en estos retos, por tal motivo se proponen adaptaciones al contexto militar colombiano, como la incorporación de algunos programas formales de ciberseguridad en academias militares y la adaptación a los estándares internacionales.

**Palabras clave:** Capacitación; Ciberseguridad; Ciberdefensa; CONPES; Ejército Nacional de Colombia; Normas ISO; Vulnerabilidades.

**Abstract:** The growing dependence of the Armed Forces on technological systems exposes the Colombian National Army to cyber threats that can compromise national security. However, serious deficiencies have been identified in the training of officers to detect and mitigate vulnerabilities in military networks. This paper reviews recent academic sources and normative documents (CONPES, ISO) to analyze these shortcomings. It is evident that there is still a low level of specialized training

* Mayor del Ejército Nacional de Colombia. Candidato a magíster en Ciberseguridad y Ciberdefensa, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Profesional en Ciencias Militares, Escuela Militar de Cadetes "General José María Córdova", Colombia. https://orcid.org/0000-0003-2004-7466 - Contacto: miguel.giraldo@esdeg.edu.co.

and insufficient integration of cyber defense in the institutional structure. Based on international frameworks and experiences of advanced countries, adaptations to the Colombian military context are proposed, such as the incorporation of formal cybersecurity programs in military academies and the adoption of global standards.

**Keywords:** Training; Cybersecurity; Cyberdefense; CONPES; Colombian National Army; ISO standards; Vulnerabilities**.**

# Introducción

En un entorno geopolítico cada vez más dependiente de infraestructuras digitales, la ciberseguridad es clave para la Defensa Nacional. Según la UIT, los ciberataques globales crecieron un 38% entre 2021 y 2022, afectando a gobiernos e instituciones militares. En Colombia, un ciberataque masivo en septiembre de 2023 expuso datos sensibles de millones de ciudadanos, comprometiendo la seguridad de entidades públicas, incluido el Ejército Nacional.

La ciberdefensa es una prioridad estratégica ante la rápida evolución de las amenazas cibernéticas. Esto requiere personal capacitado, especialmente oficiales, para prevenir, detectar y neutralizar vulnerabilidades en redes militares. A pesar de avances como la creación de la unidad de ciberdefensa en 2012 y las políticas CONPES 3701 y 3995, persisten deficiencias en la formación técnica y operativa de los oficiales.

El Ejército enfrenta retos significativos debido a la falta de una cultura organizacional en ciberseguridad y programas de capacitación limitados, según Peña (2023). El hackeo de 2023, que vulneró redes estatales, evidenció estas carencias, poniendo en riesgo la integridad, disponibilidad y confidencialidad de la información. Esta falta de preparación no solo afecta las operaciones militares, sino la seguridad nacional en su conjunto, generando desconfianza en las capacidades del Estado.

El problema abarca todo el territorio colombiano, dado que las redes militares tienen cobertura nacional. Las consecuencias también impactan a la sociedad civil, al erosionar la confianza en la defensa estatal. Surge entonces la pregunta: ¿Cuáles son las

deficiencias en la formación en ciberdefensa de los oficiales del Ejército para proteger redes informáticas?

Este estudio evalúa la necesidad de fortalecer las capacidades de ciberdefensa del Ejército en un entorno digital complejo, donde la dependencia tecnológica en operaciones militares exige infraestructura robusta y talento humano capacitado. La investigación propone estrategias alineadas con estándares internacionales para cerrar brechas, reducir vulnerabilidades y aumentar la resiliencia institucional, contribuyendo al cumplimiento de las políticas CONPES 3701 (2011) y 3995 (2020).

El análisis aborda el estado actual de la formación en ciberdefensa de los oficiales, revisando antecedentes, marcos normativos, pedagogías y estándares internacionales. Se identifican las principales deficiencias que obstaculizan la protección de redes militares y se ofrecen recomendaciones para mejorar los procesos de capacitación. Estas buscan consolidar una cultura organizacional sólida en seguridad digital, fortaleciendo al Ejército frente a los desafíos cibernéticos contemporáneos y las amenazas híbridas.

## Metodología

La investigación utiliza un enfoque cualitativo interpretativo para analizar las deficiencias en la formación en ciberdefensa de oficiales del Ejército Nacional de Colombia, combinando un diseño documental-descriptivo con un componente empírico. El estudio mixto, de predominio cualitativo, incluye una revisión de literatura científica, normativa (CONPES 3701, 3854, NIST CSF 2.0, NICE, ISO/IEC 27035) y doctrinal,

priorizando fuentes de los últimos cinco años. Se aplicó análisis de contenido para identificar brechas formativas y se elaboró una matriz DOFA para evaluar capacidades y oportunidades de mejora.

El componente empírico consistió en una encuesta estructurada vía Google Forms, dirigida a personal del Ejército involucrado en formación o soporte de redes y ciberdefensa (oficiales superiores, subalternos y otros roles). La muestra no probabilística por conveniencia, complementada con bola de nieve, incluyó 143 respuestas (141–142 válidas por ítem). La encuesta, validada por expertos, recopiló datos sobre rango (30 subalternos, 23 superiores, 88 otros), tiempo de servicio (1 menos de 5 años, 73 entre 5–10 años, 68 más de 10 años), suficiencia de formación (39 totalmente suficiente, 45 suficiente, 30 neutro, 25 insuficiente, 3 totalmente insuficiente), simulaciones (37 nunca, 28 rara vez, 37 ocasionalmente, 13 frecuentemente, 27 siempre), autoeficacia (promedio 3,02) y cultura organizacional (5 no existe, 31 débil, 70 en consolidación, 36 consolidada). Sobre formación complementaria, 25 nunca, 54 una vez y 63 varias veces.

El análisis combinó enfoques cuantitativo y cualitativo. Se calcularon frecuencias y porcentajes para ítems cerrados, representados en tablas y gráficos. Las respuestas abiertas (118 sobre deficiencias, 120 sobre mejoras) se procesaron mediante análisis temático, identificando categorías como: falta de simulaciones y cyber ranges, necesidad de actualización curricular, fortalecimiento de cultura institucional, mejora en infraestructura, articulación interinstitucional, controles sobre redes sociales y lineamientos obligatorios en cursos de ascenso. La triangulación de hallazgos con la revisión documental y la matriz DOFA generó recomendaciones alineadas con NIST CSF 2.0, NICE e ISO/IEC 27035,

incluyendo rutas formativas por rol, ejercicios red team vs. blue team, implementación de cyber ranges y ajustes doctrinales.

Las limitaciones incluyen el muestreo no probabilístico, posible sesgo de autoselección y heterogeneidad del perfil "otro", que restringen la generalización. El autorreporte introduce sesgos de percepción, mitigados mediante triangulación con fuentes normativas y cualitativas, y reporte transparente del número de respuestas válidas por ítem.

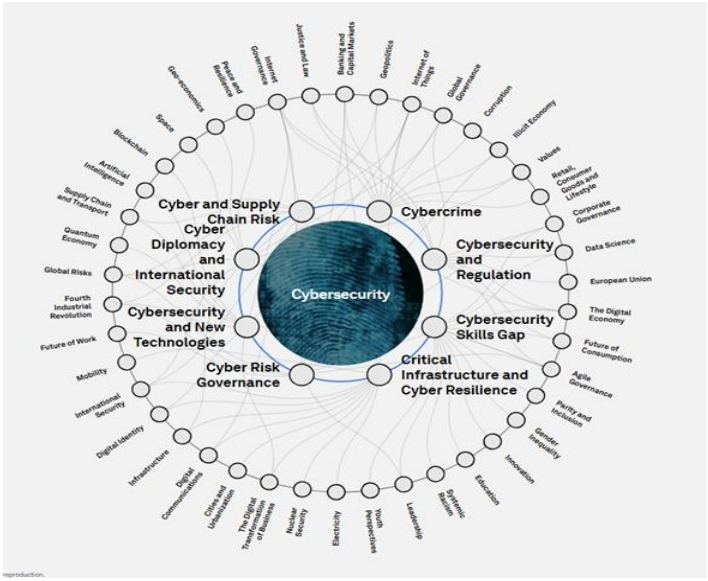
## Análisis de las deficiencias en los programas de formación y capacitación en ciberdefensa del Ejército Nacional

Hoy en día, el ciberespacio emerge como un dominio estratégico clave, pero trae consigo amenazas y vulnerabilidades inéditas para los estados. El CONPES 3701 (2011) define la ciberseguridad como la capacidad del Estado para minimizar riesgos ante amenazas cibernéticas, y la ciberdefensa como la habilidad para prevenir y contrarrestar incidentes que atenten contra la soberanía nacional. Estas definiciones subrayan que proteger la seguridad digital de la sociedad y defender la soberanía son prioridades absolutas (CONPES 3701, 2011).

