Estandarización del Protocolo de Ingreso a las Unidades Militares como modelo de seguridad integral nacional

Mayor (EJC) Carlos Mario Piedrahita Olaya

Artículo para optar al título profesional:

Magister en Seguridad y Defensa Nacionales

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) Carlos Mario Piedrahita Olaya
Identificación	**:**	1.110.460.508
Programa académico	**:**	Maestría en Seguridad y Defensa Nacionales
Tutor metodológico	**:**	DO. Jonnathan Jiménez Reina
Tutor temático	**:**	CR. ® Guillermo Orozco Becerra
Fecha de entrega	**:**	27 de Agosto 2025
Extensión	**:**	8611

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

Estandarización del Protocolo de Ingreso a las Unidades Militares como modelo de seguridad integral nacional

Standardization of the Protocol of Entry to Military Units as a model of integral national security.

Carlos Mario Piedrahita Olaya*
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: El artículo propone un modelo nacional estandarizado de control de ingreso y salida en unidades militares, articulado en cuatro dimensiones (normativa, tecnológica, humana y procedimental). Mediante una revisión exploratoria (2000–2025) de literatura, doctrina y reportes, identifica brechas: dispersión normativa, asimetrías tecnológicas, baja interoperabilidad de datos, inspecciones incompletas y débil formación del personal de guardia. Se sistematizan incidentes (infiltraciones, VBIED, *insider threats* y ciberataques) y se fijan requisitos mínimos bajo defensa en profundidad. Se plantea un Protocolo Operativo Estandarizado de cinco capas (disuasión, detección, verificación, control humano y respuesta), con listas de chequeo por flujo, matriz RACI y 12 indicadores (eficacia, eficiencia, cumplimiento). La implementación sigue un ciclo PHVA/PDCA con auditorías, simulacros y mejora continua, integrando biometría/QR–RFID–ANPR conectada a inteligencia. Se propone directiva marco, plan por fases (0–3) y hoja de ruta para interoperabilidad y capacitación.

Palabras clave: Amenazas, gestión del riesgo, protocolo de ingreso, seguridad integral, unidades militares, vulnerabilidades.

Palabras clave:

Abstract: The article proposes a standardized national model for controlling entry and exit in military units, articulated in four dimensions (regulatory, technological, human, and procedural). Through an exploratory review (2000–2025) of literature, doctrine, and reports, it identifies gaps: regulatory dispersion, technological asymmetries, low data interoperability, incomplete inspections, and weak training of guard personnel. Incidents (infiltrations, VBIEDs, insider threats, and cyberattacks) are

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

systematized, and minimum requirements are set under defense in depth. A five-layer Standardized Operating Protocol (deterrence, detection, verification, human control, and response) is proposed, with flow checklists, a RACI matrix, and 12 indicators (effectiveness, efficiency, compliance). Implementation follows a PDCA cycle with audits, drills, and continuous improvement, integrating biometrics/QR–RFID–ANPR connected to intelligence. A framework directive phased plan (0–3), and roadmap for interoperability and training are proposed.

Key words: Key words: Threats, risk management, entry protocol, integrated security, military units, vulnerabilities.

Introducción

La presente investigación aborda la problemática del ingreso no controlado a unidades militares en Colombia, en un contexto de amenazas crecientes por parte de grupos armados ilegales, criminalidad organizada y riesgos internos. El evento ocurrido en septiembre de 2024 en la base militar de Puerto Jordán (Arauca), donde un ataque del ELN dejó dos soldados muertos y 26 heridos, evidencia fallas en los esquemas de seguridad perimetral y de control de ingreso (Deutsche Welle, 2024). Asimismo, hechos recientes como la infiltración de insurgentes, el uso de vehículos explosivos y el empleo de drones para fines hostiles han demostrado que los protocolos actuales son insuficientes, desactualizados y dispares entre unidades.

La estandarización de los protocolos de ingreso en las unidades militares es esencial para fortalecer la seguridad y proteger recursos estratégicos. En respuesta a amenazas como el uso de drones con fines hostiles, el Ministerio de Defensa de Colombia implementó en enero de 2025 sistemas avanzados de defensa anti-drones para proteger infraestructuras críticas. Estas medidas reflejan el compromiso del país en adoptar tecnologías avanzadas para mitigar riesgos y fortalecer la seguridad nacional(Ministerio de Defensa Nacional, 2024). Por lo tanto, se formuló la siguiente pregunta de investigación: **¿Cómo establecer un protocolo**

de ingreso estandarizado en las unidades militares para mejorar la seguridad física y proteger los recursos y activos en las unidades militares a nivel nacional?

El problema de investigación se inserta en el actual contexto de persistencia del conflicto armado interno, reconfiguración de las amenazas híbridas y debilitamiento de las capacidades institucionales de protección. A pesar del Acuerdo de Paz de 2016, subsisten amenazas por parte de disidencias de las FARC, el ELN, bandas criminales y actores transnacionales, que han enfocado sus ataques contra instalaciones militares como estrategia de desestabilización y propaganda. Este escenario exige una respuesta institucional basada en estándares modernos de seguridad.

La realidad operacional de muchas unidades militares colombianas, especialmente aquellas en zonas de alto riesgo, se caracteriza por esquemas de control de acceso heterogéneos, ausencia de tecnologías avanzadas, deficiencia en registros, y brechas doctrinales en la formación del personal de guardia. Normativas como la Ley 1621 de 2013 (Inteligencia y Contrainteligencia), el Manual EJC 3-37 de Protección y el Boletín CACIM 2022 señalan la obligación de identificar, mitigar y prevenir riesgos de seguridad, así como estandarizar procedimientos para salvaguardar la infraestructura crítica. Sin embargo, la falta de una política nacional de estandarización de protocolos de ingreso sigue siendo una deuda estructural.

Adicionalmente, la importancia de este estudio radica en la identificación de vulnerabilidades existentes en los procedimientos de ingreso a las unidades militares y en la formulación de un modelo estandarizado que garantice un acceso seguro, eficiente y alineado con las mejores prácticas de seguridad**.** Además, se busca contribuir al fortalecimiento de la seguridad integral mediante el uso de tecnología de punta, estrategias operativas optimizadas

y un enfoque integral que combine elementos humanos, tecnológicos y procedimentales. A nivel nacional, este estudio es relevante para el Ejército Nacional de Colombia, dado que la implementación de un protocolo unificado podría mejorar la coordinación, reducir los riesgos de infiltración y fortalecer la protección de la infraestructura y el personal militar.

Para abordar esta problemática, la investigación emplea un enfoque cualitativo, que permite un análisis detallado de los factores y dinámicas que inciden en la implementación de estos protocolos. Se llevará a cabo una revisión documental, en la que se analizarán estudios previos, normativas vigentes y experiencias internacionales en materia de seguridad militar. En los siguientes apartados, el lector encontrará un análisis detallado sobre el estado del arte en materia de seguridad militar, una revisión de modelos y tecnologías aplicadas a la vigilancia y control de acceso, así como una propuesta de mejora para la implementación de un protocolo de ingreso estandarizado.

La estandarización de los protocolos de ingreso a las unidades militares no solo es una respuesta táctica a las amenazas actuales, sino una necesidad estratégica que define el nivel de resiliencia institucional frente a conflictos híbridos y ataques asimétricos. Defender esta idea implica comprender que la seguridad no puede depender de criterios aislados o medidas reactivas, sino que debe consolidarse mediante un modelo nacional que integre tecnología, doctrina, formación del personal y control normativo. Solo a través de una política unificada y técnicamente robusta, se logrará blindar los accesos, garantizar la protección del personal y mantener la continuidad operacional del aparato de defensa del Estado.

Metodología

La presente investigación es de enfoque cualitativo y de tipo descriptivo-aplicado. Se basa en un análisis documental de normativa, doctrina y reportes institucionales, complementado con una revisión comparativa entre unidades militares. La técnica de análisis empleada fue el análisis categorial y triangulación de fuentes, siguiendo la guía PRISMA-ScR(Tricco et al., 2018). El corpus documental se delimitó aplicando criterios de inclusión: (i) estudios, manuales doctrinales y reportes institucionales publicados entre 2000 y 2025; (ii) enfoque en seguridad física, control de acceso o gestión del riesgo en instalaciones militares; (iii) disponibilidad de texto completo y metodología explícita o marco analítico verificable. Se excluyeron documentos sin pertinencia operativa, sin rigor metodológico o centrados exclusivamente en aspectos históricos. Para garantizar validez y confiabilidad, se realizó doble lectura independiente de los documentos seleccionados, con resolución de discrepancias por consenso, y se empleó una matriz de extracción categorial (normativa, tecnológica, humana, procedimental) que permitió sistematizar los hallazgos(Domínguez, 2007).

Para delimitar el universo documental, se establecieron criterios de elegibilidad claros y estrictos. Se seleccionaron únicamente aquellos documentos que abordaran temáticas directamente relacionadas con seguridad física, control de acceso, gestión de riesgos o protección de instalaciones militares. Se dio prioridad a investigaciones aplicadas al contexto colombiano o, en su defecto, a estudios en países con condiciones geopolíticas y operativas comparables, como escenarios de postconflicto o zonas con presencia de grupos armados organizados. Solo se incluyeron publicaciones con acceso al texto completo y que

presentaran una metodología explícita o un marco analítico verificable. Las fuentes debían haber sido publicadas entre el año 2000 y el 2025, permitiendo así una mirada comprehensiva a lo largo de los últimos 25 años(Quispe, 2023).

