Estrategias de Mitigación de Riesgo de Amenazas Cibernéticas en la Cadena de Abastecimientos: Enfoque en el Ejército Nacional

Mayor John Kevin Noya Duarte

Artículo para optar al título profesional:

Magister en Ciberseguridad y Ciberdefensa

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

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

DATOS GENERALES		
Nombre del estudiante	**:**	Mayor JOHN KEVIN NOYA DUARTE
Identificación	**:**	1032380008
Programa académico	**:**	Maestría en Ciberseguridad y Defensa
Tutor metodológico	**:**	CR. Aldemar Serrano Cuervo
Tutor temático	**:**	CR. Aldemar Serrano Cuervo
Fecha de entrega	**:**	17 de Octubre de 2025
Extensión	**:**	10.506 palabras

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

Estrategias de Mitigación de Riesgo de Amenazas Cibernéticas en la Cadena de Abastecimientos: Enfoque en el Ejército Nacional

Mitigation Strategies for Cyber Threat Risks in the Supply Chain: An Approach for the Colombian Army

John Kevin Noya Duarte[1]

[1] Mayor del Ejército Nacional de Colombia. Candidato a Magíster en Ciberseguridad y Ciberdefensa, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Profesional en Ciencias Militares, Escuela Militar de Cadetes "General José María Córdova". Profesional en Administración de Empresas, Universidad Militar "Nueva Granada" Colombia. https://orcid.org/0009-0008-1232-2935 - Contacto: john.noya@esdeg.edu.co.

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

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: La cadena de abastecimiento militar es esencial para el sostenimiento en conflictos híbridos y de sexta generación, pero la digitalización de sistemas como SAP-SILOG amplía la superficie de ataque. Este artículo analiza la evolución doctrinal y tecnológica de la logística militar y propone un modelo estratégico de mitigación cibernética adaptado al contexto colombiano. Metodológicamente combina revisión doctrinal con simulaciones dinámicas que evalúan el impacto de DDoS, ransomware e inyección de datos en inventarios y procesos críticos. El modelo integra la Arquitectura Zero Trust (NIST SP 800-207), la matriz MITRE ATT&CK**,** IA/ML para detección de anomalías y blockchain para trazabilidad. Se plantea su implementación mediante pilotos y manuales técnicos. El aporte radica en un marco replicable para prevenir, detectar, responder y adaptarse, fortaleciendo la resiliencia, disponibilidad y flexibilidad logística en operaciones conjuntas.

Palabras clave: logística militar; ciberseguridad; cadena de abastecimiento; ciber resiliencia; ciberdefensa; operaciones conjuntas; inteligencia artificial; blockchain.

Abstract: The military supply chain is critical to sustaining operations under hybrid and sixth-generation conflicts, yet digital platforms such as SAP-SILOG increase the attack surface. This paper analyzes doctrinal and technological advances in military logistics and proposes a strategic cyber risk mitigation model for Colombia's Armed Forces. The methodology combines doctrinal review with **dynamic simulations** assessing the impact of DDoS, ransomware, and data tampering on critical processes. The model incorporates Zero Trust Architecture (NIST SP 800-207), the MITRE ATT&CK framework**,** AI/ML anomaly detection, and blockchain for data integrity and traceability. A roadmap for institutionalization is outlined through technical manuals and pilot projects. The contribution is a replicable framework to prevent, detect, respond, and adapt to cyberattacks, enhancing resilience, availability, and flexibility in joint military logistics.

Keywords: military logistics, cybersecurity, supply chain, cyber resilience, cyber defense, joint operations, artificial intelligence, blockchain.

Estrategias de Mitigación de Riesgo de Amenazas Cibernéticas en la Cadena de Abastecimientos: Enfoque en el Ejército Nacional

1. Introducción.

La logística militar ha sido históricamente la fuerza vital de las operaciones militares, actuando como la columna vertebral que sostiene el despliegue, sostenimiento y reconfiguración de las fuerzas en el terreno. En Colombia, la doctrina logística adoptada por las Fuerzas Militares ha evolucionado de modelos tradicionales a sistemas cada vez más integrados, automatizados y adaptativos. Este proceso ha sido impulsado por la necesidad de responder a amenazas complejas y multiformes que incluyen desde conflictos irregulares hasta desafíos transnacionales, donde la velocidad de respuesta y la trazabilidad de los recursos logísticos son elementos determinantes para el éxito operacional (Serrano et al., 2025)

En Colombia, el sistema de información logística SAP-SILOG constituye actualmente la herramienta principal utilizada por las Fuerzas Militares para la planificación, seguimiento y control de procesos logísticos en tiempo real. Aunque su implementación ha permitido una mejora progresiva en la trazabilidad y eficiencia de los recursos, su uso sigue limitado a una perspectiva nacional. A nivel mundial, diversas fuerzas armadas han adoptado plataformas ERP más especializadas o adaptadas a sus necesidades estratégicas, como el GCSS-Army (Global Combat Support System) en EE. UU., el DLMS (Defense Logistics Management Standards) y el LOGFAS (Logistics Functional Area Services) en contextos OTAN. (Joint Logistics JP 4-0, 2019)

Estos sistemas no solo permiten una integración operativa entre dominios, sino que también incorporan módulos de ciberdefensa, inteligencia logística y capacidades predictivas a través de inteligencia artificial y gemelos digitales. Según Isaza, (2012), "el desafío no está solo en distribuir los recursos, sino en proteger los datos, los nodos logísticos y las redes que hacen viable el soporte operacional" (p. 28), resaltando la necesidad de avanzar hacia una arquitectura logística resiliente y robustecida frente a amenazas cibernéticas en un entorno conjunto e interagencial.

En el actual entorno operacional, caracterizado por la conectividad total y la convergencia entre dominios físicos y digitales, la ciberseguridad ha pasado de ser una función complementaria para convertirse en un pilar estratégico. Las operaciones del ciberespacio, como lo establece el MCE 3-12, son esenciales para garantizar la superioridad operacional, y su integración en las funciones logísticas no es una opción, sino una exigencia doctrinal (MCE 3-12 Operaciones del Ciberespacio, 2021).

Las infraestructuras logísticas son objetivos frecuentes de actores maliciosos que buscan interrumpir la cadena de suministro, generar desinformación o capturar información estratégica. Esta vulnerabilidad se acentúa en contextos donde se desarrollan operaciones conjuntas, donde interoperabilidad, coordinación y sincronización logística son cruciales. Como lo advierte la doctrina estadounidense en el informe *Sustaining Multidomain Operations*, las fuerzas deben estar preparadas no solo para resistir ataques cinéticos, sino también ciberataques que busquen desarticular la sostenibilidad logística desde sus nodos de mando y control (Quinn, 2023)

Dado el contexto planteado, esta investigación busca dar respuesta a la siguiente pregunta: **¿Cómo mitigar el riesgo de amenazas cibernéticas en el desarrollo de las operaciones logísticas en la cadena de abastecimiento?** Para ello, se establece como objetivo general**:** Diseñar una estrategia de mitigación de riesgos cibernéticos para las operaciones logísticas en la cadena de abastecimientos. Conllevando a determinar como objetivos específicos**:**

1. Caracterizar las vulnerabilidades actuales en los sistemas de información logística en el procedimiento de la cadena de abastecimientos.
2. Realizar Ciberataques simulados en la caracterización de la cadena de abastecimientos en las Operaciones Logísticas.
3. Proponer un modelo de prevención mediante herramientas tecnológicas cibernéticas.

2. Metodología

Esta investigación adopta un enfoque metodológico mixto, en el que se articulan herramientas de análisis cualitativo y cuantitativo con el objetivo de comprender integralmente las vulnerabilidades cibernéticas en la cadena de abastecimientos militar y proponer estrategias efectivas de mitigación adaptadas al entorno del Ejército Nacional de Colombia.

Desde una perspectiva cualitativa, se realiza una revisión documental y doctrinal de más de 80 fuentes especializadas, incluyendo manuales de doctrina conjunta de las Fuerzas Militares y de cada Fuerza, informes técnicos (MITRE ATT&CK, 2025; Rose et al., 2020),

y casos de estudio de países miembros de la OTAN, Estados Unidos, la Unión Europea y América Latina. Esta revisión busca identificar los avances doctrinales y tecnológicos en materia de logística militar y ciberseguridad aplicada, así como extraer lecciones aprendidas frente a incidentes reales de ciberataques a infraestructuras logísticas.

En cuanto al componente cuantitativo, se emplearán el software Arena para la caracterización de la Cadena de Abastecimientos normal dentro de las FFMM y bajo posibles ciberataques, lo que permitió representar los diferentes tipos de amenaza en la cadena de abastecimiento militar en condiciones normales (ataques de denegación de servicio, inyección de malware, manipulación de datos) en las operaciones logísticas de la cadena de abastecimientos (recepción, almacenamiento, transporte, entrega) y reconocer los puntos de mayor vulnerabilidad. A partir del análisis teórico de esta caracterización, se podrán proponer las TTP's (Técnicas, Tácticas y Procedimientos) dentro de la trazabilidad de incidentes y sostenibilidad operativa.

El procedimiento se estructura en las siguientes fases:

1. Caracterización de la Cadena de Abastecimientos conjunto actual, incluyendo el flujo doctrinal de los procesos logísticos y los sistemas de información disponibles.
2. Identificación de vulnerabilidades a partir del análisis documental, y categorización mediante marcos de referencia como MITRE ATT&CK.
3. Identificación de escenarios de ciberataques, describiendo la técnica de la amenaza y el impacto esperado en la Operación Logística que afecta el flujo de la Cadena de Abastecimientos.

4. Propuesta de un modelo estratégico de mitigación, sustentado en tecnologías emergentes como inteligencia artificial, Blockchain, MFA y sistemas de ciberinmunidad, con base en las recomendaciones técnicas y doctrinales recogidas en la revisión.

3. Fundamentos doctrinales y evolución de la logística militar

3.1 Historia y principios de la logística militar

Desde las antiguas campañas de Alejandro Magno hasta los despliegues modernos de coaliciones multinacionales, la logística militar ha sido el componente invisible que define la capacidad real de combate. El Coronel George C. Thorpe, (1986), uno de los primeros teóricos logísticos del siglo XX, sentenció que "la logística es la médula espinal de la guerra"(p. 10), destacando su rol como garante del sostenimiento estratégico y operacional de las tropas.

La evolución de la logística ha transitado desde el abastecimiento básico de tropas con alimentos y armas, hasta convertirse en una ciencia multidimensional que integra transporte, almacenamiento, distribución, mantenimiento, infraestructura, comunicaciones y ahora ciberseguridad. Henry Eccles, propuso una diferenciación entre logística estratégica, operacional y táctica, abriendo el camino para el diseño de modelos doctrinales que siguen vigentes en el planeamiento conjunto (Eccles, 1959).

En el contexto del Ejército de Colombia, bajo el concepto del Sostenimiento como principio de las Funciones de Conducción de la Guerra, se señala en el Manual Fundamental

del Ejército (MFE 4-0 Sostenimiento, 2016) la definición del concepto de la logística como herramienta esencial para el "Planeamiento y ejecución del movimiento y el apoyo de las fuerzas" (p. 1). Este principio demuestra que el cumplimiento de la misión se logra mediante la provisión de capacidades que garanticen sostenimiento y libertad de acción, de la misma forma este concepto ha sido incorporado en las operaciones conjuntas, en la doctrina estandarizada para la Armada y Fuerza Aeroespacial, bajo la conducción del Comando General de las Fuerzas Militares (MFC 5-0 Planeamiento Conjunto, 2024) .

3.2 Transformación doctrinal: de la logística tradicional a la logística en red

La evolución de la doctrina logística militar ha transitado desde un modelo secuencial y lineal, centrado en el abastecimiento reactivo, hacia una concepción en red, interoperable y anticipativa. En el modelo tradicional, cada fuerza (Ejército, Armada, Fuerza Aeroespacial) gestionaba sus recursos logísticos de forma autónoma, con sistemas cerrados, dependientes de registros físicos o bases de datos locales, lo cual dificultaba la trazabilidad, coordinación y respuesta en escenarios conjuntos (Manual FF.MM. 4-9, 2012).

