La ciberseguridad un enfoque de aprendizaje, desde el rol del suboficial del Ejército Nacional de Colombia

Cybersecurity a Learning approach from the role of a non-commissioned officer of the Colombian National Army

Recibido: 27 de julio de 2023
Aceptado: 24 de agosto de 2023
DOI: 10.22517/25393812.25519
pp. 190-209

Como citar este artículo APA7:
Rivera, L. y Hernández, S. (2023). La ciberseguridad un enfoque de aprendizaje, desde el rol del suboficial del Ejército Nacional de Colombia. Revista Miradas 18(2) , 190-209.

Lina María Rivera Alturo*
lmrivera18@gmail.com
Sussy Alejandra Hernández García**
trabajosocialsussy@gmail.com

Revista de investigación
miradas
ISNN Digital N° 2539-3812
ISNN Impreso N° 0122994X
Universidad Tecnológica de Pereira
Facultad de Ciencias de la Educación

* Docente hora catedra - Escuela Militar de Suboficiales "Sargento Inocencio Chincá" - Grupo de investigación INTEMIL - Nilo, Cundinamarca – ORCID: 0009-0008-6695-679X.

** Docente hora catedra - Escuela Militar de Suboficiales "Sargento Inocencio Chincá" - Grupo de investigación INTEMIL - Nilo, Cundinamarca – ORCID: 0000-0002-7819-6459

Resumen

El rol docente en una asignatura como lo es la seguridad informática es un reto desde muchas perspectivas, teniendo en cuenta la particularidad de los alumnos al tener incidencia en las siguientes generaciones, siendo los encargados de velar por la seguridad de la nación; situación que atenúa los distintos lineamientos de alta exigencia que tiene el Ejército Nacional de Colombia. Todo ello, para generar modelos de aprendizaje acordes a las garantías necesarias que busquen un balance de lo esperado en la práctica a partir de un tiempo real, el cual posibilite impartir detalles rigurosos que se encuentren enlazados a la información, recursos y acompañamiento acorde. Generando un despliegue de abundancia frente a resultados óptimos para cumplir con los procesos y tareas predispuestas por el personal de mando superior que se encuentra implicado en la ciberdefensa de la seguridad nacional, la cual es reconocida como un área de operación para el suboficial.[1]

Palabras clave: Ciberseguridad, ciberdefensa, rol docente, proceso de enseñanza - aprendizaje en seguridad de la información, Ejército Nacional

Abstract

Teaching IT security is challenging from multiple perspectives, including ensuring the nation's security and the impact on future generations of students. This situation alleviates the various high-demanding requirements of the National Army of Colombia. It is necessary to design effective learning models to meet guarantees that balance expectations with real-time practice. This balance allows for providing rigorous details linked to information, resources, and support. The aim is to achieve abundant deployment to ensure optimal results, fulfilling the processes and tasks set by high command staff in cyber defense, an essential operational area for a non-commissioned officer.

Keywords: Cybersecurity, cyber defense, teaching role, teaching-learning of IT security, National Army of Colombia.

1 Análisis del proceso de Enseñanza- Aprendizaje de la Ciberseguridad, en los suboficiales del Ejército Nacional de Colombia - Semillero de investigación Vestigio, Escuela Militar de Suboficiales, Sargento Inocencio Chincá (EMSUB) – Grupo de Investigación INTEMIL – Tolemaida, Nilo, Cundinamarca – Colombia.

DOI: https://doi.org/10.22517/25393812.25519

Introducción

En las generaciones actuales y en las venideras, la ciberseguridad viene tomando cada vez más fuerza, relevancia e incluso preocupación, dado que nos encontramos con una inmersión digital la cual es indispensable para nuestro diario vivir en cuestión de identificación y almacenamiento con información y documentos personales, de acuerdo a datos básicos como nombre y documento de identificación, datos bancarios y financieros, adicional, datos empresariales frente auditorías, niveles de finanzas y otros, además de material gubernamental, los cuales se mantienen resguardados en altos niveles de seguridad, con el fin de evitar fraudes, robo de información valiosa, extorsiones u otros casos ocasionados por personas inescrupulosas o detractores, conforme a delitos informáticos.