La búsqueda de información se desarrolló en bases de datos científicas de amplio reconocimiento como Scopus, Web of Science y Google Scholar, así como en repositorios institucionales especializados, incluyendo el de la Universidad Militar Nueva Granada. Adicionalmente, se consultaron revistas académicas nacionales de defensa y seguridad, informes oficiales del Ministerio de Defensa Nacional, y documentos técnicos emitidos por el Comando General de las Fuerzas Militares y el Comando de Educación y Doctrina (CEDOE)(Tricco et al., 2018).

De la misma manera, la estrategia de búsqueda empleada se fundamentó en una ecuación booleana compuesta, diseñada para maximizar la recuperación de estudios relevantes tanto en español como en inglés. La fórmula utilizada combinó términos clave como "seguridad física", "seguridad militar", "control de acceso", "brecha de seguridad" e "incidente de seguridad", junto con descriptores de ubicación como "base militar", "unidad militar" e "instalación militar", y tipos de amenaza como "ataque", "infiltración", "intrusión" o "sabotaje", todo ello enmarcado en el contexto colombiano y con restricción temporal entre 2000 y 2025.

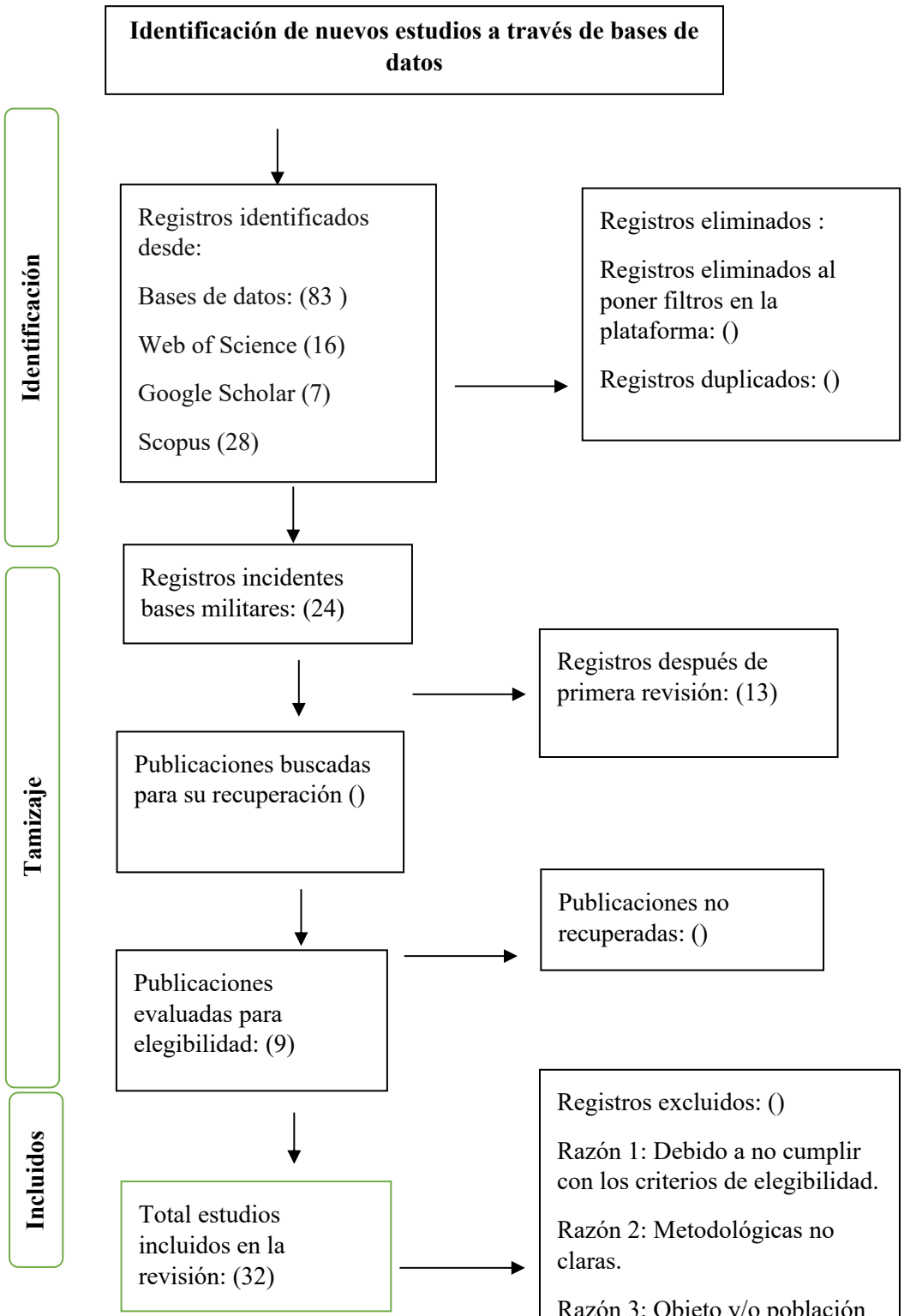
Identificación de los estudios

Para buscar literatura académica sobre estos temas en bases de datos como Scopus o Web of Science, se recomienda utilizar una ecuación booleana que combine sinónimos en inglés y español, términos específicos y operadores lógicos. Por ejemplo:

En ese sentido, se tiene la siguiente ecuación boleana "seguridad física" OR "seguridad militar" OR "security breach" OR "brecha de seguridad" OR "incidente de seguridad" OR "control de acceso") AND ("base militar" OR "instalación militar" OR "instalaciones militares" OR "unidad militar" OR "guarnición militar" OR "military base" OR "military installation") AND ("ataque" OR "ataques" OR "atentado" OR "sabotaje" OR "infiltración" OR "intrusión" OR "attack" OR "attacks" OR "sabotage" OR "infiltration" OR "intrusion") AND (Colombia OR Colombiano OR Colombian) AND (2000 OR 2001 OR ... OR 2025)

De la misma manera, esta ecuación incluye términos en español e inglés para no perder investigaciones relevantes publicadas en cualquiera de los dos idiomas. Se utilizan comillas para frases exactas (p. ej. "seguridad física", "base militar") y el operador OR para abarcar sinónimos o términos relacionados. El operador AND asegura que los resultados contengan todos los grupos de conceptos clave: seguridad, tipo de instalación militar, tipo de incidente, y contexto colombiano. Por ende, la última parte AND (2000 ... 2025) es opcional; en Scopus/WoS usualmente se filtraría por año de publicación por medio de filtros de interfaz. Se incluyó aquí para enfatizar el rango temporal de interés (2000 a la fecha).

Tabla 1. *Metodología prisma*



Nota. Fuente: Elaboración propia

En el proceso de revisión sistemática, se identificaron un total de 83 registros a través de diversas bases de datos, distribuidos de la siguiente manera: Web of Science (16), Google Scholar (7) y Scopus (28), además de 24 registros documentados relacionados específicamente con incidentes en bases militares. Tras aplicar filtros en las plataformas y eliminar duplicados, se procedió a una primera revisión, quedando 13 registros para evaluación más detallada. De estos, 9 publicaciones fueron evaluadas para verificar su elegibilidad, excluyéndose aquellos que no cumplían con los criterios definidos por razones como falta de claridad metodológica, objeto o población no pertinente, o por no ajustarse al enfoque de la investigación. Finalmente, se seleccionó un subconjunto de estudios pertinentes (cantidad aún por definir) que cumplen con los requisitos de calidad y relevancia, los cuales conforman el cuerpo de evidencia utilizado para sustentar los hallazgos del presente estudio en total 32.

Caracterización de los estudios

Tabla 2. *Estudios e informes clave documentados (2000-2025)*

Autores (Año)	Título (Fuente)	Resumen de hallazgos relevantes	Enlace/Referencia
González Prieto, J.A. (2013)	*Administración de riesgos en unidades militares* (Ensayo UMNG)	analiza casos como la Operación Ballena Azul (robo de arsenal en Cantón Norte) y el atentado con carro bomba de 2006 en la Escuela Superior de Guerra. Concluye que la falta de controles de acceso y protocolos de seguridad permitió estos hechos, comprometiendo la reputación del Ejército . Recomienda implementar una gestión de riesgos integral para mitigar vulnerabilidades.	Repositorio UMNG
Guanotoa Maldonado, A. (2012)	*Herramientas para evitar la infiltración y penetración en el Ejército Nacional de Colombia* (Ensayo USB Cali/UMNG)	Estudio de caso sobre infiltraciones en el Ejército. Revisa técnicas de "penetración" e "infiltración" empleadas por grupos ilegales para introducir *"topos"* en instituciones militares.	Repositorio UMNG