Con el avance doctrinal y tecnológico, se impulsó la transformación hacia la logística en red**,** basada en la centralización de la información, la interoperabilidad entre sistemas y la automatización de procesos mediante sistemas ERP logísticos como LOGFAS (NATO), DLMS (DoD USA) o SAP-SILOG. Esta evolución responde a la necesidad de adaptar la logística a entornos operacionales dinámicos, multidominio y de alta incertidumbre. Como lo plantea el JP 4-0 del Estado Mayor Conjunto de EE. UU., la logística moderna debe

integrar capacidades conjuntas, interagenciales y multinacionales, empleando flujos de información en tiempo real y coordinación a nivel estratégico, operacional y táctico (NATO, 2018).

En Colombia, este cambio se ha implementado con el Sistema de Información Logístico SAP-SILOG, al igual que se plantea la activación del Comando Logístico Conjunto (COLOC), que busca consolidar la función logística como eje transversal del poder conjunto. Según el (REGLAMENTO FF.MM. 4-2, 2016), esta transformación implica una migración del enfoque de "suministro por demanda" hacia un "suministro por previsión y modelado", el cual debe ser apoyado en tecnologías emergentes como la inteligencia artificial, la sensorización (IoT) y la gestión de datos logísticos desde el nivel estratégico (REGLAMENTO FF.MM. 4-2, 2016).

Este tránsito también es respaldado en el marco OTAN dentro de la doctrina AJP-4.0, donde se establece que el soporte logístico debe integrarse desde la planeación inicial de la operación, asegurando interoperabilidad y sostenibilidad en tiempo real y de manera suficiente (NATO, 2018). Así, la logística en red no solo optimiza tiempos y recursos, sino que blinda el sistema logístico ante amenazas.

3.3 Soporte Logístico Integrado (ILS): aplicación OTAN y EE.UU.

El concepto de Soporte Logístico Integrado (ILS, por sus siglas en inglés: Integrated Logistics Support) constituye una de las transformaciones más significativas en la evolución de la logística militar moderna. El ILS es una metodología de planeación y ejecución que busca garantizar la operatividad de un sistema complejo (como una aeronave, buque o

vehículo blindado) desde su adquisición hasta su retiro, asegurando su sostenibilidad a lo largo del ciclo de vida con el menor costo posible y con alta disponibilidad (Navarro, 1999).

De acuerdo con la doctrina OTAN, el ILS se define como "una estrategia para asegurar que todos los aspectos de apoyo logístico, desde el mantenimiento, entrenamiento, repuestos y documentación técnica, sean considerados desde las fases tempranas del diseño y adquisición de un sistema" (NATO, 2018, pp. 3–15). Esta visión integrada ha sido adoptada por países miembros de la OTAN y el Departamento de Defensa de Estados Unidos (DoD), donde su implementación es obligatoria en grandes programas de defensa, según estándares como MIL-STD-1388 y el modelo Product Support Business Case Analysis (PS-BCA) (Naval War College Foundation, 2020).

Uno de los casos más destacados es el programa estadounidense del F-35 Joint Strike Fighter, donde el ILS ha permitido consolidar un sistema logístico digital que monitorea en tiempo real las fallas, mantiene inventarios predictivos y reduce tiempos de mantenimiento gracias a una plataforma global integrada (U. S. Government Accountability Office, 2024). En la OTAN, el uso de herramientas como LOGFAS (Logistics Functional Area Services) permite coordinar el ILS entre países aliados en operaciones conjuntas, mejorando la interoperabilidad logística y asegurando que todos los actores cuenten con los insumos y soporte requeridos antes, durante y después de la misión (NATO, 2018).

En el contexto colombiano, aunque el concepto de ILS no ha sido adoptado de manera formalizada como en los países miembros de la OTAN, sus principios ya se reflejan en documentos como la Doctrina Logística de la Armada Nacional y el Reglamento

Logístico Conjunto CGFM (2016), los cuales proponen la estandarización del mantenimiento, el fortalecimiento del ciclo de vida de los sistemas logísticos y la integración entre las fuerzas. No obstante, aún existen desafíos en términos de interoperabilidad, trazabilidad de activos y uso efectivo de plataformas digitales para soportar una verdadera implementación de ILS a nivel conjunto (ARC OP4-1.1 DOCTRINA NAVAL, 2021).

De cara a los retos de ciberseguridad, el ILS ofrece una ventaja crítica: al prever desde el diseño los mecanismos de soporte, también puede incluir protocolos de ciberdefensa integrados, asegurando que tanto el software como el hardware tengan planes de respuesta ante eventos disruptivos. Según el informe *Robust and Resilient Logistics Operations in a Degraded Information Environment*, los modelos de soporte logístico en red que integran ciberseguridad desde el diseño permiten a las fuerzas adaptarse con mayor rapidez a ataques dirigidos contra su infraestructura logística (Snyder et al., 2017a).

3.4 Logística disputada y Logística cognitiva

La evolución de los conflictos armados y las operaciones militares modernas ha transformado profundamente la manera en que se concibe y ejecuta la logística militar. En este nuevo entorno, caracterizado por la interacción de dominios físicos, informacionales y cibernéticos, emerge el concepto de *logística disputada*, que hace referencia a las operaciones logísticas realizadas en entornos VICA altamente hostiles o interrumpidos, donde las rutas de abastecimiento, los centros de distribución o los sistemas digitales pueden ser atacados deliberadamente (Joint Logistics JP 4-0, 2019).

Esta noción es ampliada por el Coronel Aldemar Serrano, quien en su artículo "Correlación entre logística militar, estudios estratégicos y seguridad y defensa nacional" plantea que la logística ya no debe entenderse únicamente como una función de soporte, sino como un instrumento estratégico que contribuye a la disuasión, a la capacidad de proyección del poder militar y al sostenimiento del Estado en escenarios híbridos y multidominio (Serrano et al., 2025). En este contexto, introduce el concepto de *logística cognitiva*, entendida como la integración entre los principios de apoyo logístico tradicional y la inteligencia situacional generada a través del análisis de datos, sistemas interconectados e inteligencia artificial (Serrano et al., 2025).

La *logística cognitiva* implica dotar al sistema logístico de capacidades predictivas y adaptativas, que no solo respondan a la demanda, sino que anticipen las necesidades y condiciones cambiantes del campo de batalla. Esta capacidad se basa en tecnologías como *Machine Learning*, *Big Data*, *IoT* y plataformas *C4ISR*, permitiendo que el sistema logístico actúe como un "organismo vivo" que se adapta, detecta y responde frente a amenazas cibernéticas o físicas (Naval War College Foundation, 2020, p. 9; Snyder et al., 2017a, p. 17)

Por su parte, el Departamento de Defensa de EE.UU., en su doctrina de *Sustaining Multidomain Operations*, establece que las fuerzas deben estar preparadas para operar en entornos logísticos disputados, donde la ciberdefensa se convierte en parte esencial del planeamiento logístico desde el nivel estratégico hasta el táctico. Aquí, los nodos logísticos no solo deben estar blindados digitalmente, sino ser capaces de operar con autonomía si son desconectados del sistema central (*Sustaining Multidomain Operations*, s/f).

Asimismo, en el entorno OTAN, el concepto de logística cognitiva se refleja en las prácticas de interoperabilidad que integran sistemas como *LOGFAS* con módulos de ciberseguridad, sensores en cadena y algoritmos para trazabilidad logística. Según la doctrina *AJP-4.0*, "el soporte logístico debe estar preparado para responder ante amenazas que afecten la disponibilidad de suministros, pero también la integridad de la información logística" (NATO, 2018, pp. 4–2).

En América Latina, aunque este enfoque aún no ha sido plenamente adoctrinado, algunos esfuerzos teóricos como los de Rodrigo M. Díaz, Lissette Casadiego y Carlos Bermúdez plantean modelos para medir la madurez cibernética de los sistemas logísticos, implementar visores de trazabilidad y desarrollar estrategias de ciberinmunidad frente a ataques a la cadena de abastecimiento (Bermúdez, 2022, p. 38; Casadiego et al., 2023, p. 75; R. M. Díaz, 2022, p. 61).

Esta transformación tiene un impacto directo en la cadena de abastecimiento militar en la Logística Militar Conjunta, donde el contexto operacional incluye amenazas cibernéticas, criminalidad organizada transnacional y alta dependencia tecnológica. La adopción de una logística cognitiva, en este caso, permitiría no solo proteger los sistemas de información logística, sino además optimizar el despliegue de recursos, predecir interrupciones logísticas, fortalecer la resiliencia operacional y brindar una ventaja estratégica en escenarios disputados, en especial para la seguridad informacional de los sistemas como *SAP-SILOG*.

3.5 Conceptos de Cadena de Suministro y Cadena de Abastecimientos

En la literatura especializada, los términos "cadena de suministro" (*supply chain*) y "cadena de abastecimiento" suelen utilizarse indistintamente, aunque presentan diferencias semánticas y operacionales según el enfoque y el contexto en el que se apliquen. En términos generales, la cadena de suministro se refiere a un sistema completo que abarca todas las actividades, recursos, infraestructuras, organizaciones y tecnologías necesarias para transformar materias primas en productos terminados y entregarlos al consumidor final (Christopher, 2011, p. 55). Por su parte, la cadena de abastecimiento, en contextos militares y de defensa, tiende a enfocarse más específicamente en la provisión, almacenamiento, transporte y distribución de recursos esenciales para el sostenimiento operacional de las tropas, con un énfasis particular en la eficiencia, continuidad y seguridad del flujo logístico (Thorpe, 1986).

En los entornos militares, esta distinción se vuelve crucial debido a las implicaciones operacionales de cada término. Mientras que la cadena de suministro contempla una visión empresarial y de mercado, la cadena de abastecimiento militar se estructura bajo parámetros doctrinales de sostenimiento y movilidad estratégica (Joint Logistics JP 4-0, 2019). Como lo señala Kress, (2016), la logística operacional moderna debe integrar capacidades tecnológicas, mecanismos de interoperabilidad y estructuras logísticas que permitan mantener la cadena de abastecimiento incluso bajo condiciones de guerra irregular, ciberataques o sabotajes físicos.

Autores como Kress, (2016) y Pagonis & Krause, (1992) han enfatizado que la planificación logística en el ámbito militar requiere un enfoque orientado a escenarios,

donde la sincronización de cada eslabón del proceso, desde el punto de origen hasta el punto de consumo operativo, sea lo suficientemente robusta para sostener operaciones multidominio y conjuntas.

En la doctrina militar de Colombia, el término "cadena de abastecimiento" ha sido adoptado en documentos como el Manual de Doctrina Logística Conjunta (Manual FF.MM. 4-9, 2012) y el Reglamento Logístico Conjunto del Comando General de las Fuerzas Militares (REGLAMENTO FF.MM. 4-2, 2016), en los cuales se describe este proceso como la "secuencia integrada de actividades que permiten satisfacer los requerimientos logísticos de los componentes operativos, desde la planificación de necesidades hasta la entrega final del recurso" (p. 119) (p. 120). Dichas doctrinas han sido reforzadas por experiencias internacionales de la OTAN y el Departamento de Defensa de EE.UU., quienes proponen marcos funcionales como el Soporte Logístico Integrado (ILS) y los sistemas LOGFAS, GCSS-Army y DLMS, donde la automatización, trazabilidad y seguridad cibernética se consolidan como ejes estratégicos de la sostenibilidad logística (NATO, 2018).

De forma complementaria, el concepto de "supply chain resilience" o resiliencia de la cadena logística ha cobrado fuerza en las últimas décadas, al reconocer que no basta con lograr eficiencia en tiempos de paz, sino que se requiere anticipar, absorber, adaptarse y recuperarse de disrupciones significativas como ataques cibernéticos, fallas tecnológicas o colapsos de infraestructura (Díaz del Río, 2011).

