Ciber seguridad para la Protección del Sistema Integrado de Catalogación de Defensa SICAD

Mayor (EJC) Mauricio Gómez Rodríguez

Artículo para optar al título profesional:

Magister en Ciberdefensa y Ciberseguridad

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) Mauricio Gómez Rodríguez
Identificación	**:**	80245291
Programa académico	**:**	Maestría en Ciberdefensa y Ciberseguridad
Tutor metodológico	**:**	Omitido
Tutor temático	**:**	Dr. Jaider Ospina Navas
Fecha de entrega	**:**	26 de agosto de 2025
Extensión	**:**	7.820 palabras

DECLARACIÓN DE ORIGINALIDAD Y CESIÓN DE DERECHOS

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

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

El autor acepta ceder los derechos de publicación en favor de la ESDEG y su Sello Editorial de acuerdo con los términos de la licencia Creative Commons: Reconocimiento-NoComercial-SinObrasDerivadas.

AUTORIZACIÓN DE PUBLICACIÓN

El autor autoriza que este artículo sea publicado por el Sello Editorial ESDEG en su repositorio institucional y esté disponible bajo una modalidad de acceso abierto.

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

Ciber seguridad para la Protección del Sistema Integrado de Catalogación de Defensa SICAD.

Cybersecurity for the Protection of the Integrated Defense Cataloging System (SICAD).

Mauricio Gómez Rodríguez[1]
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: El presente artículo aborda la importancia de la ciberseguridad en el Sistema Integrado de Catalogación de Defensa (SICAD). Este sistema es considerado el corazón de la logística militar colombiana, pero su digitalización lo expone a una red de amenazas invisible. Por ello, a través de una metodología descriptiva con enfoque de tipo cualitativo y con técnicas de revisión documental, se hace una exploración sobre los ataques externos y las vulnerabilidades internas del SICAD, asimismo, el trabajo sugiere una propuesta de blindaje tecnológico con cifrado y defensa perimetral, lo cual ha de requerir una urgente adaptación legal, en el sentido de que el marco normativo colombiano tiene vacíos que dificultan la persecución de ciberdelitos y la cooperación internacional. En conclusión, proteger al SICAD es una carrera contrarreloj donde la tecnología, las leyes y, sobre todo, la consciencia de cada miembro del Ejército son cruciales para blindar la defensa de la nación.

Palabras clave: Ciberseguridad, Defensa, Estrategia, Gobernanza, Logística, Riesgo

Abstract: This article addresses the importance of cybersecurity in the Integrated Defense Cataloging System (SICAD). This system is considered the heart of Colombian military logistics, but its digitalization exposes it to an invisible network of threats. Therefore, through a descriptive methodology with a qualitative approach and document review techniques, an exploration of external attacks and internal vulnerabilities of SICAD is undertaken. The article also suggests a proposal for technological protection with encryption and perimeter defense, which will require urgent legal adaptation, given that the Colombian regulatory framework has gaps that hinder the prosecution of

[1] Mayor del Ejército Nacional de Colombia. Candidato a Magister en Ciberdefensa y Ciberseguridad, 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/0009-0003-7299-5924 - Contacto: mauricio.gomezr@esdeg.edu.co.

cybercrimes and international cooperation. In conclusion, protecting SICAD is a race against time where technology, laws, and, above all, the awareness of each member of the Army are crucial to safeguarding the nation's defense.

Keywords: Cybersecurity, Defense, Governance, Logistics, Risk, Strategy

Introducción

El Sistema Integrado de Catalogación de Defensa (SICAD), adoptado por Colombia en 2013, es el cerebro de la logística militar, garantizando la trazabilidad de los bienes y optimizando los recursos (CEDE4, 2021). Aunque su arquitectura es una herencia del Sistema OTAN de Catalogación (SOC), su protección es una responsabilidad exclusivamente colombiana, y opera bajo la jurisdicción exclusiva del Ejército Nacional. Esta soberanía digital es crucial, ya que la información del SICAD es un activo crítico para la seguridad del país, y su integridad es vital para prevenir el desvío, la falsificación o el tráfico ilícito de material (CEDE4, 2021).

La defensa del SICAD requiere una estrategia integral. En primer lugar, se debe fortalecer su infraestructura tecnológica con tecnologías de encriptación y autenticación avanzadas, como la criptografía de clave pública y la autenticación multifactorial (CEDE4, 2021). Por ello, la implementación de un sistema de monitoreo continuo y un Sistema de Detección y Respuesta a Incidentes (IDR) son esenciales para reaccionar rápidamente ante cualquier ciberataque. En segundo lugar, se encuentra el factor humano. De igual forma, la capacitación del personal en ciberseguridad es vital para que los usuarios reconozcan tácticas de fraude como el *phishing* y el *spear phishing*, y sean conscientes de la importancia de contraseñas seguras y un manejo responsable de la información (CEDE4, 2021).

La protección del SICAD enfrenta desafíos normativos y legales. A pesar de los avances en la legislación colombiana (Ley 1273 de 2009), existen vacíos que dificultan la persecución de ciberdelincuentes transnacionales. Es urgente que el marco normativo se adapte a la complejidad de estas amenazas, estableciendo sanciones claras y facilitando la cooperación internacional (Ley 1581 de 2012).

A nivel teórico, esta problemática se enmarca en la Teoría de la Guerra de Clausewitz, que concibe el ciberespacio como un nuevo teatro de guerra, donde los Estados-Nación se enfrentan para alcanzar sus objetivos (Benítez, 1986). La evolución de la logística militar

hacia la digitalización subraya la importancia de la ciberseguridad para la eficiencia operativa (Celemín, 2015).

Por otro lado, el entorno competitivo actual exige la adopción constante de nuevas tecnologías en el sector logístico, lo que a su vez incrementa la exposición a amenazas y vulnerabilidades cibernéticas (Bermúdez y Cano, 2023). Un informe de la CEPAL (Díaz, 2021) confirma que el sector logístico se ha visto especialmente afectado por ciberataques, lo que resalta la urgencia de fortalecer la seguridad.

Además, la armonización de los marcos normativos a nivel regional podría generar importantes beneficios económicos y sociales, promoviendo la confianza de los inversionistas y la interoperabilidad de sistemas (Díaz & Núñez, 2023).

Adicional a lo anterior, y para darle una mayor claridad a la temática objeto de estudio, se han encontrado diversos trabajos académicos, que subrayan la necesidad de que las Fuerzas Militares de Colombia actualicen sus capacidades cibernéticas para salvaguardar la información y la infraestructura crítica del Estado :

En primera instancia, se tiene el trabajo de Barrios (2024) "*La cadena logística del Ejército Nacional de Colombia y ciberseguridad y ciberdefensa: atención a la academia"* el cual menciona el interés del Ejercito Nacional colombiano en ampliar el conocimiento sobre las actividades de ciberseguridad y ciberdefensa vinculadas a la logística militar. Barrios (2024), enfatiza en darle importancia de tipo estratégico a las capacidades logísticas militares, señalando que de no hacerlo, se convertiría en falencias operativas, asimismo indica que toda la cadena logística de las FF.MM. ha de analizarse desde la perspectiva del contexto cibernético de seguridad.