La ciberseguridad o seguridad informática, según podemos encontrar en la página de International Business Machines (2020) para habla hispana, "Es la práctica de proteger los sistemas importantes y la información confidencial de los ataques digitales" (p. 1). También se debe reconocer el rol y prioridad bajo la protección de la tecnología de la información (TI), como mencionamos antes, los recursos se encuentran alojados en internet y de un buen alcance de seguridad informática influye tanto en los *softwares* implementados en los dispositivos, como también la preparación y manejo de estos.

> Por tal razón, en Colombia, el desarrollo académico referente a los temas de ciberseguridad y ciberdefensa se ha centrado en un análisis de la regulación normativa e institucional de dinámicas variadas presentes en el ciberespacio, y ha dejado de lado el nivel de autonomía que han tenido las fuerzas militares en la gestión de seguridad y defensa en el ciberespacio. (Castañeda, 2019, p. 358)

De este ejercicio de recolección de datos, se obtienen resultados que muestran efectos positivos y verídicos frente al proceso de enseñanza- aprendizaje desde el rol del docente,

dado que se tiene una perspectiva firme y clara de la ciberseguridad, como una necesidad y aporte importante desde los inicios de su formación profesional como futuros Suboficiales, siendo este un punto de partida crucial para una revisión, análisis y posteriormente preparación más rigurosa de la institución en sus diferentes aspectos que compete en ciberseguridad.

Precedentes y contextualización global, era digital 4.0

Debido a la llegada de la pandemia, todo cambió, incluyendo la ciberseguridad, debido a que casos textuales, como las organizaciones encargadas de protección de sistemas digitales y *software* en pro a la invasión de códigos maliciosos y otros, tuvieron que enviar a todo el personal a trabajar en remoto, digiriendo operaciones desde sus casas, siendo este modelo inesperado y sin el total de recursos disponibles. Según Cano (2008):

> Existe un nuevo escenario de riesgo y amenaza donde la información es considerada un arma estratégica y táctica, cuestionando la gobernabilidad de una organización o de la misma nación. El proceso de enseñanza en ciberseguridad debe garantizar que se tengan competencias específicas en la detección de riesgos y a su vez los sistemas de información, conserven la integridad, disponibilidad y confidencialidad de la información. (p. 1)

Se resaltan datos como lo público la compañía ESET en su *Security Report* para Latinoamérica de año 2021, compartieron el hallazgo de "códigos maliciosos son la principal preocupación (64 %) y la primera causa de incidentes de seguridad (34 %) en las empresas Latinoamericanas" esta cifra es bastante alta, donde se deduce a incrementar y evolucionar los modelos de ciberseguridad, donde siendo mucho más textuales frente a la realidad nacional, Colombia está en el top 10 de los países más atacados cibernéticamente, al registrar once millones de amenazas durante 2021, lo que la sitúa en el rango máximo de riesgos recibidos, creciendo por el orden del 105 %. (Reporte Symantec, 2022, p. 4).

DOI: https://doi.org/10.22517/25393812.25519

De acuerdo a lo anteriormente expuesto, se denota el interés de conocer la conceptualización de la era 4.0 en donde Banquez et al., (2021) resalta en su artículo que, "la incorporación de la competencia digital en el contexto educativo, corresponde a la necesidad que precede la transformación digital y su integración en la sociedad del conocimiento" (p. 132). Por tal razón, se infiere en que, el uso educativo de las tecnologías de la información y la comunicación por parte de los docentes universitarios aporta en la contextualización de problemáticas surgidas desde el quehacer docente y establece distintos aportes del proceso de enseñanza – aprendizaje.

La cultura de la protección de datos desde la docencia.

Hay que resaltar otro factor importante como lo es la docencia, debido a que su rol es imprescindible independiente del nivel de educación, gracias a preparaciones en los diferentes formatos, áreas y temáticas se llega a impactar y dar bases sólidas a futuros profesionales en campos privados o públicos, donde en este caso de manera textual se hace mención al programa la formación complementaria en la tecnológica de criminalística de campo, que tiene gran relevancia en el Ejército Nacional y principalmente para los futuros Cabos Tercero[1]. Es por esta razón que se hace búsqueda exhaustiva de perfiles civiles que imparten la cátedra.

