Protocolo de identidad digital aplicando ciberseguridad coadyuvando a la capacidad distintiva seguridad militar, en autenticación, confirmación y tratamiento de datos del Estudio de Seguridad de Personal (ESP) CYBERESP

Mayor (EJC) Andres Camilo Cotes Cadena

Artículo para optar al título profesional:

Magister en Ciberseguridad y Ciberdefensa Nacional

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) Andres Camilo Cotes Cadena
Identificación	**:**	1.032.374.978
Programa académico	**:**	Maestría en Ciberseguridad y Ciberdefensa Nacional
Tutor metodológico	**:**	Omitido
Tutor temático	**:**	DR, Jaider Ospina Navas
Fecha de entrega	**:**	28 de Septiembre de 2025
Extensión	**:**	7432 palabras

DECLARACIÓN DE ORIGINALIDAD Y CESIÓN DE DERECHOS

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

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

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

AUTORIZACIÓN DE PUBLICACIÓN

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

Protocolo de identidad digital aplicando ciberseguridad coadyuvando a la capacidad distintiva seguridad militar, en autenticación, confirmación y tratamiento de datos del Estudio de Seguridad de Personal (ESP) CYBERESP

Digital identity protocol applying cybersecurity, contributing to the distinctive military security capacity, in authentication, confirmation and data processing of the Personnel Security Study (ESP) CYBERESP

Andres Camilo Cotes Cadena[*]

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen:

El protocolo actual de seguridad en el Ejército Nacional de Colombia, relacionado con el Estudio de Seguridad Personal (ESP) resulta tener bajos niveles de seguridad, convirtiéndose en una vulnerabilidad para el personal, instalaciones e información al interior de los cantones militares de la fuerza, por lo anterior se busca desarrollar un protocolo adecuado que mitigue los riesgos que se presentan actualmente en la identificación y así mismo poder corroborar mediante la interoperabilidad los documentos necesarios para establecer la veracidad y confiabilidad de cada una de las personas que laboran para la fuerza o poseen cualquier vinculo con ella.

Palabras clave: Estudio de Seguridad Personal; Vulnerabilidad; protocolo; confiabilidad.

Abstract: The current security protocol in the National Army of Colombia, related to the Personal Security Study (ESP), turns out to have low levels of security, becoming a vulnerability for the personnel, facilities and information within the military cantons of the force. Therefore, it seeks to develop an adequate protocol that mitigates the risks that currently arise in identification and also to be able to corroborate through interoperability the documents necessary to establish the veracity and reliability of each of the personnel who work for the force or have any link with it.

Keywords: Personal Safety Study; Vulnerability; protocol; reliability.

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

Introducción

En el mundo contemporáneo, la transformación digital ha redefinido la forma en que los Estados gestionan la seguridad y la defensa, constituyéndose en un factor disruptivo que modifica las prácticas tradicionales y plantea nuevos desafíos estratégicos. Este cambio ha impactado de manera directa en el paradigma de seguridad nacional, al impulsar la implementación de sistemas autónomos de defensa y enfrentar la evolución de las amenazas cibernéticas (Herrera, 2025, p. 2). En este escenario, el incremento de los ciberataques contra infraestructuras críticas y la vulnerabilidad de la información estratégica han llevado a organismos internacionales a reconocer al ciberespacio como un dominio de operaciones tan relevante como los ámbitos terrestre, marítimo o aéreo. De este modo, los datos y la información se consolidan como activos estratégicos cuya protección resulta indispensable para garantizar tanto la seguridad nacional como la confianza institucional.

Las Fuerzas Militares de Colombia y en especial el Ejército Nacional de Colombia, durante la historia ha optado por adaptarse a el avance de las tecnologías para optimizar los procesos institucionales (Espitia, Agudelo, Ramírez, 2021, p. 87). En 2021, por ejemplo, se presentó "el Documento de Identidad Digital (DID) para los servidores públicos del Ministerio de Defensa Nacional y los uniformados de las Fuerzas Militares, como una herramienta tecnológica" (Comando General de las Fuerzas Militares de Colombia, 2021). Sin embargo, ha sorteado grandes desafíos referentes a seguridad de personas, bien sea personal orgánico de la institución, prestadores de servicio, contratistas o aspirantes. De

acuerdo con lo anterior, los protocolos de verificación del personal presentan fallas permanentes en su aplicación y así mismo en la corroboración de los datos.

Determinando la importancia de la necesidad de tener personas confiables al interior de la institución, el presente artículo busca implementar un protocolo que permita la corroboración de datos consignados, con un aporte de identidad digital que al ser corroborado con las bases de datos existentes en la institución y organismos de control se determine la confiabilidad del personal que realiza mencionado protocolo, permitiendo garantizar la seguridad de personas, instalaciones e información vitales para el Ejército Nacional.

En este sentido, el artículo considera los datos como el activo más importante para el ámbito público o privado, pero pasando al ámbito ciber, este tema no se le da la relevancia del caso y sabiendo que el gobierno establece políticas desde 2011 que brinda del inicio partiendo de las palabras mencionadas en CONPES 3701 (Departamento Nacional de Planeación, 2011), "El conocimiento en el área de ciberseguridad y ciberdefensa tanto en el sector público como en el privado es limitado" (p.18), cuanta verdad en las palabras anteriores, pero aterrizando en el sujeto principal de estudio que es Ejército Nacional de Colombia, el ámbito de manejo de estos datos su responsabilidad principal está en manos de la seguridad militar y define esta competencia distintiva según el manual:

> Hace parte de las competencias distintivas de la contrainteligencia; su objetivo se centra en generar condiciones de seguridad enfocadas en la preservación de la integridad, la credibilidad y la confiabilidad de los elementos que comprenden la Fuerza o los asociados de la acción unificada (información, personas, material,

instalaciones, entre otros) MCE 3-37.3 SEGURIDAD MILITAR (Ejército Nacional de Colombia, 2023, p. 15).

Lo anterior demuestra la persistente brecha entre la formulación de políticas nacionales en materia de ciberseguridad y ciberdefensa y la implementación práctica dentro de las instituciones militares. Aunque el marco normativo reconoce la importancia de los datos y de su protección como un recurso estratégico, en la práctica el Ejército Nacional enfrenta limitaciones estructurales y procedimentales que dificultan consolidar protocolos robustos de verificación y resguardo de la información. Teniendo en cuenta que, "la ciberseguridad se orienta hacia la provisión de un entorno digital seguro que permita disfrutar de la libertad y protección de los datos personales y de la privacidad" (Peña, 2023, p. 339).

Con el fin de desarrollar el proyecto bajo un esquema teórico que respalde la rigurosidad académica de la investigación académica se proponen los siguientes conceptos claves para orientar la formulación de protocolos para la protección del personal militar y sus datos. En primer lugar, la identidad digital se define como "el conjunto de datos o atributos asociados de manera unívoca a un mismo identificador" (Llaneza, 2021, p.28), lo que implica que cada individuo, al interactuar en entornos digitales, construye una huella que lo representa en múltiples sistemas y plataformas. Otra perspectiva de la identidad digital es la ofrecida por Augusto Ho, quien la entiende como: "una identidad fluida, transformativa y cambiante, la cual cuenta con aquellas características, atributos, habilidades, y diversas funcionalidades inherentes a un individuo, así como puede ser lugares o cosas" (Ho, 2022, p.139). En este sentido, la identidad digital es dinámica, pues permite la actualización, modificación o eliminación de atributos vinculados al usuario

conforme cambian sus funciones o contextos, sin que esto requiera la emisión de un nuevo identificador.