Como complemento al anterior documento referido en materia de desafíos en ciberseguridad se encuentra el de Peña (2023) "*Ciberseguridad, un desafío para las Fuerzas Militares colombianas en la era digital"* que señala la necesidad de actualizar constantemente las capacidades de las Fuerzas Militares colombianas en el campo cibernético con el objeto de salvaguardar la información de la institución y la infraestructura

critica del Estado, dado que existen un sinnúmero de tecnologías disruptivas, entre ellas la Inteligencia Artificial y los virus informáticos, que tienen como finalidad afectar los sistemas informáticos relacionados con los entornos sociales, económicos y políticos vinculados tanto al Estado como a la sociedad.

El tema de las ciberamenazas a la seguridad de la información del Ejército colombiano, es una problemática que de no tratarse a tiempo, podría comprometer la seguridad nacional. Esta temática es retratada en el artículo de investigación de Mozo Rivera & Ardila Contreras (2022) *"El fenómeno de las ciberamenazas: afectaciones a la ciberseguridad del Ejército nacional de Colombia"* en el cual se explican cuáles son los tipos de riesgos asociados a ciberataques y el impacto que pueden generar en la institución, además hace una reflexión crítica sobre la imperiosa necesidad de que el Ejército Nacional integre sus capacidades cibernéticas en conjunto con actores del sector privado y público para prevenir y contrarrestar las amenazas que vulneran los activos estratégicos de la institución.

Un trabajo que refiere la importancia de que los ejércitos del mundo busquen el apoyo de fuerzas militares afines en el campo logístico para potenciar la efectividad de sus resultados operacionales es el presentado por Sánchez Hurtado et al., (2011) "*Logística militar en los conflictos del siglo XXI. El espacio y los retos ofrecidos por la guerra asimétrica*" que indica que a raíz de los sucesos del 11 de septiembre de 2001 en Estados Unidos y las nuevas tendencias de la guerra asimétrica, los Estados han de invertir en la ampliación de las habilidades para contrarrestar enfrentamientos asimétricos, con la condición de que han de apoyarse sobre una fuerza logística superior, por ejemplo de operaciones conjuntas entre unidades de Fuerzas Especiales, agencias de inteligencia y unidades de poder aéreo, terrestre, marítimo o fluvial.

Por lo anterior, el fortalecimiento de la legislación en torno a la ciberdefensa aplicada a la logística militar debe ser una prioridad. Es necesario que los marcos legales adapten sus disposiciones a las nuevas amenazas tecnológicas, estableciendo sanciones claras y proporcionadas para los infractores y dotando a las autoridades competentes con las herramientas necesarias para investigar y perseguir delitos cibernéticos complejos. La cooperación internacional en este ámbito también es esencial, ya que los ciberdelincuentes

que operan en el ámbito de la logística militar a menudo utilizan redes transnacionales, lo que exige una respuesta conjunta de los países afectados (Ley 1581 de 2012)

Por ello, con toda la información anteriormente presentada, se hace necesario la formulación de la siguiente pregunta de investigación: *¿Cómo puede la ciberseguridad fortalecer la protección del Sistema Integrado de Catalogación de Defensa (SICAD) para garantizar la integridad de los datos logísticos del Ejército Nacional?* Interrogante al cual se le dará solución según el objetivo general de este articulo el cual es *Proponer una estrategia que permita el fortalecimiento desde la ciberseguridad, de la protección del Sistema Integrado de Catalogación de Defensa (SICAD) del Ejército Nacional.* Dicho objetivo estará acompañado de 3 objetivos específicos que al mismo tiempo son los 3 capítulos de este documento, estos son:

- Analizar las vulnerabilidades y riesgos de manipulación ilícita de los datos logísticos de la institución y las limitaciones legales para sancionar a los responsables.
- Identificar las amenazas cibernéticas que ponen en riesgo la integridad de los datos del SICAD en la gestión logística del Ejército Nacional.
- Formular una estrategia de ciberseguridad implementada para proteger la información del SICAD.

Metodología

El desarrollo del presente trabajo académico adoptará una metodología descriptiva con enfoque cualitativo, siguiendo los parámetros estipulados por Hernández – Sampieri & Mendoza (2018) para proyectos de investigación y el documento de Bernal (2016) "*Metodología de la investigación*", la ejecución de este trabajo se realizara a través de técnicas de revisión documental, que analizará la relación entre el ciberdelito y la vulneración de la información en el Sistema Integrado de Catalogación de Defensa (SICAD), destacando la insuficiencia de la legislación colombiana en esta materia.

El proceso de revisión documental consiste en hacer una exploración a través de los distintos repositorios académicos existentes en la web y los más reconocidos. Es entonces que se indagara sobre el tema en las bases de datos tales como Redalyc, Scielo, Researchgate, Academic.edu, entre otros, y a través de combinaciones de palabras clave que se colocaran en la pestaña de los motores de búsqueda de estos repositorios, se obtendrá la información precisa para la construcción de este trabajo.

Con respecto al proceso de construcción de este trabajo, consistirá en 3 fases importantes: la primera es de recopilación de la información, que consistirá en el proceso de revisión documental que se mencionó en el anterior párrafo, la segunda fase, es la de selección y consolidación de la información, en donde se han de depurar la información relevante de cada uno de los contenidos en los documentos adquiridos en el buscador, y así con esta valiosa información construir los apartados de este artículo, y la tercera fase, consiste en la revisión y entrega del articulo al docente encargado.

Análisis de las vulnerabilidades y riesgos de manipulación ilícita de los datos logísticos de la institución y las limitaciones legales para sancionar a los responsables:

La gestión logística del Ejército Nacional de Colombia se constituye en un pilar fundamental para optimizar su capacidad de respuesta frente a las diversas amenazas y desafíos que enfrenta la nación. Esta gestión, inherentemente compleja y manejada a través de sistemas de información que almacenan datos críticos sobre inventarios, mantenimiento, transporte, personal y recursos, se encuentra en un entorno digital cada vez más dinámico y amenazante. En ese sentido, la integridad, confidencialidad y disponibilidad de los datos logísticos se erigen como elementos esenciales para la toma de decisiones estratégicas, la planificación operativa y la ejecución exitosa de las misiones militares (Barrios, 2024).

Sin embargo, esta dependencia de los datos digitales también conlleva vulnerabilidades significativas que pueden exponer a la institución a riesgos crecientes de

manipulación ilícita. Ese tipo de manipulaciones, bien sea de origen interno o externo, accidentales o intencionadas, pueden tener consecuencias devastadoras para la capacidad operativa del Ejército, la seguridad nacional y la gestión eficiente de los recursos del Estado (Barrios, 2024).

Paralelamente a la identificación y mitigación de estas vulnerabilidades y riesgos, surge la cuestión crucial de la capacidad del marco legal colombiano para sancionar de manera efectiva a los responsables de tales actos ilícitos. Aunque existen leyes que abordan delitos informáticos y la protección de la información, su aplicabilidad específica al contexto de la información sensible del Ejército Nacional y las particularidades de su gestión logística, presenta limitaciones y desafíos que requieren un análisis detallado (Barrios, 2024).

Por lo tanto, esta introducción busca establecer el contexto crítico en el que se manifiestan las vulnerabilidades y los riesgos de manipulación ilícita de los datos logísticos del Ejército Nacional de Colombia. Comprender este contexto es el primer paso esencial para abordar de manera integral los desafíos de ciberseguridad y garantizar la protección de la información logística del Ejército Nacional.