Sin dejar a un lado que: "resulta paradójico que la profesión docente aparezca solo tangencialmente en las estrategias gubernamentales dentro de los planes de desarrollo" (Cabezas, et al., 2018, p. 55) donde todo el peso negativo recae la mayoría de veces para los docentes, sin embargo, aquí se encuentran ciertas diferencias, ya que la EMSUB tiene como enfoque con el propósito de trascender por medio de la capacitación y especialización en

1 Cabo Tercero: Primer Rango de los Suboficiales del Ejército Nacional de Colombia, Líderes y administradores de una escuadra de soldados a su cargo, que garantizan el orden Constitucional de la Nación.

relación con el análisis y manejo del lugar de los hechos, aplicando conocimientos en investigación criminal y en su actuación como primer respondiente en procesos judiciales y tratamiento de material probatorio y evidencias bajo la capacidad de apropiar la legislación vigente aplicada a procedimientos relacionados con delitos Informáticos (Ley 1273 de 2009).

Además, desde este rol de docente, se pretende alcanzar resultados de aprendizaje y competencias que se buscan desarrollar en la asignatura de Seguridad Informática, como lo es identificar términos legales y protocolos de la seguridad informática, para aplicarlos al manejo de la información en custodia desde su perfil laboral y profesional. Como competencia general, el utilizar con idoneidad las tecnologías de la información y la comunicación, principios de seguridad, aspectos legales, para identificar, construir, validar, autenticar, presentar y explicar datos que sean válidos dentro del proceso de Formación del futuro Cabo Tercero, bajo el gran compromiso y acompañamiento ligado al docente para así alcanzar altos niveles de protección en el Área de Operaciones denominada Ciberespacio.

Ciberseguridad, principio de protección

La ciberseguridad es la práctica, implementación de procesos y herramientas que se encargan de la protección de computadoras, sistemas electrónicos, servidores, aplicaciones digitales, dispositivos móviles, redes y todo tipo de datos que se encuentren almacenados, evitando ataques digitales maliciosos. “Las medidas de ciberseguridad o seguridad cibernética están diseñadas para combatir las amenazas contra sistemas en red y aplicaciones, ya sea que esas amenazas se originen dentro o fuera de una organización” (IBM, s.f).

A su vez, se encarga de proteger y almacenar con total confianza y seguridad compañías especializadas que brindan modelos eficaces y con un porcentaje mínimo de error, para generar comodidad y garantías a los diversos clientes, ya sea alguien del común, proveedores, grandes compañías e incluso todo un mercado en general.

DOI: https://doi.org/10.22517/25393812.25519

Ciberseguridad a través del tiempo

Para hacer un contexto inicial, cabe aclarar la diferencia entre hacker, que significa ser una persona que indaga e interviene en los sistemas, ingresando por medios de los fallos detectados y así mismo ser mejorados, lo contrario a un cracker, siendo este un ciberdelincuente, ya que aprovecha estos fallos para sacar explotación al máximo y obtener grandes beneficios.

De acuerdo a lo referido por Han (2020) el primer hacker reconocido en la historia, Nevil Maskelyne quien logra una de sus hazañas en 1903, intercepta la primera transmisión de telégrafo inalámbrico. Seguidamente, surge el primer cracker en la historia, John Draper o también llamado "Captain Crunch", quien logra tomar ventaja con el silbato que venía en las cajas de cereal de "Cap'n Crunch" y engaña a la central telefónica, realizando llamadas gratuitas por medio del artificio de la señal.

Con el fin de contrarrestar riesgos y aumentar la seguridad de la información en los años 70's, surge el primer malware o virus malicioso denominado Creeper, replicando el mensaje *I'm the Creeper, ¡catch me if you can!*, llevando la necesidad de crear el primer antivirus y nace Reaper, encargado de eliminar las acciones generadas por Creeper. Debido al paso y evolución de tecnologías, el aumento de información, recursos y datos toma mayor auge. Sobre los 80's se incrementa la presencia de malwares, llevando a pulir y desarrollar antivirus más eficientes, dando pasos importantes para la protección de información digital. A finales de esta década el personaje Kevin Mitnick crea un ciberataque por medio de ingeniería social de modo que se obtuvo información personal y confidencial, siendo hasta la fecha un método recurrente para sacar mucha información a personas comunes y también empresas, por lo que se ha creado una rigurosa preparación para prevenir estos ataques y no ser vulnerables.

Sobre el año 1995 en Europa se crea el comité de expertos en delitos informáticos, enfocados en crear y trabajar en estrategias para minimizar los ataques en internet. Todas

las partes están de acuerdo en crear políticas penales para proteger a la población frente a la ciberdelincuencia, dando origen seguidamente en 2001 a la aprobación del Convenio de Budapest, integrado por cincuenta y seis países.