No obstante, el CONPES alerta sobre graves debilidades en las capacidades estatales actuales, destacando la ausencia de una estrategia nacional integral contra ciberataques. En esencia, hay falencias institucionales significativas para enfrentar riesgos que van desde la integridad de sistemas críticos hasta la estabilidad política.

Un ejemplo ilustrativo son los ataques masivos reportados en 2024, donde casi el 90% de las organizaciones sufrieron algún ciberataque, y solo dos de cada diez empresas estaban preparadas para responder (El País, 2023). Esto evidencia la urgencia de fortalecer las defensas cibernéticas a nivel nacional.

**Figura 1.** *Mapa conceptual global sobre la ciberseguridad*




Nota. Fuente: (World Economic Forum, 2025)

El mapa conceptual sobre ciberseguridad posiciona "Cybersecurity" como eje central, interconectado con dominios estratégicos, técnicos, regulatorios y sociales. Convergen ocho categorías principales: Cybercrime, Cybersecurity and Regulation, Cybersecurity Skills Gap, Critical Infrastructure and Cyber Resilience, Cyber Risk Governance, Cybersecurity and New Technologies, Cyber Diplomacy and International Security, y Cyber and Supply Chain Risk (World Economic Forum, 2025).

Por ejemplo, Cybercrime se vincula a crimen financiero, robo de datos, protección de menores en línea y gobernanza de internet. Cybersecurity and Regulation asocia IA,

economía digital y protección del consumidor, destacando necesidades normativas éticas. Cybersecurity Skills Gap revela escasez de profesionales, relacionada con educación y economías digitales. Critical Infrastructure and Cyber Resilience enfatiza vulnerabilidades en energía, salud, transporte y telecomunicaciones. Cyber Risk Governance centra en gestión de riesgos, cumplimiento y transparencia para gobernanza efectiva.

Cybersecurity and New Technologies aborda blockchain, IA, computación cuántica e IoT, ampliando riesgos. Cyber Diplomacy and International Security promueve cooperación global, disuasión y normas contra conflictos híbridos como espionaje digital. Cyber and Supply Chain Risk identifica exposiciones en cadenas digitalizadas de defensa y manufactura (World Economic Forum, 2025).

Globalmente, incidencias cibernéticas aumentaron 75%, con déficit de 4 millones de profesionales (CCIT, 2024). Esto evidencia brechas en gobernanza, coordinación y capacitación, dejando vulnerabilidades abiertas. En el ámbito militar colombiano, las Fuerzas Armadas deben proteger soberanía digital (Art. 217, Constitución Política de Colombia, 1991), colaborando con OTAN para equipos y personal (Peña, 2023). Sin embargo, no se traduce en defensa cibernética efectiva para el Ejército Nacional.

En la encuesta (Sección 4), la pregunta sobre deficiencias en formación de oficiales analizó 118 respuestas cualitativamente, revelando problemáticas estructurales, metodológicas y organizacionales. Principalmente, falta capacitación especializada y continua: muchos oficiales sin formación o limitada a charlas ocasionales sin actualización, agravada por escaso tiempo para competencias técnicas y estratégicas.

Se menciona énfasis teórico excesivo y carencia de prácticas reales, sin simulaciones, cyber ranges o escenarios de guerra cibernética para respuestas efectivas (Balto et al., 2023).

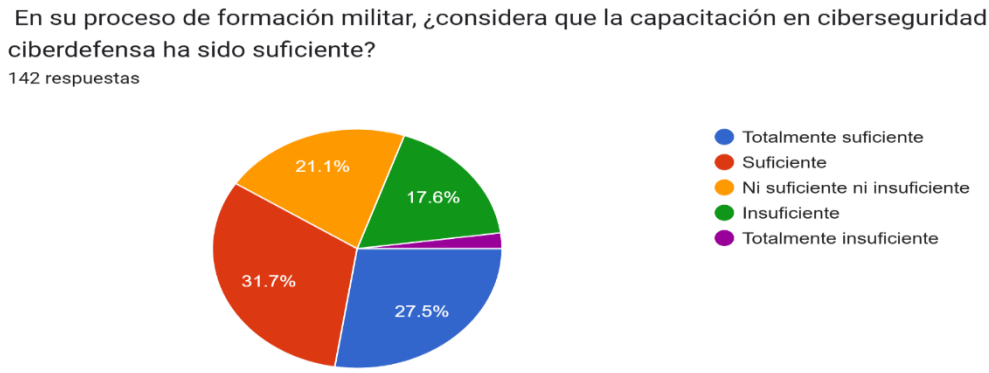
Ausencia de programas diferenciados por roles (estratégicos, técnicos, inteligencia); formación genérica. Debilidad cultural: baja sensibilización, mal uso de redes sociales y percepción de tema exclusivo de especialistas en comunicaciones o inteligencia. Finalmente, insuficiente infraestructura: falta laboratorios y herramientas modernas para entrenamiento práctico (Calderón, 2025). Escasez de expertos y rutas de desarrollo, dificultando capacidades sostenibles. Urge transformación con pedagogías prácticas, recursos adecuados y planes profesionales para fortalecer competencias ante desafíos cibernéticos (Cubeiro, 2020).

**Deficiencias en la capacitación en ciberseguridad**

La percepción del personal militar confirma las brechas formativas descritas en la literatura. Al preguntarles En su proceso de formación militar, ¿considera que la capacitación en ciberseguridad y ciberdefensa ha sido suficiente?, las respuestas revelan un panorama preocupante: solo un 17,6 % considera la formación totalmente suficiente y un 21,1 % la califica como suficiente, mientras que un 31,7 % la evalúa como ni suficiente ni insuficiente y un 27,5 % como insuficiente. Este resultado indica que más de la mitad del personal percibe que su preparación no es adecuada frente a los retos actuales del ciberespacio. Tales datos reflejan las carencias señaladas por Durán (2024) y Calderón (2025), quienes advierten sobre la limitada preparación en protección de infraestructuras críticas, la ausencia de personal especializado y la escasez de programas formativos avanzados. La Figura 1 ilustra gráficamente esta distribución, evidenciando la necesidad de

replantear los programas de capacitación y fortalecer las competencias del talento humano militar en el ámbito de la ciberdefensa (Calderón, 2025).

**Figura 2.** *Resultado de la Encuesta*




Fuente: elaboración propia con base en resultados del cuestionario aplicado al personal militar (2025).

Los resultados indican que el 59,2% del personal militar considera inadecuada su formación en ciberseguridad para enfrentar desafíos actuales, confirmando observaciones de Durán (2024) y Calderón (2025) sobre escasez de programas especializados, falta de capital humano capacitado y debilidades institucionales técnicas. La Figura 2 ilustra esta distribución, urgencia de revisar programas y fortalecer competencias en ciberdefensa.

Ausencia de especialistas y gestión inadecuada de RRHH agravan brechas competenciales. Globalmente, brecha de 4 millones de expertos (KPMG, 2024); solo 20% de organizaciones preparadas para incidentes. En ámbito castrense, limitada oferta formativa mantiene cibercultura incipiente. Oviedo (2023) enfatiza fomentar capacitación sostenida: "la capacitación en cibercultura está al alcance de todo el personal militar y por tal motivo de fomentarse a corto mediano y largo plazo" (p. XX). Ejército explora aprendizaje virtual y sensibilización, pero fragmentarias y voluntarias. Fonseca (2023)

propone capacitar oficiales, suboficiales y civiles en cibercultura para cultura digital sostenible.

Estratégicamente, Política Nacional de Seguridad Digital (CONPES 3854) promueve comportamientos responsables (Consejo Nacional de Política Económica y Social [CONPES], 2016), pero Ejército carece de sistema articulador de cursos, certificaciones y ejercicios en carrera militar. Genera vacíos técnicos-operacionales; Durán (2024) advierte vacíos organizacionales en formación de capital humano para sistemas de defensa cibernética. Capacitación no a altura de amenazas, creando carencias clave (Durán, 2024).