Hallazgos del análisis de vulnerabilidades para el SICAD: puntos de falla críticos

De acuerdo a la información proporcionada por el trabajo de Barrios (2024), Piñeros (2020) y Quesada (2018) El análisis revela un panorama de vulnerabilidades que van más allá de fallas técnicas, extendiéndose a la estructura misma de la gestión logística:

1. Sistemas descentralizados y heterogéneos: La existencia de múltiples sistemas de información no integrados crea puntos débiles. Esta falta de unificación permite la manipulación de datos sin una detección centralizada, generando duplicidades y una visión fragmentada que dificulta el control y facilita las inconsistencias (Barrios, 2024).
2. Controles de acceso insuficientes: Las contraseñas débiles, la falta de autenticación multifactorial y los permisos de acceso excesivamente amplios son fallas explotables. Estas debilidades son una invitación a que personal no autorizado, interno o externo,

acceda y altere datos críticos con facilidad, comprometiendo la confidencialidad (Barrios, 2024).

3. Falta de auditoría y trazabilidad: Un sistema sin registros detallados de sus actividades es un punto ciego. La ausencia de un registro exhaustivo y auditable de las transacciones y modificaciones dificulta enormemente la detección de manipulaciones y la identificación de los responsables, permitiendo que los actos ilícitos queden impunes (Barrios, 2024).
4. Vulnerabilidades en el software y hardware: El uso de software obsoleto sin parches de seguridad y el hardware con fallas conocidas son puertas de entrada para ciberataques. Estas debilidades técnicas son fácilmente explotables por actores malintencionados para comprometer la integridad y disponibilidad de los datos logísticos (Barrios, 2024).
5. Factores humanos y de ingeniería social: La vulnerabilidad del personal militar a técnicas como el *phishing* y el *spear phishing* es una de las mayores debilidades. La falta de capacitación en ciberseguridad es un punto de quiebre crítico, ya que los atacantes pueden engañar a los usuarios para que revelen credenciales o realicen acciones que faciliten el robo y la manipulación de la información.

Riesgos de manipulación ilícita de los datos logísticos

Los riesgos de la manipulación ilícita de datos logísticos del Ejército Nacional no son abstractos; son la consecuencia directa y explotable de las vulnerabilidades que ya hemos identificado. Las fallas en el sistema SICAD no solo representan debilidades, sino que son puertas de entrada para consecuencias devastadoras. Por tanto, y según lo consignado en el trabajo de Barrios (2024), La manipulación de datos logísticos puede desencadenar riesgos graves y multifacéticos, cada uno de ellos conectado a una vulnerabilidad específica del sistema:

1. Deterioro de la capacidad operacional: La descentralización y falta de integración de los sistemas (como se mencionó en el análisis de vulnerabilidades) facilita que la información sobre inventarios, municiones o mantenimiento sea alterada sin

detección. Si un atacante, interno o externo, explota esta vulnerabilidad para cambiar datos críticos, el Ejército podría creer que tiene los recursos necesarios para una misión cuando en realidad no los tiene, lo que afecta directamente su capacidad para operar de manera efectiva.

2. Ineficiencia y despilfarro de recursos: La falta de controles de acceso y auditoría permite que los datos de adquisiciones y distribución sean manipulados. Un atacante podría explotar esta debilidad para crear registros falsos, duplicar pedidos o alterar cantidades. Esto lleva a decisiones logísticas erróneas, generando pérdidas económicas significativas y el despilfarro de recursos del Estado.
3. Compromiso de la seguridad nacional: Las vulnerabilidades en el software, hardware y la dependencia de proveedores externos son fallas que pueden ser explotadas por actores hostiles. Si estos vulneran el sistema, pueden acceder y manipular información sensible sobre despliegues o capacidades logísticas, lo que compromete la seguridad de la nación.
4. Facilitación de actividades ilícitas: La falta de trazabilidad y el riesgo de amenazas internas son vulnerabilidades que permiten que un atacante manipule datos para ocultar el desvío de recursos. Por ejemplo, al explotar una cuenta de usuario con permisos amplios (vulnerabilidad de control de acceso), un atacante podría alterar los registros para justificar la desaparición de armamento, facilitando el tráfico de armas o la corrupción.
5. Pérdida de confianza pública: La debilidad en los factores humanos y la falta de capacitación en ciberseguridad pueden llevar a filtraciones de datos o a la exposición pública de manipulaciones ilícitas. Esto no solo genera una crisis interna, sino que también erosiona la confianza de la ciudadanía en la transparencia y la integridad de la institución.
6. Riesgos para la seguridad del personal: Cuando un atacante explota la vulnerabilidad de la falta de cifrado robusto, puede interceptar y manipular información sobre la planificación de operaciones o el suministro de equipos de protección. El personal militar puede verse expuesto a situaciones de riesgo por la alteración de esta información crítica.

Limitaciones legales para sancionar a los responsables

Si bien el ordenamiento jurídico colombiano contempla mecanismos para sancionar conductas ilícitas relacionadas con la manipulación de datos, acorde al trabajo de Piñeros (2020) y Barrios (2024), existen limitaciones específicas en el contexto de la información del Ejército Nacional:

1. Tipificación penal específica: Aunque existen delitos como el acceso abusivo a sistemas informáticos (Ley 1273 de 2009), la violación de datos personales, el daño informático y el hurto o apropiación indebida (si se manipulan activos tangibles a través de la información), hasta el momento no existe una tipificación penal *específica* para la manipulación de datos logísticos militares en todas sus formas y con las agravantes propias del contexto de la seguridad nacional. Dicho vacío legal dificulta la adecuación típica precisa de la conducta.
2. Prueba y atribución de responsabilidad: En entornos complejos como las redes militares, la identificación y atribución de responsabilidad a los autores de la manipulación ilícita siempre es un desafío técnico y probatorio, puesto que rastrear el origen de un ataque cibernético o demostrar la intención maliciosa de un actor interno, requiere de una investigación forense digital exhaustiva y la presentación de pruebas contundentes (Barrios, 2024).
3. Jurisdicción y competencia: Dependiendo de la naturaleza del delito y la calidad del infractor (civil o militar), la competencia para investigar y juzgar tanto puede recaer en la justicia ordinaria o en la justicia penal militar. La delimitación de competencias y la posible existencia de fueros especiales pueden generar complejidades procesales (Piñeros, 2020).
4. Clasificación de la información y secreto militar: La naturaleza sensible y clasificada de gran parte de la información logística del Ejército impone restricciones en la divulgación de pruebas durante una investigación judicial, lo que dificulta la acusación y el juzgamiento de los responsables. La protección del secreto militar

entonces entra en conflicto con el derecho a la prueba y la transparencia judicial (Piñeros, 2020).

5. Leyes de protección de datos y su aplicabilidad: Si bien la Ley 1581 de 2012 (Protección de Datos Personales) es relevante, la información logística del Ejército no cae completamente bajo su ámbito, especialmente aquella que no contenga datos personales identificables, con lo cual, se limita el uso de esta legislación para sancionar ciertas manipulaciones.
6. Cooperación internacional: En casos de ataques cibernéticos transfronterizos, la falta de acuerdos de cooperación internacional efectivos impide la identificación y extradición de los responsables (Piñeros, 2020).
7. Vacíos legales y necesidad de actualización: La continua transformación de las tecnologías de la información crea vacíos legales que no contemplen nuevas formas de manipulación ilícita de datos. Es posible que la legislación actual necesite revisarse en materia de seguridad nacional y la información militar (Piñeros, 2020).
8. Sanciones administrativas y disciplinarias: Dentro del régimen disciplinario militar existen mecanismos para sancionar conductas irregulares relacionadas con la gestión de la información. Sin embargo, la gravedad de la sanción administrativa puede ser inferior a la penal para actos de manipulación ilícita grave (Piñeros, 2020).