Ortiz Chávez, E.M. (2014)	*Sistemas de control de acceso para unidades militares* (Monografía UMNG)	Evalúa los sistemas tecnológicos y procedimientos de control de acceso en guarniciones militares colombianas. Señala que las bases deben contar con controles vehiculares y peatonales robustos (biometría, tarjetas, barreras, detectores) para impedir ingreso de personas no autorizadas.	Repositorio UMNG
Bolívar Cardozo, L.N. (2019)	*Consideraciones para los sistemas de control de acceso a las instalaciones de cantones militares* (Trabajo de grado UMNG)	Analiza la efectividad de los elementos de seguridad física (personal, tecnología y protocolos) en cantones militares bajo la amenaza de grupos armados organizados. Identifica deficiencias en la implementación de medidas de acceso en varios cantones (p.ej., falta de detectores de metales, control débil de visitantes).	Repositorio UMNG
Redacción Semana (2007)	*"La infiltrada"* – Revista Semana, ed. 1332	Reportaje investigativo sobre Marilú Ramírez Baquero, integrante de las FARC que logró infiltrarse en 2005 como civil invitada al Curso Integral de Defensa Nacional (CIDENAL) de la	Semana
El Tiempo (2015)	*"Capturado guerrillero que se infiltró en Escuela de Suboficiales"* – El Tiempo	Nota periodística sobre un miembro del ELN de 23 años que se hizo pasar por alumno en la Escuela de Suboficiales del Ejército (Tolemaida) durante un año Las autoridades reforzaron las verificaciones de identidad y antecedentes tras este incidente.	El Tiempo
Reuters/Acosta, L.J. (2021)	*"Explosión de coche bomba en batallón... deja 36 heridos"* – Reuters (15/06/2021)	Crónica del atentado con carro bomba contra la Brigada 30 del Ejército en Cúcuta (Junio 2021), que dejó 36 heridos.	*[Fotografía del atentado en Brigada 30]*
El Espectador (2024)	*"Posible infiltración de disidencias en base militar de Putumayo"* – El Espectador	Cobertura de un incidente interno: un soldado regular asesinó a tres compañeros en la base de La Tagua, Putumayo (febrero de 2024). Se investiga si el soldado fue contactado o inducido por disidencias de las FARC para sabotear desde adentro. El Ejército confirmó la posible infiltración a nivel de recluta y reportó los hechos a la justicia.	El Espectador

Nota. Fuente: Elaboración propia

Los trabajos académicos citados corresponden a ensayos o tesis de especialización/maestría de oficiales y expertos en seguridad. Estos documentos, aunque no siempre publicados en revistas indexadas, aportan análisis de casos colombianos reales y recomendaciones prácticas. Además de las fuentes listadas, informes gubernamentales (p. ej. comunicados del Ministerio de Defensa) y documentos de organismos internacionales sobre terrorismo en Colombia complementan la comprensión de estos incidentes, aunque generalmente no profundizan en detalles tácticos por seguridad nacional.

Identificación de Vulnerabilidades y Riesgos en los Procedimientos de Ingreso y Salida de las Unidades Militares

La gestión de riesgos constituye la base para mejorar la seguridad castrense. Según la doctrina de administración de riesgos, cuantificar y cualificar vulnerabilidades y amenazas es esencial para su adecuada identificación, análisis y tratamiento. En el contexto militar colombiano, se entiende que la función de protección busca preservar la integridad de los elementos de la fuerza (información, personas, material, instalaciones) mediante procedimientos de seguridad que analicen constantemente amenazas, riesgos y vulnerabilidades. Así, es imprescindible evaluar los protocolos de control de acceso actuales para detectar brechas de seguridad.

En la práctica, muchos cantones militares presentan carencias tecnológicas y procedimentales que facilitan la introducción de riesgos. Por ejemplo, se ha reportado que en las entradas vehiculares de varios cantones no se dispone de detectores de metales u otros equipos avanzados de inspección, limitando el tamizaje eficiente de vehículos ajenos. Del

mismo modo, la inspección de visitantes suele ser poco exhaustiva: habitualmente se solicita la apertura de maleteros y la visualización de pertenencias, pero solo se revisa físicamente a las personas cuando existe personal femenino disponible, lo cual crea disparidad en el nivel de control según turno.

Por lo tanto, otra fuente de vulnerabilidad es la inconsistencia entre unidades y la obsolescencia de los protocolos. Pocas unidades han integrado plataformas digitales comunes para registro de ingresos, lo que dificulta la trazabilidad interinstitucional. Asimismo, una carga de trabajo excesiva o rutinas repetitivas puede llevar al personal de guardia a omitir pasos de control. En suma, las debilidades identificadas incluyen: ausencia de tecnologías de detección eficientes, procedimientos de inspección voluntarios o parciales, falta de registros de acceso compartidos y entrenamiento deficiente del personal de seguridad. Estas fallas procedimentales amplían la exposición al riesgo en las unidades militares.

Tabla 1. Ejemplos de vulnerabilidades en los accesos a unidades militares.

Vulnerabilidad o Riesgo	**Descripción**
Documentación fraudulenta	Personas no autorizadas acceden con cédulas o pases falsos.
Inspección física incompleta	Falta de detectores de metales/escaners en entradas vehiculares.
Personal interno sin registro exhaustivo	Miembros orgánicos ingresan mostrando solo su ficha de unidad.
Protocolos inconsistentes	Diferencias entre unidades permiten brechas de seguridad (falta de norma única).
Capacitación insuficiente	Mal entrenados son más propensos a ser engañados o pasar por alto medidas de seguridad.

Nota. Fuente: Elaboración propia

Uno de los principales riesgos identificados en los procedimientos de ingreso a unidades militares es el uso de documentación fraudulenta. Individuos no autorizados han logrado burlar los controles mediante la presentación de cédulas falsificadas, pases adulterados o credenciales robadas. Esta vulnerabilidad es especialmente grave cuando los

dispositivos de verificación son manuales o no están interconectados con bases de datos en tiempo real, lo cual impide detectar irregularidades de forma inmediata.

Asimismo, se observa una inspección física incompleta, particularmente en los accesos vehiculares. En varias instalaciones militares no se cuenta con detectores de metales, arcos de seguridad o escáneres para revisar el contenido de los automóviles, motos o camiones que ingresan. Esta omisión técnica reduce la eficacia del control de amenazas materiales como explosivos, armas ocultas o sustancias ilícitas. En muchos casos, la revisión se limita a una inspección visual externa, lo cual deja espacios para el ingreso de elementos peligrosos que comprometen la seguridad de la base.

Otra debilidad es el ingreso de personal interno sin un registro exhaustivo. Mientras que los visitantes civiles deben someterse a múltiples filtros de seguridad, el personal militar orgánico a menudo solo presenta su ficha de la unidad o carné de identificación sin pasar por inspección detallada ni escaneo de sus pertenencias. Esta asimetría en el control genera una zona de confort para la posible comisión de actos indebidos desde el interior, ya sea por descuido, corrupción o infiltración de actores hostiles haciéndose pasar por militares activos.

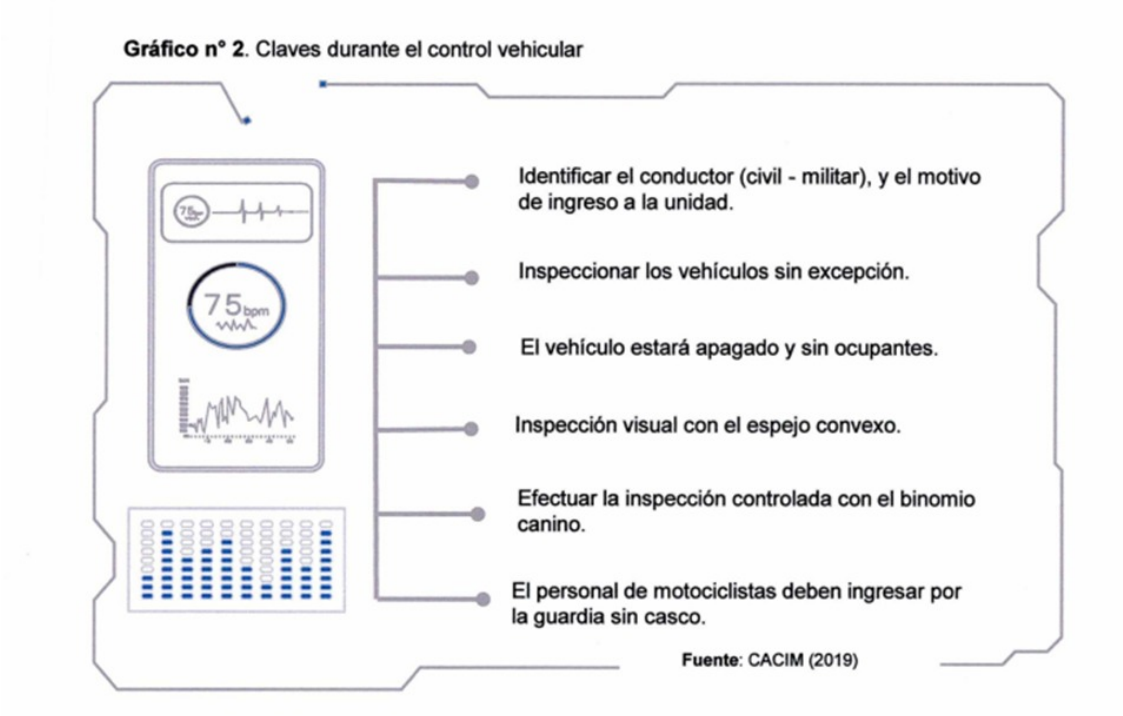
Además, La falta de una directiva única y estandarizada provoca que el nivel de exigencia varíe de un lugar a otro, debilitando la capacidad de respuesta coordinada y permitiendo que individuos malintencionados detecten y aprovechen los puntos más vulnerables del sistema. Finalmente, una capacitación insuficiente del personal encargado de la vigilancia y control de acceso se presenta como un factor crítico. La rotación constante del personal de guardia y la ausencia de entrenamiento especializado en detección de comportamientos sospechosos, manejo de tecnologías de inspección y protocolos de respuesta rápida, contribuyen a errores humanos y decisiones erradas.

Procesos Actuales de Control de Acceso

El control de acceso en las unidades militares es un aspecto fundamental para garantizar la seguridad del personal, los recursos estratégicos y la infraestructura. Actualmente, se han implementado diversos protocolos y tecnologías que permiten una verificación exhaustiva de personas, vehículos y bienes que ingresan a las instalaciones. Estas medidas buscan minimizar riesgos de infiltración, contrabando o amenazas a la seguridad nacional.