Este concepto adquiere especial relevancia en escenarios de seguridad y defensa, donde la protección de los datos personales no solo garantiza la privacidad de los usuarios, sino que también constituye un factor crítico para la confiabilidad institucional. Como proceso la gestión de la identidad digital permite interacciones remotas confiables entre una organización y un individuo. Este proceso es cíclico y fundamental. Para que un individuo sea conocido por el sistema, debe primero registrarse (proceso de enrolamiento), durante el cual se verifican las condiciones relacionadas con su identidad o atributos de identidad para que se le pueda proporcionar un conjunto de credenciales. Posteriormente, el acceso a los recursos se valida mediante la autenticación de estas credenciales, lo cual establece confianza en la identidad del usuario (OCDE, 2011, p. 4).

Al ofrecer seguridad y privacidad, este proceso habilita el establecimiento de una relación de confianza entre las partes remotas (OCDE, 2011, p.5). Además, al proporcionar una gama de niveles de aseguramiento (bajo, medio o alto) que se alinean con el nivel de riesgo de las interacciones, se garantiza la proporcionalidad, lo cual es fundamental para el desarrollo de servicios de alto valor y para la seguridad del individuo (por ejemplo, con respecto a sus datos personales como un historial médico).

Es claro, que al construir la identidad se recopilan una serie de datos que se convierten en información valiosa para la toma de decisiones, tal como lo menciona Augusto Ho "con mayor frecuencia las personas y empresas navegan por las redes sociales para investigar la identidad digital de un candidato y tomar decisiones sobre él/ella. No son

pocos los casos de personas que pierden oportunidades laborales o de negocios por enviar el mensaje equivocado en sus publicaciones; pero es tema aparte" (p. 141).

La recopilación de esta información conlleva una responsabilidad para la institución, y es donde recobra importancia la ciberseguridad militar, esta se entiende bajo las consideraciones de la ISO/IEC 27032_2013 citada por Vargas, Reyes y Herrera (2017), es decir, las dos dimensiones del término: "La primera, desde un ámbito más estratégico, en la que se identifica la condición de un ciberespacio libre de amenazas, peligros y daños, así como el nivel de riesgo al que están expuestos sus organizaciones y ciudadanos" (p. 34); así, la ciberseguridad busca garantizar un ciberespacio seguro, evaluando continuamente los riesgos a los que se enfrentan organizaciones y ciudadano. En la segunda dimensión, se comprende de forma "más operativa, trata de preservar la confidencialidad, integridad y disponibilidad de la información en el ciberespacio, entre otros atributos" (Vargas et al., 2017, p. 34). Ambas dimensiones tienen relevancia en la presente reflexión académica, pues se busca proponer desde un ámbito estratégico un protocolo desarrollar un protocolo adecuado que mitigue los riesgos que se presentan actualmente en la identificación y así mismo poder corroborar mediante la interoperabilidad los documentos necesarios para establecer la veracidad y confiabilidad de cada una de las personas que laboran para la fuerza o poseen cualquier vínculo con ella.

De manera complementaria, la interoperabilidad se establece como la capacidad de diferentes entidades y sistemas de intercambiar información de forma estandarizada y segura, condición indispensable para articular las bases de datos de organismos estatales que apoyan el Estudio de Seguridad de Personal (ESP) (European Union, 2017).

Finalmente, la confianza digital se concibe como el grado de seguridad percibido al interactuar en entornos electrónicos, fundamentado en la autenticación, la integridad y la disponibilidad de los datos, aspectos que, en el ámbito castrense, resultan determinantes para garantizar que solo personal debidamente validado pueda acceder a instalaciones o información crítica de la institución (NIST, 2020).

Es importante establecer que la carta magna de Colombia dentro de su Artículo 15 donde establece:

> Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.(Asamblea Nacional Constituyente, 1991, p. 3)

En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.

Estableciendo la importancia de lo anterior los datos son un tema de bastante relevancia y es por esto por lo que, en la actualidad, se han convertido en un activo de la organización, sin embargo, para ahondar más en mi afirmación me permito citar las palabras de Nelson Remolina Angarita

> "La información lo es todo". Esta frase, merecedora de algunos reparos, parece cobrar cada día mayor fuerza respecto de los datos personales en el ámbito empresarial. Desde hace varias décadas viene consolidándose una economía basada en el conocimiento y la utilización ética e inteligente de las

> tecnologías dentro de la cual la información sobre las personas es un bien crucial. Como el tratamiento (recolección, almacenamiento, circulación, etc.) indebido de datos personales vulnera derechos de las personas, el artículo 15 de la Constitución consagró derechos en cabeza de ellas e impuso obligaciones a los administradores de datos personales, como lo son los empresarios respecto de los datos de sus clientes, sus trabajadores, sus proveedores y terceros. Los datos personales1 o la información personal se han convertido en un bien permanentemente comercializado a escala nacional e internacional y en un insumo diario de los sistemas de información privados y del Gobierno (Nelson Remolina Angarita, 2022, p. 1)

Una vez observado el contexto de la problemática en la institución en el tema de verificación de la información suministrada en los distintos procesos de vinculación y en la forma en la que actualmente se utilizan los datos, la estructura del presente artículo se realiza en cumplimiento de los objetivos específicos de la siguiente manera: en primer lugar, se analiza la construcción de la identidad digital dentro de la institución, identificando las fallas en el protocolo del (ESP) en el Ejército Nacional, en segundo lugar, se establece la importancia de proteger los datos del personal orgánico del Ejercito Nacional aplicando el marco normativo colombiano, en tercer lugar, se analiza la necesidad de que el protocolo de ciberseguridad digital garantice interoperabilidad con entidades clave, tales como la Registraduría Nacional del Estado Civil, la Contraloría, la Procuraduría, la Policía Nacional (DIJIN-INTERPOL), Migración Colombia y CREMIL. Y finalmente, se proponer el

protocolo de ciberseguridad digital que mitigue la necesidad de autenticación, confirmación y tratamiento de datos a los funcionarios del Ejército Nacional.

Metodología

La investigación plantea una problemática que requiere de una recolección de información y sistematización cuyo análisis se alinea con el método cualitativo, debido a que la identidad digital como concepto se ha y se sigue construyendo a través de redes de significados sociales. En este sentido, se prioriza la interpretación sobre la medición, atendiendo a las dinámicas discursivas, recordando que, la investigación "puede ser vista como el intento de obtener una comprensión profunda de los significados y definiciones de la situación tal como nos la presentan las personas, más que la producción de una medida cuantitativa de sus características o conducta" (Salazar, 2020, p.103). Así, el enfoque metodológico busca comprender cómo diferentes actores producen, disputan y legitiman sentidos en torno a la identidad digital, lo que hace necesario el uso de fuentes documentales, análisis de contenido y contraste con marcos teóricos que permitan desentrañar estas construcciones.