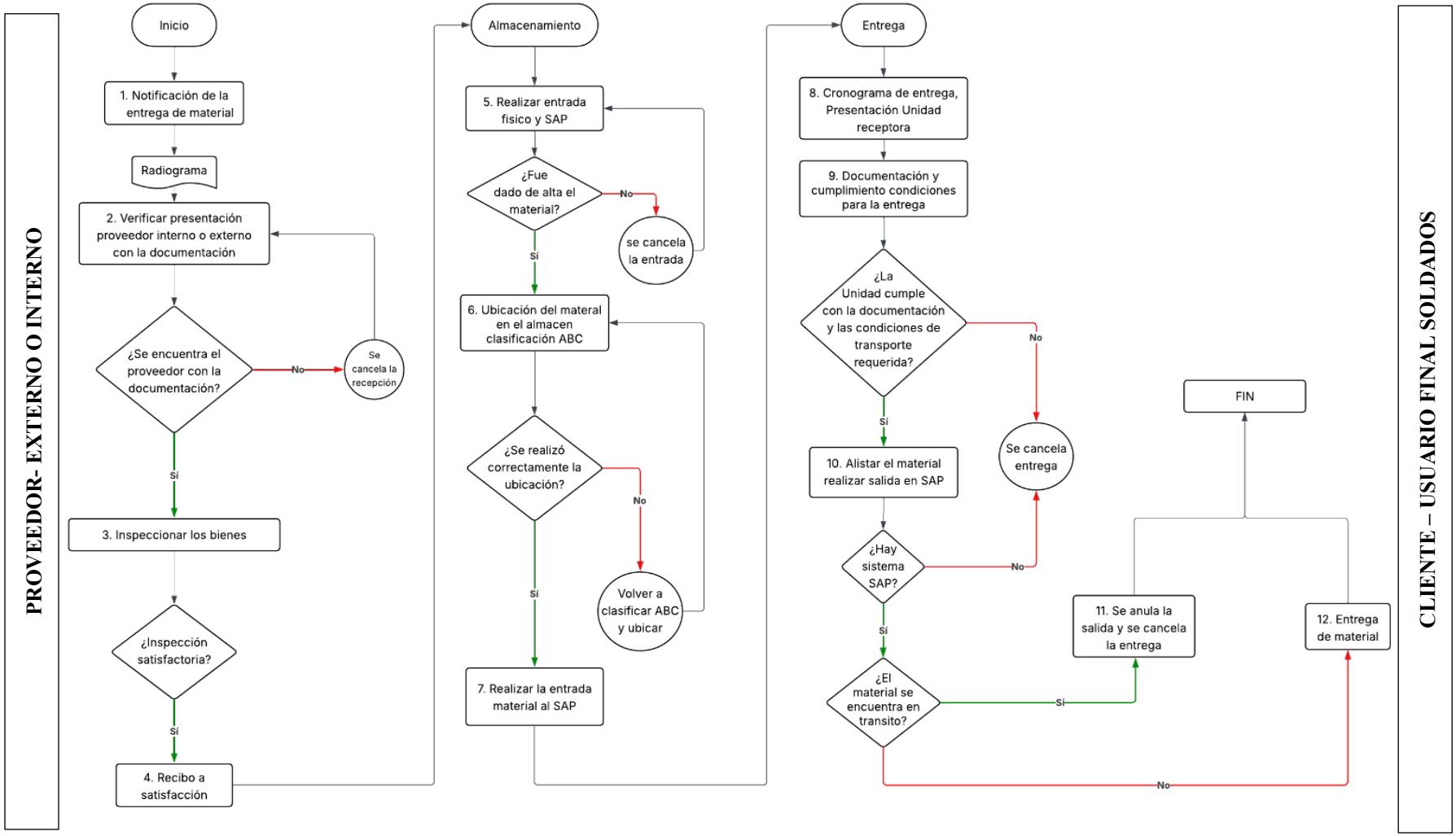
Finalmente, es importante señalar que ambas expresiones "cadena de suministro y cadena de abastecimiento" pueden considerarse válidas siempre que se especifique su

contexto de uso. En el presente artículo, se empleará principalmente el término cadena de abastecimiento militar conjunta, por ser el más representativo y coherente con la doctrina vigente de las Fuerzas Militares de Colombia.

3.5.1 Caracterización Cadena de Abastecimientos

En consecuencia, se hace necesario determinar la caracterización de la Cadena de Abastecimientos en las Fuerzas militares para conocer el procedimiento empleado dentro de la Logística Militar, que aporta al sostenimiento de las operaciones militares, siendo punto clave para identificar las posibles vulnerabilidades que se pueden reflejar durante el desarrollo de la Cadena de Abastecimientos, como se señala a continuación:

Figura 1. Caracterización Cadena de Abastecimientos



Fuente: Elaboración propia

4 Sistemas de Información Logística

4.1 Sistemas que se emplean en la cadena de abastecimientos a nivel mundial

En el ámbito militar global, los sistemas de información logística constituyen un pilar estratégico que permite integrar, coordinar y asegurar la cadena de abastecimientos en operaciones conjuntas y multinacionales. Estos sistemas, conocidos como Enterprise Resource Planning (ERP), permiten centralizar procesos de adquisición, inventario, mantenimiento y distribución de insumos críticos. A nivel OTAN, se emplea el LOGFAS (Logistics Functional Area Services), un conjunto de aplicaciones modulares que gestiona desde la planificación estratégica hasta el apoyo táctico de la logística multinacional, permitiendo interoperabilidad entre naciones aliadas y facilitando la ejecución de movimientos logísticos conjuntos en tiempo real (NATO, 2018).

Por otra parte, en Estados Unidos, se implementa el Global Combat Support System-Army (GCSS-Army), un ERP integral que reemplazó más de 40 sistemas heredados, consolidando la planificación de requerimientos, órdenes de trabajo, inventarios y recursos financieros en una sola plataforma. Este sistema se basa en SAP ECC, con módulos diseñados específicamente para la gestión logística táctica, y garantiza trazabilidad, reducción de redundancias y fortalecimiento de la ciberseguridad mediante la segmentación de redes y controles de acceso granulares (Naval War College Foundation, 2020) (Joint Logistics JP 4-0, 2019).

Otro ejemplo es el Defense Logistics Management Standards (DLMS), empleado por el Departamento de Defensa estadounidense como arquitectura estandarizada para la

administración y automatización de procesos logísticos y financieros, asegurando integración de datos y cumplimiento normativo (Winegardner, 2025).

En Europa, sistemas como SAP Defense Forces & Public Security han sido adoptados por países como Alemania y España, integrando planeamiento de operaciones, contratos, mantenimiento de flotas y simulaciones de demanda para optimizar la sostenibilidad operativa (SAP, 2025).

Finalmente, en América Latina, la mayoría de fuerzas armadas, incluida Colombia, implementan sistemas adaptados como el SAP-SILOG, orientado a procesos de almacenamiento y entrega de recursos en tiempo real, pero con limitaciones frente a plataformas de ciberdefensa y planeamiento avanzado (Morales, 2012).

La tendencia global en sistemas de información logística apunta hacia la integración de módulos de inteligencia artificial, análisis predictivo, algoritmos de optimización, blockchain para trazabilidad y ciberinmunidad para defensa proactiva ante ciberamenazas, generando un cambio doctrinal hacia la logística cognitiva y algorítmica como ejes de transformación digital en las fuerzas militares (Casadiego et al., 2023).

4.2 Operaciones logísticas: sistemas que aportan en conflictos disputados

Las operaciones logísticas en conflictos disputados requieren capacidades tecnológicas avanzadas, integración doctrinal multinivel y una visión estratégica de resiliencia para garantizar la continuidad del sostenimiento operacional. Según Kaddoussi et al., (2011), la gestión de disrupciones en la logística militar demanda optimización de flujos, simulación

de escenarios de interrupción y desarrollo de algoritmos que prioricen rutas críticas y reconfiguración de redes de abastecimiento en tiempo real (p. 2).

La integración de sistemas de información logística en entornos de guerra híbrida y multidominio se ha convertido en un factor decisivo. El informe *Conflict in the 21st Century: The Rise of Hybrid Wars* (Hoffman, 2007) señala que las cadenas de suministro se convierten en blancos estratégicos de adversarios no convencionales, lo que obliga a implementar sistemas ERP con arquitectura de confianza cero y multifactorialidad para reducir el impacto de accesos no autorizados.

En este sentido, la incorporación de sistemas ERP en la nube con robustos esquemas de ciberseguridad, como los analizados por Madhava Varma et al., (2023), permiten desplegar plataformas logísticas con protección multicapa, cifrado de extremo a extremo y segmentación de bases de datos para operaciones distribuidas en escenarios de contingencia.

La doctrina logística conjunta estadounidense (Joint Logistics JP 4-0, 2019) y la OTAN (NATO, 2018) enfatizan la necesidad de que los sistemas logísticos cuenten con interoperabilidad para escenarios disputados, integración C4ISR y módulos de inteligencia artificial para priorización dinámica de recursos y predicción de disrupciones.

Por su parte, el documento *CAP3 Correlación entre Logística Militar, Estudios Estratégicos y Seguridad y Defensa Nacional* resalta la logística como arquitectura invisible del poder, que se materializa en la capacidad de sostener simultáneamente operaciones en diferentes teatros, mediante la integración de sistemas SAP-SILOG,

LOGFAS (OTAN), DLMS (DoD EE.UU.) y emergentes como Quantum Supply Chain Modelling (Serrano, 2025).

El reporte de ENISA, (2021) advierte que los ciberataques a la cadena de suministro han aumentado un 400% en la última década, incluyendo sabotaje a plataformas logísticas militares mediante backdoors en software de gestión, lo cual resalta la urgencia de fortalecer la ciberdefensa integrada de los sistemas ERP y sus módulos críticos.

Finalmente, la *Gestión Logística Integral* (Mora, 2023) subraya que la resiliencia logística en conflictos disputados no solo depende de la infraestructura tecnológica, sino también de la flexibilidad doctrinal, la descentralización de la toma de decisiones y la articulación de capacidades conjuntas y multinacionales en un mismo sistema operativo logístico.

4.3 Conflictos regionales en logística focalizada: aumento de las capacidades en EE.UU y otros países

La logística militar ha evolucionado en función de las lecciones aprendidas en los conflictos regionales recientes, donde el sostenimiento y la resiliencia logística se han convertido en factores estratégicos determinantes. En el caso de Estados Unidos, durante la Guerra del Golfo, la operación *Desert Storm* demostró la importancia de la planificación logística anticipada, consolidando el concepto de logística como "factor de éxito o fracaso en las operaciones militares" (Pagonis & Krause, 1992).

Posteriormente, en Afganistán e Irak, el modelo logístico estadounidense enfrentó desafíos significativos en transporte estratégico, protección de convoyes y mantenimiento operacional. Para resolverlo, se implementaron sistemas de soporte logístico integrado (ILS), inteligencia logística, algoritmos para optimización de rutas y capacidades de respuesta cibernética ante sabotajes de la cadena digital (Naval War College Foundation, 2020). De acuerdo al informe RAND Corporation (2017b), la estrategia logística actual en EE.UU. contempla el uso de IA y gemelos digitales para evaluar escenarios de degradación de información y ataques cibernéticos en la cadena de abastecimiento (Snyder et al., 2017b).

En Europa, la OTAN ha modernizado sus capacidades logísticas a través de LOGFAS y el reforzamiento de la interoperabilidad en operaciones conjuntas. Durante la crisis en Kosovo (1999), se evidenciaron limitaciones logísticas debido a la falta de integración de sistemas de información, lo cual condujo a la actualización doctrinal de AJP-4.0 para incluir interoperabilidad, sostenibilidad multinacional y ciberseguridad logística (NATO, 2018).

En América Latina, la doctrina logística aún se encuentra en transición hacia modelos más avanzados. No obstante, Chile y Brasil han fortalecido su cadena de abastecimiento mediante la adopción de sistemas ERP y simuladores de modelamiento logístico para operaciones en escenarios multiamenaza. Según Díaz, (2022), la ciberseguridad es un factor emergente en las fuerzas latinoamericanas debido a la creciente digitalización y las amenazas cibernéticas a infraestructuras críticas (R. M. Díaz, 2022).