Por lo tanto, uno de los procedimientos esenciales es la inspección y verificación del ingreso vehicular, donde se llevan a cabo controles estrictos. En este proceso, se identifica al conductor, verificando si es personal militar o civil y determinando el motivo de su ingreso. Además, todos los vehículos son inspeccionados sin excepción para evitar el ingreso de elementos prohibidos. Como parte de la inspección, el vehículo debe estar apagado y sin ocupantes, permitiendo una revisión más detallada. Se utilizan espejos convexos para la inspección visual de la parte inferior del vehículo, mientras que binomios caninos entrenados detectan posibles amenazas como explosivos o sustancias ilícitas. En el caso de motociclistas, se les exige ingresar sin casco para facilitar su identificación facial. Estas medidas fortalecen la seguridad perimetral y reducen los riesgos de incidentes dentro de las unidades militares.

Figura 1. *Elementos claves del control Vehicular*



Nota. Fuente: (Comando de Educación y Doctrina, 2022a)

Paralelamente, se ha implementado un sistema de identificación del personal y control de credenciales, el cual permite una verificación más rápida y segura de los individuos que acceden a las instalaciones. Para ello, se utilizan tarjetas de identificación militar con un código QR integrado. Estas tarjetas incluyen datos personales como nombre, cédula, grado y unidad de servicio del militar, además de información sobre acceso vehicular, como el número de placa y el parqueadero asignado. El código QR permite un escaneo instantáneo para verificar la autenticidad del documento y su vigencia, reduciendo el riesgo de falsificaciones o suplantaciones. Asimismo, la firma de autorización de un oficial de seguridad certifica la validez del acceso del portador.

Figura 2. *Elementos clave de la tarjeta*

Nota. Fuente: (Comando de Educación y Doctrina, 2022a)

En conjunto, estos procedimientos representan un modelo de seguridad integral que combina factores humanos, tecnológicos y normativos para fortalecer la protección de las unidades militares. No obstante, la continua modernización de estos procesos con herramientas como la biometría avanzada, inteligencia artificial y bases de datos

interconectadas podría optimizar aún más la eficacia del control de acceso y reforzar la seguridad en los entornos militares(Comando de Educación y Doctrina, 2022a).

Principales amenazas y riesgos en la seguridad de las unidades militares

Las unidades militares colombianas enfrentan un amplio espectro de amenazas externas e internas. Históricamente, las guerrillas y grupos paramilitares han atacado instalaciones castrenses para debilitar al enemigo (por ejemplo, el robo de armas realizado por el M-19 en 1978 o el atentado con carro bomba de las FARC contra la Escuela Superior de Guerra en 2006) En la actualidad, aunque el conflicto armado ha evolucionado, subsisten amenazas similares: disidencias de las FARC, el ELN y bandas criminales organizadas (BACRIM) siguen activos y con capacidad ofensiva contra las fuerzas militares. Estos grupos emplean tácticas terroristas (minas antipersona, ataques a bases) y contra sabotaje (infiltración de saboteadores) para generar víctimas y pánico(Suarez, 2024).

Por ejemplo, el ataque con carro bomba en la Escuela Superior de Guerra (19 oct. 2006) demostró que las FARC aún podían vulnerar las instalaciones de mayor seguridad: *"*23 heridos, 6 vehículos destruidos develaron la falta de medidas antiterroristas efectivas en ese momento(Sánchez et al., 2007). Del mismo modo, la infiltración de insurgentes ha sido un riesgo crítico. Informes de inteligencia revelan que las FARC llegaron a infiltrar a un técnico aeronáutico en la Fuerza Aérea para robar datos de pilotos en la base de Apiay (2010) . Asimismo, en 2010 se conoció que seis oficiales y varios civiles habían sido detenidos como presuntos infiltrados de las FARC en las Fuerzas Militares, evidenciando la amenaza interna que representan agentes dobles o informantes. Más recientemente, casos como el de Putumayo (febrero 2024) muestran la persistencia del problema: un recluta asesinó a tres

compañeros, y se investiga si él y otros soldados fueron captados por las disidencias de las FARC (estructura Carolina Ramírez) para perpetrar el ataque.

Otra dimensión de riesgo son las brechas informativas y la corrupción interna. Grupos armados ilegales buscan filtraciones de inteligencia militar. En 2025 se descubrió que al menos seis soldados del Ejército en Arauca estaban implicados en la entrega de información operativa al ELN y a las disidencias de las FARC, e incluso sustrajo armamento oficial.

Por último, en el nuevo entorno se suman amenazas cibernéticas y transnacionales. Estudios recientes alertan que entre 2019 y 2020 el Ejército Nacional fue blanco de ciberataques dirigidos a sus sistemas de información, poniendo en riesgo datos estratégicos y operaciones(Mozo & Ardila, 2022). Esto obliga a integrar contramedidas de ciberdefensa (encriptación, monitoreo) dentro del esquema general de seguridad. En síntesis, las principales amenazas a la seguridad de las unidades militares incluyen las acciones de grupos armados ilegales (guerrilla, narcotraficantes y bandas criminales), el terrorismo selectivo, el espionaje/infiltración interna y los ataques informáticos.

Brechas de Seguridad en la Operatividad Militar

Las brechas de seguridad operativa surgen cuando los protocolos establecidos no se aplican integralmente o el personal carece de conciencia preventiva. Una brecha común es la fuga de información operativa, ya sea por descuidos tecnológicos o por infiltración deliberada. Como señala la experiencia, muchos ataques a bases se facilitan porque "en la mayoría de los casos ha logrado llevarse a cabo por la fuga de información que suministran personal infiltrado o penetrado".Esto incluye entregas de planes de despliegue, mapas de fortificaciones o códigos de comunicación. Asimismo, la falta de un "sistema integrado de

seguridad" es una brecha crítica: al no centralizar ni actualizar los registros y protocolos de protección, cada unidad queda más expuesta.(Velásquez & Torres, 2023)

De la misma manera, existe una brecha cultural: la distracción o normalización del riesgo, personal sobrecargado puede omitir revisiones, y la disciplina de contrainformación (rotación de cargas, manejo de datos confidenciales) a veces se descuida en el día a día. La insuficiente capacitación en detección de engaños (ingeniería social, manipulaciones) amplía esta brecha. En el caso de emergencias (autores múltiples, ataques simultáneos), la coordinación interdependencias es escasa, lo cual limita la respuesta defensiva.

Finalmente, la seguridad física de la infraestructura a menudo adolece de rutinas claras. Por ejemplo, estudios técnicos muestran que algunas instalaciones poseen cámaras de vigilancia o barreras, pero carecen de sensores modernos o sistemas de alerta temprana. En la práctica, la falta de un registro único de ingreso para personal militar y civil de apoyo significa que no se puede rastrear eficazmente quién entra o sale en cada turno. Todo ello crea una brecha operativa que los adversarios pueden explotar: desde robo de armamento en depósitos (caso del M-19 de 1978, debido a seguridad deficiente) hasta ataques sorpresa basados en inteligencia privilegiada.

Elementos Claves para un Sistema de Seguridad Física Efectivo en Instalaciones Militares

El desarrollo del presente capítulo se estructuró a partir de una estrategia de análisis categorial, sustentada en una revisión sistemática de literatura y documentos técnicos. Se identificaron cuatro dimensiones fundamentales (normativa, tecnológica, humana y procedimental), que funcionaron como ejes de análisis transversal. Estas categorías se seleccionaron con base en los principios de seguridad física y en los marcos doctrinales de protección militar (EJC 3-37 y 3-63). Cada sección fue construida desde la identificación de brechas, riesgos y vulnerabilidades, y se complementó con casos reales y análisis comparativo. Esta lógica metodológica permitió un abordaje integral de los factores que inciden en el control de ingreso a instalaciones militares.

Un sistema de seguridad física de alta confiabilidad combina múltiples capas de protección. En términos arquitectónicos, esto implica barreras físicas y disuasorias (cerco perimetral, muros, iluminación, torniquetes, cerraduras reforzadas) que retardad posibles intrusiones. A nivel operacional, es clave contar con personal capacitado y procedimientos claros (guardias, revisiones periódicas, monitoreo continuo) que regulen el ingreso de personas y vehículos.

Tabla 3. *Elementos claves para un sistema de seguridad física*

Categoría	Elementos principales
Elementos arquitectónicos	Vallas, muros, portones, iluminación anti-intrusión, señalización de acceso permitido
Elementos operacionales	Personal de seguridad (guardias, patrullas), capacitación continua, protocolos de revisión de credenciales
Elementos tecnológicos	Tarjetas inteligentes y lectores, torniquetes y molinetes, cámaras de CCTV, sistemas de alarma conectados a un centro de control

Nota. Fuente: Elaboración propia

Estos componentes deben organizarse en una defensa en profundidad, con medidas detectivas (cámaras, guardias identifican accesos no autorizados), preventivas (vigilancia, cercas que disuaden) y correctivas (planes de respuesta ante intrusión). Cabe recordar que la seguridad física reduce, pero no elimina totalmente el riesgo: su eficacia radica en la combinación de factores humanos, tecnológicos y procedimentales para cumplir objetivos de disuadir, demorar, detectar, activar respuesta y denegar accesos ilegítimos. No basta con la tecnología avanzada si los recursos (humanos y económicos) no se planean según el nivel de riesgo de cada zona; por ello, es fundamental asignar recursos adecuados y actualizar permanentemente el sistema para proteger los activos críticos(Bolívar, 2019).