En este orden de ideas, se empleó como herramienta de recolección de fuentes diferentes artículos académicos sobre el tema en cuestión, en las diferentes bases de datos como Scielo, Doaj, Redalyc, Google Scholar, así como las investigaciones consignadas en el repositorio institucional de la Escuela Superior de Guerra "General Rafael Reyes Prieto". Además de esta información se recurrió a documentos institucionales que dan cuenta del proceso de creación de identidad digital dentro de la institución y para comprobar sus fallas se analizaron fuentes periodísticas que dan cuenta de algunos incidentes que prueban los

argumentos. Cabe resaltar, que, como punto de partida, la metodología y el tema de investigación surgió de una observación constante por parte del investigador.

Como resultado de la triangulación de los hallazgos, se elaboró un protocolo representado en un diagrama de flujo, orientado a identificar riesgos permanentes en la institución y a señalar áreas de mejora. Si bien el artículo reconoce la existencia de proyectos destinados a fortalecer la ciberseguridad en los procesos de verificación de identidad, su propósito trasciende dicha perspectiva al proponer una reflexión más amplia que contribuya a optimizar la práctica institucional.

Creación de identidad digital en el tratamiento de datos del Estudio de Seguridad de Personal (ESP)

La creación de la identidad digital en la institución militar está vinculada a la recopilación de datos personales y profesionales que crean un identificador dentro del ciberespacio institucional. Si se retoma las recomendaciones de la OCDE (2011) en este tema, el proceso de creación y validación de la identidad digital inicia con el registro, para que el individuo sea conocido por el sistema, "debe registrarse primero en él y se debe verificarse las condiciones relacionadas con su identidad o atributos de identidad para que se le pueda proporcionar un conjunto de credenciales; este es el llamado proceso de registro o inscripción" (p. 4).

En el caso del registro en el Ejército Nacional, el personal debe cumplir con una lista de requisitos para suministrar la información suficiente para acreditar su identidad y crear las credenciales necesarias. Para ello se inicia con el diligenciamiento de un documento en el que se ingresa la información del individuo. Como primera instrucción se

señala que debe llenarse en su totalidad de forma legible por el funcionario o contratista, además se menciona que, "la información y documentos que a continuación suministrará de forma voluntaria, serán sometidos a verificación y en caso de que estos no coincidan con la realidad, se procederá a informar a la autoridad competente para los tramites de ley" (Ejército Nacional, 2017).

También se advierte que al ser diligenciado y entregado la información adquiere el carácter de reserva según la Ley 1621 de 2013 "por medio de la cual se expiden normas para fortalecer el marco jurídico que permite a los organismos que llevan a cabo actividades de inteligencia cumplir con su misión constitucional y legal, y se dictan otras disposiciones" (Congreso de la República de Colombia, 2013). Como primeros identificadores se encuentran los datos personales básicos y dos fotografías, estos se complementan con datos familiares y personales, los cuales se desglosan en barios detalles, especialmente en los vínculos más cercanos, así como los datos de actividad financiera más relevantes.

Estos datos dan cuenta de la trayectoria y construcción de identidad de los individuos que van hacer parte de la institución, al diligenciar estos datos ocurren dos procesos, en primer lugar, se reconoce al individuo como parte del equipo de trabajo del Ejército Nacional, y en segundo lugar, la ciberseguridad adquiere la responsabilidad de salvaguardar la información suministrada de forma voluntaria por el individuo, lo cual puede resultar de forma positiva o negativa, ya que se debe realizar un proceso de verificación riguroso que compruebe la veracidad de la información.

Este proceso ha sido el resultado de una constante evolución, tal como lo muestra el control de actualizaciones, desde el 13 de mayo de 2009 se están realizando actualizaciones

para optimizar el proceso de vinculación al Ejército Nacional, en 2022 se desarrollaron finalmente los flujogramas de actividades como un proyecto que permitiría una mejor organización de todo el proceso en la práctica. (Ejército Nacional, 2022). Sin embargo, en la práctica la gestión no es invulnerable, de hecho, presenta algunas fallas que ponen en riesgo la ciberseguridad, como los que se analizan a continuación:

Fallas en el protocolo del ESP en el Ejército Nacional:

Las diferentes falencias que posee el protocolo de Estudio de Seguridad Personal que establece en que han identificado los Batallones de Seguridad Militar, adscritos a la Brigada de Contrainteligencia Militar N°2 que pertenecen al Comando de Apoyo de Contrainteligencia Militar del Ejército Nacional, que, aunque figuran dentro de documentos de carácter reservado los cuales no se pueden mostrar ni citar por su clasificación, para comprobar su eficiencia se tomaron en consideración algunos casos difundidos por los medios de comunicación. Las dificultades acaecidas en la aplicación de este protocolo dentro del Ejercito Nacional las cuales fueron las siguientes:

1. Falsificación de diplomas por parte del personal de prestadores de servicio para contratación: En este punto se observa con gran recurrencia que falsifican diplomas de pregrado o especializaciones con el fin de hacerse acreedores al cargo o ascenso. Un ejemplo de esta práctica es el caso de Daisy Carolina Sosa Hernández una Mayor quien realizó contratos con la institución por un valor de $345'181.200 para prestar "servicios como anestesióloga en las salas de cirugía del dispensario, a pesar de no estar acreditada ni contar con la idoneidad necesaria para ejercer dicha especialidad" (Muñoz, 2025). Este tipo de prácticas no solo evidencian graves falencias en los mecanismos de control y verificación dentro de la institución, sino que también ponen en riesgo la seguridad y el

bienestar de los usuarios del servicio, al permitir que personas sin la idoneidad requerida asuman responsabilidades de alta prioridad.

2. Diligenciamiento de una vivienda donde la persona no vive: Este punto es constante y representa una falencia grande, ya que en el momento de realizar visitas domiciliarias se evidencia que no residen en la vivienda, dificultando el proceso.

3. Plasman en el formato de información personal referencias que no contestan o que no los conocen: Es claro que en el momento de la corroboración de datos no podría dar certeza del funcionario.

4. No plasman en el formato de información personal las investigaciones, procesos jurídicos o de policía que han tenido: Es uno de los aspectos mas recurrentes, ya que saben que en el momento de presentar antecedentes, serán descartados del proceso de selección y es en ese momento que se convierte en un riesgo para la institución.

5. Formatos de Información Personal diligenciados con letra que no se entiende: El proceso manuscrito genera traumatismo en la verificación, ya que la caligrafía y forma de escritura retrasa el proceso a un 70%

6. En el Formato de información personal no se entrega con sus anexos ejemplo (cédula, última declaración de renta, diplomas): Este punto en especial se genera porque en su ultima pagina se brindan las indicaciones, pero la gran mayoría se encuentran un poco exhaustos de leer y escribir y no se percatan de estos documentos anexos.

7. Demoras en la entrega del formato: No se entiende muchas veces un formato que es relativamente fácil de diligenciar o entregar en los tiempos estipulados o muchas veces no llegan a entregarlo.

8. En el caso de personal analfabeta, no tienen una orientación adecuada en el diligenciamiento del formato: Es un tema muy recurrente en conscriptos y reclutas, desafortunadamente la gran mayoría de soldados que tenemos poseen bajos niveles de educación, situación que en el momento de realizar el diligenciamiento del formato generan errores garrafales dentro del mismo.