Tabla 1. Conflictos regionales y aumento de capacidades logísticas

CONFLICTOS REGIONALES Y LOGÍSTICA	
CONFLICTO	**CAPACIDAD ADOPTADA**
EE.UU. Desert Storm	Planificación anticipada, modelamiento estratégico
Afganistán e Irak	ILS, IA, protección de convoyes, Ciberdefensa
Kosovo (OTAN)	Interoperabilidad, integración de sistemas
Chile y Brasil	ERP, simuladores logísticos, Ciberseguridad

Fuente: Elaboración propia

Este esquema resume los conflictos analizados y las capacidades logísticas que se han fortalecido como consecuencia de sus aprendizajes. Destaca que la tendencia global apunta hacia la integración de tecnologías avanzadas, la protección cibernética y la interoperabilidad conjunta como factores críticos de sostenimiento estratégico.

4.4 Operatividad de la cadena de abastecimientos con nuevas tecnologías: aplicación logística algorítmica, cognitiva y cuántica

La cuarta revolución industrial y la inminente transición hacia la quinta revolución industrial han traído consigo un cambio paradigmático en la gestión logística global, militar y empresarial. Este cambio se manifiesta en la incorporación de tecnologías disruptivas como la computación cuántica, los algoritmos inteligentes y el machine learning en los sistemas de la cadena de abastecimientos, transformando radicalmente su operatividad.

La logística algorítmica, definida como el empleo de algoritmos computacionales para optimizar procesos logísticos complejos, permite la resolución de problemas de asignación de recursos, rutas de transporte y gestión de inventarios en tiempo real,

mediante la integración de modelos predictivos y de optimización matemática (Correll et al., 2023). Por ejemplo, en escenarios militares, los algoritmos de machine learning pueden analizar datos de inteligencia logística, condiciones meteorológicas y amenazas en ruta para recalcular itinerarios de abastecimiento de manera automática y segura.

Por su parte, la logística cognitiva, como lo menciona Serrano (2023), implica un salto desde la logística digital (automatizada) hacia sistemas que aprenden y se adaptan de manera autónoma al entorno operacional, mediante la combinación de inteligencia artificial, big data, IoT (Internet de las Cosas) y plataformas C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance). Este enfoque cognitivo convierte la cadena de abastecimientos en un sistema vivo, capaz de anticipar demandas, detectar anomalías, reconfigurar sus rutas de distribución y protegerse frente a amenazas cibernéticas y físicas en tiempo real (Serrano, 2025).

Finalmente, la computación cuántica aplicada a la logística militar y empresarial representa el siguiente nivel de transformación. Según Phillipson, (2025), la computación cuántica permite resolver problemas logísticos de optimización combinatoria que serían intratables para los sistemas clásicos, tales como la minimización de costos en la distribución multinivel o la programación simultánea de mantenimiento y transporte en redes logísticas militares globales (Phillipson, 2025). Por ejemplo:

- **Quantum annealing:** se ha empleado para optimizar secuenciación de rutas en cadenas de abastecimiento complejas con múltiples restricciones operacionales (Correll et al., 2023).

- **Quantum Neural Networks:** han demostrado su potencial para realizar predicciones de demanda de manera exponencialmente más rápida y precisa que los algoritmos convencionales, permitiendo ajustes en inventarios en tiempo real y evitando sobrecostos (Correll et al., 2023).

Un ejemplo reciente en la industria global es el estudio desarrollado por D-Wave Systems, donde se utilizó un modelo de optimización cuántica para reducir en un 40% el tiempo total de entrega en redes de transporte multinodal, demostrando su aplicabilidad en el entorno civil y su potencial estratégico en el entorno militar (Weinberg et al., 2023).

En el contexto de las Fuerzas Militares de Colombia, aunque estas tecnologías aún no han sido plenamente adoptadas, su implementación podría fortalecer la capacidad de planeamiento operacional, aumentar la resiliencia de los sistemas de información logística y mejorar la sincronización de abastecimientos en operaciones conjuntas, especialmente en entornos disputados con amenazas cibernéticas avanzadas y alta incertidumbre táctica.

En síntesis, la integración de logística algorítmica, cognitiva y cuántica no es un objetivo de futuro lejano, sino una necesidad estratégica para la sostenibilidad de las cadenas de abastecimiento en escenarios de conflicto multidominio. Su adopción progresiva permitirá a las Fuerzas Militares adaptarse de manera más ágil, eficiente y segura a los retos operacionales del siglo XXI.

5 Amenazas emergentes en la cadena de abastecimiento

En el contexto actual de la logística militar, las amenazas emergentes en la cadena de abastecimiento representan uno de los riesgos estratégicos más relevantes para la seguridad y sostenibilidad operativa de las Fuerzas Armadas a nivel mundial. Estas amenazas se han intensificado como consecuencia de la digitalización y la hiperconectividad de los sistemas de información logística (SIL), generando un aumento exponencial en la superficie de exposición a ciberataques (CrowdStrike, 2025).

La ciberseguridad logística enfrenta múltiples desafíos derivados de las ciberamenazas avanzadas persistentes (APT), el malware especializado, el ransomware dirigido y los ataques de denegación de servicio distribuido (DDoS) que tienen como objetivo la interrupción del flujo logístico y la captura de información crítica para el mando y control. Como señalan Zambrano et al., (2024), los ciberataques en la región de América Latina han evolucionado hacia técnicas más sofisticadas como el secuestramiento de sistemas de control logístico mediante inyección de scripts maliciosos y explotación de vulnerabilidades zero-day**.**

De acuerdo con Alzahrani & Asghar, (2024), en su estudio sobre detección de vulnerabilidades cibernéticas en sistemas IoT logísticos, los puntos más críticos de exposición se ubican en los sensores de inventario, las gateways de comunicación y los módulos ERP integrados, ya que presentan deficiencias en la aplicación de arquitecturas de confianza cero y de protocolos de autenticación robusta (Alzahrani & Asghar, 2024).

Por su parte, el informe de Adrian Davis, (2015) destaca que la resiliencia cibernética en la cadena de suministros no puede limitarse a la implementación de firewalls o sistemas anti-malware, sino que requiere un enfoque integral que incluya análisis de amenazas, gestión de vulnerabilidades, monitoreo continuo, respuestas automatizadas y simulación de ataques (Davis, 2015).

El documento *Arquitectura de Confianza Cero* (Rose et al., 2020) subraya que el paradigma Zero Trust (Confianza Cero) es esencial para proteger las cadenas de abastecimiento, al establecer que ningún dispositivo o usuario, interno o externo, debe ser confiable por defecto, y que todo acceso debe ser verificado y monitoreado constantemente.

En el contexto militar de Estados Unidos y la OTAN, las amenazas emergentes han incluido también los ataques dirigidos a los sistemas de planeamiento y simulación logística de alta performance (HPC), necesarios para el modelado de escenarios multidominio. La aplicación de técnicas de computación cuántica en ciberataques, aunque incipiente, plantea un desafío potencial a la criptografía tradicional empleada en sistemas logísticos cifrados (Correll et al., 2023).

Finalmente, en el ámbito latinoamericano, Quevedo, (2023) señala que las Fuerzas Armadas enfrentan no solo ciberamenazas estatales o de grupos criminales organizados, sino también de mercenarios cibernéticos (cybermercenaries) que ofrecen servicios de intrusión en sistemas logísticos para alterar las operaciones militares y la seguridad nacional (Quevedo, 2023).

En síntesis, las amenazas emergentes en la cadena de abastecimiento se caracterizan por su capacidad de adaptación, persistencia y escalabilidad en múltiples dominios, representando un riesgo estratégico que exige la implementación de tecnologías de detección avanzada, modelos predictivos de Machine Learning y arquitecturas de confianza cero, así como el fortalecimiento de la resiliencia cibernética operacional y de mando en las Fuerzas Militares colombianas.

5.1 Histórico de ciberamenazas en la cadena de abastecimientos y consecuencias

La creciente dependencia de sistemas digitales para la gestión logística ha intensificado la superficie de ataque de las cadenas de abastecimiento militar y civil. Este fenómeno se ha evidenciado en ciberataques de alto impacto que han paralizado operaciones logísticas críticas a nivel global.

Por ejemplo, durante el ataque de ransomware NotPetya en 2017, empresas de logística como Maersk se vieron obligadas a detener completamente sus operaciones, afectando la trazabilidad y entrega de suministros en más de 130 países (CrowdStrike, 2025). Dicho ataque evidenció la falta de segmentación de redes y el riesgo de vulnerabilidades en sistemas ERP centralizados. De acuerdo con Zambrano et al., (2024), la principal causa de estos ciberataques es la explotación de vulnerabilidades de software no actualizadas y la ingeniería social para acceso inicial.

En América Latina, M. Díaz & Núñez, (2023) destacan que los ciberataques dirigidos a la cadena logística en Colombia y Brasil han tenido como objetivo los sistemas ERP, con intenciones de sabotaje y robo de datos críticos, incluyendo planos y rutas de

abastecimiento estratégico (M. Díaz & Núñez, 2023). La afectación a SAP-SILOG o plataformas de planeamiento logístico podría interrumpir la operación militar conjunta, comprometiendo la seguridad nacional.

Según Alzahrani & Asghar, (2024), los sistemas basados en Internet de las Cosas (IoT) amplían aún más los riesgos en la cadena de abastecimientos, pues su baja capacidad de procesamiento limita la implementación de medidas de seguridad robustas, generando vulnerabilidades explotables en redes de sensores logísticos. Además, la arquitectura de confianza cero (Zero Trust Architecture) se propone como mecanismo para mitigar accesos no autorizados en entornos altamente distribuidos como la cadena de abastecimiento militar (Rose et al., 2020).

En términos doctrinales, la doctrina JP 4-0 del Departamento de Defensa de EE.UU. indica que los ciberataques a la logística pueden crear efectos en cascada, generando desabastecimientos críticos, imposibilidad de reabastecimiento de municiones y fallas en los sistemas de mantenimiento predictivo, poniendo en riesgo la fuerza conjunta (Joint Logistics JP 4-0, 2019; Smith, 2022).

Por último, el informe de Suramericana, (2022) subraya que los ciberataques a la cadena de suministros en América Latina han alcanzado cifras récord, con un crecimiento de más del 200% en los últimos tres años, siendo el malware especializado en sistemas ERP y las vulnerabilidades de firmware en dispositivos logísticos los vectores más utilizados.

5.2. Evaluación de niveles de madurez de ciberseguridad logística

La evaluación de los niveles de madurez de la ciberseguridad en la logística militar es un proceso que permite identificar el grado de implementación, integración y robustez de los controles y procesos de ciberseguridad en la cadena de abastecimientos. Según Casadiego et al., (2023), este tipo de evaluaciones permite identificar las brechas existentes, planificar procesos de mejora y priorizar inversiones en tecnologías de protección para garantizar la continuidad operacional.

En la práctica, los modelos de madurez se estructuran en niveles que van desde el inicial (sin procesos definidos ni formalizados) hasta el nivel optimizado, donde la ciberseguridad es parte integral de la cultura organizacional y se cuenta con monitoreo, respuesta y actualización continua de las capacidades. Alzahrani & Asghar, (2024) destaca que este tipo de evaluaciones permite a los tomadores de decisiones priorizar qué sistemas requieren intervención urgente y cuáles pueden mantenerse con sus niveles actuales de protección.

Para la cadena de abastecimientos militar conjunta en Colombia, implementar un modelo de madurez permitiría:

- Identificar vulnerabilidades en sistemas ERP como SAP-SILOG.
- Priorizar la integración de marcos de seguridad Zero Trust (Rose et al., 2020)
- Desarrollar planes de capacitación progresiva para el personal logístico.
- Estandarizar controles de ciberseguridad en el ciclo de vida logístico desde la planificación hasta la entrega.

5.3. Marco MITRE ATT&CK y su aplicación para la ciberlogística

El marco MITRE ATT&CK es una base de datos de conocimiento de tácticas y técnicas empleadas por ciber adversarios en las diferentes fases del ciclo de ataque. Este marco ha sido adaptado en el ámbito militar para mapear amenazas y planificar defensas en sistemas logísticos, C4ISR y plataformas ERP (MITRE ATT&CK, 2025).

Para la cadena de abastecimientos militar, su aplicación permite:

- Mapear amenazas específicas en SAP-SILOG y otros sistemas logísticos militares (Winegardner, 2025).
- Diseñar simulaciones de ciberataques para evaluar el tiempo de respuesta y la resiliencia de la cadena logística.
- Integrar los hallazgos a modelos de evaluación de madurez para priorizar técnicas de mitigación (CrowdStrike, 2025).