Factores Humanos en la Seguridad de Acceso

El elemento humano es crítico en el control de accesos. Los guardias y operadores son la primera línea de defensa ante acciones delictivas o errores. Por ello, se debe enfatizar la formación, disciplina y profesionalismo del personal. En instalaciones de alta seguridad, se exigen niveles muy elevados de competencias: los operadores deben actuar con excelencia, proactividad y atención al detalle(López et al., 2023). Un buen vigilante debe ser proactivo, estar *antes* de que sucedan los acontecimientos, identificar herramientas y actuar contra posibles amenazas basadas en el análisis de riesgos.

Uno de los factores humanos más determinantes en la seguridad de acceso a instalaciones militares es el adiestramiento constante del personal encargado del control de ingreso. Este entrenamiento debe incluir el dominio de los protocolos actualizados, la familiarización con tecnologías de identificación como sistemas biométricos o tarjetas

inteligentes, y la capacidad de respuesta ante situaciones imprevistas. La realización periódica de simulacros de intrusión y análisis de casos reales contribuye significativamente a fortalecer la toma de decisiones en contextos de presión, mejorando así la capacidad de reacción frente a posibles intentos de infiltración o sabotaje(Machay & Llano, 2024).

La disciplina y la actitud del personal de seguridad también son aspectos críticos. Se requiere un desempeño riguroso y sistemático que incluya la revisión minuciosa de documentos, el cumplimiento de rondas programadas y el respeto por los tiempos de control. En este sentido, la calidad humana del vigilante, entendida como la combinación entre autoestima, sentido de pertenencia y claridad de los objetivos institucionales, es clave para consolidar una cultura de seguridad sólida y profesional(Elías, 2021).

Otro aspecto esencial es la adecuada gestión del error y de la rotación del personal. La fatiga, la rutina o el estrés acumulado pueden derivar en omisiones críticas, como permitir el ingreso de personas sin la debida verificación de credenciales. Por tal motivo, se recomienda implementar políticas de rotación de turnos, supervisar los descansos y actualizar los procedimientos de forma regular, con el fin de minimizar los riesgos asociados al agotamiento laboral y la complacencia operativa.

Finalmente, es importante tener en cuenta que las amenazas no siempre provienen del exterior. En muchas ocasiones, los riesgos más difíciles de detectar tienen origen interno. Empleados civiles, subcontratistas o incluso personal militar con acceso regular a las instalaciones pueden convertirse en agentes infiltrados o colaboradores de grupos externos. Esta amenaza interna exige la aplicación de medidas complementarias como la verificación múltiple de identidades, el fortalecimiento de sistemas de contrainteligencia, la activación de

mecanismos de denuncia anónima y la adecuada separación de funciones entre quienes custodian y quienes operan dentro del recinto militar .

Tecnologías Aplicadas al Control de Ingreso

Las tecnologías de control de acceso han experimentado una notable evolución en las últimas décadas, incorporando sistemas electrónicos y biométricos de alta seguridad que permiten optimizar la protección de instalaciones estratégicas como las unidades militares. Entre las tecnologías más comunes se encuentran las tarjetas electrónicas y los códigos numéricos, que fueron de los primeros sistemas implementados. Estos operan mediante el uso de tarjetas con chip RFID o la introducción de códigos PIN a través de teclados o lectores magnéticos. Al validar la credencial, se activan mecanismos de acceso como molinetes o puertas eléctricas. Sin embargo, aunque siguen siendo ampliamente utilizadas, presentan vulnerabilidades como la pérdida de tarjetas o la posible duplicación de los códigos de acceso(San José et al., 2012).

A partir de estas limitaciones, ha ganado protagonismo la biometría fisiológica, que permite el reconocimiento de rasgos únicos del cuerpo humano, tales como huellas dactilares, patrones faciales, escaneo de iris o retina, e incluso la verificación de venas de la mano. Este tipo de tecnología ofrece una mayor precisión, ya que se basa en características anatómicas irrepetibles. Por ejemplo, las huellas dactilares contienen en promedio alrededor de 30 minucias, lo que hace prácticamente imposible que dos personas compartan las mismas, incluso si se trata de gemelos(Sánches, 2020).

Complementariamente, la biometría multimodal incrementa los niveles de seguridad mediante la combinación de múltiples métodos biométricos en un solo proceso de autenticación(Visitación et al., 2023). Por ejemplo, un sistema puede requerir

simultáneamente el escaneo del iris y la verificación de la huella dactilar. Esto reduce significativamente la probabilidad de suplantación, ya que obliga a coincidir en dos (o más) puntos de identificación distintos (Maureira & González, 2023).

En cuanto a la vigilancia inteligente, las cámaras de seguridad modernas han integrado inteligencia artificial para realizar análisis de video en tiempo real. Estos sistemas no solo graban, sino que detectan comportamientos anómalos como la presencia de objetos abandonados, intrusiones fuera del horario permitido o movimientos sospechosos(Alejandra, 2016). Al identificar estos eventos, emiten alertas automáticas al centro de control, permitiendo una reacción inmediata. Este tipo de videovigilancia se considera "proactiva" porque no depende exclusivamente del operador humano, y puede gestionarse en escalas masivas mediante sistemas distribuidos(Guido Nobili, 2021).

Otras tecnologías complementarias en los accesos militares incluyen sensores de presencia, barreras físicas automatizadas como torna barras y bolardos retráctiles, lectores de matrículas (ANPR) para vehículos, detectores de metales, arcos de seguridad y sistemas de identificación por radiofrecuencia (RFID/UHF). Además, se está comenzando a utilizar drones de patrullaje y soluciones basadas en el Internet de las Cosas (IoT) para el monitoreo remoto e inteligente de perímetros (Barrera & Martin, 2023).

Procedimientos Normativos y Regulatorios

Los procedimientos normativos y doctrinales que regulan el control de acceso a unidades militares están fundamentados en un marco técnico-operativo derivado de la Función de Conducción de la Guerra – Protección (FOG Protección), tal como lo establece el Manual de Referencia del Ejército EJC 3-37. Esta doctrina establece los cinco principios que deben regir toda estrategia de protección: absoluta, integrada, multinivel, repetitiva y perdurable, lo que

implica que todo esquema de seguridad debe ser planificado, ejecutado y evaluado de manera sistemática, constante y adaptada al entorno operacional.

Dentro del componente normativo interno, el Manual EJC 3-231 regula los procedimientos de seguridad militar, enfatizando en la implementación de protocolos de inspección física y documental, el uso de tecnologías de identificación, la verificación cruzada con dependencias receptoras, y el registro obligatorio de visitantes, vehículos y proveedores.

Por su parte, el Manual EJC 3-63 sobre Sistemas de Seguridad para Puestos de Mando y Bases Fijas detalla los componentes físicos, tecnológicos y humanos requeridos para garantizar un entorno controlado, incluyendo barreras físicas, sistemas CCTV, controles biométricos y medidas antiterroristas. Complementariamente, la Guía de funciones y protocolos de seguridad para la guardia (2019) elaborada por el CACIM ha sido adoptada como instrumento de referencia para estandarizar prácticas operativas y fortalecer el desempeño del personal de seguridad en unidades tácticas.

Desde el punto de vista funcional, la doctrina también establece que todo acceso debe ser controlado y monitoreado, en atención a las amenazas persistentes que enfrentan las Fuerzas Militares, como infiltraciones, ataques con artefactos explosivos improvisados (AEI) o sabotajes. En efecto, la doctrina insiste en que un esquema de seguridad eficaz depende tanto de la planificación basada en inteligencia como de la correcta aplicación de medidas de mitigación de riesgos, incluyendo el empleo de medidas activas y pasivas de protección.

Estas disposiciones se alinean con estándares internacionales de seguridad como la ISO 28000 (gestión de la seguridad en la cadena de suministro) y la ISO 18788 (gestión de

operaciones de seguridad privada), que han sido adoptados por algunas dependencias logísticas del sector defensa en Colombia. Además, la normatividad nacional complementaria como la Ley 1621 de 2013 (Inteligencia y Contrainteligencia) y el Código Nacional de Seguridad y Convivencia (Ley 1801 de 2016), refuerzan el marco de legalidad en el control de accesos, especialmente en lo que respecta al tratamiento de información clasificada y la restricción del ingreso a zonas de interés estratégico. A continuación, se presenta una tabla comparativa que sintetiza las principales fortalezas y debilidades identificadas en las dimensiones normativa, tecnológica y humana, junto con recomendaciones estratégicas formuladas con base en la doctrina institucional (EJC 3-37, CACIM), teorías de seguridad (Buzan, 1991) y literatura especializada (Bolívar, 2019).

Tabla 4. *Cuadro comparativo*

Categoría	Fortalezas identificadas	Debilidades identificadas	Recomendaciones estratégicas (basadas en teoría)
Normativa	Existencia de manuales doctrinales (EJC 3-231, EJC 3-63), Guía CACIM.	Ausencia de protocolo nacional unificado; dispersión y desactualización frente a amenazas emergentes.	Aplicar el principio de "protección integrada y perdurable" (EJC 3-37); unificar doctrina vía directiva nacional.
Tecnología	Uso incipiente de biometría, CCTV, lectores QR, ANPR en algunas unidades.	Sistemas no interoperables; ausencia de bases de datos en tiempo real; desigualdad tecnológica entre guarniciones.	Aplicar el enfoque de **defensa en profundidad** (Bolívar, 2019); conectar tecnologías al Centro de Inteligencia Militar.
Factores humanos	Personal con experiencia táctica en zonas de riesgo; protocolos básicos establecidos.	Alta rotación, falta de capacitación en tecnologías, perfilación y detección de amenazas internas.	Implementar el enfoque de "seguridad humana integral" (Buzan, 1991); crear escuela de formación permanente y certificación.