Nace en 2003 el grupo hacktivista más grande a nivel internacional hasta la actualidad, Anonymous, con un fin descentralizado, provocando ciberataques para llamar la atención y exponer sus indiferencias frente a temas políticos, como también haciendo visibles a la luz de toda información clasificada de personal de alto poder.

Llegando a finales de los 2000 la preocupación aumenta debido a que se lleva a cabo el surgimiento del Internet de las Cosas (IOT), ya que elementos encontrados en hogares, como electrodomésticos, cámaras e incluso juguetes, se vinculaban a internet del cual, para llegar a tener ventajas a los usuarios, los ciberdelincuentes aprovechan el poder sacar suficiente información de estos recursos, llevando a seguir aumentando la ciberseguridad para evitar robos por medio de dispositivos promedios.

En la actualidad la ciberseguridad tiene la gran responsabilidad de llevar buenas prácticas y resultados en la inteligencia artificial (IA), ya que el desarrollo de esta ha trascendido a niveles muy altos a comparación de otro tipo de tecnologías, a modo que se viene integrando algoritmos eficientes para detección de amenazas en tiempo real, como también se puede encontrar la incorporación de motores de correlación de amenazas para detectar ataques desde una primera etapa, logrando evitar el desenvolvimiento de *malwares* encriptados. A pesar del nivel que se encuentra a esta época, la evolución de ataques maliciosos sigue aumentando constantemente.

Ciberseguridad en el Ejército Nacional de Colombia

> En la Constitución Política de Colombia y su Artículo 217. La Nación tendrá para su defensa unas Fuerzas Militares permanentes constituidas por el Ejército, la Armada y la Fuerza Aérea. Las Fuerzas Militares tendrán como finalidad primordial la defensa

DOI: https://doi.org/10.22517/25393812.25519

de la soberanía, la independencia, la integridad del Territorio Nacional y del orden constitucional. (Constitución Política de Colombia, 1991), haciendo claridad a lo anterior, tenemos presente que el Ejército de Colombia, tiene como objetivo garantizar a nivel defensa, la integridad de sus recursos, entra aquí el apoyo de estar al tanto de la Ciberseguridad, con la que cuenta el país debido a que este también es un dominio de guerra el cual puede llegar a presentarse en diferentes momentos, teniendo presente esto se conformó la comisión intersectorial constituida por ColCERT, CCP (Centro Cibernético Policial de Colombia) y el comando cibernético de las Fuerzas Militares de Colombia, en donde su función es velar por la Ciberdefensa y ciberseguridad del país (Capitán Gómez, 2020).

Figura 1

Comisión intersectorial

Nota: Análisis y estrategia de implementación de un marco de trabajo de ciberseguridad para la unidad de Ciberdefensa del Ejército Nacional. Capitán Gómez (2020).

La aplicación de ciberdefensa en Colombia

La Ciberdefensa es el conjunto de acciones u operaciones activas o pasivas desarrolladas en el ámbito de las redes, sistemas, equipos, enlaces y personal de los recursos informáticos y teleinformáticos de la defensa, a fin de asegurar el cumplimiento de las misiones o servicios para los que fueran concebidos a la vez que se impide que fuerzas enemigas los utilicen para cumplir los suyos (Cari, 2013).

Además, tomando un mayor enfoque y posición de este término, también se considera como "controlar las amenazas, peligros o riesgos de naturaleza Cibernética, con el fin de permitir el uso del Ciberespacio con normalidad, bajo la protección de los derechos, libertades y garantías de los ciudadanos, en apoyo a la defensa de la soberanía" (Vargas y Recalde, 2017, p. 37).

Colombia, un país rico en diversidad, fauna y flora, también como otras Naciones, ha sufrido ataques Cibernéticos, generando que salga a la luz información que en su momento era privada y que para ello es importante que se fortalezca la Ciberseguridad en las diferentes plataformas del Estado, evitando así una amenaza a futuro.

Tomando en cuenta que un código malicioso, también conocido como malware, según Kaspersky (s.f) "es un código informático o script web dañino diseñado para crear vulnerabilidades en el sistema que permiten la generación de puertas traseras, brechas de seguridad, robo de información y datos, así como otros perjuicios potenciales en archivos y Sistemas Informáticos" del cual se busca día a día la intensificación a los diferentes modelos que puede presentarse. (p.