### Evaluación de la Falta de Integración Estratégica

Falta integración entre políticas nacionales de ciberseguridad y capacidades militares de ciberdefensa. CONPES 3701 recomendó instancias coordinadoras (comisión intersectorial, grupo respuesta, comando conjunto), pero persiste baja articulación y ausencia de estrategia consolidada (CONPES, 2011). Iniciativas dispersas (unidades por fuerza, proyectos MinTIC) resultan fragmentarias y reactivas (Durán, 2024).

Retraso en integración con operaciones militares: carencia coordinación para proteger infraestructuras críticas (comandos, logística, comunicaciones) con políticas civiles. Estudios urgen cooperación internacional y enfoque multisectorial, sin ejercicios conjuntos periódicos. Peña Suárez (2023) resalta colaboración FF.MM. con aliados para soberanía digital. Inexistencia mando unificado y protocolos limita respuestas.

Doctrinalmente, ciberdefensa como parte espectro guerra, pero vista complementaria (Osorio et al., 2017). Falta doctrina conjunta actualizada refleja vacíos

organizacionales (Durán, 2024). Sin estrategia unificada integrando ciberdefensa con seguridad convencional y políticas nacionales, capacidades Ejército subutilizadas y fragmentadas (Cáceres, 2022).

**Deficiencias en los programas de formación y capacitación**

En paralelo con lo anterior, los diferentes programas institucionales que presentan fallas sustanciales, Las academias y las escuelas castrenses no disponen aún de currículos amplios en ciberseguridad que abordan competencias técnicas, análisis de amenazas ni respuestas a incidentes. Montañez (2022) constató que las FFMM proyectan necesidades digitales, pero carecen de una formación reglada adecuada, por lo que los cadetes solo adquieren conocimientos básicos estándares. En el nivel de Postgrado, la recién activación o creación de la maestría de ciberseguridad y ciberdefensa en la ESDEG es un avance significativo, pero esto requiere también incluir ciberseguridad en otros programas como pregrados, entrenamientos regulares y especializaciones técnicas.

Las carencias metodológicas y logísticas agravan el problema. Duran (2024) destaca que los actuales cursos para oficiales enfocados en tecnologías sueles ser genéricos y no profundizan en campos claves como la inteligencia cibernética o contramedidas digitales. Además de esto, la infraestructura de laboratorios y simuladores de ataques cibernéticos en el Ejército Nacional es prácticamente inexistente. Por otra parte, el enfoque en la formación es mayoritariamente conceptual; faltan entrenamientos prácticos continuos (ejercicios de guerra cibernética, "red teaming" internos, etc.). Este panorama coincide con el contexto global:  un informe señala que 8 de cada 10 empresas sufrieron brechas y aun así la fuerza

de trabajo aumentará solo en un 32% en la próxima década, evidenciando a urgencia de programas eficientes (KPMG, 2024).

El CONPES 3854 (2016) identifica la necesidad de capacitar al personal en comportamientos seguros, pero en el Ejército esta capacitación se ha visto de forma general y como opcional o por vía de charlas ocasionales, mas no por la necesidad. El estudio de Oviedo (2023) nos propone un sistema de cibercultura continuo: en el cual se basa en un modelo de capacitación virtual que permita al personal de todas las jerarquías internalizar las buenas prácticas y afrontar la digitalización organizacional. De forma critica, la evidencia reunida muestra que falta programas de capacitación formalizados y actualizados, tanto en el nivel básico como para el avanzado, dejando al Ejército dependiente de iniciativas AD-HOC. Solo un plan de estudios sistemáticos (por ejemplo, incorporación en el marco DigComp2.2 o NICE en los cursos militares podrá subsanar estas deficiencias (Fonseca, 2023).

**Estudio de marcos de referencia y normativos internacionales.**

En el ambiente internaciones existen diversos marcos de referencia y normas para guiar la ciberseguridad, que pueden orientas al Ejército en la modernización y actualización de su estrategia. Como ejemplo, el marco de ciberseguridad del NIST (EE. UU) es voluntario, pero ampliamente reconocido: el cual ofrece un enfoque basado en cinco funciones (identificar, proteger, detectar, responder, recuperar) para la gestión del riesgo cibernético corporativo (Federal Trade Commission, 2024). Según su descripción oficial, este marco "ayuda a los negocios de todo tamaño a comprender mejor sus riesgos de ciberseguridad,

administrar y reducir sus riesgos y proteger sus redes y datos. El Ejército podría optar por este modelo para estructurar sus protocolos de seguridad y medidas de protección digital. De igual modo, el Cybersecurity Workforce Framework (NICE) del propio NIST (Estados Unidos) establece los estándares de competencia y roles para profesionales, el esquema menciona al analiza la carencia de expertos militares (NIST, 2017).

**Figura 3.** *Categorías de roles laborales del marco NICE*


Nota. Fuente: (NIST, 2017).

El marco NICE, desarrollado por el NIST, organiza las competencias en ciberseguridad en siete áreas clave: Oversight & Governance, que abarca la supervisión estratégica y el cumplimiento normativo; Design & Development, centrada en el diseño y creación de soluciones tecnológicas seguras; Implementation & Operation, dedicada a la operación y mantenimiento de sistemas protegidos; Protection & Defense, enfocada en la defensa activa contra amenazas; Investigation, orientada a la respuesta ante incidentes y análisis forense digital; Cyberspace Intelligence, que trata la recolección y análisis de

inteligencia en el ciberespacio; y Cyberspace Effects, dirigida a la ejecución de operaciones ofensivas o disruptivas en el entorno digital.

Este marco sirve como guía para la planificación del TH en las organizaciones públicas, privadas y sobre todo militares, alineando los perfiles profesionales con las necesidades actuales del sistema de ciberseguridad.

Al respecto y entre otros referentes útiles es el Marco Europeo DigComp2.2, el cual nos data sobre las competencias digitales. En la experiencia Colombia mas reciente, se ha propuesto su uso para medir y desarrollar las habilidades digitales en los mandos militares (Vera & Navarro, 2022). La inclusión de este marco en la Escuela Militar de Cadetes (CASD) se ha planteado para proyectar los conocimientos como parte de su forma básica (Fonseca, 2023).

A nivel de política, la Unión Europea y la OTAN han difundido documentos como la estrategia global de ciberdefensa de la OTAN, que ha enfatizado en la defensa colectiva contra los ataques cibernéticos. De igual forma, dentro de Latinoamérica organizaciones como lo es la OEA promueve principios de cooperación digital y la protección de las infraestructuras críticas. Es importante resaltar que la política Nacional de Seguridad digital de Colombia (CONPES 3854) ha incorporado lineamientos globales al hablar de los riesgos digitales intersectoriales. Sin embargo, al colocar en práctica estos estándares se requiere adaptaciones concretas: el Ejército Nacional debe alinear sus normas internas (doctrina, reglamentos, manuales) con estas guías internacionales y de esta forma adecuar los modelos de gestión de riesgos civiles al ámbito castrense (CONPES, 2016).

Por último, los estudios académicos locales abogan por adoptar estos Marcos en los programas de formación. Durán (2024) destaca la importancia de la *gestión de proyectos*

*tecnológicos* y el diseño de sistemas digitales basados en estándares NIST para fortalecer la ciberdefensa. Por tanto, los modelos internacionales representan fuentes de mejores prácticas: su estudio y transferencia (por ejemplo, la experiencia de Estonia en la integración Cívico-militar o la sistemática De Israel) puede enriquecer la estrategia colombiana.

## Mejores prácticas internacionales en formación y capacitación en ciberdefensa

Para que el Ejército Nacional de Colombia pueda adoptar y así mismo adaptar estos modelos con total éxito, es necesario contextualizarlos a las condiciones operativas y culturales. Un paso inicial es incorporar por ejemplo las competencias definidas por DigComp y NICE en la formación militar. La edición reciente de la revista *ciberespacio, tecnología e innovación* presentó un proyecto para que la Escuela Militar de Cadetes desarrolle competencias digitales de acuerdo con DigComp2.2, enfatizando la formación en áreas de ciberseguridad como parte de su currículo básico.