Nota: Fuente: Elaboración propia con base en Bolívar (2019), Buzan (1991), Manual EJC 3-37 y Guía CACIM (2019).

Al cierte de este capítulo se logra evidenciar que existe dispersión en los protocolos doctrinales de ingreso. Aunque el Manual EJC 3-231 y la Guía CACIM (2019) proporcionan lineamientos, no hay una directiva nacional que unifique criterios mínimos de seguridad física. Las normas están desactualizadas frente a las amenazas actuales (p. ej., uso de drones, suplantación con biometría falsa). Se evidencian grandes asimetrías entre unidades militares. Algunas implementan biometría y CCTV, mientras otras aún operan con registros manuales. La falta de interoperabilidad de sistemas y la ausencia de bases de datos en tiempo real aumentan los riesgos de suplantación e ingreso no autorizado. Se detectó debilidad en la capacitación del personal de guardia, alta rotación y poca especialización en técnicas de perfilación de amenazas internas. Los insider threats y el agotamiento operativo son factores que afectan la efectividad de los controles. Hay protocolos fragmentados, inspecciones no estandarizadas y procedimientos reactivos, no preventivos. Falta trazabilidad en los ingresos y registros cruzados con inteligencia militar.

Estrategias de Mejora para la Implementación de un Protocolo de Ingreso Estandarizado

El Protocolo Operativo Estandarizado (POE) se presenta con estructura de procedimiento institucional, siguiendo las directrices de manuales doctrinales como EJC 3-231 y Guía CACIM (2019). Este documento incluye: (a) objetivo general y específicos del control de ingreso; (b) alcance en términos de instalaciones, personal y recursos cubiertos; (c) identificación de responsables primarios y secundarios; (d) descripción secuencial de actividades para cada flujo de acceso (peatonal, vehicular y de carga), representadas en diagramas de flujo; (e) listas de chequeo operativas con campos para registro de fecha, hora,

firma del responsable y observaciones; y (f) anexos técnicos con fichas de equipos recomendados, indicadores de desempeño y formatos de reporte de incidentes.

Cada fase y componente del POE se fundamenta en disposiciones doctrinales y normativas nacionales e internacionales. La fase de disuasión y control perimetral se alinea con el principio de "protección integrada" del Manual EJC 3-37 (Ejército Nacional, 2017). La verificación de identidad mediante biometría y credenciales QR/RFID responde a las recomendaciones de la ISO 28000:2022 sobre gestión de la seguridad en la cadena de suministro. El procedimiento de inspección física y documental sigue las directrices del Manual EJC 3-231 y la Guía CACIM (2019) para la guardia. La integración tecnológica e interoperabilidad con bases de datos en tiempo real se fundamenta en la ISO 18788 sobre gestión de operaciones de seguridad.

David A. Baldwin distingue entre seguridad como bajo nivel de daño a valores adquiridos y la necesidad de especificar "qué seguridad, para quién, frente a qué amenazas(Sakiko & Carol, 2012). Este enfoque teórico permite diseñar un protocolo que defina claramente quiénes acceden (militares, proveedores, civiles), qué valores se protegen (personas, información, infraestructura), y en qué condiciones (zonas de alta amenaza). Por otro lado, la seguridad multidimensional de Barry Buzan sugiere considerar ámbitos político, militar, tecnológico y humano en el modelo, evitando una visión reduccionista centrada solo en lo físico.

Tabla 5. *Correspondencia del POE con normas y guías vigentes*

Elemento del POE	Norma/Guía aplicable	Coincidencia con el modelo	Mejora propuesta
Disuasión y control perimetral	EJC 3-37 – Principios de protección	Uso de barreras físicas y señalización	Añade iluminación inteligente y sensores perimetrales IoT
Verificación de identidad	ISO 28000 / EJC 3-231	Validación documental y física	Integra biometría multimodal + QR/RFID conectados a inteligencia
Inspección de carga y vehículos	Guía CACIM (2019)	Registro e inspección física	Suma caninos EDS y ANPR para trazabilidad vehicular
Interoperabilidad tecnológica	ISO 18788	Gestión coordinada de operaciones	Plataforma centralizada con monitoreo en tiempo real
Capacitación de personal	EJC 3-231 / Buzan (1991)	Entrenamiento básico de guardia	Escuela de certificación y simulacros trimestrales

Nota. Fuente: Elaboración propia con base en Ejército Nacional (2017, 2019), Guía CACIM (2019), ISO 28000:2022, ISO 18788:2015, y Buzan (1991).

Los manuales EJC 3-37 y 3-63 establecen principios como la protección "absoluta, integrada, multinivel, repetitiva y perdurable". Una directiva nacional que reitere estos principios para el control de ingreso permitiría homogeneizar procesos entre unidades, garantizando un mismo nivel de exigencia en infraestructura, personal, tecnología y registros. Se deben estandarizar en todas las unidades los mecanismos de inspección: detectores de metal, arcos vehiculares, cámaras CCTV con análisis de video basado en inteligencia artificial, binomios caninos, escáneres de QR y validación biométrica. Integrar roles y credenciales mediante un sistema central nacional y mecanismos interoperables permitirá detectar credenciales duplicadas o fraudulentas en tiempo real, garantizando trazabilidad integrada(Ejército Nacional, 2019).

La propuesta se encuentra alineada con la doctrina vigente del Ejército Nacional (EJC 3-37, EJC 3-231) y con estándares internacionales de seguridad (ISO 28000, ISO 18788), lo que facilita su eventual adopción como directiva nacional. Su implementación, validada preliminarmente contra estos marcos, permitiría homogeneizar criterios, reducir brechas

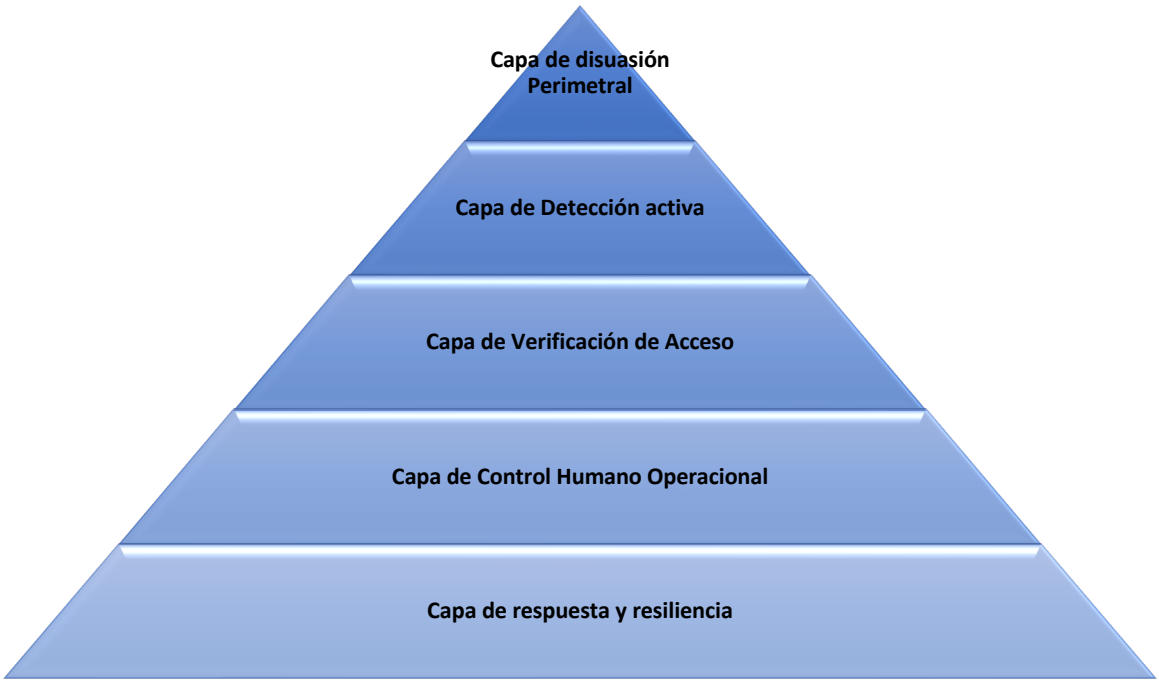
tecnológicas y cumplir con exigencias de interoperabilidad y trazabilidad definidas en auditorías institucionales.

Modelo integral de seguridad en el control de ingreso

El modelo integral de seguridad en el control de ingreso está inspirado en el principio de defensa en profundidad, una estrategia militar que busca construir múltiples líneas de protección consecutivas para debilitar y retrasar cualquier intento de intrusión(Bolívar, 2019). En el contexto de la Brigada 13 y otras unidades del Ejército Nacional, este enfoque permite distribuir los controles desde el perímetro hasta el interior de las instalaciones, integrando funciones físicas, tecnológicas y humanas para lograr una protección coherente y escalable(Comando de Educación y Doctrina, 2022b).

La primera capa de defensa incluye elementos arquitectónicos y de disuasión como cercas perimetrales, iluminación de alta eficiencia y señalización restrictiva. Estos generan una barrera pasiva que, en unidades como la Brigada 13, reduce los intentos oportunistas de acceso ilícito, al mismo tiempo que alerta al personal y a los sistemas de vigilancia ante movimientos sospechosos.