Por ejemplo, en EE.UU., el marco ATT&CK se ha utilizado en ejercicios de Red Team y Blue Team para simular ataques en redes logísticas y validar los procedimientos de recuperación (Quinn, 2023).

5.4. Estrategias de mitigación de amenazas y tecnologías emergentes

Ante la creciente sofisticación de los ciberataques, se requieren estrategias de mitigación integrales y tecnologías emergentes que fortalezcan la ciberdefensa logística. Entre estas destacan:

- **Inteligencia Artificial (IA):** Para análisis predictivo de fallos en la cadena de abastecimientos, detección de anomalías en flujos de información y gestión anticipada de inventarios (Correll et al., 2023).
- **Blockchain:** Garantiza la trazabilidad de las transacciones logísticas, evitando alteraciones maliciosas en el registro de inventarios y pedidos (Valdés et al., 2021).
- **Zero Trust Architecture:** Establece controles de seguridad en cada nodo de la red, eliminando la confianza implícita entre usuarios, dispositivos y aplicaciones (Rose et al., 2020)
- **Ciberinmunidad (Cyber Immunity):** Nuevo paradigma de seguridad propuesto para sistemas industriales y militares, orientado a crear arquitecturas capaces de resistir ataques sin interrumpir la operación (R. Díaz, 2020).
- **Quantum Computing:** Se proyecta como tecnología disruptiva para resolver problemas complejos de optimización en la cadena logística y fortalecer la encriptación de datos críticos (Phillipson, 2025).

6 Modelos de Simulación de Ciberataques y Evaluación de vulnerabilidades: dinámica en entornos logísticos disputados

La simulación de ciberataques en cadenas de abastecimiento militar se ha convertido en una herramienta crítica para la evaluación de vulnerabilidades en entornos logísticos disputados. Según Casadiego (2023), la simulación permite anticipar los puntos críticos y generar estrategias de mitigación basadas en escenarios reales de ataque. Para este

propósito, se recomienda el uso de herramientas, que permitan construir modelos dinámicos sistémicos donde se representen las interacciones entre nodos logísticos, sistemas ERP, bases de datos de inventario y redes de transporte (Casadiego et al., 2023).

La metodología incluye las siguientes fases:

1. Definición del sistema y variables críticas.
2. Modelado causal y de flujos.
3. Simulación de escenarios con variables de ataque (denegación de servicio, modificación de datos, inyección de malware).
4. Análisis de resultados y generación de indicadores de vulnerabilidad y resiliencia.

Este tipo de modelos han sido aplicados por el DoD y RAND Corporation en escenarios multidominio para prever impactos en la continuidad de operaciones. En el contexto colombiano, la aplicación de simulación sistémica permitirá fortalecer la capacidad de anticipación frente a ciberamenazas, estableciendo un marco de resiliencia adaptativa y preventiva.

Con base en la página oficial de MITRE ATT&CK para técnicas de cadena de suministro, se presenta la siguiente matriz adaptada y resumida para el contexto de operaciones logísticas militares**,** estructurada en tácticas, técnicas y detección, aplicada al análisis del artículo y al contexto de simulación y modelo estratégico propuesto:

Tabla 2. MODELO MATRIZ ADAPTADA PARA CADENA DE ABASTECIMIENTOS

Táctica	Técnica MITRE ATT&CK	Descripción resumida (adaptada)	Detección recomendada
Inicial Access (Acceso inicial)	**Supply Chain Compromise (T0862)**	Compromiso a través de terceros o proveedores externos, inyectando código malicioso en actualizaciones, software ERP o hardware de la cadena de suministro.	Monitoreo de integridad de archivos, auditorías de proveedores, Zero Trust, análisis de IoCs.
Execution (Ejecución)	**Malicious Code Injection (T1055)**	Inserción de código malicioso en procesos legítimos del sistema ERP o bases de datos logísticas para ejecución no autorizada.	Uso de EDR, análisis heurístico, whitelisting de procesos y aplicaciones.
Persistence (Persistencia)	**Supply Chain Compromise Persistence Mechanism (T1195.002)**	Mecanismos instalados para garantizar persistencia en el sistema comprometido, incluyendo scripts automáticos en actualizaciones de proveedores o firmware de hardware militar.	Monitoreo de registros de instalación, validación de actualizaciones y firmas digitales de proveedores.
Privilege Escalation (Escalada de privilegios)	**Valid Accounts (T1078)**	Uso de cuentas legítimas (de proveedores o integradores) para acceder a mayores privilegios en la red logística.	MFA, revisión periódica de cuentas privilegiadas y rotación de credenciales.
Defense Evasion (Evasión de defensas)	**Obfuscated Files or Information (T1027)**	Ocultamiento de archivos, scripts y logs modificados para evadir controles de seguridad durante el compromiso de la cadena de suministro.	Escaneo de archivos sospechosos, técnicas de sandboxing, DLP y análisis de tráfico cifrado.
Credential Access (Acceso a credenciales)	**Credential Dumping (T1003)**	Robo de credenciales en sistemas ERP, servidores logísticos y bases de datos a través de herramientas de dumping o malware especializado.	Monitoreo de procesos anómalos, alertas de acceso a memoria crítica, segmentación de dominios.

Discovery (Reconocimiento)	**Network Service Scanning (T1046)**	Escaneo de servicios y puertos en la red logística para mapear infraestructura crítica y posibles puntos de acceso.	IDS/IPS, detección de escaneo de puertos, honeypots en entornos logísticos sensibles.
Lateral Movement (Movimiento lateral)	**Pass the Hash (T1075)**	Uso de hashes capturados para autenticarse en otros sistemas dentro de la red logística sin necesidad de descifrar contraseñas.	Habilitar restricciones NTLM, monitoreo de autenticaciones Kerberos, segmentación y Zero Trust.
Collection (Colección de información)	**Data from Information Repositories (T1213)**	Acceso no autorizado a repositorios de información logística, ERP y bases de datos para recopilar inteligencia crítica operativa.	Monitoreo de consultas y acceso masivo de datos, alertas SIEM por patrones anómalos.
Exfiltration (Exfiltración de datos)	**Exfiltration Over Command and Control Channel (T1041)**	Exfiltración de información crítica a través de canales de C2 cifrados o protocolos permitidos, dificultando su detección en redes logísticas militares.	Inspección profunda de paquetes (DPI), análisis de tráfico cifrado, bloqueo de dominios C2 conocidos.
Impact (Impacto)	**Data Manipulation (T1565)**	Manipulación de datos en ERP, inventarios o sistemas de órdenes logísticas, generando desinformación, fallas en la planificación y efectos en cascada en la cadena de abastecimientos.	Detección de cambios no autorizados, auditoría de integridad de bases de datos, redundancia en backups.

Fuente: Matriz MITRE ATT&CK Supply Chain

Esta matriz se emplea para caracterizar tácticas y técnicas relevantes para la simulación dinámica y la propuesta de modelo estratégico de mitigación de ciberamenazas en la cadena de abastecimientos, integrando sus hallazgos en el marco doctrinal, conceptual y tecnológico. (MITRE ATT&CK, 2025).

7 Modelo Estratégico de Mitigación de Riesgos Cibernéticos en la Cadena de Abastecimiento: prevención y respuesta

Como resultado de los hallazgos, se propone un Modelo Estratégico de Mitigación que integre prevención y respuesta ante ciberataques, alineado con los flujos de la cadena de abastecimiento.

- **Componentes del modelo:**

- **Arquitectura de Confianza Cero (Zero Trust Architecture - ZTA):** Basada en el documento NIST SP 800-207, implementando controles de acceso continuo y verificación de identidad.
- **Integración de sistemas ERP (SAP-SILOG):** con monitoreo en tiempo real mediante IA y algoritmos de machine learning, para detección de anomalías.
- **Aplicación del marco MITRE ATT&CK:** para caracterizar amenazas y estructurar la defensa cibernética logística (MITRE ATT&CK, 2025).
- **Implementación de Blockchain:** para trazabilidad y verificación de la integridad de datos en órdenes de pedido, inventarios y entregas (R. M. Díaz, 2022).

Este modelo fortalece los principios de oportunidad, sostenibilidad, disponibilidad y flexibilidad, esenciales en la doctrina logística conjunta FF.MM (Manual FF.MM. 4-9, 2012).

I. Enfoque General del Modelo

Objetivo:

Prevenir, detectar, responder y adaptarse frente a ciberataques que afecten la cadena de abastecimiento, garantizando oportunidad, sostenibilidad, disponibilidad y flexibilidad (Manual FF.MM. 4-9, 2012).

II. Componentes del Modelo

a. Prevención: validación de accesos, encriptación de datos, segmentación de redes.

- Autenticación multifactor (MFA).
- Segmentación de redes logísticas.
- Permisos de acceso mínimos.
- Monitoreo continuo de identidades y credenciales. (Rose et al., 2020).

b. Detección: SIEM (Security Information and Event Management) con inteligencia artificial.

- Integración de SAP-SILOG con algoritmos de detección de anomalías y alertas en tiempo real.
- Aplicación de la matriz MITRE ATT&CK: para caracterizar tácticas, técnicas y procedimientos de amenazas sobre cadena de suministro (MITRE ATT&CK, 2025).

Tabla 3. Matriz MITRE ATT&CK

Táctica	Técnica	Detección requerida
Reconocimiento	T0862 Supply Chain Compromise	Monitoreo de cambios no autorizados en software o hardware de proveedores
Ejecución	T1204 User Execution	SIEM con IA para ejecución de procesos sospechosos
Persistencia	T1078 Valid Accounts	Auditoría de accesos y cuentas privilegiadas
Defensa Evasión	T1562 Impair Defenses	Integración con Zero Trust y detección ML (Machine Learning)
Comando y Control	T1071 Application Layer Protocol	Inspección profunda de tráfico
Exfiltración	T1041 Exfiltration Over Command Channel	Detección de transferencias inusuales

Fuente: MITRE ATT&CK, 2025 (Adaptada).

c. **Respuesta:** protocolos de recuperación y continuidad basados en escenarios simulados.

- Protocolos de recuperación ante ataques ransomware y denegación de servicio.
- Blockchain para trazabilidad de pedidos, inventarios y entregas sin manipulación (R. M. Díaz, 2022).

d. Adaptación y Resiliencia Cognitiva

- Logística cognitiva: análisis de datos para anticipación y planeamiento predictivo.
- Logística algorítmica: optimización de rutas, inventarios y mantenimiento mediante ML (Machine Learning).
- Logística cuántica: aplicación futura de Quantum Neural Networks y Quantum Annealing para resolver problemas complejos de la cadena de suministro en tiempo real (Weinberg et al., 2023).

7.1. Modelo Plan de contingencia y respuesta eficaz ante Ciberataques a la Cadena de Abastecimientos FFMM (P.C.r.E)

De acuerdo con Ávila & Ramón (2025), un Plan de contingencia y respuesta ante Ciberataques considera y proporciona una estrategia estructurada y adaptable para mejorar la resiliencia de una organización, con posterioridad a un ciberataque. Para tal efecto, los autores consideran cuatro fases principales, cuya ejecución puede darse simultáneamente o con independencia entre fases, para ello es necesario considerar la severidad del ataque, así como su correspondiente tipo o tipos de ataque. Es importante recalcar que el nivel de implementación y ejecución de cada fase se encuentra directamente relacionado con el nivel de madurez de seguridad de cada organización.

Tabla 4. Escenario de los tipos de Ciberamenazas:

Tipo de ataque	Descripción técnica	Impacto esperado en operaciones logísticas
DDoS (Denegación de Servicio Distribuido)	Saturación de red logística, afectando ERP SAP-SILOG y plataformas integradas.	Interrupción de la plataforma de pedidos y recepciones; aumento de tiempos de entrega y desabastecimiento de inventarios críticos.
Malware (ransomware y troyanos)	Infección en equipos logísticos o servidores SAP que cifran datos y exigen rescate.	Paralización completa de procesos de despacho y almacenamiento; posible pérdida de datos sensibles e inventarios.
Inyección de datos (SQL Injection)	Alteración de bases de datos de inventarios, modificando registros y órdenes.	Genera órdenes falsas, despachos incorrectos, hurtos internos encubiertos y pérdidas materiales estratégicas.