9. No se realizan las visitas domiciliarias debido a la falta de medios humanos y técnicos: Este es un factor fundamental en el cual se falla constantemente, ya que muchos aspectos se pudiesen evidenciar con el simple hecho de ir a cada uno de los domicilios y realizar la visita con los parámetros establecidos.

10. No se le brinda la importancia al cargo de Seguridad Militar por tal motivo a la hora de diligenciar el formato el personal no posee la idoneidad para realizar la verificación acuciosa de la documentación: Debido a que no se presta la importancia al cargo de seguridad militar, se entrega el cargo a personas que no observan la importancia del cargo y cometen errores que realmente pueden afectar la integridad del personal de las guarniciones militares que se tienen a cargo.

11. Todas las unidades no cuentan con la Red Unificada de Comunicaciones, situación que limita el acceso a los datos que necesita el modulo de seguridad militar para la corroboración de documentos: Este factor representa un tema generalizado en las redes del Ejército Nacional de Colombia.

Las deficiencias detectadas han puesto en evidencia las vulnerabilidades estructurales de la ciberseguridad institucional, manifestadas en episodios críticos como el registrado el 19 de septiembre en Bogotá. En dicho caso, cuatro individuos fueron judicializados por delitos relacionados con revelación de secreto, concierto para delinquir,

fraude procesal y prevaricato por omisión, tras suplantar a oficiales del Ejército con el propósito de infiltrarse en unidades estratégicas y acceder a información sensible sobre la seguridad y las actividades del presidente Gustavo Petro (Rodríguez, 2025). Este hecho ilustra no solo la fragilidad de los mecanismos de control, sino también el potencial impacto de estas brechas en la gobernanza y en la seguridad nacional.

Otro caso ejemplificante de estas vulnerabilidades fue el ocurrido con el individuo capturado al intentar ingresar a la Brigada 11 del Ejército en septiembre de 2022, el hombre en cuestión vestía prendas de la institución y portaba la insignia del grado de sargento segundo (Ejército Nacional, 2022). En otras situaciones se suplanta a la institución en las redes para delinquir utilizando el nombre de la institución o de sus integrantes por medio de la suplantación, como se constató en la investigación adelantada en 2023 en la que se descubrió una red de terceros que ofertaba vinculaciones laborales con el nombre y cargo de los militares. (Ejército Nacional, 2023).

Lo anterior no figura en documentos oficiales que sustenten las diferentes fallas es más un trabajo de campo el cual reúne conceptos y aportes de personas de los diferentes Batallones de Seguridad Militar y oficinas de seguridad militar de las diferentes unidades que permitieron determinar las fallas generalizadas, que vislumbra la importancia que se tiene que brindar al tema de seguridad física, seguridad de personas y aún más importante la seguridad de información.

La importancia de proteger los datos del personal orgánico del Ejercito Nacional aplicando el marco normativo colombiano.

Las diferentes situaciones de seguridad en las que se han visto involucrados los cantones militares del Ejército Nacional de Colombia establecen un desafío en modernizar su

infraestructura. No obstante, pocas veces se hace énfasis en la actualización de la seguridad con enfoque especifico en control de accesos y protección de datos dificultando el cumplimiento de la teórica básica de la ciberseguridad.

Por otro lado, la transformación del Ejército, orientada a preservar el patrimonio institucional, fortalecer al ser humano como eje central de la organización e implementar un modelo que lo proyecte a la vanguardia regional y al nivel de los ejércitos más prestigiosos del mundo, enfrenta limitaciones significativas. Estas se evidencian en la ausencia de desarrollos sólidos en ciberseguridad y ciberdefensa, lo que genera riesgos potenciales sobre los datos del personal orgánico y de los prestadores de servicio. Además, la amenaza emergente del uso criminal de la inteligencia artificial, cuyo acceso por parte de actores ilícitos se facilita gracias a los elevados recursos económicos que producen las economías ilegales y que permiten adquirir sistemas robustos capaces de vulnerar información sensible. Asimismo, persisten vulnerabilidades asociadas a la custodia física de documentos en recintos que carecen de condiciones mínimas de seguridad, lo cual incrementa la exposición institucional frente a filtraciones internas y externas.

De acuerdo con lo anterior, el Ejército Nacional ha sufrido cambios generacionales que obligan a cambiar sistemas de seguridad física, seguridad de personas y seguridad de instalaciones, que equipare a las todas las megatendencias del Siglo XXI en tecnología y digitalización, lo anterior pone en evidencia la fragilidad de que los procesos de seguridad se sigan manejando de forma física, ya que existen directivas tales como la Directiva 02 del 2022, en la cual se establece, en su numeral 5:

> Adoptar la seguridad digital con un enfoque preventivo y proactivo basado en la gestión efectiva de riesgos en el entorno digital, priorizando la

> protección de datos personales e información sensible de la entidad o que goza de reserva legal, al igual que de los servicios y sistemas de información e infraestructuras críticas (Presidencia de la República, 2022, p. 1)

Es así como los procesos de la capacidad distintiva de Seguridad Militar deban anticipar riesgos que se puedan materializar desde una simple infiltración, hasta temas delicados de espionaje y tráfico de armas que redundan en el ambiente estratégico siempre enmarcado en el marco de la ley 1581 de 2012 y su ámbito establecido en el Artículo 2:

> Ámbito de aplicación. Los principios y disposiciones contenidas en la presente ley serán aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada. La presente ley aplicará al tratamiento de datos personales efectuado en territorio colombiano o cuando al responsable del Tratamiento o Encargado del Tratamiento no establecido en territorio nacional le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales.(Congreso de Colombia, 2012, p. 1)

Desde la perspectiva teórica, este marco normativo respalda la realidad en la que se encuentra en la actualidad la identidad digital, pues esta se ha convertido en una "herramienta que permite singularizar, asociar información e interconectar a las personas físicas, entidades y objetos en un contexto digital" (Hurtado, 2020, p. 116). Para que las personas se sientan seguras en este nuevo entorno es necesario dar cumplimiento a las leyes que respaldan su seguridad, algo que, como se ha observado a lo largo de la investigación, resulta una tarea compleja si no se cuenta con los recursos suficientes y si no se integra la perspectiva teórica de la ciberseguridad en sus dos dimensiones: en el ámbito estratégico de

detección temprana y en el campo operativo de preservar la confidencialidad, integridad y disponibilidad de la información en el ciberespacio (Vargas et al., 2017, p. 34).

El primer paso, sería consolidar una estrategia integral que articule la modernización tecnológica con el fortalecimiento institucional, garantizando que la implementación de medidas en ciberseguridad y ciberdefensa no se limite a una respuesta reactiva frente a incidentes, sino que configure un modelo preventivo y sostenible en el tiempo. Ello implica asignar recursos adecuados, capacitar al personal en competencias digitales, establecer protocolos claros de protección de datos y armonizar la seguridad física con la digital. Estos puntos se exploran con mayor detenimiento en el siguiente apartado.

El protocolo de ciberseguridad digital, interoperabilidad con entidades del Estado.