Los datos logísticos del Ejército Nacional de Colombia están expuestos a una variedad de vulnerabilidades que facilitan su manipulación ilícita, con riesgos significativos para la operatividad y la seguridad nacional. Si bien el marco legal colombiano ofrece herramientas para sancionar a los responsables, existen limitaciones importantes relacionadas con la tipificación específica de los delitos, la prueba y atribución de responsabilidad en entornos complejos, la jurisdicción, la protección del secreto militar y la posible necesidad de actualización legislativa (Piñeros, 2020).

Para mitigar estos riesgos y fortalecer la capacidad de sanción, es fundamental que el Ejército Nacional invierta en robustecer sus sistemas de ciberseguridad, mejorar los controles de acceso y la auditoría, capacitar a su personal en seguridad de la información y colaborar

con las autoridades judiciales y legislativas para asegurar que el marco legal sea adecuado y efectivo para proteger la información crítica de la institución (Piñeros, 2020).

Identificación de las amenazas cibernéticas que ponen en riesgo la integridad de los datos del SICAD en la gestión logística del Ejército Nacional

Es importante tener en cuenta que la información sobre ataques cibernéticos a sistemas gubernamentales específicos a menudo no se hace pública por razones de seguridad y para evitar alertar a posibles atacantes.

Específicamente no hay una evidencia de amenaza directa en el contexto cibernético para el SICAD, teniendo en cuenta que este aplicativo es propiedad de España. Sin embargo, para el caso colombiano, existen algunos antecedentes clave sobre amenazas cibernéticas en Colombia que podrían afectar la integridad del SICAD, para lo cual el Ministerio de Defensa ha de enfocarse en solidas estrategias de ciberseguridad y ciberdefensa. Este tipo de antecedentes son:

- Ataques de grupos cibernéticos como hackers, en especial uno de ellos, denominado Guacamayas, que ingreso a los sistemas informáticos de las Fuerzas Armadas y obtuvo alrededor de 390 mil mensajes, 255.000 emails, y 178.000 documentos, que contenían información sobre actos de corrupción, irregularidades en operativos militares y demás documentos de seguridad nacional (Álzate León, 2023).
- Ataques cibernéticos durante el transcurso del 2022 a otras entidades del Estado tales como la Fiscalía, el Departamento Nacional de Estadística (DANE), el Invima y entidades del sector privado de salud como Keralty –operador de EPS Sanitas– sufrieron ataques cibernéticos durante el 2022 (Álzate León, 2023).
- Ataques cibernéticos del grupo de hackers denominado Anonymous, a la página web del Ejercito Nacional de Colombia, durante las manifestaciones de la protesta social de abril del 2021, con el objeto de reclamar justicia social ante el Estado colombiano

por las represiones de la fuerza pública contra la población manifestante (DIARIO AS, 2021).

- En otras ocasiones este grupo Anonymous también ha intervenido en los sistemas informáticos de las entidades del Estado colombiano, como sucedió en la época de 2011, cuando este grupo internacional se atrevió a desconectar las páginas web del Ministerio del Interior, el Ministerio de Defensa y la Presidencia de la Republica por más de 8 horas (DIARIO AS, 2021).
- En ese mismo año, también sucedieron ataques a otras entidades tales como la Universidad El Bosque en el mes de junio, la Aeronáutica civil para el mes de agosto, Empresas Publicas de Cali en el mes de octubre y la Pontificia Universidad Javeriana en el mes de octubre (Novoa Serrano, 2023).

Aunque no hay antecedentes públicos específicos de ataques cibernéticos contra el SICAD, el contexto general de las amenazas cibernéticas en Colombia y la sensibilidad de la información que maneja el SICAD lo convierten en un objetivo potencial. Por lo cual el gobierno colombiano ha estado implementando estrategias y fortaleciendo las capacidades en ciberseguridad para proteger las entidades públicas, incluyendo la creación del Centro de Operaciones de Seguridad Nacional (SOC) y la actualización del Modelo de Seguridad y Privacidad de la Información por el Ministerio TIC. La Policía Nacional también cuenta con un CAI Virtual para reportar delitos informáticos y ofrece recomendaciones en ciberseguridad (Impacto TIC SAS, 2025).

Algunas medidas adoptadas por el Ministerio de Defensa han sido: la formulación de Estrategia de ciberseguridad y ciberdefensa para 2011, ya que el Consejo Nacional de Política Económica y Social (CONPES) aprobó la estrategia de ciberseguridad y ciberdefensa para contrarrestar amenazas informáticas en el país. Además se crearon tres dependencias clave: el Grupo de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT), encargado de coordinar aspectos de ciberseguridad a nivel nacional; el Comando Conjunto Cibernético de las Fuerzas Militares, responsable de salvaguardar los intereses nacionales en el ciberespacio y el Centro Cibernético Policial, encargado de prevenir, investigar y apoyar la judicialización de delitos informáticos (Castillo & Jiménez, 2024).

La gestión logística del Ejército Nacional de Colombia, probablemente soportada por el Sistema de Comando y Control (SICAD) u otros sistemas de información relacionados, es vulnerable a diversas amenazas cibernéticas que podrían comprometer la integridad de sus datos. Estas amenazas pueden tener graves consecuencias para la operatividad, la seguridad y la planificación estratégica de la institución (Cámara Colombiana de Informática y Telecomunicaciones, 2024).

Amenazas Externas a la integridad del SICAD

Según el trabajo de Díaz & Cremades (2024) se encuentran las siguientes amenazas cibernéticas de carácter externo que podrían afectar la integridad del SICAD:

- Ataques de malware (Virus, Gusanos, Troyanos, Ransomware): Estos programas maliciosos pueden infiltrarse en el sistema a través de correos electrónicos infectados, dispositivos externos comprometidos o vulnerabilidades en el software. Pueden alterar, cifrar o eliminar datos del SICAD, interrumpiendo la gestión logística y potencialmente exigiendo un rescate (ransomware).
- Ataques de phishing y spear phishing: A través de correos electrónicos o mensajes fraudulentos que simulan ser comunicaciones legítimas, los atacantes pueden engañar al personal del Ejército para que revelen sus credenciales de acceso al SICAD, permitiendo el acceso no autorizado a la información logística. El *spear phishing* se dirige a individuos específicos con información personalizada para aumentar la probabilidad de éxito.
- Ataques de denegación de servicio (DoS y DDoS): Estos ataques buscan sobrecargar los servidores del SICAD con un volumen masivo de tráfico ilegítimo, impidiendo que el personal autorizado acceda al sistema y a los datos logísticos necesarios para la toma de decisiones y la ejecución de operaciones.
- Ataques a la cadena de suministro de software: Si los proveedores de software o hardware utilizados en el SICAD son comprometidos, los atacantes podrían

introducir vulnerabilidades o código malicioso que afecte la integridad de los datos logísticos.