Paralelo con esto, Duran (2024) propone en su investigación un plan institucional de formación de oficiales que incluya cursos avanzados en gerencia de proyectos tecnológicos y diseño de sistemas de defensa digital, esto con el fin de reforzar los lineamientos de los CONPES 3701 y 3975 (Departamento Nacional de Planeación, 2019). Estas iniciativas ilustran como marcos foráneos (europeos y estadounidenses) pueden traducirse a programas concretos en la Escuela Militar de Cadetes o en la misma ESDEG.

Además, la cultura organizacional del Ejército debe evolucionar hacia una mentalidad de ciberseguridad. Esto implica aprender de los casos internacionales: Por

ejemplo, adaptar ejercicios combinados de tipo "mesa redonda" con los aliados (inspirados en ejercicios de la OTAN) o impulsar simulacros nacionales de ataques cibernéticos sobre las instalaciones militares. También es fundamental adaptar las normas existentes: la doctrina militar conjunta debe actualizarse para incluir capítulos de guerra cibernética y asignar roles específicos a unidades del Ejército Nacional, (designar oficiales que sirvan de enlace con el comando cibernético). Estudios recientes resaltan además que la educación continua; la propuesta de Oviedo (2023) de un sistema de capacitación virtual es un buen ejemplo de cómo mantener al personal actualizado en tecnologías emergentes, algo esencial dado el ritmo al cual evolucionan las amenazas.

Finalmente, la adaptación debe pasar por la integración institucional: los marcos internacionales no solo son el conjunto de técnicas, sino que también filosofías organizacionales. El Ejercito debe aprender a coordinarse con entidades civiles como (MinTIC, MDN, PONAL) bajo un mismo plano, tal como sugieren los lineamientos internacionales, en síntesis, la mejor estrategia es tomar las guías globales ("qué" hacer) y convertirlas en procedimientos, currículos y estructuras de ejercicios propios para el ejército. Solo de esta forma se podrá cerrar las brechas detectadas: formando un capital humano competente, integrado en esfuerzos sectoriales y actualizando la doctrina militar, de manera que el Ejército Nacional se encuentra preparado para afrontar todas las dimensiones del ciberespacio en el cumplimiento de su misión constitucional.

## Marcos y estándares internacionales aplicables

El ecosistema para estructurar la formación en ciberdefensa de oficiales se basa en tres marcos complementarios. Primero, el NIST Cybersecurity Framework (CSF) 2.0 (2024) organiza la gestión de riesgos en seis funciones: Govern, Identify, Protect, Detect, Respond y Recover, con outcomes y prácticas por categorías. Su enfoque sector-agnóstico y énfasis en Govern alinean gobierno, estrategia y operaciones, ideal para estandarizar riesgos en redes militares, defensas por capas y medición de madurez.

En práctica, la guía SP 1299 facilita adopción modular, permitiendo perfiles personalizados (ej. continuidad C2, protección táctica) y métricas de mejora. Favorece coordinación interinstitucional, pero limita al no prescribir controles detallados ni certificaciones de personal, requiriendo integración con SP 800-53 y políticas de talento para cerrar ciclo gobierno-personas-tecnología.

Segundo, el NICE Cybersecurity Workforce Framework ofrece lenguaje común con categorías, 52 roles de trabajo y declaraciones de tareas (T), conocimientos (K) y habilidades (S). Permite diseñar currículos, alinear cursos, descripciones de cargo y evaluaciones, mapeando progresión de oficiales (ej. desde Cyber Defense Analyst a forense o inteligencia).

Ejemplo: DoD EE.UU. vía programa 8140.03 (2023) adopta enfoque rol-basado con DCWF (derivado NICE), exigiendo evidencias y matrices de cualificación por rol, demostrando viabilidad en contextos castrenses escalables.

Finalmente, la pregunta de encuesta "¿Se han incluido simulaciones prácticas o ejercicios de guerra cibernética durante su formación?" mide incorporación de actividades

prácticas esenciales. La teoría sola es insuficiente; simulaciones desarrollan competencias reales, evaluando preparación operativa e institucional ante incidentes, replicando amenazas para respuestas efectivas.

Estos marcos integrados promueven formación holística: estratégica (NIST), competencial (NICE) y práctica (simulaciones), cerrando brechas en preparación militar.

**Figura 4.** *Resultado de la Encuesta*

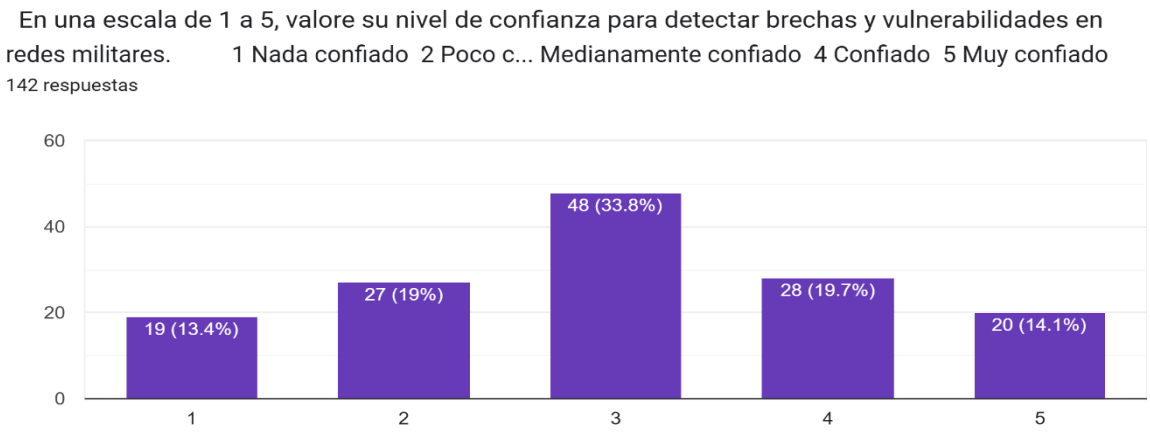

Fuente: elaboración propia con base en resultados del cuestionario aplicado al personal militar (2025).

Los resultados revelan una clara insuficiencia en la incorporación de prácticas dentro de los programas de formación. Solo un 19% de los encuestados afirmó que siempre ha participado en simulaciones, y un 9,2% indicó que esto ocurre frecuentemente. En contraste, el 26,1% señaló que dichas actividades se realizan ocasionalmente, mientras que un porcentaje igual (26,1%) manifestó que nunca se han llevado a cabo. Adicionalmente, el 19,7% respondió que estas prácticas se desarrollan rara vez. Estos datos evidencian que la

mayoría del personal militar recibe una formación limitada en ejercicios prácticos, lo que representa un obstáculo significativo para fortalecer las capacidades de respuesta ante incidentes cibernéticos y refleja una brecha importante entre la formación actual y las necesidades estratégicas del entorno digital.

Además del análisis sobre la frecuencia de ejercicios prácticos, se evaluó el nivel de confianza del personal en sus propias competencias técnicas mediante la pregunta: En una escala de 1 a 5, valore su nivel de confianza para detectar brechas y vulnerabilidades en redes militares.

**Figura 5**. *Resultado de la Encuesta*



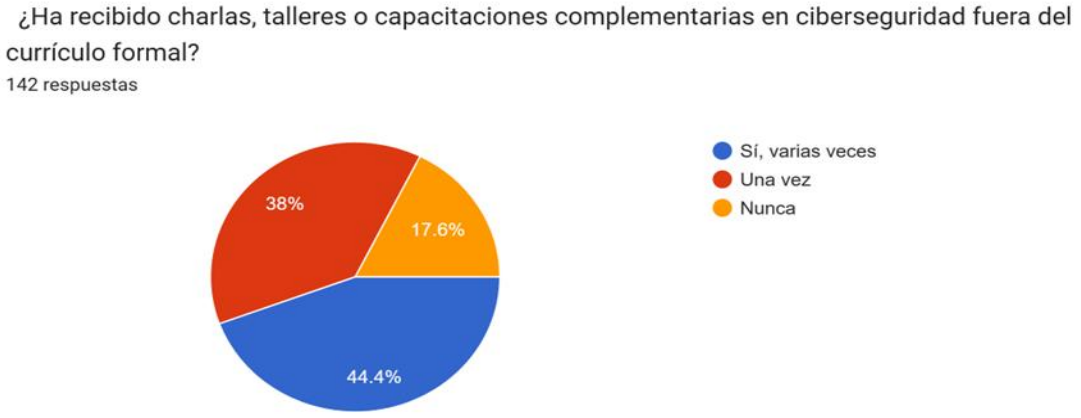

Fuente: Elaboración propia con base en resultados del cuestionario aplicado al personal militar (2025).