Las diferentes amenazas han desarrollado capacidades de infiltración, penetración y espionaje de los miembros del Ejército Nacional los cuales generan desafíos para los módulos de seguridad Militar, pero se hace necesario aprovechar las capacidades que se tienen a nivel de convenios interinstitucionales tales como los que maneja CEDE 2, el cual vincula entidades que serian de vital importancia para lograr la mitigación de riesgos que se puedan presentar en el momento del diligenciamiento del documento digital, en vista de los anterior es necesario que se aplique interoperabilidad con las diferentes entidades tomando la mayor a menor importancia pero que el trabajo conjunto brindara la eficiencia al protocolo las cuales son:

1. **Migración Colombia**

   Su importancia se fundamenta en controlar y vigilar el movimiento de personas, tanto nacionales como extranjeros, dentro de su misión se expone "Ejercer control como autoridad migratoria a ciudadanos nacionales y extranjeros en el territorio colombiano

de manera técnica y especializada, brindando servicios de calidad, en el marco de la Constitución y la ley" (Migración Colombia, 2024). Los segundos en su orden son los de mayor importancia ya que se vinculan a la institución en su gran mayoría por contratistas los cuales incluyen a su mano de obra esta clase de personal con el fin de tener un beneficio económico, por otro lado, ya se tienen antecedentes de planes de espionaje los cuales debemos ser anticipativos a las intenciones de la amenaza.

2. **Policía Nacional (DIJIN-INTERPOL)**

Su importancia radica en la investigación criminal y la cooperación internacional policial, en su misión se señala que, "tiene como alcance el proceso de Investigación Criminal y los activos de información gestionados por las dependencias internas del nivel central, con el fin de garantizar la disponibilidad, confidencialidad e integridad de la información basados en buenas prácticas" (Policía Nacional de Colombia, 2024). , a nivel del proyecto se detectarían aquellas órdenes de captura de nivel nacional o internacional que mitiga cualquier amenaza que tenga intenciones contra la institución, lo anterior ya que existen personas al interior del Ejercito Nacional que pueden tener órdenes de captura vigentes o antecedentes judiciales que representan un riesgo.

3. **Registraduría Nacional del Estado Civil**

Es la responsable de llevar el registro de nacimientos, matrimonios, defunciones, entre otros (Registraduría Nacional de Colombia, 2025). Sin embargo, a nivel de proceso planteado es de vital importancia corroborar la identidad del funcionario que quiere acceder a las instalaciones con el fin de evitar las suplantaciones.

4. **Contraloría**

Su función principal radica en vigilar la gestión fiscal de la administración pública y de quienes manejan fondos o bienes del Estado, tanto a nivel nacional como territorial. (Contraloría General de la República de Colombia, 2022). Por tal motivo, es necesario verificar los antecedentes que posee el funcionario que quiere pertenecer o ingresar a la institución.

5. **Procuraduría**

Su función radica en vigilar la conducta de los servidores públicos, defender el orden jurídico y el patrimonio público, así como proteger los derechos humanos. (Procuraduría General de la Nación, 2024). Con lo anterior, es importante establecer que personas poseen antecedentes en los ítems nombrados anteriormente.

6. **Caja de Retiro de las Fuerzas Militares (CREMIL)**

Es una entidad encargada de reconocer y pagar la asignación de retiro y sustitución pensional a los miembros de las Fuerzas Militares y sus beneficiarios.

7. **La Superintendencia de Notariado y Registro (SNR)**

La Superintendencia de Notariado y Registro (SNR) es una entidad colombiana adscrita al Ministerio de Justicia y del Derecho. Su función principal es inspeccionar, vigilar y controlar los servicios públicos de notariado y registro de instrumentos públicos, asegurando la seguridad jurídica en la formalización y registro de bienes inmuebles.

Por último, y no menos importante como es nombrado dentro del artículo 2.3.1.4.13.1 que establece el Decreto 1070 de 2015 Sector Administrativo de Defensa en el tema de interoperabilidad; así:

> Interoperabilidad con entidades para fines de definición de la situación militar. Con el propósito de reducir los trámites presenciales de los

> ciudadanos para la definición de la situación militar, se adelantarán los convenios o actos administrativos de interoperabilidad, de que trata el artículo 66 la Ley 1861 de 2017, en los términos de la Ley 489 de 1998 en concordancia con la Ley 1266 de 2008, y las demás normas relacionadas con la colaboración armónica entre las entidades del Estado, protección de datos y reserva de la información, conforme al Artículo 2.3.1.4.1.4. del presente Decreto.(Presidente de la República, 2015, p. 259).

Propuesta de protocolo de ciberseguridad digital que mitigue la necesidad de autenticación, confirmación y tratamiento de datos a los funcionarios del Ejército Nacional.

La transformación digital de las Fuerzas Militares de Colombia exige la implementación de un protocolo robusto de ciberseguridad digital que garantice la autenticación, confirmación y tratamiento seguro de la información del personal, contratistas y aspirantes. El protocolo propuesto busca mitigar las falencias identificadas en los capítulos anteriores y consolidar la capacidad distintiva de seguridad militar, alineada con el marco normativo colombiano Ley 1581 de 2012; Directiva Presidencial 02 de 2022 y estándares internacionales NIST SP 800-63; GDPR; Tallinn Manual 2.0; por lo anterior, se propone un modelo que cumple con parámetros adaptados así:

Principios rectores del protocolo: El diseño del protocolo debe enmarcarse en los siguientes principios, teniendo en cuenta que, dentro de este proceso se recopilan datos e información que comienzan a ser parte de la responsabilidad de la institución, es decir, de su ciberseguridad. Entre ellos:

- **Legalidad:** Cumplimiento estricto de la normatividad nacional sobre protección de datos y reserva legal.
- **Confidencialidad**: Protección de la información contra accesos no autorizados mediante cifrado y segmentación de datos.
- **Integridad**: Garantía de que los datos no sean alterados durante su captura, procesamiento y almacenamiento.
- **Disponibilidad**: Acceso oportuno y seguro de la información por personal autorizado.
- **Interoperabilidad:** Integración con bases de datos de entidades estatales (Registraduría, DIJIN-INTERPOL, Migración, Procuraduría, Contraloría, SNR y CREMIL).
- **No repudio y trazabilidad**: Registro auditable de todas las acciones realizadas en el sistema.

Fases del protocolo propuesto, el protocolo se estructura en cinco fases que garantizan la confiabilidad del ESP:

1. **Autenticación digital del personal:** Implementación de un sistema de identidad digital militar basado en credenciales únicas emitidas por la institución.
   Uso de doble factor de autenticación (2FA) combinando credenciales institucionales con biometría (huella, reconocimiento facial o iris).
   Incorporación de certificados digitales expedidos por una Infraestructura de Clave Pública (PKI militar) para firmar electrónicamente documentos.