Para ello, el gobierno colombiano ha implementado controles referentes al tema de la ciberdefensa con el objetivo de evitar una ciberguerra en internet; el Ministerio de las Telecomunicaciones ha implementado un Nodo de Seguridad que permite fortalecer la protección

DOI: https://doi.org/10.22517/25393812.25519

del Ciberespacio, la infraestructura del Estado y los servicios del ciudadano, de esta manera se da lugar a generar, adoptar y usar nuevas tecnologías (Camacho, 2016).

Todo esto consignado en el Código Penal Colombiano y la Ley 1273 de 2009 que nos indica los delitos y sus penalidades que van implicados en la Seguridad Informática y de las Comunicaciones.

El Modelo de enseñanza - aprendizaje y la docencia en la Escuela Militar de Suboficiales

El modelo pedagógico del cual se hace énfasis en el Ejército Nacional y la EMSUB es el modelo constructivista, del cual se desencadena una serie de procesos y actividades durante el tiempo de duración de la asignatura, en donde cabe aclarar que gran parte de la enseñanza es aplicada por el mismo alumno, debido a que es quien debe encargarse de hacer una intervención de autonomía, exploración, descubrimiento y a su vez manipulación de los materiales o recursos suministrados por los docentes en el aula de clase, como también accesos a plataforma como bancos de datos y guías.

Es de gran aporte, gracias a que el docente, es considerado en las instituciones de formación, como un canal de información, guía y orientador (pilar fundamental) y de mucha relevancia, ya que los próximos Suboficiales van a salvaguardar la vida a partir de la protección del Ciberespacio, con su proceso de enseñanza enfocado en competencias que se han generado en aquellos jóvenes adultos.

La Ciberseguridad como enfoque pedagógico de la ciberdefensa

Desde la complementariedad de la tecnología en criminalística de campo para el futuro cabo tercero se hace esencial el énfasis en delitos informáticos y protocolos, ahora bien, desde la asignatura de seguridad informática se centra la metodología de esta investigación a partir de un enfoque cuantitativo y de método deductivo, utilizando la técnica de Encuesta,

de lo cual se genera un cuestionario dirigido a una muestra poblacional de los alumnos que conforman esta tecnología (ciento diez alumnos), por tanto, se evidencia que al analizar las variables de estudio definidas como la apropiación de las temáticas, desarrollo y transversalidad con el perfil de egreso del futuro suboficial del Ejército Nacional, poseen un enfoque de aprendizaje en pro de la articulación del desarrollo profesional del militar. El presente estudio revela una gran transformación curricular para la apropiación de conocimiento de la asignatura en seguridad informática en las siguientes generaciones de la EMSUB con énfasis en criminalística de campo, entendiéndose al área de la ciberseguridad como potencial en la identificación, y procedimientos del protocolo de seguridad que organizaciones gubernamentales como el Ejército Nacional trabajan desde el área operacional ciberespacio, la cual comprende a la información como el principal activo organizacional del mismo.