Figura 3. Modelo Piramidal de Seguridad en el Control de Ingreso



Nota. Fuente: Elaboración Propia

La segunda capa corresponde a la detección activa. Aquí se implementan sensores de movimiento, arcos y detectores de metales, binomios caninos y videovigilancia con analítica de video. En Brigada 13, la integración de CCTV y sensores ha permitido identificar anomalías de manera más efectiva, tanto de día como de noche, y activar de inmediato alertas al puesto de control(Barhate et al., 2024). La selección de tecnología responde a una seguridad basada en riesgos, priorizando los equipos más eficaces frente a amenazas confirmadas por inteligencia institucional.

La tercera capa es la verificación de acceso. Se combinan lectores biométricos (huella o iris), escaneo de credenciales con QR o RFID, y validación cruzada con bases de datos conectadas al Centro Conjunto de Inteligencia Militar(San José et al., 2012). La Brigada 13 ha servido de piloto para este sistema, permitiendo detectar intentos de suplantación o uso de

credenciales falsificadas, garantizando que solo el personal autorizado ingrese tras sobrepasar los controles previos.

La cuarta capa es el control humano en línea, compuesto por guardias entrenados en perfilación conductual, revisión manual de equipaje y procedimientos de respuesta rápida. Estos actuantes reciben capacitación específica para manejar situaciones que involucran amenazas híbridas (drones, AEI, ataques selectivos), y participan en simulacros periódicos junto con la Brigada 13 para mantener la efectividad operativa(Prieto, 2023).

Ahora bien, la capa de respuesta y resiliencia consiste en medidas correctivas y de contingencia. Al detectar anomalías, se activa un plan de respuesta inmediata, que incluye bloqueos físicos, alerta a unidades de reacción y análisis forense del evento. Esta capa también alimenta un ciclo de retroalimentación que permite corregir fallas, actualizar protocolos y ajustar el modelo según nuevos patrones de amenaza(Ejército Nacional, 2019).

Este diseño multinivel encuentra fundamento en doctrinas militares como el Manual EJC 3-37 y en principios de gestión de seguridad estatal que proponen niveles diferenciados de salvaguarda, redundancia tecnológica y control humano convergente. La aplicación práctica en la Brigada 13 demuestra que un esquema integral de defensa disminuye significativamente las probabilidades de éxito de ataques a veces imprevistos o complejos, al maximizar las capas de protección y asegurar que, si una capa es vulnerada, otras continúan funcionando eficazmente(Ejército Nacional, 2017).

Integración de Tecnologías de Seguridad en el Control de Acceso

En instalaciones militares de alta seguridad, la biometría multimodal combina múltiples rasgos (huella digital, reconocimiento facial, iris, voz), incrementando la precisión y

reduciendo el riesgo de suplantación(Moreno, 2008). Empresas como Thales y HID Global han demostrado la eficacia de sistemas biométricos certificados que permiten autenticar identidades en tiempo real en bases militares, reforzando la verificación al cruzar múltiples datos. Este enfoque se ajusta perfectamente al control de ingreso en unidades del Ejército Colombiano, donde la autenticación dual por biometría y credencial digital minimiza la falsificación.

La videovigilancia IP con analítica impulsada por IA se ha convertido en un pilar tecnológico en defensa. Este tipo de sistema permite detectar comportamientos anómalos presencia fuera de horario, situaciones de aglomeración, vehículos sospechosos y enviar alarmas automáticas al centro de control(Illanas & Madueño, 2024). Además, puede integrarse con reconocimiento de matrícula (ANPR) y facial, facilitando el seguimiento automatizado de individuos o vehículos con historial de alerta.

La interoperabilidad tecnológica, concepto esencial en doctrinas de comando y control, se sustenta en arquitecturas basadas en microservicios, redes 5G e IoT(Nagothu et al., 2018). Como complemento, los sensores perimetrales inteligentes, arcos detectores y binomios caninos electrónico-asistidos, permiten realizar una inspección física robusta y adaptativa. En combinación con biometría móvil de campo (escáneres portátiles conectados a bases de datos nacionales), esto garantiza control continuo, incluso en zonas remotas, sin pérdida de trazabilidad.

Finalmente, la adopción de estas tecnologías debe estar alineada con un marco de ciberdefensa y transformación digital. Como propone el estudio "Usos militares de la IA y la automatización", la inteligencia artificial puede servir tanto para fortalecer vigilancia como para robustecer mecanismos de defensa ante amenazas cibernéticas, siempre bajo el control

humano(Centro Conjunto de Desarrollo de Conceptos, 2020). Un sistema digital seguro, interoperable y supervisado garantiza que el control de acceso sea ágil, preciso y resiliente frente a amenazas emergentes.

Plan de actualización y mejora continua en la seguridad de acceso

La seguridad en el control de ingreso a instalaciones militares no puede ser concebida como un sistema estático. Por el contrario, requiere de un proceso de mejora continua que garantice su capacidad de adaptación frente a amenazas dinámicas y cambiantes. Para tal fin, se propone un plan estratégico de actualización y mejora continua sustentado en el ciclo PHVA (Planificar–Hacer–Verificar–Actuar), ampliamente adoptado en gestión de calidad y seguridad, y aplicado exitosamente en entornos de defensa (Martín, 2021).

En la fase de planificación, se parte de un diagnóstico exhaustivo de las vulnerabilidades actuales en el sistema de acceso. Este diagnóstico debe contemplar auditorías internas, análisis de amenazas (ATA), y matrices de riesgo actualizadas trimestralmente. A partir de estos insumos, se formulan planes de intervención que incluyan la actualización de tecnología (por ejemplo, escáneres biométricos de nueva generación), fortalecimiento doctrinal y capacitación permanente del personal encargado del control. Las líneas de acción deben jerarquizarse según la criticidad de la unidad militar, el nivel de exposición al riesgo y los recursos disponibles(ISOTools, 2018).

La fase de ejecución (Hacer) contempla la implementación progresiva de las mejoras priorizadas. Esto incluye la actualización de protocolos operacionales conforme al Manual EJC 3-231 y la Guía de Funciones de Guardia (2019), la renovación de credenciales con tecnología RFID/QR, y la realización de ejercicios tácticos de control de ingreso con

simulacros de intrusión, vehículos bomba o ingreso de personal no autorizado. Las unidades deben establecer un cronograma institucional para incorporar estas prácticas, garantizando que los equipos humanos y tecnológicos operen en condiciones óptimas(Barrera & Martin, 2023).

Posteriormente, en la fase de verificación, se debe evaluar el grado de cumplimiento e impacto de las medidas aplicadas. Esta evaluación se materializa mediante inspecciones de seguridad no anunciadas, revisión de incidentes reportados, entrevistas al personal de guardia y análisis de indicadores clave de desempeño (KPIs), como el tiempo promedio de validación de ingreso, fallas técnicas en los sistemas o casos de ingreso indebido.

Finalmente, la fase de acción correctiva consiste en ajustar los procesos a partir de los resultados obtenidos. Esto implica reformular protocolos ineficaces, actualizar procedimientos operativos estandarizados (POE) y modificar procesos administrativos o disciplinarios si se detectan negligencias reiteradas. La retroalimentación obtenida debe ser sistematizada por la Dirección de Seguridad Militar o su equivalente y compartida con todas las unidades a través de boletines doctrinales, como los elaborados por el Centro de Doctrina del Ejército y la Dirección de Lecciones Aprendidas.

Experiencias exitosas en unidades como la Brigada 13 del Ejército Nacional han demostrado que los sistemas de control de ingreso mejoran sustancialmente cuando se combinan simulacros periódicos, mantenimiento preventivo, y actualización doctrinal con ciclos PHVA semestrales. Adicionalmente, países como España y Chile han implementado planes similares con apoyo de sus sistemas de inteligencia, destacando la importancia de la interoperabilidad entre sistemas tecnológicos y humanos, así como el almacenamiento digital centralizado de datos de ingreso y egreso.

Conclusiones

El presente articulo respondió a la pregunta de investigación orientada a identificar los factores normativos, tecnológicos y humanos que inciden en la vulnerabilidad de los sistemas de control de ingreso en instalaciones militares. A partir del enfoque cualitativo y el análisis documental sistemático, se concluye que la falta de un sistema unificado, actualizado y preventivo de seguridad física representa un riesgo persistente para la protección del personal, los activos y la infraestructura estratégica. La ausencia de un marco doctrinal robusto y transversal ha generado una aplicación desigual de medidas de seguridad, lo cual incrementa las probabilidades de ingreso no autorizado, especialmente en contextos de amenazas híbridas e internas.

En cuanto al primer objetivo, se evidenció que la normativa actual sobre seguridad física y control de acceso en instalaciones militares presenta dispersión y obsolescencia frente a las amenazas contemporáneas, como el uso de drones, la suplantación biométrica o las infiltraciones internas. Si bien existen documentos como el Manual EJC 3-231 o la Guía CACIM, no existe una directiva de cumplimiento obligatorio que estandarice procedimientos en todas las unidades. Esta carencia normativa favorece una interpretación fragmentada de los protocolos, lo que debilita la eficacia de los anillos de seguridad y la trazabilidad de los ingresos. Es imperativo que el Ejército Nacional consolide una doctrina única y adaptable, que integre estándares internacionales de seguridad física, pero también consideraciones contextuales del conflicto colombiano.

Respecto al segundo objetivo, el análisis reveló una marcada desigualdad tecnológica entre las unidades militares. Algunas cuentan con sistemas avanzados como control biométrico, ANPR, lectores QR y videovigilancia con inteligencia artificial; otras aún dependen de registros manuales y listas en papel. Esta asimetría tecnológica, sumada a la falta de interoperabilidad entre plataformas y la inexistencia de bases de datos centralizadas en tiempo real, compromete la capacidad de detectar suplantaciones o ingresos no autorizados. Se hace necesario establecer una red tecnológica nacional de control de ingreso, articulada al Centro de Inteligencia Militar, que permita monitoreo, trazabilidad y análisis predictivo de amenazas internas y externas en tiempo real.