Parámetros evaluados:

- Tiempos de respuesta y recuperación (RTO/RPO).
- Afectación de inventarios por día de inactividad.
- Número de pedidos críticos retrasados.
- Pérdida económica calculada.

Tabla 5. Impacto al sistema por amenaza emergente según tipo de ataque.

Tipo de ataque	Amenaza emergente	Impacto
Inyección SQL	Generación de órdenes falsas, despachos incorrectos, hurtos internos encubiertos y pérdidas materiales estratégicas.	Muy Alto
Malware	Paralización completa de procesos de despacho y almacenamiento; posible pérdida de datos sensibles e inventarios.	Muy Alto
DDoS	Interrupción de la plataforma de pedidos y recepciones; aumento de tiempos de entrega y desabastecimiento de inventarios críticos.	Muy Alto

Fuente: Elaboración propia

Un plan de contingencia y respuesta eficaz ante ciberataques implica identificar el nivel de ciberresiliencia de la organización, entendido como la habilidad de la organización para asumir y sobrepasar el estrés, las fallas, peligros y amenazas de sus ciberrecursos al interior de la organización, así como en su ecosistema, de tal forma la organización cumplirá su misión, fortaleciendo su cultura y manteniendo su forma deseada de operación. (World Economic Forum, 2022).

The Cyber Resilience Index: Advancing Organizational Cyber Resilience (World Economic Forum, 2022) incluye una guía de buenas prácticas para crear ciberresiliencia con perspectiva holística. Para tal efecto, en su marco de trabajo de la ciberresiliencia, formula seis principios fundamentales, así como actividades asociadas y subactividades, por medio de las cuales los ciber-lideres definen el nivel de ciberresiliencia más beneficioso para la organización.

Tabla 6. Resumen del marco de trabajo de ciber resiliencia - WEF

No	Principios	No. Actividades	No. Subactividades
1	Evaluar y priorizar periódicamente el riesgo cibernético	3	6
2	Establecer y mantener los fundamentos básicos de seguridad	6	12

3	Incorporar la gobernanza de la ciberresiliencia en la estrategia empresarial	3	6
4	Fomentar la resiliencia sistémica y la colaboración	3	6
5	Asegúrese de que el diseño favorezca la resiliencia cibernética	4	8
6	Cultivar una cultura de resiliencia	5	10

Fuente: Adaptado de The Cyber Resilience Index: Advancing Organizational Cyber Resilience (2022)

El modelo del Plan de contingencia y respuesta eficaz ante Ciberataques a la Cadena de Abastecimientos FFMM (P.C.r.E), propone como factores clave: Gestionar cultura ciberresiliente, Priorizar e invertir en ciberresiliencia, Ejecutar el P.C.r.E, Diseñar, organizar, gerenciar y garantizar estrategia ciberresiliente. Estos factores son decisivos para identificar el nivel de resiliencia y respuesta de la organización ante ciber ataques, dependiendo de los tipos de ataque, asi como, sus amenazas. El modelo tambien considera un rendimiento estimado que integra las fases de ciberdefensa (prevención, detección, respuesta, recuperación) con el nivel de implementación – esfuerzo organizacional (personas, tiempo, recursos financieros).

Cada actividad o eslabon de la cadena de abastecimientos se caracteriza con el tiempo minimo de la operación, para el caso del modelo se analiza un dia de trabajo con 8 horas laborales. A su vez el modelo contempla el tiempo adicional ocasionado por los ciberataques, según su severidad y el tipo de ataque que recibe la cadena de abastecimientos. Para efectos del modelo, se emplea el tiempo promedio estimado de detección con Sistema IA, el tiempo de respuesta ante incidentes con Sistema IA, tasa de falsos positivos, los cuales han sido estimados por Domecq, Diaz, Dominguez, & Osurak (2024).

El modelo propone el empleo de arquitectura Zero Trust, la apropiada integracion con Inteligencia Artificial - MITRE ATT&CK – BLOCKCHAIN, todas ellas como parte del sistema propuesto en el Plan de contingencia y respuesta eficaz ante Ciberataques a la Cadena de Abastecimientos FFMM (P.C.r.E), asumiendo los conceptos generales del índice de ciberresiliencia, las fases de ciberdefensa, así como el nivel de implementación según la madurez en seguridad que tiene la organización. El modelo simula la severidad del ataque, es decir, si se recibe un ataque combinado, por ejemplo Inyección SQL, Malware, DDoS al mismo tiempo o si se recibe uno o dos al tiempo y su posible impacto al sistema.

En la imagen se observan diferentes eventos cuya severidad de ataque tipo 3, atacan la cadena de abastecimientos mediante los tipos de ataque Inyección SQL, Malware y DDoS de manera conjunta, con muy alto impacto para la cadena de abastecimientos, según las amenazas emergentes, como generacion de ordenes falsas, despachos incorrectos, cierre total procesos de despacho y almacenamiento, asi como aumento en los tiempos de entrega y de respuesta de la cadena de abastecimientos, entre otros. El rendimiento del modelo, restringido al nivel de implementacion de ciberresiliencia de la organización, responde ante cada evento, sin embargo todos los ataques caracterizados con nivel de severidad 3, generaran incremento estimado en el consumo de recursos de la organización.

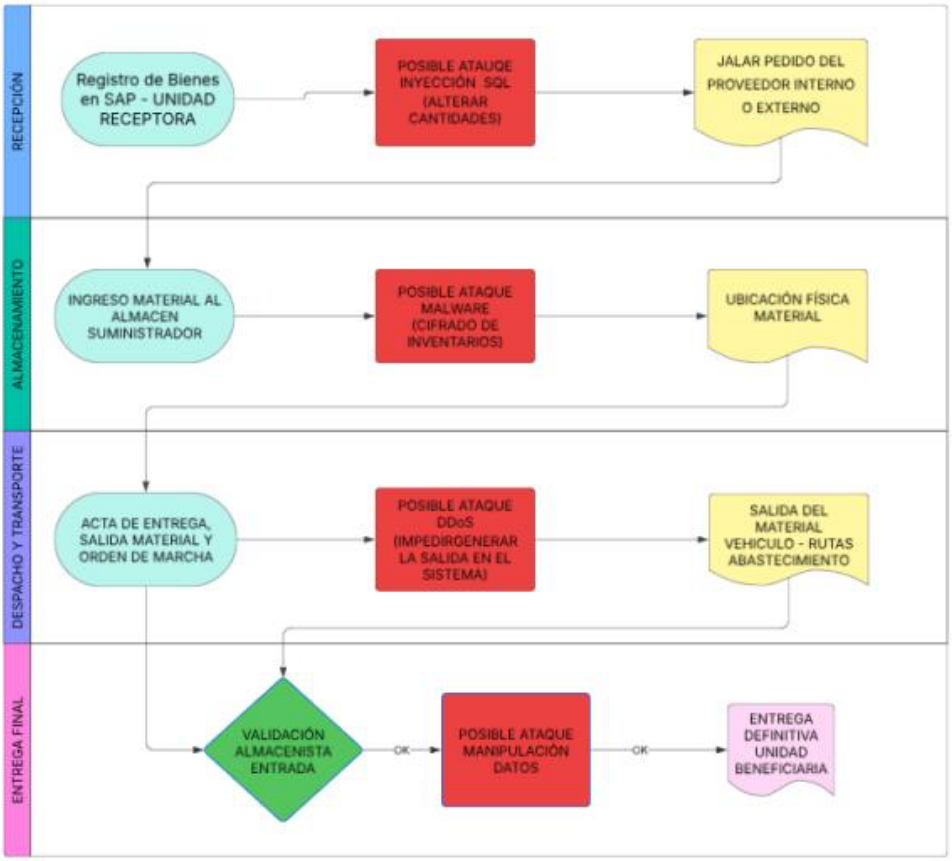
Diagrama 1. Resumen de eventos según severidad del ataque y su correspondiente incremento estimado del tiempo a las actividades de la cadena de abastecimientos.

Evento	Severidad ataque	Inyección SQL		Malware		DDoS		Demora simulada del	Nivel de implementación Ciberresiliencia				RENDIMIENTO MODELO	SC Mean Time_Base	Tiempo total del sistema con	Incremento estimado en recursos
		Ataque	Impacto	Ataque	Impacto	Ataque	Impacto		Prevención	Detección	Respuesta	Recuperación				
1	3	1	5	1	4	1	5	93%	5	4	4	4	0,85	1.920	2.193	14,23%
2	2	1	5	1	5	0	0	67%	3	3	5	3	0,7	1.920	2.313	20,47%
3	2	1	5	1	5	0	0	67%	4	5	5	4	0,9	1.920	2.051	6,82%
4	1	1	4	0	0	0	0	27%	3	5	3	4	0,75	1.920	2.056	7,06%
5	2	1	4	1	5	0	0	60%	5	4	5	5	0,95	1.920	1.979	3,08%
6	1	1	5	0	0	0	0	33%	5	5	3	5	0,9	1.920	1.987	3,49%
7	1	1	4	0	0	0	0	27%	4	5	4	5	0,9	1.920	1.974	2,82%
8	3	1	5	1	4	1	4	87%	5	3	5	4	0,85	1.920	2.174	13,23%
9	1	1	4	0	0	0	0	27%	4	3	5	5	0,85	1.920	2.001	4,23%

Fuente: Elaboracion propia

El diagrama representa nueve eventos con diferente severidad, en aquellos con severidad 3, se reciben simultaneamente los tipos de ataque inyección SQL, Malware y DDoS, cada uno de ellos con un determinado impacto al sistema, generando retrasos, demoras, exponiendo el sistema a las diferentes amenazas emergentes. Posteriormente, a partir de la implementacion de las variables de ciberresiliencia en cada fase del Plan de contingencia y respuesta eficaz ante Ciberataques a la Cadena de Abastecimientos FFMM (P.C.r.E), se estima el rendimiento del modelo, asumiendo la arquitectura y diseño Zero Trust- IA - MITRE ATT&CK – Blockchain. La afectación a la cadena de abastecimientos es asumida en variable temporal, debido a que cualquier tipo de ataque impacta el tiempo de respuesta de la cadena de abastecimientos. El modelo, por su parte, considera que cualquier incremento estimado en recursos por encima del 5%, genera un impacto negativo para la organización. El modelo propuesto permite inferir que el incremento estimado en los recursos para la gestion de la cadena de abastecimientos, se encuentra directamente relacionado con la severidad del ataque y el nivel de implementacion de las variables de ciberresiliencia al interior de la organización.

Diagrama 2. Esquema visual de puntos críticos vulnerables en el proceso



Fuente: Elaboración propia

CADENA DE ABASTECIMIENTOS CON AMENAZAS:

1. **Recepción**
    - Registro de bienes en SAP-SILOG.
    - **Posibles ataques:** Inyección SQL alterando cantidades o proveedores.
2. **Almacenamiento**
    - Control de inventarios, ubicación física.
    - **Posibles ataques:** Malware cifrando bases de datos de inventarios.
3. **Despacho y transporte**
    - Generación de OT (órdenes de transporte).

- **Posibles ataques:** DDoS impidiendo generación y transmisión de documentos de salida.

4. **Entrega final**
    - Validación por unidad beneficiaria.
    - **Posibles ataques:** Manipulación de datos en guías de entrega, ocultando hurtos.

Consecuencias de los ataques:

- Hurtos de material sin trazabilidad.
- Pérdida o alteración de información estratégica.
- Afectación de la sostenibilidad operacional.