Los resultados obtenidos en la encuesta sobre el nivel de confianza del personal militar para detectar brechas y vulnerabilidades en redes muestran un panorama intermedio con importantes oportunidades de mejora. La media general fue de 3,02, lo que indica un nivel de confianza moderado. El 33,8% de los encuestados se considera medianamente

confiado, mientras que un 19,7% manifiesta estar confiado y un 14,1% se declara muy confiado. En contraste, un 19% indicó sentirse poco confiado y un 13,4% reconoció no tener confianza en sus capacidades. Este resultado evidencia que, aunque existe una base de conocimientos en ciberseguridad, aún no se alcanzan niveles óptimos de autoeficacia técnica en la mayoría del personal, lo que refuerza la necesidad de fortalecer los programas de entrenamiento práctico, las certificaciones técnicas y los escenarios simulados que mejoren la capacidad operativa frente a incidentes reales.

La incorporación de espacios de formación complementaria, como charlas, talleres o capacitaciones fuera del currículo formal, es un elemento clave para fortalecer las competencias en ciberseguridad y ciberdefensa del personal militar. Estos espacios permiten actualizar conocimientos, adquirir habilidades prácticas y fomentar una cultura organizacional orientada a la protección del ciberespacio, complementando la instrucción recibida en los programas formales y adaptándola a las dinámicas cambiantes de las amenazas digitales (Ver figura 6).

**Figura 6.** *Resultado de la Encuesta*




Fuente: Elaboración propia con base en resultados del cuestionario aplicado al personal militar (2025).

Los resultados de la encuesta muestran una participación significativa en este tipo de actividades adicionales: el 44,4% de los encuestados afirmó haber recibido charlas o capacitaciones en varias ocasiones, mientras que un 38% indicó haber participado solo una vez. Sin embargo, un 17,6% manifestó no haber recibido nunca formación complementaria en esta materia. Estos datos reflejan que, aunque existe un esfuerzo por ofrecer espacios adicionales de aprendizaje, aún persiste un porcentaje considerable de personal sin acceso a este tipo de oportunidades, lo que sugiere la necesidad de ampliar la cobertura y frecuencia de estas iniciativas para fortalecer las capacidades institucionales en ciberseguridad.

A partir del análisis de los resultados obtenidos en la encuesta aplicada al personal militar, sobre formación, prácticas, nivel de confianza y capacitación complementaria en ciberdefensa, se elaboró un análisis DOFA que sintetiza las principales fortalezas, debilidades, oportunidades y amenazas del Ejército Nacional en este ámbito. Este diagnóstico permite identificar brechas formativas y áreas estratégicas de mejora, orientando el diseño de acciones que fortalezcan las capacidades institucionales frente a los desafíos del ciberespacio.

**Tabla 1**. *Análisis DOFA – Formación en Ciberdefensa Militar*

| Fortalezas | Oportunidades |
|---|---|
| **1. Marco normativo sólido:** Documentos CONPES 3701 (2011), 3854 (2016) y 3995 (2020) establecen lineamientos claros para ciberseguridad y ciberdefensa, reconociendo la importancia de fortalecer el talento humano. Esto da respaldo legal y político a la incorporación de formación especializada en academias y escuelas militares. | **1. Cooperación internacional con la OTAN**: Posibilidad de acceder a programas de entrenamiento, ejercicios combinados y doctrinas consolidadas en ciberdefensa, como el "Locked Shields" del Centro de Excelencia en Ciberdefensa de Tallin, que permitiría capacitar a oficiales en escenarios de ciberataques simulados a gran escala. |
| **2. Creación de unidades especializadas:** Desde 2012 existe la Unidad de Ciberdefensa en las Fuerzas Militares, lo que facilita un canal institucional para implementar programas formativos estructurados y asignar roles operativos según el marco NICE. | **2. Acceso a marcos y estándares internacionales**: Disponibilidad de frameworks como NIST CSF 2.0, NICE y DigComp 2.2, que permiten diseñar currículos alineados con mejores prácticas globales y adaptarlos al contexto colombiano. |
| **3. Experiencia en operaciones conjuntas:** El Ejército cuenta con capacidades previas en coordinación interinstitucional y multinacional, lo | **3. Creciente oferta académica en ciberseguridad**: Apertura de programas de maestría y especialización en instituciones militares (ESDEG) y civiles, que |

| | |
|---|---|
| que facilita la integración de ciberdefensa con operaciones convencionales y de inteligencia. | pueden servir como fuente de actualización continua para el personal en servicio. |
| **4. Cultura de disciplina y jerarquía:** La estructura castrense favorece la implementación de programas formativos normados y obligatorios, asegurando cumplimiento y continuidad en los planes de capacitación. | **4. Incremento de cooperación regional**: Alianzas con países latinoamericanos con avances en ciberdefensa (Chile, Brasil) para compartir experiencias y protocolos de formación. |

| Debilidades | Amenazas |
|---|---|
| **1. Falta de infraestructura práctica:** Ausencia de laboratorios especializados, entornos de simulación y plataformas de "cyber range" para entrenar en condiciones reales de ataque y defensa. | **1. Escalada de ataques híbridos y cibernéticos**: Amenazas combinadas que afectan infraestructuras críticas militares y civiles, exigiendo respuestas más rápidas y especializadas. |
| **2. Formación fragmentada y genérica:** Los cursos actuales carecen de profundidad técnica en áreas clave (inteligencia cibernética, análisis forense avanzado, operaciones de defensa proactiva), lo que limita la efectividad operativa**.** | **2. Déficit global de talento en ciberseguridad**: Según ISC², hay una brecha mundial de más de 4 millones de profesionales, lo que intensifica la competencia por personal cualificado y dificulta retenerlo en el sector defensa. |
| **3. Escasa integración doctrinal:** La ciberdefensa aún no se reconoce plenamente como parte integral de la doctrina de guerra, lo que retrasa la actualización de manuales y protocolos. | **3. Dependencia de tecnología extranjera**: Vulnerabilidad ante restricciones, sanciones o discontinuidad en el suministro de hardware, software y servicios críticos. |
| **4. Carencia de rutas formativas claras:** No existe una malla curricular estandarizada por roles, basada en marcos como NICE, que permita el desarrollo progresivo de competencias desde cadetes hasta mandos superiores. | **4. Evolución acelerada de las amenazas**: El desarrollo de nuevas técnicas de ataque (uso de IA generativa, exploits zero-day) puede superar la capacidad de adaptación de los programas formativos actuales. |

**Fuente:** Elaboración propia con base en CONPES 3701 (2011), CONPES 3854 (2016), CONPES 3995 (2020), NIST (2024), NICE (2017), DigComp 2.2 (2022), Peña (2023), Durán (2024) y datos de la OTAN (2023).

El análisis DOFA revela fortalezas en la formación del Ejército: marco normativo claro, unidades especializadas y cooperación internacional. Oportunidades incluyen estándares globales (NIST CSF 2.0, NICE, DigComp 2.2) y alianzas regionales (Möller, 2023). Estos ayudan a superar debilidades como falta de infraestructura práctica, formación fragmentada e integración doctrinal insuficiente, ante amenazas híbridas y déficit global de talento. Estrategia prioritaria: actualizar currículos combinando funciones CSF 2.0 con roles NICE; invertir en simuladores y laboratorios para entrenamientos realistas; integrar ciberdefensa en doctrina militar; establecer rutas escalonadas desde básica a estratégica (NIST, 2024).

Así, se desarrollan competencias técnicas y estratégicas para proteger redes y responder a amenazas complejas.

Para el Ejército, definir rutas por rol (Operaciones de Defensa, Respuesta a Incidentes, Inteligencia Cibernética), enlazando cursos, ejercicios y certificaciones. Fortaleza de NICE: granularidad en gestión de talento; límite: no detalla procesos técnicos ni operativos, requiriendo integración con CSF 2.0, marcos de control y doctrina.