En relación con el tercer objetivo, se identificaron debilidades estructurales en el componente humano de la seguridad física. La alta rotación del personal de guardia, la escasa capacitación en técnicas de perfilación y en tecnologías emergentes, así como la limitada especialización en análisis conductual, dificultan una respuesta efectiva ante amenazas internas. Los denominados *insider threats*, el agotamiento operativo y la falta de protocolos preventivos generan condiciones propicias para fallas en la detección de conductas sospechosas o vulneraciones de seguridad. Se requiere consolidar una escuela permanente de formación en seguridad física y control de ingreso, con enfoque en inteligencia humana, análisis del comportamiento y uso de tecnologías para detección de anomalías.

En síntesis, este trabajo aporta a la doctrina de protección militar al evidenciar que la seguridad física no puede concebirse como un conjunto de medidas reactivas o exclusivamente tecnológicas, sino como un sistema integral que exige articulación normativa, interoperabilidad tecnológica y especialización del recurso humano. Además, propone una visión preventiva, centrada en la anticipación del riesgo y la protección del

personal, más allá de los perímetros físicos. Estas conclusiones pueden ser insumo para la formulación de una política nacional de seguridad física para instalaciones militares, con estándares mínimos obligatorios, mecanismos de control interno y adaptación continua frente a amenazas dinámicas. El trabajo también abre camino para futuras investigaciones en temas como inteligencia artificial aplicada a seguridad perimetral, análisis de biometría conductual y perfilación de amenazas internas.

Referencias

Alejandra, M.-O. D. (2016). Re-identificación de personas a través de sus características soft-biométricas en un entorno multi-cámara de video-vigilancia. *Ingeniería, Investigación y Tecnología*, *17*(2). https://doi.org/10.1016/j.riit.2016.06.010

Barhate, M. M., Inamdar, C. S., Ingale, C. D., Inamdar, Y. S., Humne, S. S., Mahendrakumar, H. I., & Hulenwar, H. P. (2024). Drone Detection Through CCTV. *International Journal for Research in Applied Science and Engineering Technology*, *12*(1). https://doi.org/10.22214/ijraset.2024.57107

Barrera, G., & Martin, L. (2023). *Una aproximación a las Tecnologías RFID: Usos y Aplicaciones. Seguridad y defensa.* https://revistas.universu.com.co/index.php/rices/article/view/3

Bolívar, C. (2019). Consideraciones para los sistemas de control de acceso a las instalaciones de cantones militares [Trabajo de grado, Universidad Militar Nueva Granada]. *Universidad Militar Nueva Granada, Facultad de Relaciones Internacionales, Estrategia y Seguridad.*

Centro Conjunto de Desarrollo de Conceptos. (2020). *Usos militares de la inteligencia artificial, la automatización y la robótica (IAA&R)*. https://publicaciones.defensa.gob.es/media/downloadable/files/links/u/s/usos_militares_inteligencia_artificial.pdf

Comando de Educación y Doctrina. (2022a). *Centro de Doctrina del Ejército, Dirección de Lecciones Aprendidas. (2022, marzo). Seguridad de una unidad mediante el enfoque de la protección. Boletín de Lecciones Aprendidas. RESTRINGIDO.*

Comando de Educación y Doctrina. (2022b). Dirección de Lecciones Aprendidas, Seguridad de una unidad mediante el enfoque de la protección [Boletín de Lecciones Aprendidas, restringido]. Ejército Nacional de Colombia. *Centro de Doctrina Del Ejército*. https://www.ejercito.mil.co/enio/recurso_user/doc_contenido_pagina_web/800130633_4/616477/4._boletin_48_seguridad_de_una_unidad_mediante_el_enfoque_de_la_proteccion.pdf

Domínguez, Y. (2007). Análisis de información y las investigaciones cuantitativas y cualitativas. *Revista Cubana Salud Pública*, *33*(2).

Ejército Nacional. (2017). Manual de referencia del Ejército EJC 3-37 Protección,. *Bogota: Ejército Nacional.*

Ejército Naional. (2019). Guia de funciones y protocolos de seguridad para Ia guardia. *Bogota: Ejército Nacional* .

Elías, F. (2021). Modernización del sistema de control de acceso para las instalaciones militares de la guarnición de Lima [*. , Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"]. Repositorio Institucional EMCH.* https://repositorio.escuelamilitar.edu.pe/items/4f57fdbb-a632-47da-a82f-db0b9bee4dfe

Guido Nobili, G. (2021). Los sistemas de vídeovigilancia para prevenir la delincuencia. Lecciones aprendidas. *Constructos Criminológicos*, *1*(1). https://doi.org/10.29105/cc1.1-7

Illanas, G., & Madueño, Á. (2024). Fundamentos históricos de la biometría aplicada a la Defensa y sus planteamientos éticos. . *Debate Historiográfico, (63), Invierno.* https://historia-actual.org/Publicaciones/index.php/hao/article/view/2313

ISOTools. (2018). ¿En qué consiste el ciclo PHVA de mejora continua? In *Plataforma Tecnológica Para La Gestión De La Excelencia*.

López, S. R., Jiménez, A. J., & Catató, A. J. (2023). Desarrollo y validación de un nuevo método de evaluación de riesgos eléctricos para la prevención y mitigación de daños a personas e instalaciones. *Ingeniare. Revista Chilena de Ingeniería*, *31*, 0–0. https://doi.org/10.4067/S0718-33052023000100204

Machay, T., & Llano, Q. (2024). *Elaboración de un módulo de videovigilancia con inteligencia artificial* . http://dspace.istvidanueva.edu.ec/handle/123456789/420

Martín, T. de la R. (2021). Automatización De Un Sistema De Gestión De Seguridad De La Información Basado En La Norma ISO/IEC 27001. *Industry and Higher Education*, *13*(5).

Maureira, V. M., & González, G. D. (2023). La digitalización de la vida contemporánea: el saber, el poder y la subjetivación como vías de acceso a la experiencia digital. *Papeles Del CEIC*. https://doi.org/10.1387/pceic.23092

Ministerio de Defensa Nacional. (2024). Colombia refuerza su seguridad con sistemas avanzados de defensa contra drones para proteger a la comunidad, la fuerza pública y el territorio nacional. . *Ministerio de Defensa Nacional de Colombia.* https://www.mindefensa.gov.co/prensa/noticia-visualizacion/noticias-prensa-colombia-refuerza-su-seguridad

Moreno, J. P. P. (2008). Tecnología biométrica con huellas digitales. *Estudios En Seguridad y Defensa*, *3*(6). https://doi.org/10.25062/1900-8325.130

Mozo, R. O., & Ardila, C. 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

Nagothu, D., Xu, R., Nikouei, S. Y., & Chen, Y. (2018). A Microservice-enabled Architecture for Smart Surveillance using Blockchain Technology. *2018 IEEE International Smart Cities Conference, ISC2 2018*. https://doi.org/10.1109/ISC2.2018.8656968

Prieto, F. J. M. (2023). El papel de la tecnología RFID como herramienta para el entrenamiento militar. *Publicaciones e Investigación*, *17*(1). https://doi.org/10.22490/25394088.6663

Quispe, M. R. A. (2023). Investigación Cualitativa en Educación. In *Investigación Cualitativa en Educación*. https://doi.org/10.37073/feunah.39

Sakiko, F.-P., & Carol, M. (2012). Human Security: A critical review of the literature. *Centre for Research on Peace and Development (CRPD) Working Paper*, *11*.

San José, J., Pastor, J., & García, A. (2012). RFID: La Identificación por Radiofrecuencia como futuro de la identificación de objetos. *Revista de Investigación Universitaria Studia Académica*, *18*(October).

Sánches, G. J. (2020). Biometría y la seguridad informática en los métodos de autenticación. In *Human Relations* (Vol. 3, Issue 1).

Sánchez, V., Barreto, I., Correa, D., & Fajardo, M. (2007). Representaciones sociales de un grupo de estudiantes universitarios frente a un acto terrorista en Bogotá. *Diversitas*, *3*(2). https://doi.org/10.15332/s1794-9998.2007.0002.09

Suarez, P. R. A. (2024). *La prohibición de uso de minas antipersonas en el conflicto armado colombiano; caso Catatumbo, Norte de Santander*. https://repository.unilibre.edu.co/handle/10901/28953

Tricco, A. C., Lillie, E., Zarin, W., O'Brien, K. K., Colquhoun, H., Levac, D., Moher, D., Peters, M. D. J., Horsley, T., Weeks, L., Hempel, S., Akl, E. A., Chang, C., McGowan, J., Stewart, L., Hartling, L., Aldcroft, A., Wilson, M. G., Garritty, C., … Straus, S. E. (2018). PRISMA extension for scoping reviews (PRISMA-ScR): Checklist and explanation. In *Annals of Internal Medicine* (Vol. 169, Issue 7). https://doi.org/10.7326/M18-0850

Velásquez, C. P. A., & Torres, G. M. A. (2023). Militares víctimas en los conflictos armados. Normativa internacional e interna. *Escuela Superior de Guerra "General Rafael Reyes Prieto"*. https://esdeglibros.edu.co/index.php/editorial/catalog/download/126/192/2449?inline=1

Visitación, M. Á., Mogollón, R. F., & Mendoza, de los S. A. (2023). Beneficios de sistemas biométricos basados en lectura de Iris. *Perfiles de Ingeniería*, *18*(18). https://doi.org/10.31381/perfilesingenieria.v18i18.5398