2. **Confirmación de datos e interoperabilidad:** Conexión en tiempo real con bases de datos de: Registraduría Nacional: verificación de identidad y antecedentes de suplantación. DIJIN-INTERPOL: validación de antecedentes judiciales y órdenes de captura. Migración Colombia: control de doble nacionalidad, entradas y salidas del país. Procuraduría y Contraloría: consulta de sanciones disciplinarias y fiscales. CREMIL: verificación de situación militar y antecedentes en el sistema de retiro. Esto con ayuda después de la creación de un módulo de interoperabilidad digital mediante API seguras bajo estándares de intercambio de datos (REST/JSON, SOAP/XML) y protocolos de cifrado TLS.
3. **Tratamiento y almacenamiento seguro de la información:** Implementación de una plataforma centralizada de gestión de expedientes digitales con acceso restringido y segmentación por niveles de clasificación. Cifrado de la información en reposo mediante algoritmos AES-256 y en tránsito con TLS 1.3. Política de ciclo de vida de los datos, definiendo plazos de conservación, eliminación segura y auditorías periódicas. Almacenamiento en infraestructuras híbridas seguras (servidores militares y nube soberana con respaldo en territorio nacional).
4. **Auditoría y monitoreo continuo:** Integración de un *Security Information and Event Management (SIEM)* para monitorear accesos, intentos de intrusión y anomalías en tiempo real. Mecanismos de auditoría forense digital para trazabilidad de acciones de usuarios. Simulación periódica de pruebas de penetración y ejercicios de Red Team/Blue Team en las instalaciones militares.

5. **Capacitación y cultura de ciberseguridad:** Entrenamiento obligatorio concienciación, *ciberhigiene* militar para funcionarios, contratistas, personal recientemente incorporados y conscriptos. Creación de un manual institucional de ciberseguridad en procesos de personal, actualizado de acuerdo con amenazas emergentes. Campañas de sensibilización para prevenir ingeniería social, phishing y manipulación de credenciales.

Modelo de gobernanza del protocolo: El éxito del protocolo depende de una estructura de gobernanza que defina responsabilidades:

- Comando de Apoyo de Contrainteligencia Militar (CACIM): coordinación y supervisión del sistema.
- Dirección de Telemática del Ejército: gestión tecnológica e interoperabilidad con entidades externas.
- Centros de Protección de Datos: velar por el cumplimiento de la Ley 1581 de 2012 y demás normas.
- Unidades operativas menores: responsables de aplicar los procedimientos y alimentar el sistema de manera transparente.

Beneficios esperados: La implementación del protocolo fortalecerá la seguridad institucional en tres dimensiones principales:

- **Operativa:** reducción de infiltraciones, fraudes documentales y riesgos internos.
- **Estratégica**: consolidación de la confianza pública en la Fuerza y cumplimiento de estándares internacionales.

- **Doctrinal:** alineación con las capacidades distintivas de seguridad militar, potenciando la ciberdefensa nacional en el ámbito de personal.

Esta propuesta se fundamenta en principios que se han implementado en otros países destacados en este tema, uno de ellos es Estados Unidos, este ha adoptado un enfoque híbrido que combina marcos voluntarios con regulaciones obligatorias. El Instituto Nacional de Estándares y Tecnología (NIST) desarrolla marcos como el NIST Cybersecurity Framework, que, aunque no es jurídicamente vinculante, es ampliamente adoptado en sectores como el financiero y el sanitario (Ceinterim, 2023).

Ya para entrar en materia se ha diseñado un protocolo establecido mediante un diagrama de flujo el cual evidencia lo relacionado a lo largo del presente articulo y que busca principalmente la materialización de riesgos permanentes en la institución, el cual es el siguiente:

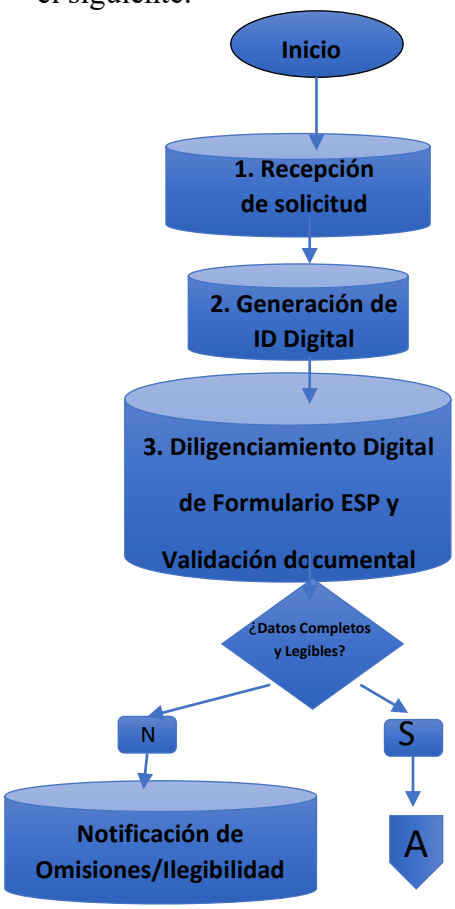

Diagrama de flujo (actividad)	Descripción de la actividad	Registro de la actividad	Responsable
1. Recepción de la solicitud de ingreso	El sistema recibe la solicitud del funcionario o contratista que desea iniciar el proceso de validación.	Número de radicado electrónico generado automáticamente.	Oficina de Seguridad Militar
2. Generación de ID Digital Provisional	El solicitante se autentica mediante credenciales institucionales y segundo factor biométrico (huella o rostro).	Token de autenticación y registro biométrico.	Oficina de Seguridad Militar
3.Diligenciamiento Digital de Formulario ESP y Validación documental	Carga digital de cédula, diplomas, antecedentes y demás documentos requeridos. Datos Completos y Legibles? **SI:** Autenticación Biométrica/Identificación Digital Directa **NO:**Notificación de Omisiones/Ilegibilidad **Se evalua si procede de nuevo a paso tres**	Expediente digital inicial en el sistema.	Funcionario de Seguridad Militar

Diagrama de flujo (actividad)	Descripción de la actividad	Registro de la actividad	Responsable
4.Interoperabilidad con entidades externas	Cruce automático de información con Registraduría, DIJIN, Procuraduría, Contraloría, Migración, SNR y CREMIL. Identidad Confirmada? **SI:** Verificación de Documentos Adjuntos **NO:**Alerta de Suplantación, Bloqueo de Proceso y Notificación a Contrainteligencia Militar Adicional es importante Confirmación de antecedentes Revisión de posibles sanciones, procesos judiciales o fiscales asociados al solicitante. NOTA: En caso de presentar antecedentes de cualquier índole se finaliza el proceso de inmediato y se realiza informe a autoridad competente	Informe de interoperabilidad con estado de cada verificación. Registro consolidado en el expediente digital.	-CEDE 2 -Dirección de Telemática. -Migración -Registraduría Procuraduría, Contraloría, DIJIN