Este enfoque holístico aprovecha fortalezas y oportunidades para mitigar debilidades y amenazas, elevando resiliencia institucional.

***Experiencias de países líderes***

Estonia, tras ciberataques de 2007, implementó estrategia integral con infraestructura y formación especializada. Alberga el NATO CCDCOE (2008), centro de excelencia en ciberseguridad. Clave: ejercicio anual Locked Shields (desde 2010), simulando ataques masivos con equipos blue/red para desarrollar habilidades técnicas, estratégicas, gobernanza y comunicación (NATO, 2022).

Israel consolidó ecosistema cibernético vía Unit 8200, élite militar que forma líderes tech y defensa digital (Kruppa & Perry, 2024). Israel Cyber Campus (2022, Tel Aviv) ofrece entrenamiento avanzado con simuladores reales y docentes ex-inteligencia militar.

Integración regional: Baltic Defence College capacita oficiales de Estonia, Letonia y Lituania en seguridad estratégica. Ejercicios como Operation Saber Strike unen fuerzas EE.UU. y bálticas para interoperabilidad ante amenazas complejas.

Estas prácticas destacan formación práctica, ejercicios simulados y colaboración internacional como pilares para resiliencia cibernética.

## Estrategias para el fortalecimiento de los programas de formación y capacitación en ciberdefensa

El análisis cualitativo de 120 respuestas sobre estrategias para fortalecer capacitación y cultura de ciberseguridad revela consenso: incrementar formación continua, especializada y práctica, diferenciada por niveles jerárquicos y funciones. Se priorizan contenidos técnicos avanzados (análisis forense, gestión vulnerabilidades, detección intrusiones, ISO/IEC 27001), incluir ciberseguridad desde etapas iniciales y cursos de ascenso, más simulaciones realistas, ejercicios de guerra cibernética y escenarios híbridos para competencias operativas y respuesta a incidentes.

Además, urge fortalecer cultura organizacional: campañas permanentes de concientización, centros de entrenamiento con cyber ranges, actualización infraestructura tecnológica, cooperación OTAN, módulos en liderazgo estratégico, uso responsable de redes sociales y mecanismos de control-evaluación. Estas propuestas muestran disposición del personal a mejorar, con apoyo institucional.

Partiendo de capacidades actuales (Comando Apoyo Operacional Comunicaciones y Ciberdefensa, BRICC, Batallón Ciberdefensa), se propone integrar marcos internacionales: NIST Cybersecurity Framework, NICE Workforce Framework e ISO/IEC 27035 para competencias técnicas, roles operativos y procedimientos respuesta (ISO/IEC/IEEE, 2017).

Recomendaciones clave: invertir en cyber ranges y simuladores para ejercicios ofensivos-defensivos realistas (estilo Locked Shields OTAN); integrar doctrinalmente ciberdefensa en manuales, reglamentos y planeamiento. Establecer rutas formativas escalonadas: básicas de cibercultura (todo personal), certificaciones técnicas (especialistas)

y liderazgo estratégico (oficiales), asegurando continuidad y sostenibilidad desde táctico a estratégico.

Este enfoque transforma brechas en capacidades robustas, alineadas con estándares globales.

## Adaptación de estándares internacionales al contexto colombiano

La adaptación de estándares internacionales de ciberseguridad al contexto colombiano, y en particular a la estructura del Ejército Nacional, requiere un enfoque que armonice las mejores prácticas globales con las capacidades y funciones específicas de unidades como el Comando de Apoyo Operacional de Comunicaciones y Ciberdefensa (CAOCC), la Brigada de Interoperabilidad de Comunicaciones, Computación y Ciberdefensa (BRICC) y el Batallón de Ciberdefensa y Ciberseguridad**.** El NIST Cybersecurity Framework (CSF), con sus funciones de identificar, proteger, detectar, responder y recuperar, puede servir como guía para priorizar riesgos en redes críticas del Ejército, adaptando sus categorías y subcategorías a entornos operacionales militares. Esto implicaría mapear las funciones del CSF con procesos de mando y control, sistemas de comunicaciones y plataformas de interoperabilidad de combate, asegurando que la protección y respuesta se integren en los planes operacionales.

**Tabla 2.** *Roles NICE adaptados al Batallón de Ciberdefensa y Ciberseguridad con certificaciones y entrenamientos recomendados*

| **Área NICE (Categoría)** | **Rol adaptado al Ejército Nacional** | **Funciones clave en el contexto militar** | **Certificaciones y entrenamientos recomendados** |
|---|---|---|---|
| | Analista de Ciberdefensa | Monitoriza redes críticas militares, identifica intrusiones y coordina medidas defensivas. | CompTIA Security+, EC-Council CEH, Curso interno de monitoreo de redes tácticas. |

| | | | |
|---|---|---|---|
| **Protección y Defensa** | Especialista en Respuesta a Incidentes | Lidera la contención, erradicación y recuperación ante incidentes en sistemas de mando y control y plataformas operacionales. | GIAC Certified Incident Handler (GCIH), ISO/IEC 27035, entrenamiento OTAN en respuesta a incidentes. |
| | Administrador de Seguridad de Redes | Configura y mantiene dispositivos de seguridad, cortafuegos y segmentación en redes tácticas y estratégicas. | Cisco CCNA Security, Fortinet NSE 4-6, curso militar de seguridad perimetral. |
| **Investigación** | Analista Forense Digital | Recopila, preserva y analiza evidencias digitales tras incidentes cibernéticos contra infraestructura militar. | CHFI (Computer Hacking Forensic Investigator), GIAC GCFA, curso forense digital de la Escuela de Comunicaciones. |
| | Investigador de Amenazas | Identifica y documenta tácticas, técnicas y procedimientos (TTP) de adversarios estatales y no estatales. | Threat Intelligence Analyst (CTIA), MITRE ATT&CK training, análisis de inteligencia cibernética OTAN. |
| **Inteligencia en el Ciberespacio** | Analista de Inteligencia Cibernética | Procesa y analiza datos de ciberamenazas para apoyar la toma de decisiones operacionales. | GIAC Cyber Threat Intelligence (GCTI), análisis de inteligencia OTAN, curso de inteligencia militar aplicada. |
| | Operador de Reconocimiento en el Ciberespacio | Ejecuta operaciones de vigilancia y exploración digital para anticipar ataques. | OSINT Framework Training, Recon-ng, curso de recolección de inteligencia técnica. |
| **Diseño y Desarrollo** | Ingeniero de Seguridad | Diseña arquitecturas seguras para sistemas de mando y control, comunicaciones y armas inteligentes. | CISSP, SABSA Security Architecture, curso de arquitectura de ciberseguridad en sistemas militares. |
| | Especialista en Criptografía | Implementa soluciones criptográficas para proteger comunicaciones militares y datos clasificados. | EC-Council ECES (Encryption Specialist), curso de criptografía militar, Certificado en Criptografía Aplicada. |
| **Implementación y Operación** | Técnico de Soporte de Ciberseguridad | Instala, configura y mantiene sistemas seguros en zonas de operación. | CompTIA A+, CompTIA Security+, entrenamiento interno en despliegue de sistemas seguros. |
| | Operador de Guerra Electrónica Cibernética | Integra capacidades cibernéticas con operaciones de guerra electrónica en escenarios híbridos. | Curso de Guerra Electrónica del Ejército, GIAC GRID, entrenamiento combinado ciber-electrónico OTAN. |
| | Planificador de Operaciones Cibernéticas | Coordina operaciones ofensivas y defensivas en conjunto con otros componentes militares. | Certified Information Security Manager (CISM), planeamiento operacional OTAN, curso de estrategia cibernética militar. |

| | | | |
|---|---|---|---|
| | Especialista en Operaciones Ofensivas | Ejecuta acciones cibernéticas para degradar, negar o interrumpir capacidades adversarias. | Offensive Security Certified Professional (OSCP), GIAC Penetration Tester (GPEN), curso de operaciones cibernéticas ofensivas. |

**Fuente:** Elaboración propia con base en National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, NIST Special Publication 800-181 Rev. 1 (2020), y doctrina organizacional del Ejército Nacional de Colombia (Comando de Apoyo Operacional de Comunicaciones y Ciberdefensa, Batallón de Ciberdefensa y Ciberseguridad).