- Amenazas Persistentes Avanzadas (APT): Grupos de ciberdelincuentes sofisticados o patrocinados por estados pueden llevar a cabo ataques dirigidos y prolongados para infiltrarse en el SICAD, obtener acceso a información sensible de logística y potencialmente manipularla sin ser detectados durante largos periodos.
- Ataques de intercepción (Man-in-the-Middle): Los atacantes podrían interceptar las comunicaciones entre los usuarios y los servidores del SICAD para robar o modificar datos logísticos en tránsito.
- Explotación de vulnerabilidades de software y hardware: Fallos de seguridad no parcheados en el sistema operativo, las aplicaciones o los dispositivos de red que soportan el SICAD pueden ser explotados por los atacantes para obtener acceso no autorizado y manipular la información logística.

Amenazas internas a la integridad del SICAD

Siguiendo el trabajo de Díaz Acevedo (2023), dentro del tipo de amenazas internas de carácter cibernético que ponen en riesgo la integridad de los datos del SICAD en la gestión logística del Ejército Nacional, se encuentran las siguientes a continuación:

- Empleados maliciosos: Personal interno con acceso legítimo al SICAD podría intencionalmente alterar, eliminar o robar datos logísticos por motivos personales, financieros o ideológicos.
- Empleados negligentes o no capacitados: La falta de conciencia sobre las buenas prácticas de ciberseguridad por parte del personal puede llevar a acciones involuntarias que comprometan la integridad de los datos, como hacer clic en enlaces maliciosos, compartir credenciales o conectar dispositivos no seguros a la red del Ejército.
- Errores humanos: Errores en la entrada de datos, la configuración del sistema o la gestión de los mismos pueden llevar a la corrupción o pérdida de información logística.

- Ingeniería social interna: Los atacantes podrían manipular o engañar a empleados del Ejército para obtener acceso físico a sistemas o información sensible relacionada con la gestión logística.

Consecuencias del Compromiso de la Integridad de los Datos del SICAD

Acorde a Montero & Garzón (2024), el personal a cargo de la logística que mantiene la integridad de los datos del SICAD, tiene una responsabilidad sumamente variada y compleja, el hecho de no cumplir cabalmente con dichas obligaciones traería serias consecuencias tales como:

- Interrupción de la cadena de suministro: La alteración de datos sobre inventarios, envíos o mantenimiento podría paralizar la logística del Ejército, afectando la disponibilidad de recursos críticos para las operaciones.
- Toma de decisiones erróneas: Información logística manipulada podría llevar a decisiones estratégicas y tácticas incorrectas, con graves consecuencias para la seguridad nacional.
- Pérdida de confianza: Un incidente de ciberseguridad que comprometa la integridad de los datos del SICAD podría erosionar la confianza del público y de otras instituciones en la capacidad del Ejército para proteger información sensible.
- Vulnerabilidad operacional: La manipulación de datos sobre despliegues, capacidades o recursos podría crear vulnerabilidades que podrían ser explotadas por adversarios.
- Pérdidas económicas: La recuperación de un incidente de ciberseguridad, la investigación y la implementación de medidas correctivas pueden generar costos significativos.

Es crucial que el Ejército Nacional de Colombia implemente medidas de ciberseguridad robustas para prevenir, detectar y responder a estas amenazas, protegiendo así la integridad de los datos del SICAD y garantizando la continuidad de sus operaciones logísticas. Estas medidas deben incluir la capacitación del personal, la implementación de

controles de acceso estrictos, la monitorización continua de la red, la aplicación de parches de seguridad y la elaboración de planes de respuesta a incidentes.

Formulación de una estrategia de ciberseguridad implementada para proteger la información del SICAD

En la era digital contemporánea, donde la información se ha consolidado como el activo estratégico más valioso de cualquier nación, la protección de infraestructuras críticas y sistemas de información sensibles no es simplemente una prioridad, sino un pilar fundamental de la seguridad nacional y la soberanía. Por lo tanto, el Estado colombiano, inmerso en un panorama geopolítico dinámico y un ciberespacio global cada vez más volátil y permeado por amenazas persistentes, reconoce el hecho trascendental de salvaguardar sus activos digitales más críticos.

Dentro de este contexto, el Sistema Integrado de Catalogación de Defensa (SICAD) emerge como el soporte indispensable para la operatividad y eficiencia de las Fuerzas Militares y la Policía Nacional. Al consolidar, organizar y estandarizar la información logística, de equipamiento y de recursos de toda la cadena de suministro del área de defensa colombiana, el SICAD no solo optimiza la toma de decisiones y la asignación de recursos, sino que también garantiza la interoperabilidad y la preparación operativa.

Por ello, la presente estrategia de ciberseguridad para el SICAD, está basada tanto en las políticas nacionales como internacionales, lineamientos del Ministerio de Defensa (2018) el Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de Tecnologías de la Información y las Comunicaciones (2025), así como de los estándares de la OTAN, a los que Colombia se adhiere. Igualmente se encuentra inspirada en el Modelo de Seguridad y Privacidad de la Información (MSPI) de Colombia, estructurándose en varios pilares clave para proteger la integridad, confidencialidad y disponibilidad de la información.

La estrategia de ciberseguridad para el SICAD no es una simple formalidad, sino una respuesta directa y holística a los hallazgos críticos de los objetivos anteriores: las

vulnerabilidades estructurales y las amenazas cibernéticas que hoy exponen la logística del Ejército.

Gestión del riesgo en la seguridad digital

Se espera que la presente iniciativa se imponga no como un simple plan estático, sino que actué como un organismo vivo que se adapte a un entorno complejo y volátil de amenazas que mutan diariamente.

En ese sentido, el primer pilar sobre el cual descansa esta propuesta se enfoca en la implementación de políticas de seguridad digital específica para el SICAD alineadas con el MSPI de Colombia y los estándares internacionales (ISO/IEC 27001), y con la Resolución 500 de 2021 del MinTIC y la Directiva Permanente No. 34 de 2018 del Ministerio de Defensa Este ha de ser el manual operativo que todo el personal ha de seguir.

Este pilar aborda las vulnerabilidades estructurales del SICAD, como los sistemas descentralizados y la falta de auditoría y trazabilidad. La gestión de riesgos se implementará como un proceso continuo y proactivo, utilizando el Marco de Ciberseguridad del NIST (2024), un estándar global de gestión de riesgos. Esta metodología no solo identifica, evalúa y mitiga amenazas, sino que también se alinea con la propuesta de un sistema de análisis continuo y proactivo, garantizando que la estrategia no sea un simple plan estático, sino un organismo vivo que se adapte y anticipe a amenazas en constante mutación. La inteligencia de amenazas será vital para modelar escenarios de ataque y entender cómo adversarios externos e internos podrían explotar estas vulnerabilidades para manipular datos, como se evidenció en el ataque de Guacamayas a las Fuerzas Armadas (Álzate León, 2023).

La metodología NIST, en su enfoque de gestión de riesgos, se divide en tres niveles de análisis interconectados:

- Nivel 1: Análisis a Nivel de Negocio (Tier 1 a Tier 4): Este nivel evalúa cómo las decisiones de ciberseguridad se integran con los objetivos de la misión del Ejército. Al analizar los riesgos desde una perspectiva estratégica, se logra una comprensión

profunda de cómo una brecha en el SICAD podría afectar directamente la toma de decisiones y la operatividad de la fuerza.