Fuente: Elaboración propia con base en el protocolo de reclutamiento

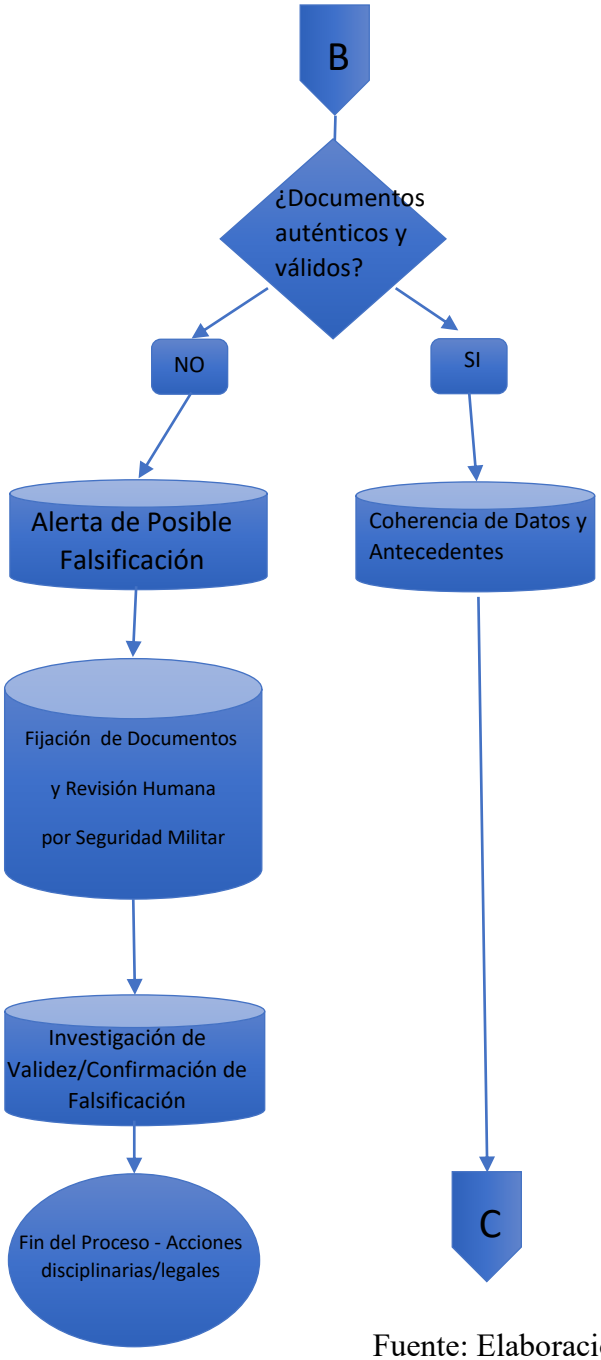

Diagrama de flujo (actividad)	Descripción de la actividad	Registro de la actividad	Responsable
4.Interoperabilidad con entidades externas	Cruce automático de información con Registraduría, DIJIN, Procuraduría, Contraloría, Migración y CREMIL. SNR Documentos auténticos y válidos? **SI:** Coherencia de Datos y Antecedentes **NO:**Alerta de Posible Falsificación Fijación de Documentos y Revisión Humana por Seguridad Militar Investigación de Validez/Confirmación de Falsificación Fin del Proceso - Acciones disciplinarias/legales	Informe de interoperabilidad con estado de cada verificación. Registro consolidado en el expediente digital.	-CEDE 2 -Dirección de Telemática. - Comité de Seguridad Militar

Fuente: Elaboración propia con base en el protocolo de reclutamiento

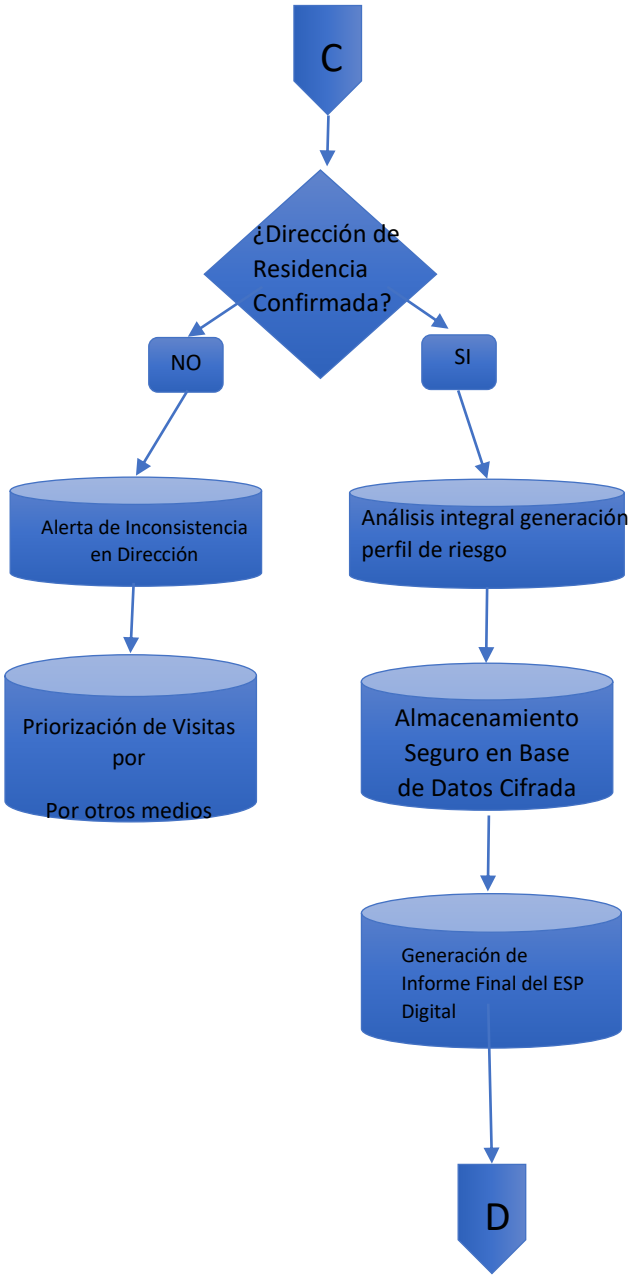

Diagrama de flujo (actividad)	Descripción de la actividad	Registro de la actividad	Responsable
5. Análisis integral generación perfil de riesgo	El Comité de Seguridad revisa el expediente digital y emite concepto sobre la confiabilidad del solicitante.	Acta digital de aprobación o rechazo.	Comité de Seguridad Militar
Almacenamiento seguro de datos	Los expedientes aprobados se almacenan en servidores militares con cifrado AES-256 y respaldo seguro.	Archivo digital clasificado y encriptado.	Centro de protección de Datos
Monitoreo y auditoría continua	El sistema registra intentos de acceso, modificaciones y auditorías periódicas.	Bitácora digital de seguridad.	Oficial de Protección de Datos + Auditoría Interna