Tabla 7. Plan de mitigación inmediata basado en la matriz MITRE ATT&CK

Táctica (MITRE)	Técnica (MITRE)	Medidas de prevención y respuesta recomendadas
Initial Access	Supply Chain Compromise (T0862)	Auditorías de proveedores, Zero Trust, segmentación de red logística.
Execution	Malicious Code Injection (T1055)	EDR con machine learning, whitelisting de scripts de ERP.
Persistence	Supply Chain Compromise Persistence Mechanism (T1195.002)	Monitoreo de integridad de archivos y actualizaciones.
Privilege Escalation	Valid Accounts (T1078)	MFA, rotación de credenciales, revisión cuentas privilegiadas.
Defense Evasion	Obfuscated Files or Information (T1027)	Análisis heurístico, sandboxing, inspección DPI.
Credential Access	Credential Dumping (T1003)	Segmentación de dominios y autenticaciones, SIEM para logs.
Discovery	Network Service Scanning (T1046)	IDS/IPS, detección de puertos anómalos, honeypots.
Lateral Movement	Pass the Hash (T1075)	Restricciones NTLM, Zero Trust, monitoreo Kerberos.
Collection	Data from Information Repositories (T1213)	SIEM, análisis de consultas masivas y patrones anómalos.
Exfiltration	Exfiltration Over Command and Control Channel (T1041)	DPI, DLP, bloqueo de C2 conocidos.
Impact	Data Manipulation (T1565)	Auditoría de integridad, redundancia en bases de datos, backups seguros.

Fuente: Elaboración propia

Integración con innovaciones previas (Logística cognitiva, algorítmica y cuántica):

a) **Logística cognitiva**: Implementar sistemas de IA para detección temprana de ataques y correlación de eventos (como machine learning adaptativo).
b) **Logística algorítmica**: Aplicar algoritmos para predicción de afectaciones logísticas ante cada ataque, en tiempo real.
c) **Logística cuántica**: Emplear en futuro cercano métodos de cifrado cuántico (quantum encryption) y simulaciones logísticas cuánticas para planeamiento de escenarios de amenazas complejas.

El diseño de modelos de simulación, esquemas de afectación y planes de mitigación basados en MITRE ATT&CK permite a las Fuerzas Militares de Colombia anticipar, absorber y responder de forma inmediata ante ciberataques en su cadena de abastecimientos. La integración de logística cognitiva, algorítmica y cuántica fortalece la resiliencia estratégica y sostenibilidad operacional, alineándose a los objetivos de la investigación y estándares como ISO/IEC 27001 y NIST SP 800-207.

8. Integración de simulaciones dinámicas y modelos de mitigación de riesgos de amenazas cibernéticas

El desarrollo de este estudio evidencia que la cadena de abastecimiento militar enfrenta crecientes amenazas cibernéticas en un contexto de operaciones multidominio e híbridas. La integración de simulaciones dinámicas y modelos de mitigación basados en

ciberseguridad adaptativa representa un avance estratégico para las Fuerzas Militares de Colombia. Los principales hallazgos indican que:

- La dependencia de sistemas ERP como SAP-SILOG requiere la implementación de arquitecturas de confianza cero y blockchain para blindar la integridad de los procesos (R. M. Díaz, 2022; NIST, 2020).
- El uso de simulaciones sistémicas permite anticipar las disrupciones logísticas en tiempo real, fortaleciendo la resiliencia ante ciberataques (Casadiego et al., 2023).
- La integración de frameworks como MITRE ATT&CK facilita la caracterización de amenazas y el diseño de estrategias de defensa en capas (MITRE ATT&CK, 2025).

El presente estudio permite comprender la importancia de la ciberseguridad como un factor transversal para garantizar el éxito operacional en la cadena de abastecimientos militar conjunta. A partir de la caracterización doctrinal, tecnológica y estratégica realizada en los numerales previos, se evidencia que los objetivos específicos planteados son interdependientes y fundamentales para el cumplimiento del objetivo general, en tanto abordan la problemática desde un enfoque integral que combina análisis, simulación y diseño de soluciones. Logrando así el propósito para *Diseñar una estrategia de mitigación de riesgos cibernéticos para las operaciones logísticas en la cadena de abastecimientos.* Permitiendo que para este fin, se requirió primero:

1) Caracterizar las vulnerabilidades actuales en los sistemas de información logística.

La caracterización realizada muestra que la dependencia de plataformas ERP como SAP-SILOG, sin integración de arquitecturas de confianza cero o tecnologías blockchain, deja expuestos múltiples nodos críticos de la cadena de abastecimientos militar. Como lo señala Díaz (2022) en su estudio sobre ciberseguridad logística en América Latina, los sistemas de información militar no han implementado de manera integral la segmentación de redes, el cifrado end-to-end ni mecanismos de autenticación multifactorial robusta, lo que incrementa su superficie de ataque (R. M. Díaz, 2022).

Asimismo, la revisión de Casadiego (2023) sobre los niveles de madurez logística evidencia que el 60% de los sistemas evaluados en el sector defensa latinoamericano no superan un nivel intermedio de madurez cibernética, careciendo de capacidades de detección y respuesta proactiva ante incidentes (Casadiego et al., 2023).

2) Realizar ciberataques simulados en la caracterización de la cadena de abastecimientos.

La modelación sistémica aplicada y abordada en el numeral 6 y 7, permitió simular escenarios de ataques de denegación de servicio (DoS), manipulación de inventarios y acceso no autorizado a SAP-SILOG, identificando que dichos eventos pueden generar altos impactos en cascada sobre:

- **Tiempo de ciclo logístico**, duplicándolo o triplicándolo dependiendo del nodo afectado (Casadiego et al., 2023).
- **Disponibilidad de recursos críticos** para misiones conjuntas, al imposibilitar su trazabilidad o confirmación de stock en tiempo real.
- **Continuidad de operaciones tácticas**, exponiendo vulnerabilidades en las unidades de combate si los suministros no llegan a tiempo (Kress, 2016).

Estos hallazgos reafirman la necesidad de incorporar el marco MITRE ATT&CK para la identificación exhaustiva de TTPs (Tácticas, Técnicas y Procedimientos) usadas en ciberataques contra sistemas logísticos militares, y su adaptación a la arquitectura de red, roles y dispositivos existentes en las Fuerzas Militares de Colombia.

3) Proponer un modelo de prevención mediante herramientas tecnológicas cibernéticas.

Finalmente, con base en la caracterización y simulación, se diseñó el modelo estratégico de mitigación descrito en el numeral 7, que integra las siguientes capacidades:

- **Confianza Cero (Zero Trust Architecture)**: segmentación de red y verificación continua de identidad, como propone NIST SP 800-207 (NIST, 2020).
- **Blockchain** para la trazabilidad y autenticidad de transacciones logísticas.
- **Machine Learning** para la detección de anomalías operacionales y ciberataques a los sistemas de información logística (Alzahrani & Asghar, 2024).
- **Simulación dinámica y escenarios multidominio** como metodología de validación y entrenamiento.

La integración de estos tres objetivos es indispensable para cumplir con el objetivo general. En un entorno de operaciones multidominio, donde la ciberdefensa y la logística convergen como funciones estratégicas, la adopción de modelos innovadores, como la: logística cognitiva, algorítmica y cuántica, siendo imperativo para garantizar la sostenibilidad, flexibilidad, oportunidad y disponibilidad de los recursos en cualquier escenario operacional (Manual FF.MM. 4-9, 2012).

Esta investigación evidencia, de forma metodológica y aplicada, que, sin caracterización exhaustiva, simulación validada y diseño de modelos de prevención, no es posible establecer estrategias de mitigación de ciberamenazas efectivas para la cadena de abastecimientos militar, situación que dejaría expuestas las capacidades estratégicas y la integridad de la fuerza frente a actores adversarios en el ciberespacio.

9. Conclusiones

- La integración de la ciberseguridad como componente estratégico de la logística militar es un imperativo doctrinal y operacional**.** El análisis realizado evidencia que la cadena de abastecimientos se encuentra expuesta a ciberataques que comprometen la sostenibilidad operativa de las Fuerzas Militares de Colombia, afectando principios como la oportunidad, flexibilidad y disponibilidad (Manual Doctrina Logística FFMM 4-9, 2014; JP 4-0, 2019). Los datos estadísticos presentados en los casos de estudio de ENISA (2023) y CrowdStrike (2025) revelan que más del 53% de las intrusiones cibernéticas en el sector defensa a nivel global han estado dirigidas a los sistemas logísticos y de gestión de la cadena de

suministro, destacando la urgencia de fortalecer los sistemas nacionales con base en normas internacionales como ISO/IEC 27001:2022 (ISO/IEC 27001:2022, 2022).

- La propuesta del modelo estratégico de mitigación presentado es coherente con las exigencias de ciberseguridad establecidas en la norma ISO/IEC 27001:2022, el NIST SP 800-207 (Zero Trust Architecture) y los marcos de MITRE ATT&CK para cadenas de suministro. El diseño contempla medidas de prevención, detección y respuesta ante amenazas cibernéticas específicas a los sistemas SAP-SILOG, LOGFAS, GCSS-Army y DLMS, con un enfoque integrado de seguridad en profundidad y Zero Trust, que asegura la reducción de superficies de ataque y la continuidad operativa ante escenarios disputados y ataques complejos (MITRE ATT&CK, 2025; NIST, 2020).
- El modelo innovador propuesto articula conceptos de logística cognitiva, logística algorítmica y logística cuántica como tecnologías emergentes aplicables en defensa. Estas herramientas permiten la automatización, predicción y análisis de grandes volúmenes de datos, la creación de gemelos digitales y la aplicación de algoritmos de machine learning y quantum computing para optimizar la toma de decisiones en tiempo real, fortaleciendo la resiliencia logística frente a ciberataques persistentes avanzados y ataques disruptivos a infraestructuras críticas (Alzahrani & Asghar, 2024; Correll et al., 2023).
- La implementación de este modelo contribuiría directamente al cumplimiento de los tres objetivos específicos planteados. Primero, al caracterizar vulnerabilidades mediante matrices MITRE ATT&CK específicas para cadenas de suministro;

segundo, al proponer simulaciones de ciberataques mediante herramientas alternas con modelos de resiliencia dinámica, y tercero, al diseñar un modelo estratégico de prevención y respuesta con tecnologías cibernéticas emergentes aplicables al contexto colombiano y replicables en otros ejércitos de la región.

- Los escenarios identificados demuestran que la cadena de abastecimiento militar no sólo enfrenta amenazas cibernéticas convencionales, sino también riesgos sistémicos derivados de la transformación digital global. La digitalización de procesos logísticos sin los debidos controles de ciberseguridad incrementa las vulnerabilidades, como se observa en ataques supply chain a nivel OTAN, EE.UU. y Latinoamérica (R. M. Díaz, 2022; ENISA, 2021). Por lo tanto, la adopción de una arquitectura Zero Trust y el uso de indicadores de madurez cibernética propuestos por Casadiego et al., (2023) son fundamentales para asegurar la defensa digital de los flujos logísticos militares.
- La efectividad de este modelo estratégico de mitigación dependerá de su integración con la doctrina conjunta, la formación cibernética especializada y la interoperabilidad entre las Fuerzas Militares y los sistemas nacionales de ciberdefensa. La cultura de ciberseguridad organizacional y la concienciación de los actores logísticos y operacionales constituyen factores determinantes en la consolidación de un sistema de cadena de abastecimientos resiliente, seguro y eficaz para la defensa y seguridad nacional.
- Finalmente, esta investigación evidencia que el futuro de la logística militar está ligado inexorablemente al desarrollo de capacidades de ciberdefensa logística. La

guerra moderna se libra en el dominio físico, informacional y cibernético, siendo indispensable transitar hacia un modelo de logística en red con seguridad integral y adaptación a las tecnologías emergentes, garantizando así la protección de las tropas y el sostenimiento estratégico de las Fuerzas Militares de Colombia en escenarios multidominio.

10. Referencias

Alzahrani, A., & Asghar, M. Z. (2024). Cyber vulnerabilities detection system in logistics-based IoT data exchange. *Egyptian Informatics Journal*, *25*, 100448. https://doi.org/10.1016/j.eij.2024.100448

ARC OP4-1.1 DOCTRINA NAVAL. (2021). *DOCTRINA LOGÍSTICA ARMADA NACIONAL ARC OP4-1.1* (NIVEL OPERACIONAL, Vol. 1–Primera Edición). Direccion de Doctrina Naval. https://es.scribd.com/document/611831011/Doctrina-Logistica-Armada-Nacional-Primera-edicion-2021-V-Final-Preliminar-1-1

Avila, E., & Ramon, V. (Mayo de 2025). Desarrollo de un Plan de Contingencia y Respuesta Eficaz ante Ciberataques de Tipo Ransomware en empresas de Honduras. Tegucigalpa, Francisco Morazán, Honduras.