- Nivel 2: Análisis a Nivel de Misión/Proceso: Aquí, se identifican los procesos específicos que dependen del SICAD (logística, transporte, inventarios) y se evalúan los riesgos asociados a cada uno de ellos. Se utiliza inteligencia de amenazas para modelar escenarios de ataque y entender cómo adversarios, desde ciberdelincuentes hasta actores de estados hostiles, podrían intentar penetrar el sistema.
- Nivel 3: Análisis a Nivel de Implementación: En este nivel, se identifican las vulnerabilidades técnicas en el *hardware* y *software* del SICAD. Se realizan evaluaciones detalladas de la seguridad para encontrar debilidades en los controles de acceso, el cifrado y la arquitectura de red, y se priorizan las acciones de mitigación.

Otro aspecto es la clasificación de la información de los datos del SICAD según su nivel de sensibilidad, que ira desde el más abierto hasta el más cerrado asi: publico, reservado y confidencial. Además cada pieza de información tendrá un "nivel de blindaje" específico, con controles de acceso y monitoreo adaptados a su sensibilidad, siguiendo los principios de la Ley 1581 de 2012 sobre protección de datos (Congreso de la República de Colombia, 2012).

Control sobre la accesibilidad a la información

El segundo pilar sobre el cual gira la presente estrategia es el control de acceso, que garantiza que solo el personal autorizado puede acceder a la información y a los lugares que les corresponda. Ello comprende el proceso de autenticación de factores múltiples, que ha de consistir en biométricos o tokens de seguridad que demuestren que el usuario es quien dice ser, teniendo en cuenta principios de mínimo privilegio, al solo contar con las llaves necesarias para su labor, y los sistemas de monitoreo 24/7 que indiquen irregularidades en el acceso legítimo de los usuarios.

Este pilar es el blindaje técnico que responde directamente a las vulnerabilidades en el hardware, software y la falta de cifrado robusto, así como a las amenazas de malware, ataques a la cadena de suministro y APTs (Díaz & Cremades, 2024).

La sensible naturaleza de la información que alberga el SICAD, que van desde inventarios de armamento y equipos hasta datos de personales y cadenas de suministro críticos, lo convierte en un objetivo deseado para diversos grupos de interés con fines maliciosos: desde ciberdelincuentes que lo hacen por motivos económicos, hasta grupos auspiciados por Estados corruptos, que buscan información confidencial o generar sabotaje. Es por estas razones que una brecha de seguridad en el SICAD no se traduciría únicamente en pérdidas económicas o interrupción de servicios; sino también en la vulneración de la capacidad operativa de las fuerzas armadas, socavando la seguridad y defensa del Estado colombiano.

Protección de la arquitectura de la información y cultura digital

Este tercer pilar seria el blindaje técnico que ha de proteger el sistema de los golpes más duros. Entre sus procesos se cuentan: el cifrado de extremo a extremo, en el cual se encripta la información del SICAD, tanto al almacenarse en los servidores como cuando se navegue por la red. A esto se le suma el proceso de defensa perimetral o interna, en el cual se contaría con un ecosistema de seguridad en capas. Este enfoque, más robusto que una simple defensa perimetral, asume que una brecha es inevitable y diseña controles de seguridad en múltiples niveles para contener y mitigar el daño. Cada capa actúa como una barrera adicional, frustrando el avance de un atacante una vez que ha penetrado la primera línea de defensa. La primera capa de defensa es la piel externa, los controles perimetrales, que buscan mantener a los atacantes fuera. Sin embargo, si logran romperla, se encuentran con capas internas, cada una con sus propias barreras. Este modelo de defensa en profundidad es el núcleo de nuestro ecosistema, y vendría establecido de la siguiente forma:

Cifrado de extremo a extremo (Capa de Protección de Datos): Esta es la capa más cercana al centro de la cebolla. El cifrado de extremo a extremo garantiza que la información del SICAD se mantenga encriptada, tanto cuando se almacena en los servidores (datos en reposo) como cuando viaja a través de la red (datos en tránsito). Incluso si un atacante logra penetrar la red, la información que obtendría sería ilegible, frustrando su objetivo (Guijarro-

Rodríguez, et al., 2018). El cifrado de extremo a extremo garantiza que los datos en reposo y en tránsito permanezcan ilegibles incluso si son interceptados, mitigando el riesgo de ataques Man-in-the-Middle.

Defensa perimetral e interna (Capas de Control de Acceso a la Red): Este enfoque tiene tres elementos (CREST, 2019): Firewalls de última generación, que actúan como la primera puerta de entrada, filtrando el tráfico de aplicaciones maliciosas y bloqueando accesos no autorizados a la red, y los Sistemas de Detección y Prevención de Intrusos (IDPS), considerados como los "guardias de seguridad" que monitorean la red en busca de comportamientos sospechosos, como un acceso inusual o una transferencia masiva de datos, y bloquean la actividad de inmediato.

Cabe mencionar que los firewalls y Sistemas de Detección de Intrusos (IDPS) actúan como la primera línea de defensa contra amenazas como los ataques de Denegación de Servicio (DoS) y la explotación de vulnerabilidades.

Otro componente de este ecosistema es la microsegmentación de la red, que consiste en una capa de seguridad crucial que divide la red del SICAD en pequeños segmentos, creando barreras internas. Si un atacante logra entrar, la microsegmentación le impide moverse lateralmente a través de la red hacia activos más críticos. Es como si cada sala del edificio tuviera su propio cerrojo, evitando que un ladrón, una vez dentro, tenga acceso a todo el lugar. Esta medida mitiga el riesgo de Amenazas Persistentes Avanzadas (APT) que buscan infiltrarse y permanecer indetectadas.

La defensa no se limita a las barreras tecnológicas. Un elemento vital del ecosistema es un equipo especializado dedicado a la gestión de vulnerabilidades. Este equipo opera de forma proactiva, buscando y corrigiendo debilidades en el *hardware* y *software* del sistema antes de que sean explotadas. Su misión es la aplicación rigurosa e inmediata de parches de seguridad, cerrando las "ventanas" de oportunidad antes de que los atacantes puedan usarlas (SEI, Carnegie Mellon University, 2019).

Finalmente, el ecosistema de seguridad debe ser resiliente. Para ciberataques de alto impacto o de espectro amplio, se debe contar con un plan de copias de seguridad regular y un protocolo de recuperación ante desastres. Estos procedimientos aseguran la continuidad del servicio y la disponibilidad de los datos, permitiendo al sistema recuperarse rápidamente de un incidente sin perder información crítica (Palo Alto Networks, 2022).

Este enfoque holístico no solo protege los datos logísticos del Ejército, sino que también garantiza que la institución mantenga su capacidad operativa incluso frente a las amenazas más sofisticadas.

Por último, existe un cuarto pilar, dedicado a considerar la importancia del personal en los sistemas de seguridad, por lo cual el personal del SICAD ha de participar en simulacros de ciberataques de forma regular, con el objeto de aprender los puntos críticos para identificar el phishing reportar incidentes de seguridad y entender las tácticas del enemigo en un entorno controlado. También se necesita invertir en la generación de cultura de seguridad digital (SANS Institute, 2023), con la finalidad de que cada empleado del SICAD comprenda su rol en la protección del sistema y de los datos sensibles, promoviendo la ética y la responsabilidad.