El NICE Cybersecurity Workforce Framework proporciona taxonomía de roles y competencias para integrar en el Batallón de Ciberdefensa y Ciberseguridad, definiendo perfiles en operaciones defensivas, ofensivas, inteligencia y respuesta a incidentes. En el Ejército colombiano, implica adaptar roles NICE a rangos militares y especialidades, estableciendo rutas de capacitación y certificación alineadas con progresión de carrera.
La ISO/IEC 27035, centrada en gestión de incidentes de seguridad de la información, aplica directamente a vigilancia y respuesta del CAOCC y BRICC, estandarizando protocolos para identificación, análisis, contención y recuperación ante amenazas.

Complementariamente, ISO/IEC 27001 ofrece marco para Sistema de Gestión de Seguridad de la Información (SGSI) militar, asegurando confidencialidad, integridad y disponibilidad en operaciones y administración.

Implementación enfrenta retos: escasez de personal especializado, adecuación doctrinal para transversalidad en seguridad nacional, restricciones presupuestales en simuladores, laboratorios y plataformas avanzadas. Culturalmente, urge promover cibercultura en todos niveles, superando visión técnica exclusiva.

Estrategia progresiva: iniciar pilotos en unidades como Batallón de Ciberdefensa, con procedimientos y métricas basados en NIST CSF e ISO/IEC 27035; expandir gradualmente, vinculando formación militar a certificaciones internacionales. Así, se consolida fuerza cibernética robusta, interoperable y alineada con prácticas globales.

***Fortalecimiento de la infraestructura y metodología de enseñanza***

El desarrollo de capacidades efectivas en ciberdefensa para el Ejército Nacional exige una infraestructura tecnológica especializada que permita la simulación y el entrenamiento en entornos controlados de alta fidelidad. La implementación de *cyber ranges* militares, laboratorios virtualizados y plataformas de simulación de ataques híbridos constituye un pilar para la formación práctica de oficiales y suboficiales, complementando la instrucción teórica. Estos entornos deben replicar redes tácticas y estratégicas, sistemas de mando y control, así como infraestructuras críticas militares, permitiendo la ejecución de ejercicios en tiempo real similares a los desarrollados por la OTAN, como *Locked Shields(Balto et al., 2023)*.

**Figura 7.** *cyber ranges*

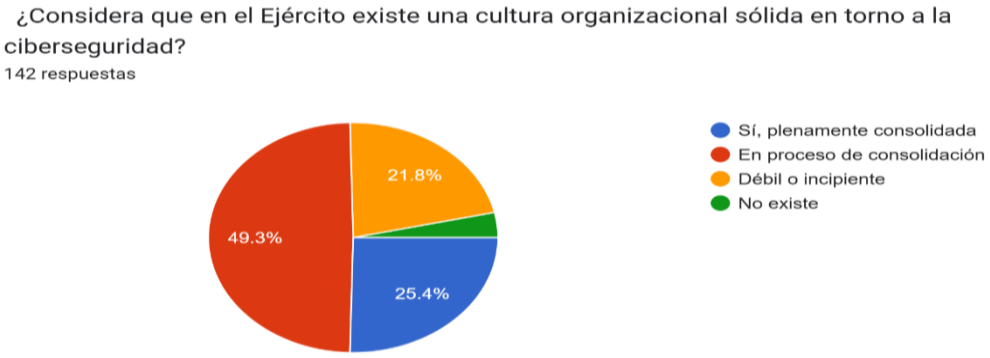

Fuente:(Balto et al., 2023)

Asimismo, la metodología de enseñanza debe migrar hacia modelos de instrucción basados en competencias, integrando el *NICE Cybersecurity Workforce Framework* para estructurar rutas formativas por roles y niveles de especialización. El aprendizaje adaptativo, el uso de *gamificación* para la resolución de incidentes y la incorporación de *war games* cibernéticos deben formar parte del currículo, fomentando habilidades técnicas, toma de decisiones estratégicas y trabajo en equipo bajo presión. La combinación de instrucción presencial, entrenamiento en línea y simulaciones inmersivas facilitará la capacitación continua y el desarrollo de capacidades escalables, asegurando la alineación con estándares internacionales como el NIST CSF 2.0 y la norma ISO/IEC 27035 para la gestión de incidentes.

### *Cultura organizacional y cooperación interinstitucional*

La cultura organizacional en torno a la ciberseguridad constituye un pilar fundamental para fortalecer las capacidades institucionales del Ejército Nacional frente a los desafíos del ciberespacio. Esta dimensión no solo implica la adopción de políticas y protocolos técnicos, sino también la generación de conciencia colectiva, hábitos seguros y coordinación efectiva entre las distintas unidades militares. Por ello, conocer la percepción del personal sobre el nivel de consolidación de dicha cultura resulta clave para identificar fortalezas, debilidades y oportunidades de mejora que orienten el diseño de estrategias institucionales.

**Figura 8**. *Resultados de la encuesta*




Fuente: Elaboración propia con base en resultados del cuestionario aplicado al personal militar (2025).

Los resultados muestran que el 49,3% de participantes ve la cultura organizacional en ciberseguridad en proceso de consolidación; 25,4% plenamente consolidada; 21,8% débil o incipiente; y 3,5% inexistente. Aunque hay avances, persisten retos en conciencia colectiva, adopción de prácticas y articulación sectorial defensa.

Consolidar capacidad robusta en ciberdefensa requiere cultura orientada a seguridad información y resiliencia cibernética, más allá de tecnología y formación. Implica integrar ciberdefensa en doctrina militar, comprendida en todos niveles mando-ejecución. Sensibilización continua, inclusión en programas liderazgo y reconocimiento prácticas internas fomentan responsabilidad digital (Cujabante et al., 2020).

Este enfoque cultural fortalece apropiación institucional, elevando resiliencia ante amenazas.

**Tabla 3.** *Tablero de acciones estratégicas y métricas – ciberdefensa*

| EJE ESTRATÉGICO | ACCIÓN ESTRATÉGICA | MÉTRICA DE ÉXITO | ESTADO |
|---|---|---|---|
| **Fortalecimiento de la infraestructura y metodología de enseñanza** | Implementar un cyber range militar para entrenamientos en tiempo real | Número de ejercicios anuales realizados y % de personal capacitado en simulaciones avanzadas | |
| | Integrar el marco NICE para estructurar rutas de formación por roles y niveles | % de planes de estudio alineados con NICE y satisfacción del personal capacitado | |
| | Adoptar metodologías de war gaming y gamificación en entrenamientos | Mejora del tiempo de respuesta y tasa de resolución en ejercicios prácticos | |
| **Cultura organizacional y cooperación interinstitucional** | Incluir la ciberdefensa en la doctrina y manuales operativos del Ejército Nacional | Incorporación documentada en doctrina oficial y grado de conocimiento medido en evaluaciones internas | |
| | Establecer convenios de cooperación técnica y de inteligencia con entidades nacionales e internacionales | Número de acuerdos firmados y cantidad de ejercicios o intercambios realizados al año | |
| | Implementar programas de sensibilización en ciberseguridad para todos los niveles jerárquicos | % de personal que completa cursos de sensibilización y reducción de incidentes por error humano | |

**Fuente:** Elaboración propia con base en *National Institute of Standards and Technology – NIST Cybersecurity Framework (CSF 2.0)*, *NICE Cybersecurity Workforce Framework*, *ISO/IEC 27001:2022*, *ISO/IEC 27035:2023* y doctrina institucional del Ejército Nacional de Colombia.

El tablero estratégico sirve como herramienta visual y operativa para monitorear avances en formación y capacidades de ciberdefensa. Estructurado en dos ejes: Fortalecimiento de infraestructura/metodología de enseñanza (implementación cyber range, integración NICE en rutas formativas, war gaming, actualización doctrinal) y Cultura organizacional/cooperación interinstitucional (convenios, programas sensibilización) (Rincón, 2022).

Cada acción incluye métricas cuantificables (porcentaje personal capacitado, tiempo respuesta simulaciones, acuerdos activos, reducción incidentes) y semáforo colores (verde, amarillo, rojo) para estado avance (Conpes 3701, 2011). Facilita a dirección identificar

áreas críticas, priorizar recursos y ajustes oportunos, asegurando efectividad programas (Bejarano, 2011).