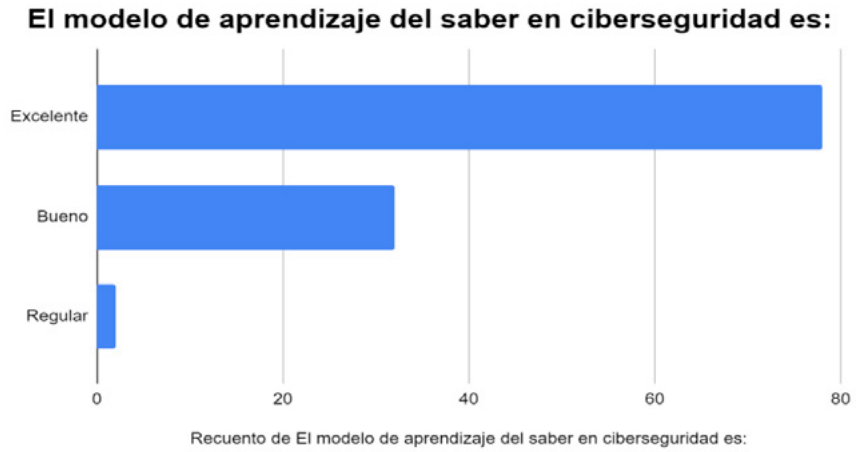
Discusión

Se percibe de manera gratificante el resultado del instrumento manejado en este caso con los futuros Suboficiales, dado que muestran de manera positiva sus percepciones con respecto al modelo de aprendizaje implementado por los docentes, al igual que los recursos empleados en la asignatura ofrecida por parte de la ESMUB, del cual se puede dejar bases sólidas para futuras generaciones, aunque en términos actuales hay un contraste con respecto a la preparación de ataques cibernéticos, y el dominio del ciberespacio por la actual era digital 4.0, el mismo contexto globalizado hacia el cual se está encaminando el perfil militar, hace pensar al alumno en su proceso de aprendizaje y las formas adecuadas de enseñanza para que estas postulaciones se ratifiquen en la toma de decisiones durante su desempeño profesional y no se perpetúe en grandes consecuencias legales para la institución o se ponga en riesgo la soberanía de la nación.

DOI: https://doi.org/10.22517/25393812.25519

Figura 2

Modelo de Aprendizaje de la Seguridad Informática en la EMSUB.



Nota: Elaboración propia

Figura 3

Importancia de la Ciberseguridad para el Suboficial

Nota: Elaboración propia

Resultados

De acuerdo con las evidencias de la investigación obtenidas por medio del instrumento aplicado, se deja abierta la posibilidad a futuras investigaciones, de mejora al currículo y el proceso de enseñanza- aprendizaje de la seguridad informática, si a bien se considera y conforme a los asertos de (Ospina & Sanabria, 2020) donde los actuales sistemas de información, el internet de las cosas y la nube como soporte del almacenamiento de la información personal, privada y organizacional, presenta fallas notorias, como la perdida de información estratégica del estado, teniendo en cuenta que todas estas hacen referencia a componentes esenciales del campo de la ciberseguridad. Se entiende como necesidad el tener en cuenta por parte de las directivas de la ESMUB, al igual que para el Ejército Nacional, la prevención, manejo y control de los Ciberataques.

No obstante a que los riesgos pueden llegar de manera inesperada y debe haber una antelación a los hechos inmediatos, se recomienda un enfoque más propicio para actualizar y blindar los *software*, bajo recursos y lineamientos planteados con anterioridad y un respectivo modelo sólido, para la recepción a múltiples ataques cibernéticos que pueden llegar desplegados de diversos lugares tanto a nivel nacional o internacional, con el fin de que se pueda estar actualizando frente a nuevas modalidades de robo de información e incluso infiltración de los *software*.

La institución tiene la responsabilidad de generar alineación y concordancia frente a hechos actuales, debido a que para un mediano y largo plazo se viene a originar una rigurosa preparación desde el rol docente, no solo con información suministrada, sino también bajo prácticas que vienen ocasionando garantías a futuro y así evitar fuertes impactos negativos, ya que puede producir un contraste poco balanceado frente a lo que se viene desarrollando desde el proceso de enseñanza-aprendizaje de la ciberseguridad y llevaría a la pérdida de tenacidad y carácter del modelo pedagógico actual.

DOI: https://doi.org/10.22517/25393812.25519

Conclusiones

Como consecuencia del proceso, los resultados evidenciados en la recolección de datos, permiten en su mayoría que las competencias adheridas al modelo de aprendizaje de la asignatura de seguridad informática de la ESMUB, proporcionen una mayor percepción a través de detalles y opiniones críticas, para que los futuros Cabos Tercero logren establecer una postura satisfactoria ante el desarrollo del currículo.

Bajo las necesidades y los recursos del cual se dispone en la institución, el rol del docente puede dejar bases sólidas en la asignatura de ciberseguridad a los Suboficiales, gracias al enfoque y disposición con el que se viene trabajando, puesto que se trabaja hacia la meta de fortalecer al personal militar en su entorno laboral con bases sólidas en ciberseguridad.

A partir de la investigación se busca que el Ejército Nacional de Colombia pueda ampliar sus modelos y procesos para la recepción a nuevas prácticas, puesto que se encuentra con un personal altamente calificado, donde debe seguirse el enfoque actual y continuar suministrando recursos a nivel de innovación y eficacia frente a la tendencia global, para así obtener mayores resultados de aprendizaje en el contexto del área operacional ciberespacio.

Referencias bibliográficas

Antonio, J. (2020). La brecha de ciberseguridad en América Latina frente al contexto global de ciberamenazas. *Revista de estudios en seguridad internacional* 6(2), 17-43. http://www.seguridadinternacional.es/resi/index.php/revista/article/view/303/349.