Ante esta realidad ineludible, la formulación de una estrategia de ciberseguridad robusta, adaptable y proactiva para el SICAD no es una opción, sino una necesidad imperante. Esta estrategia debe trascender la mera implementación de soluciones tecnológicas, a incluir una visión holística que integra personas, procesos y tecnología, y que esté alineada con los marcos normativos nacionales e internacionales, las mejores prácticas de la industria y las especificidades del entorno de defensa.

Solo a través de una aproximación profunda, concisa y concretamente planificada se podrá construir una barrera digital impenetrable, asegurando la integridad, confidencialidad y disponibilidad de la información crítica del SICAD y, con ello, fortaleciendo la capacidad de Colombia para enfrentar los desafíos de la seguridad del siglo XXI.

Conclusiones

La seguridad del Sistema Integrado de Catalogación de Defensa (SICAD) es mucho más que un desafío técnico; es un pilar fundamental de la soberanía y la seguridad nacional de Colombia. La protección de este sistema no se limita a la implementación de firewalls y antivirus, sino que exige una visión holística que integre la tecnología con una robusta gobernanza.

La interconexión de las Fuerzas Militares con redes y plataformas digitales, sumada a un panorama de amenazas cibernéticas en constante evolución, desde ciberdelincuentes hasta actores de estados hostiles, hace que el SICAD sea un objetivo de alto valor. Un ataque exitoso podría comprometer la cadena de suministro, la planificación logística e incluso las operaciones en el terreno, afectando directamente la capacidad de respuesta y la integridad de la defensa del país. Por lo tanto, cualquier estrategia de protección debe ser dinámica, proactiva y basada en inteligencia, anticipándose a los riesgos en lugar de simplemente reaccionar a ellos.

La gestión del riesgo para el SICAD requiere un enfoque meticuloso y multinivel. No es suficiente con blindar el perímetro; es crucial clasificar la información, segmentar la red y aplicar el principio de menor privilegio, garantizando que cada usuario tenga acceso solo a los datos estrictamente necesarios para sus funciones. La capacitación del personal es igualmente vital, ya que el factor humano sigue siendo el eslabón más vulnerable. Un error, una negligencia o la falta de conciencia sobre las amenazas pueden abrir una brecha crítica, sin importar cuán sofisticados sean los sistemas de seguridad.

El éxito de la protección del SICAD reside en la capacidad de las Fuerzas Militares para crear una cultura de ciberseguridad que permee todos los niveles de la organización, desde los líderes que formulan las políticas hasta el personal en el terreno. Esta cultura debe fomentar la vigilancia constante, el reporte de incidentes y la mejora continua, reconociendo que la ciberseguridad es un proceso, no un proyecto con un punto final.

Finalmente, la protección del SICAD es un reflejo de la modernización de la defensa de Colombia. La adopción de estándares internacionales como los de la OTAN, junto con una alineación con la normatividad nacional, demuestra un compromiso serio con la excelencia en ciberseguridad. Sin embargo, este esfuerzo debe ir acompañado de una inversión sostenida en tecnología, talento especializado y centros de análisis de amenazas.

La lucha por la seguridad del SICAD es una guerra silenciosa y constante, donde la victoria depende de la adaptabilidad, la inteligencia y la resiliencia. Proteger este sistema es, en esencia, salvaguardar la capacidad de Colombia para defenderse, operar de manera eficiente y mantener su liderazgo en una región donde la guerra no cinética es una realidad cada vez más presente.

Referencias

Acore (2019). Colombia ascendió en el Sistema de Catalogación de Defensa OTAN. https://www.acore.org.co/17174/colombia-ascendio-en-el-sistema-de-catalogacion-de-defensa-otan/

Aguilar, J. (2021). Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciberamenazas a la seguridad nacional y política exterior. https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0719-37692021000100169

Álzate León, J. 31 de Enero de 2023. Ataques cibernéticos en contra de las Fuerzas Armadas: 10 presuntos involucrados fueron trasladados. Infobae. Artículo en línea. Disponible en: https://www.infobae.com/colombia/2023/01/31/ataques-ciberneticos-en-contra-de-las-fuerzas-armadas-10-presuntos-involucrados-fueron-trasladados/

Barrios Torres, S. (2024). Disrupción en las cadenas de suministro: impacto en la defensa y la seguridad nacionales. Sello Editorial ESDEG. https://doi.org/10.25062/9786287602823

Barrios Torres, S. (2024). La cadena logística del Ejército Nacional de Colombia y ciberseguridad y ciberdefensa: atención a la academia. En M. E. Realpe Díaz, & A. M. González (Eds.),

Tecnologías disruptivas, logística y seguridad y defensa nacional en el ciberespacio (pp. 77-110). Sello Editorial ESDEG. https://doi.org/10.25062/9786287602700.03

Beer, M., & Nohria, N. (2003). Las dimensiones del cambio. En R. Luecke, Harvard Business. Pag. 17-24. https://hbsp.harvard.edu/product/7119BC-HCB-ENG

Benítez, R. (1986). "El pensamiento militar de Clausewitz". *Revista Mexicana de Ciencias Políticas y Sociales.* (126), 97-123.

Bermúdez, C. y Cano, J. (2023). Modelo de Ciberseguridad par Modelo de Ciberseguridad para el Sector Logístico y Transporte Terrestre. https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1001&context=isla2023

Bernal. C. 2016. *Metodología* de la investigación. Cuarta Edición. *PEARSON*. Colombia

Cámara Colombiana de Informática y Telecomunicaciones. 26 de abril de 2024. Ciberseguridad en Colombia: desafíos y perspectivas. https://www.ccit.org.co/articulos-tictac/ciberseguridad-en-colombia-desafios-y-perspectivas/

Castillo Pulido, L., & Jiménez Acosta, J. (2024). Cooperación internacional policial ante amenazas cibernéticas en Colombia: Modalidad Business Email Compromise. *Revista Logos Ciencia & Tecnología*, *16*(1), 83-107. Epub February 18, 2024.https://doi.org/10.22335/rlct.v16i1.1877

CEDE4 Directiva Permanente 00050 de 2021 Planeamiento Logístico

Celemín, C. (2015). Fortalecimiento de la logística militar como estrategia en su desarrollo ante el postconflicto en Colombia. Universidad Militar Nueva Granada. https://repository.unimilitar.edu.co/server/api/core/bitstreams/57a24d54-ed0d-4343-86df-de9137aef9f7/content

Cheung K., Bell, M. G. H. y J. Bhattacharjya. 2021. "Cybersecurity in logistics and supply chain management: An overview and future research directions, "Transportation Research Part E: Logistics and Transportation Review, 146, 102217

Congreso de la República de Colombia. (2012). Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.

CREST. (2019). *What is Cyber Threat Intelligence and how is it used?*. CREST International. https://www.crest-approved.org/wp-content/uploads/2022/04/CREST-Cyber-Threat-Intelligence.pdf

Departamento de logística del Ejército nacional de Colombia (2023) *Sistema OTAN de Catalogación*. https://www.ejercito.mil.co/sistema-otan-catalogacion/

DIARIO AS. 6 de mayo de 2021. Anonymous en Colombia: Cuál ha sido su último movimiento y qué más planean hacer. Artículo en línea. Disponible en: https://colombia.as.com/colombia/2021/05/06/actualidad/1620334033_976860.html

Díaz Acevedo, M. (2023). La evolución de la estrategia de ciberseguridad de Colombia 2011-2021. Universidad de Nebrija. 10.13140/RG.2.2.22241.58723.