Paralelamente, cooperación interinstitucional es clave contra amenazas transnacionales. Ejército debe fortalecer lazos con Comando Conjunto Cibernético, MinDefensa, Policía, CCP, industria tech nacional, y aliados como OTAN/OEA. Participación ejercicios conjuntos, intercambio inteligencia cibernética e interoperabilidad herramientas elevan respuesta a incidentes, preparación guerra híbrida y operaciones influencia cibernética (Osorio et al., 2017).

Este enfoque integrado transforma monitoreo en acción resiliente.

## Conclusiones

La evaluación revela deficiencias clave: falta de infraestructura simulada avanzada, cursos genéricos sin enfoque militar y baja integración de marcos doctrinales internacionales, limitando preparación ante amenazas complejas.

Encuesta confirma: 58,8% ve formación "insuficiente o neutra"; 45,8% simulaciones "rara vez/nunca" (solo 19% siempre); autoeficacia técnica baja (33,8% medianamente confiado en detectar vulnerabilidades, 14,1% muy alto); cultura organizacional en consolidación (49,3%) o débil (25,4%); capacitaciones complementarias irregulares (44,4% recibidas, 38% una vez, 17,6% nunca).

Ausencia de cyber ranges, war gaming y entrenamientos conjuntos reduce reacción, coordinación y decisiones bajo presión para proteger infraestructuras críticas.

En contraste, prácticas OTAN, NIST CSF y NICE ofrecen estandarización competencias, roles y riesgos. Adopción requiere adaptación a doctrina colombiana, recursos y operaciones.

Implementación exige enfoque integral: modernización tecnológica, rediseño curricular con rutas escalonadas por funciones críticas; fortalecer interoperabilidad con Fuerzas, agencias y aliados para cooperación interinstitucional/multinacional.

En síntesis, cerrar brechas une doctrina, infraestructura y talento para respuesta eficiente, anticipación amenazas. Plan robusto y continuo asegura resiliencia digital militar.

## Referencias

Balto, K. E., Yamin, M. M., Shalaginov, A., & Katt, B. (2023). Hybrid IoT Cyber Range. *Sensors*, *23*(6). https://doi.org/10.3390/s23063071

Bejarano, M. J. C. (2011). Nuevo Concepto de Ciberdefensa de la OTAN. *Instituto Español De Estudios Estrategicos*, *IEEE N° 09/2011*.

Cáceres. (2022). *Colombia, estrategia nacional en ciberseguridad y ciberdefensa. Ejército de Colombia*. https://www.airuniversity.af.edu/Portals/10/ASPJ_Spanish/Journals/Volume-29_Issue-1/2017_1_09_caceres_s.pdf#:~:text=No%20hay%20duda,Gobierno%20en%20L%C3%ADnea%20y%20de

Calderón, L. (2025). El ciberespacio como escenario de conflicto en el siglo XXI. ¿Hacia la militarización de la ciberseguridad? *Razón Crítica, (18), 1–21*. https://revistas.utadeo.edu.co/index.php/razoncritica/article/view/ciberespacio-como-escenario-conflicto-siglo-xxi

CCIT. (2024). Colombia sufrió 12.000 millones de intentos de ciberataques en 2023 según reporte de Fortinet. *FortiGuard Labs, El Laboratorio de Análisis e Inteligencia de Amenazas de Fortinet.* https://www.ccit.org.co/blog/colombia-sufrio-12-000-millones-de-intentos-de-ciberataques-en-2023-segun-reporte-de-fortinet/

CONPES. (2016). Política Nacional de Seguridad Digital. *CONPES 3854 - Política Nacional de Seguridad Digital*.

Conpes 3701. (2011). Documento Conpes 3701, Lineamientos de política para ciberseguridad y ciberdefensa. *Lineamientos De Política Para Ciberseguridad Y Ciberdefensa*.

Cujabante, V. X. A., Bahamón, J. M. L., Prieto, V. J. C., & Quiroga, A. 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). https://doi.org/10.21830/19006586.588

Departamento Nacional de Planeación. (2019). Documento Conpes 3975: Politica Nacional Para La Transformacion Digital e Inteligencia Artificial. In *Consejo Nacional de Politica Economica y Social - Republica de Colombia*.

Durán, C. G. M. (2024). Proyecto de formación de oficiales en gerencia tecnológica y diseño de sistemas digitales para la ciberdefensa. *Revista Ciberespacio, Tecnología e Innovación*, *3*(5), 59–88. https://doi.org/10.25062/2955-0270.4861

Federal Trade Commission. (2024). *Marco de ciberseguridad del NIST. Comisión Federal de Comercio.* https://www.ftc.gov/es/guia-para-negocios/protegiendo-pequenos-negocios/ciberseguridad/marco-ciberseguridad-nist#:~:text=de%20Comercio%20de

Fonseca, O. T. L. (2023). Editorial. La innovación en la ciberseguridad y ciberdefensa en escenarios complejos. *Revista Ciberespacio, Tecnología e Innovación*, *2*(4), 103–104. https://doi.org/10.25062/2955-0270.4819

ISO/IEC/IEEE. (2017). ISO/IEC/IEEE 12207:2017. *ISO/IEC/IEEE 12207:2017*, *1*.

KPMG. (2024). *Consideraciones de ciberseguridad 2024: prioridades para los CISO en inteligencia artificial, privacidad y confianza digital.* . https://kpmg.com/co/es/home/insights/2024/03/consideraciones-en-ciberseguridad-2024.html#:~:text=M%C3%A1s%20que%20nunca%2C%20los%20clientes,y%20de%20gobernanza%20(ESG).

Kruppa, & Perry. (2024). *Silicon Valley's hot talent pipeline is an Israeli Army unit: Unit 8200 has become an incubator for cybersecurity startups defending the world's biggest companies against hackers. The Wall Street Journal.* https://www.wsj.com/tech/silicon-valleys-hot-talent-pipeline-is-an-israeli-army-unit-e8368b4d?utm

Möller, D. P. F. (2023). NIST Cybersecurity Framework and MITRE Cybersecurity Criteria. In *Advances in Information Security* (Vol. 103). https://doi.org/10.1007/978-3-031-26845-8_5

NATO. (2022). *Cooperative Cyber Defence Centre of Excellence. Locked Shields.* https://ccdcoe.org/locked-shields

NIST. (2017). NIST Special Publication 800-181: National initiative for cybersecurity education (NICE) cybersecurity workforce framework. *National Institute of Standards and Technology (NIST), November*.

NIST. (2024). *Releases First 3 Finalized Post-Quantum Encryption Standards*. https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-

standards#:~:text=NIST%C2%A0announced%20its%20selection%20of%20four,is%20planned%20for%20late%202024

Osorio, L. A., Lorduy, L. G., Amaya, H. L. M., & Arenas, M. T. (2017). Ciberseguridad y ciberdefensa: pilares fundamentales de la seguridad y defensa nacional. *Revista de Las Fuerzas Armadas*, *241*. https://doi.org/10.25062/0120-0631.823

Peña, suarez, J. stiven. (2023). Ciberseguridad, un desafío para las Fuerzas Militares colombianas en la era digital. *Perspectivas En Inteligencia*, *15*(24), 333–359. https://doi.org/10.47961/2145194X.628

Politica Nacional de Seguridad Digital. (2016). CONPES 3854. *Consejo Nacional de Politica Económica y Social.*, *53*(9).

Rincón, G. M. F. (2022). Los factores armados de inestabilidad frente a la ciberseguridad y la ciberdefensa nacional. *Revista Ciberespacio, Tecnología e Innovación*, *1*(1). https://doi.org/10.25062/2955-0270.4768

Vera, B., & Navarro, G. (2022). Riesgos de la aceleración digital: una mirada desde el Marco DIGCOMP2.2 y los derechos digitales de la ciudadana. *Anuario ThinkEPI*, *16*. https://doi.org/10.3145/thinkepi.2022.e16a19

World Economic Forum. (2025). *Cybersecurity. Curated by Carnegie Mellon University, in collaboration with Matthew Butkovic. CERT Division, Software Engineering Institute.* https://intelligence.weforum.org/topics/a1Gb00000015LbsEAE?tab=publications

---

# ANEXOS

## Encuesta 143 respuestas

**https://docs.google.com/forms/d/e/1FAIpQLSdcsbbQrGkcnUsBbxolbqSHPj7cIiqobOUhGA4zOAsuTO7oYg/viewform?usp=header**

---