Roa, K., Rojas, C., González, L. y Ortiz, E. (2021). El docente en la era 4.0: una propuesta de formación digital que fortalezca el proceso de enseñanza y aprendizaje. *Revista Virtual Universidad Católica del Norte, (63)* 126-160. https://revistavirtual.ucn.edu.co/index.php/RevistaUCN/article/view/1262.

Vargas, R., Recalde, L., Reyes R. (2017). Ciberdefensa y ciberseguridad, más allá del mundo virtual: Modelo ecuatoriano de gobernanza en ciberdefensa. *Revista Latinoamericana de Estudios de Seguridad (20)*1 31-45 https://revistas.flacsoandes.edu.ec/urvio/article/download/2571/2105?inline=1

Aranda, G., Riquelme, J. & Salinas, G. (2015). La ciberdefensa como parte de la agenda de integración sudamericana. *Línea Sur (9)* 110-116. https://www.researchgate.net/profile/Sergio-Salinas/publication/296484484_La_ciberdefensa_como_parte_de_la_agenda_de_integracion_sudamericana_1/links/56d5b92408aebabdb4004cee/La-ciberdefensa-como-parte-de-la-agenda-de-integracion-sudamericana-1.pdf

Cabeza, L., Zapata, A., & Lombana, J. (2018). Crisis de la profesión docente en Colombia: percepciones de aspirantes a otras profesiones. *Educación y Educadores, 21*(1) 51-72. http://www.scielo.org.co/scielo.php?pid=S0123-12942018000100051&script=sci_arttext

Camacho, E. (2016). *Evolución de la Ciberdefensa y la Seguridad de la Información en Colombia.* [Tesis especialización, Universidad Militar Nueva Granada]. Archivo digital. https://repository.unimilitar.edu.co/bitstream/handle/10654/14382/camachogarciajuandiego2016.pdf?sequence=1&isallowed=y.

Cano, A., Díaz, J., Mendieta, C., Rivas, C., & Sánchez, N. (2014). Aporte internacional frente a los delitos informáticos en Colombia y su ejecución por parte de las autoridades competentes. [Tesis pregrado, Universidad Libre de Colombia] Archivo digital. https://repository.unilibre.edu.co/handle/10901/7695.

Cano, J. (2008). *Ciberseguridad y ciberdefensa: dos tendencias emergentes en un contexto global.* Revista Asociación Colombiana de inginieros de sistemas. Editorial https://acis.org.co/archivos/Revista/119/Editorial.pdf.

DOI: https://doi.org/10.22517/25393812.25519

Gómez, C., Franco, L. y Carlos, V. (2020) *Análisis y estrategia de implementación de un marco de trabajo de ciberseguridad para la unidad de Ciberdefensa del Ejército Nacional.* https://proyectosmaestrias.virtual.uniandes.edu.co/images/4SqhGgJEGI8iJbdVY-3BhhR0moiYeph30Ke1tQv02.pdf.

Cujabante, X., Bahamón, M., Prieto, J. & Quiroga, J. (2020). Ciberseguridad y ciberdefensa en Colombia: un posible modelo a seguir en las relaciones cívico-militares. *Revista Científica General José María Córdova, 18*(30), 357-377 https://revistacientificaesmic.com/index.php/esmic/article/view/588/666.

Cayón, J., y García, L. (2014). La importancia del componente educativo en toda estrategia de Ciberseguridad. Estudios en seguridad y defensa, 9(18), 5-13. https://esdegrevistas.edu.co/index.php/resd/article/view/9/4

Diaz, J. (2019). *La ciberseguridad en el ambito militar*. https://www.studocu.com/pe/document/universidad-peruana-de-ciencias-aplicadas/procesos-de-ingenieria/la-ciberseguridad-en-el-ambito-militar-3837348/17719519

Gómez, A. (2020). Ciberterrorismo, ¿una nueva amenaza?. *Boletín IEEE, (19)* 386-400. https://dialnet.unirioja.es/servlet/articulo?codigo=7625260.