Díaz Acevedo, M. y Cremades Guisado, Álvaro (2024) «Revisión del estado actual de la ciberseguridad en Colombia», *Estudios en Seguridad y Defensa*, 19(38), pp. 179–203. doi: 10.25062/1900-8325.1999.

Díaz del Río, J. (2011) "La ciberseguridad en el ámbito militar" en *Cuadernos de Estrategia*. N°149. Págs. 215-256.

Díaz R. 2021. "Estado de la ciberseguridad en la logística de américa latina y el caribe," Serie Desarrollo Productivo, (228), pp. 68

Díaz, R. y Núñez, G. (2023) Ciberataques a la logística y la infraestructura crítica en América Latina y el Caribe. Documentos de Proyectos (LC/TS.2023/93), Santiago, Comisión Económica para América Latina y el Caribe (CEPAL), 2023.

Función Pública (2009). Ley 1273 de 2009. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Función Pública (2014). Ley1712 de 2014. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=56882

Guijarro-Rodríguez, A., Yepez-Holgin, J. M., Peralta-Guaraca, T. J., & Ortiz Zambrano, M. C. (2018). Defensa en profundidad aplicado a un entorno empresarial. Revista Espacios, 39(42), 19.

Hernández-Sampieri, R. & Mendoza, C *(*2018*).* Metodología de la investigación. Las rutas cuantitativa, cualitativa y mixta. Editorial : Mc Graw Hill educación

Impacto TIC SAS. 19 de mar de 2025. Ciberseguridad en Colombia: Estrategias y Desafíos Actuales. En linea. Disponible en: https://impactotic.co/ciber-seguridad/ciberseguridad-en-colombia-riesgos-a-los-que-se-enfrenta-el-

pais/#:~:text=Colombia%20cada%20vez%20es%20m%C3%A1s,pa%C3%ADses%20que%20m%C3%A1s%20reciben%20ataques.

ISO/IEC (2022) *Gestión de seguridad de la información*. (ISO 27001:2022)

Jiménez, J.E. y Hernández, S. (2002). *Marco conceptual de la cadena de suministro: un nuevo enfoque logístico*. (Publicación técnica No. 215) Sanfandila, Qro, En: http://imt.mx/archivos/Publicaciones/PublicacionTecnica/pt215.pdf

Ley estatutaria 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. Octubre 17 de 2012. D. O.: 48587

Microsoft Threat Intelligence (2023) *Microsoft Digital Defense Report*. https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023

Ministerio de Defensa Nacional. (2018). Directiva Permanente No. 34 de 2018. Lineamientos y directrices para los Escalones de Catalogación del Sistema OTAN de Catalogación en las unidades ejecutoras del Ministerio de Defensa Nacional y la Policía Nacional.

Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). (2025). Estrategia Nacional de Seguridad Digital de Colombia 2025-2027.

Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). (2021). Resolución 500 de 2021. Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno DigitAlabama.

Montero Moncada, L. A., & Garzón Gómez, O. A. (2024). *Comandos. Retos de las Fuerzas Especiales e Inteligencia en la guerra contemporánea*. Sello Editorial ESDEG. https://doi.org/10.25062/9786287602809

Mozo Rivera, O., & Ardila Contreras, J. V. (2022). El fenómeno de las ciberamenazas: afectaciones a la ciberseguridad del Ejército nacional de Colombia. *Perspectivas En Inteligencia*, *14*(23), 63–95. https://doi.org/10.47961/2145194X.333

National Institute of Standards and Technology (NIST). (2024). *Marco de Seguridad Cibernética (CSF) 2.0*. Publicación especial del NIST. https://www.nist.gov/cyberframework/

Novoa Serrano, P. 10 de mayo de 2023. Ataque cibernético a entidad estatal: El reto de Colombia frente a la seguridad de la información. Asesores especializados en protección de datos

personales, derecho comercial y corporativo. Artículo en línea. Disponible en: https://mslegal.com.co/ataque-cibernetico-a-entidad-estatal-el-reto-de-colombia-frente-a-la-seguridad-de-la-informacion/

OEA (2003) Programa de Ciberseguridad. https://www.oas.org/ext/es/seguridad/prog-ciber

Palo Alto Networks. (2022). *A Practical Guide to Adopting Zero Trust in the SOC*. https://start.paloaltonetworks.com/rs/531-OCS-018/images/cortex_eb_practical-guide-to-adopting-zero-trust_092022-v2.pdf

Peña, J. (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

Piñeros Castiblanco, D. H. Pamplona. Mayo 21 de 2020. Análisis de la cadena de suministros del batallón décimo sexta brigada de Yopal Casanare. Universidad de Pamplona.http://repositoriodspace.unipamplona.edu.co/jspui/bitstream/20.500.12744/5169/1/Pi%C3%B1eros_2020_TG.pdf

Quesada Valderrama, F. Abril de 2018. Análisis de la gestión actual del centro de distribución logística del Ejército Nacional DE Colombia. Universidad Militar Nueva Granada. https://repository.umng.edu.co/server/api/core/bitstreams/0ba9f1e4-5b49-449a-b93d-984435572dad/content

RCN Noticias (2013). Colombia ingresa al Sistema Integrado de Catalogación de Defensa de la OTAN. https://www.rcnradio.com/colombia/colombia-ingresa-al-sistema-integrado-de-catalogacion-de-defensa-de-la-otan-66104

Riquelme, B. (2013). Optimización de la logística mediante la gestión de inventario. Revista de marina, tomo liv.- Valparaíso, marzo 31 de 1913.- núm. 321. http://revistamarina.cl/revistas/2013/2/RM%20N%BA%202-2013.pdf

Salamanca, I. (2015). La Catalogación OTAN y las Fuerzas Militares Colombianas. Universidad Militar Nueva Granada. https://core.ac.uk/download/pdf/143450692.pdf

Sánchez Hurtado, J. R., Montero Moncada, L. A., Ardila Castro, C. A., & Ussa Cabrera, A. J. (2011). Logística militar en los conflictos del siglo XXI. El espacio y los retos ofrecidos por la guerra asimétrica. *Revista Científica General José María Córdova*, *9*(9), 15–32. https://doi.org/10.21830/19006586.243

SANS Institute. (2023). *Cybersecurity Awareness and Training Roadmap*. URL: https://www.sans.org/whitepapers/cybersecurity-awareness-and-training-roadmap/

Sistema de Catalogación de la Defensa – SICAD (2024) *Manual de usuario*. https://working.mde.es/portalservicios/servicios/industriadefensa/catalogacion/

Software Engineering Institute (SEI), Carnegie Mellon University. (2019). *Multi-Method Modeling and Analysis of the Cybersecurity Vulnerability Management Ecosystem*. https://www.sei.cmu.edu/documents/581/2019_019_001_550437.pdf

Stanković, N. (2019). "The conceptual analysis of identities and interests in the thought of Alexander Wendt". *Politeia. 9* (18), 37-154

Tafur, Y. & Arenas, Y. (2023). Transformando la Logística Militar en Colombia mediante Inteligencia Artificial: Innovaciones y Desafíos, 4(2), 50-69. https://doi.org/10.55813/gaea/ccri/v4/n2/231

Wendt, A. (1994). "Collective identity formation and the international state". *American Political Science Review. 88* (2), 384-396