Bermúdez, C. E. (2022). *Modelo de ciberseguridad para el sector logístico y transporte terrestre en Colombia.* 13.

Casadiego, L., Bastos, E. A., Zúñiga, N. F., & Calderón, A. (2023). Metodología para evaluación de niveles de madurez de elementos logísticos del Soporte Logístico Integrado—ILS. Caso Práctico Simulado. *Prospectiva*, *21*(1), 32–47.

Christopher, M. (2011). *Logistics & Supply Chain Management*. Financial Times Prentice Hall.

Correll, R., Weinberg, S. J., Sanches, F., Ide, T., & Suzuki, T. (2023). Quantum Neural Networks for a Supply Chain Logistics Application. *Advanced Quantum Technologies*, *6*(7), 2200183. https://doi.org/10.1002/qute.202200183

CrowdStrike. (2025). *Global Threat Report para el 2025 | Resumen Ejecutivo del Global Threat Report 2025 de CrowdStrike*. CrowdStrike.com. https://www.crowdstrike.com/es-latam/global-threat-report/

Davis, A. (2015). Building Cyber-Resilience into Supply Chains. *Technology Innovation Management Review*, *5*(4), 19–27.

Díaz del Río, J. (2011). La ciberseguridad en el ámbito militar. *Cuadernos de estrategia*, *149*, 215–256.

Díaz, M., & Núñez, G. (2023). Ciberataques a la logística y la infraestructura crítica en América Latina y el Caribe. *Documentos de Proyectos*, Article 49086. https://ideas.repec.org//p/ecr/col022/49086.html

Díaz, R. (2020, noviembre 3). *La ciberseguridad en tiempos del COVID-19 y el tránsito hacia una ciberinmunidad*. https://repositorio.cepal.org/entities/publication/9c9716e2-b429-4ab5-b897-62d2c4f8eb40

Díaz, R. M. (2022). *Ciberseguridad en cadenas de suministros inteligentes en América Latina y el Caribe*. 67.

Domecq, H., Diaz, C., Dominguez, L., & Osurak, E. (8 de Agosto de 2024). El rol de la inteligencia artificial en la detección y respuesta a incidentes de ciberseguridad: un estudio de caso. Buenos Aires, Argentina.

Eccles, H. E. (1959). *FMFRP 12-14 Logistics in the National Defense* (Primera). U.S. Marine Corps. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.marines.mil/Portals/1/Publications/FMFRP%2012-14.pdf?ver=bh2uGS5SgL3sb9clGZxYgA%3d%3d

ENISA. (2021). Threat Landscape for Supply Chain Attacks | ENISA. *ENISA Reports*, 57.

Hoffman, F. G. (2007). *Conflict in the 21st Century: The Rise of Hybrid Wars* [Economic Statecraft for Business Leaders: A 21st Century Reality]. Potomac Institute for Policy Studies. https://potomacinstitute.us/reports/19-reports/1163-conflict-in-the-21st-century-the-rise-of-hybrid-wars

Isaza, C. D. (2012). SILOG, Sistema de Información al servicio del sector defensa. *Revista de las Fuerzas Armadas*, *224*, 34–39. https://doi.org/10.25062/0120-0631.997

ISO/IEC 27001:2022. (2022). *ISO/IEC 27001:2022*. ISO. https://www.iso.org/es/norma/27001

Joint Logistics JP 4-0. (2019). *Joint Publication 4-0*. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://irp.fas.org/doddir/dod/jp4_0.pdf

Kaddoussi, A., Zgaya, H., Hammadi, S., & Bretaudeau, F. (2011). Disruption Management Optimization for Military Logistics. En L. Iliadis, I. Maglogiannis, & H. Papadopoulos (Eds.), *IFIP Advances in Information and Communication Technology: Vol. AICT-364* (Número Part II, pp. 61–66). Springer. https://doi.org/10.1007/978-3-642-23960-1_8

Kress, M. (2016). *Operational Logistics—The Art and Scienceof Sustaining Military Operations* (2da Edición). Cham: Springer International Publishing. https://primoa.library.unsw.edu.au/discovery/fulldisplay?vid=61UNSW_INST:UNSWS&tab=Everything&docid=alma9950691203901731&context=L&lang=en

Madhava V., K., Deepak Ch., N., Pramod Ch., P., & Pavan K., G. (2023). Cloud based ERP systems and Data Security for Cloud based ERP Applications – SAP

S/4HANA – IJSREM. *International Journal of Scientific Research in Engineering and Management (IJSREM)*, *Volume: 07*(Issue: 02), 4.

Manual FF.MM. 4-9. (2012). *Manual de Doctrina Logística de las Fuerzas Militares*. Fuerzas Militares de Colombia. https://mindefensa-primo.hosted.exlibrisgroup.com/permalink/f/188bri2/57MDN_Aleph000070617

MCE 3-12 Operaciones del Ciberespacio. (2021). *MANUAL DE CAMPAÑA DEL EJÉRCITO MCE 3-12 OPERACIONES DEL CIBERESPACIO* (PUBLICACIONES EJÉRCITO). https://drive.google.com/file/d/1uQMhyX5wjnhw5iloMldu_huXtsqyiQoR/view?usp=sharing

MFC 5-0 Planeamiento Conjunto. (2024). Manual Fundamental Conjunto MFC 5-0: Planeamiento Conjunto. En *Sello Editorial ESDEG* (Centro de Doctrina Conjunta). Imprenta CGFM. https://doi.org/10.25062/MFC50PC

MFE 4-0 Sostenimiento. (2016). *MANUAL FUNDAMENTAL DEL EJÉRCITO MFE 4-0 SOSTENIMIENTO*. Publicaciones Ejército. https://www.cedoc.mil.co/mfe-4-0-sostenimiento/

MITRE ATT&CK. (2025). *MITRE ATT&CK®*. https://attack.mitre.org/

Mora, L. A. (2023). *Gestión logística integral - 3ra edición: Las mejores prácticas en la cadena de abastecimiento* (3ra Edición). Ecoe Ediciones. https://books.google.es/books?id=FrquEAAAQBAJ&printsec=frontcover&hl=es#v=onepage&q&f=false

Morales, C. D. I. (2012). SILOG, Sistema de Información al servicio del sector defensa. *Revista de las Fuerzas Armadas*, *224*, Article 224. https://doi.org/10.25062/0120-0631.997

NATO. (2018). AJP-4, Allied Joint Doctrine for Logistics. *NATO STANDARDIZATION OFFICE (NSO)*, *(Edition B)*(Version 1), 84.

Naval War College Foundation. (2020). 2020 Department of Defense Artificial Intelligence Education Strategy. *DoD AI Education Strategy*, 54.

Navarro, R. (1999). Introducción al Apoyo Logístico Integrado (ILS). Revista de Marina. *Revista de Marina N° 4*, 342–354.

NIST. (2020). Cybersecurity Framework. *NIST*. https://www.nist.gov/cyberframework

Pagonis, W. G., & Krause, M. D. (1992, septiembre 1). *Operational Logistics and the Gulf War*. Defense Technical Information Center. https://apps.dtic.mil/sti/citations/ADA278028

Phillipson, F. (2025). *Quantum Computing in Logistics and Supply Chain Management an Overview* (No. arXiv:2402.17520). arXiv. https://doi.org/10.48550/arXiv.2402.17520

Quevedo, C. R. (2023). Ciberdefensa y ciberseguridad en el Perú: Realidad y retos en torno a la capacidad de las FF. AA. para neutralizar ciberataques que atenten contra la seguridad nacional. *Revista de Ciencia e Investigación en Defensa*, *4*(1), Article 1. https://doi.org/10.58211/recide.v4i1.99

Quinn, B. J. (2023, abril). *Sustaining Multidomain Operations: The Logistical Challenge Facing the Army's Operating Concept* [Military Review]. Army University Press.

https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/March-April-2023/Multidomain-Operations/

REGLAMENTO FF.MM. 4-2. (2016). *REGLAMENTO DE LOGÍSTICA CONJUNTA DE LAS FUERZAS MILITARES FF.MM. 4-2*. Imprenta y Publicaciones de las Fuerzas Militares. https://es.scribd.com/document/420740676/Reglamento-de-Logistica-Conjunta-FF-MM

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero Trust Architecture* (No. NIST Special Publication (SP) 800-207). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207

SAP. (2025). *Defense and Security Industry Software*. SAP. https://www.sap.com/industries/defense-security.html

Serrano, A. (2025). *Capítulo 3. Correlación entre logística militar, estudios estratégicos y seguridad y defensa nacional: Arquitectura invisible del poder en el siglo XXI* [Text.Chapter]. Sello Editorial ESDEG. https://esdeglibros.edu.co/index.php/editorial/catalog/view/326/248/4129

Serrano, A., Barrero, D., Corcione, M. A., Acevedo, C., & López, D. (2025). Conceptualización de Estudios Estratégicos Contemporáneos como contribución multidisciplinar. En *Sello Editorial ESDEG*. Sello Editorial ESDEG. https://doi.org/10.25062/9786287602984

Smith, L. P. (2022). *Product Support Manager Guidebook*. US Department of Defense. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://aaf.dau.edu/storage/2023/09/Product-Support-Manager-PSM-Guidebook.pdf

Snyder, D., Bodine-Baron, E., Amouzegar, M. A., Lynch, K. F., Lee, M., & Drew, J. G. (2017a). *Robust and Resilient Logistics Operations in a Degraded Information Environment*. https://www.rand.org/pubs/research_reports/RR2015.html

Snyder, D., Bodine-Baron, E., Amouzegar, M. A., Lynch, K. F., Lee, M., & Drew, J. G. (2017b). *Robust and Resilient Logistics Operations in a Degraded Information Environment*. https://www.rand.org/pubs/research_reports/RR2015.html

Suramericana. (2022, septiembre 28). Los ciberataques a las cadenas de suministros ya son récord. *Suramericana*. https://suramericana.com/blog/conectividad/los-ciberataques-a-las-cadenas-de-suministros-ya-son-record/

Sustaining Multidomain Operations: The Logistical Challenge Facing the Army's Operating Concept. (s/f). Army University Press. Recuperado el 20 de junio de 2025, de https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/March-April-2023/Multidomain-Operations/

Thorpe, G. C. (1986a). *George C. Thorpe's Pure Logistics: The Science of War Preparation*. National Defense University Press. https://books.google.com.co/books/about/George_C_Thorpe_s_Pure_Logistics.html?id=De_oyA6Z5vMC&redir_esc=y

Thorpe, G. C. (1986b). *George C. Thorpe's Pure Logistics: The Science of War Preparation*. National Defense University Press. https://books.google.com.co/books/about/George_C_Thorpe_s_Pure_Logistics.html?id=De_oyA6Z5vMC&redir_esc=y

U. S. Government Accountability Office. (2024, abril 15). *F-35 Sustainment: Costs Continue to Rise While Planned Use and Availability Have Decreased | U.S. GAO*. U.S. GAO. https://www.gao.gov/products/gao-24-106703

Valdés, L., Díaz, R., & Pérez, G. (2021, julio 21). *Oportunidades y desafíos para la implementación de blockchain en el ámbito logístico de América Latina y el Caribe*. https://repositorio.cepal.org/entities/publication/0612ad64-29ed-42cc-84d0-f83b7cabdee8

Weinberg, S. J., Sanches, F., Ide, T., Kamiya, K., & Correll, R. (2023). Supply chain logistics with quantum and classical annealing algorithms. *Scientific Reports*, *13*(1), 4770. https://doi.org/10.1038/s41598-023-31765-8

Winegardner, S. (2025). ADC_1498_Administrative Update to DLM 4000.25 Vol 2 Ch 17 SDR File Attachment Size for WebSDR_MFR. *DEFENSE LOGISTICS AGENCY*, 3.

World Economic Forum. (Julio de 2022). The Cyber Resilience Index: Advancing Organizational Cyber Resilience. Cologny, Geneve, Switzerland.

Zambrano, A. D., Meza, Y. K., Villavicencio, C. M., & Rodríguez, A. R. (2024). Ciberataques en América Latina: Desafíos de la era digital. *Revista Compromiso Social*, 89–104. https://doi.org/10.5377/recoso.v1i13.19295