Grupo de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT) (2017). *Alertas de seguridad*. http://www.colcert.gov.co/

Han, X. (2020). Trastorno en el mundo inalámbrico breve historia de cibercriminalidad y los casos cibercriminales durante las pandemias sanitarias en el siglo XX. *Revista Crítica de la Historia de las Relaciones Laborales y de la Política Social, (13)* 21-36. https://dialnet.unirioja.es/servlet/articulo?codigo=8927912

IBM (s.f.) ***¿Qué es la ciberseguridad?***. https://www.ibm.com/co-es/topics/cybersecurity

Infosecurity México. (2021). *Ciberseguridad Una guía completa del concepto, tipos, amenazas y estrategias.* https://www.infosecuritymexico.com/es/ciberseguridad.html#ciberseguridad

Josue, M., Maribel, A., Fabián, A., Magali, D. & Anaid, D. (2023). Instituto de Investigaciones Transdisciplinarias Ecuador. *Capítulo 9 La Ciberseguridad en países en desarrollo* pp. 169-190. https://binario.com.ec/wp-content/uploads/2023/01/Libro-Investigacion-CIENTIFICA.pdf#page=169

Kaspersky (S.F) ***¿Qué es el código malicioso?***. https://latam.kaspersky.com/resource-center/definitions/malicious-code

Kaspersky (S.F) ***¿Qué es la ciberseguridad?***. https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

Leiva, R. (2017). Ciberdefensa, **¿hacia** un nuevo eje estratégico? *Revista Ensayos Militares, 3*(1), 77-92. https://revistaensayosmilitares.cl/index.php/acague/article/view/4/4

Morán, S. (2017). La ciberseguridad y el uso de las tecnologías de la información y la comunicación (TIC) por el terrorismo. *La ciberseguridad y el uso de las Tecnologías de la Información y la Comunicación (tic) por el terrorismo,* pp. 195-221. https://www.torrossa.com/en/resources/an/4342372.

Ospina, R. & Sanabria, E. (2020). Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia. *Revista Criminalidad, 62*(2), 199-21. http://www.scielo.org.co/scielo.php?pid=S1794-31082020000200199&script=sci_arttext

Proyecto educativo de programa (2020) *Escuela Militar de Suboficiales "Sargento Inocencio Chincá".*

DOI: https://doi.org/10.22517/25393812.25519

Realpe, M., & Cano, J. (2020). Amenazas cibernéticas a la seguridad y defensa nacional. Reflexiones y perspectivas en Colombia. In Seguridad Informática [congreso] *X Congreso Iberoamericano*. Universidad del Rosario. https://acortar.link/pVyjCB

Reyna, D., y Olivera, D. (2017). Las amenazas cibernéticas. (pp. 49-72). En Carlos Hernández Rodríguez y Raúl Manuel Arano Chávez. *10 Temas de Ciberseguridad*. Editorial Universidad de Xalapa. https://universita.ux.edu.mx/universita-ciencia/article/view/220.

Symantec. (2022). *Ciberseguridad en tiempos de pandemia.* https://web-assets.esetstatic.com/wls/2021/06/ESET-security-report-LATAM2021.pdf

Sofistic Cibersecurity. (2019). *La breve historia de la ciberseguridad.* https://www.sofistic.com/blog-ciberseguridad/la-breve-historia-de-la-ciberseguridad/

Tapia, A. & Terán, L. (2023). El terrorismo y su transformacion. *Revista de la Academia del Guerra del Ejército Ecuatoriano, 16*(1), 13-13. https://journal.espe.edu.ec/ojs/index.php/Academia-de-guerra/article/view/2938/2404

Tekman. (2021). *Modelos pedagógicos: Qué son y cuáles son los fundamentales en educación.* Página web Tekman. https://www.tekmaneducation.com/blog/modelos-pedagogicos-en-educacion/.

Torres, D. (20189. El ciberespacio como escenario estratégico de Seguridad y Defensa en el desarrollo de políticas en Colombia. [Monografía diplomado, Universidad Militar Nueva Granada]. https://repository.unimilitar.edu.co/handle/10654/18104.

Vargas, R. & Recalde, L. (2017). Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa. *URVIO Revista Latinoamericana de Estudios de Seguridad, (20)*, pp.31-45. http://scielo.senescyt.gob.ec/pdf/urvio/n20/1390-4299-urvio-20-00031.pdf

Villar, M. (2019). Las implicancias de los ciberataques del S. XXI en América Latina. Universidad San Ignacio de Loyola. https://repositorio.usil.edu.pe/entities/publication/0ea3a52c-9f03-4705-8a8b-4667411455a4.

DOI: https://doi.org/10.22517/25393812.25519