Fuente: Elaboración propia con base en el protocolo de reclutamiento

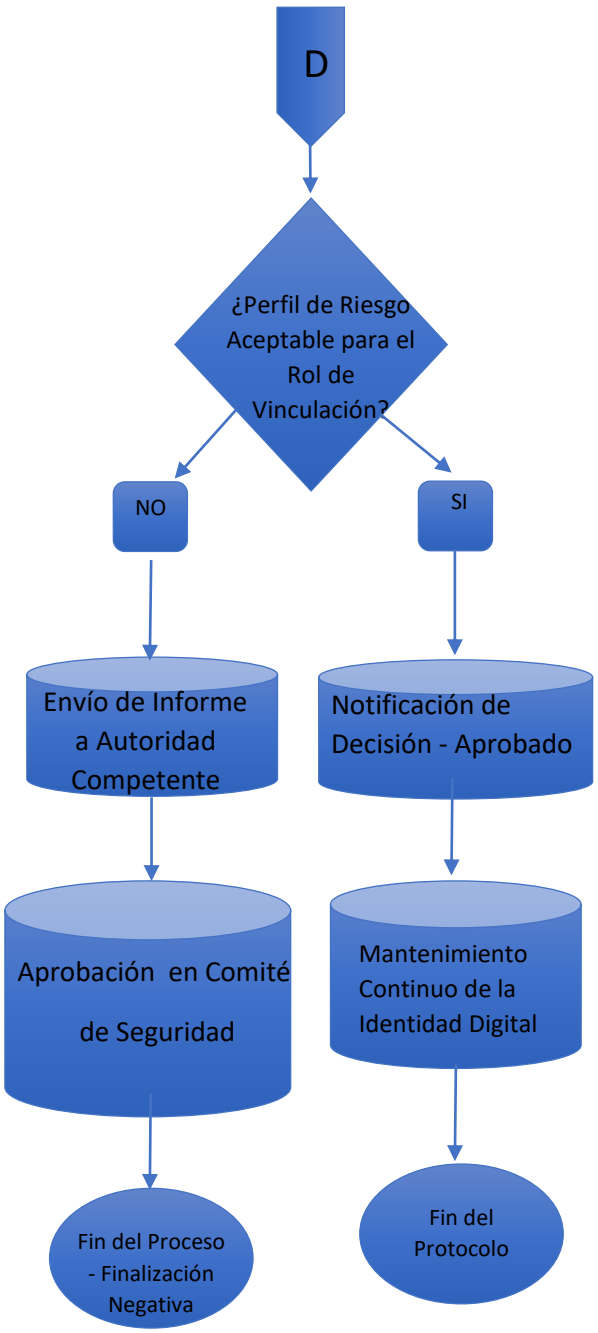

Diagrama de flujo (actividad)	Descripción de la actividad	Registro de la actividad	Responsable
5. Análisis integral generación perfil de riesgo	El Comité de Seguridad revisa el expediente digital y emite concepto sobre la confiabilidad del solicitante.	Acta digital de aprobación o rechazo.	Comité de Seguridad Militar
Almacenamiento seguro de datos	Los expedientes aprobados se almacenan en servidores militares con cifrado AES-256 y respaldo seguro.	Archivo digital clasificado y encriptado.	Centro de protección de Datos
Monitoreo y auditoría continua	El sistema registra intentos de acceso, modificaciones y auditorías periódicas.	Bitácora digital de seguridad.	Oficial de Protección de Datos + Auditoría Interna

Fuente: Elaboración propia con base en el protocolo de reclutamiento

La automatización de los procesos de autenticación, confirmación y manejo de datos mediante la herramienta n8n constituye un avance sustancial en el fortalecimiento de la

ciberdefensa institucional del Ejército Nacional de Colombia, al integrar la doctrina nacional (Ejército Nacional de Colombia, 2023a; 2023b) con marcos internacionales como el NIST SP 800-63-3 sobre identidad digital (National Institute of Standards and Technology [NIST], 2017), el marco de arquitectura de confianza cero (NIST, 2020) y el Cybersecurity Framework 2.0 (NIST, 2024). Este proceso, sustentado además en la normativa colombiana de protección de datos personales (Congreso de Colombia, 2012) y en los principios de seguridad militar (MCE 3-37.33), permite establecer flujos automatizados que combinan control humano y respuesta técnica verificable. De acuerdo con el enfoque doctrinal, la automatización no reemplaza la decisión del mando sino que la refuerza, garantizando trazabilidad, legalidad y preservación de evidencia conforme a los lineamientos de la ISO/IEC 27037:2023 sobre gestión de evidencia digital (International Organization for Standardization [ISO], 2023a). La integración de aprobaciones duales (Operaciones y Jurídica) en el flujo de órdenes críticas, complementada con sellos temporales RFC 3161 y registros SIEM, asegura la validez de las decisiones y la protección de la información clasificada bajo la Ley 1581 de 2012. Asimismo, la detección automatizada de exfiltraciones mediante DLP, EDR y ZTNA reduce significativamente el tiempo de respuesta y refuerza los principios de ciberseguridad establecidos por la OTAN a través del CCDCOE (2023), donde la automatización verificable es considerada elemento esencial de la defensa activa. En síntesis, el modelo desarrollado demuestra la viabilidad de una ciberdefensa orquestada, interoperable y conforme a la doctrina nacional e internacional, constituyéndose en un aporte técnico-académico aplicable a las operaciones militares contemporáneas (Hoffman, 2021; European Union, 2017).

Conclusiones

El análisis del protocolo vigente del Estudio de Seguridad de Personal (ESP) evidencia fallas estructurales y procedimentales que generan vulnerabilidades críticas para la Fuerza, exponiendo tanto a sus miembros como a la información sensible de la institución. Lo cual va en contravía de los principios que se analizaron teóricamente, desde el inicio de la discusión se demostró la responsabilidad que el Ejército Nacional adquiere al momento de crear la identidad digital, y esta no solamente como identificador para ingresar a las instalaciones, sino como herramienta para optimizar la ciberseguridad en sus dos dimensiones, es decir, en un mecanismo estratégico que permite evaluar y garantizar un ciberespacio seguro, libre de amenazas y daños, determinando los niveles de riesgo a los que se enfrentan tanto las organizaciones como los ciudadanos. Al mismo tiempo, cumple una función operativa al preservar la confidencialidad, integridad y disponibilidad de la información, asegurando que los sistemas, procesos y datos estén protegidos frente a vulneraciones.

En la discusión se evidenció que el Ejército Nacional de Colombia guía su Estudio de Seguridad de Personal (ESP) conforme a la normativa vigente a nivel nacional, lo que garantiza la protección de los individuos que crean su identidad digital dentro de la institución. El marco normativo colombiano, en particular la Constitución Política (art. 15) y la Ley 1581 de 2012, constituye la base legal para implementar procedimientos que aseguren la protección de datos personales, un aspecto esencial en el ámbito castrense. Esta normativa respalda tanto a quienes voluntariamente consignan sus datos como a la

institución en la identificación de posibles inconsistencias durante el proceso de verificación. No obstante, como se evidenció en los ejemplos de fallas, este proceso puede resultar complejo y, en algunos casos, profundizar las vulnerabilidades en la ciberseguridad, con implicaciones que incluso se extienden hasta la ciberdefensa.

Todo este panorama, junto con el análisis exhaustivo y analítico de los documentos de carácter reservado de vinculación a la institución, permitieron la formulación de una propuesta de protocolo de identidad digital que fortalece la capacidad distintiva de seguridad militar al garantizar procesos de autenticación confiables y trazables, reduciendo la posibilidad de suplantación o infiltración en el Ejército Nacional.

En este sentido, la propuesta buscó integrar: en primer lugar, la interoperabilidad con entidades externas como la Registraduría, DIJIN, Procuraduría, Contraloría, Migración Colombia, CREMIL y la SNR permite validar en tiempo real la autenticidad de la información presentada por funcionarios, contratistas y aspirantes, cerrando brechas históricas de verificación. En segundo lugar, la incorporación de tecnologías como la biometría, certificados digitales y PKI militar asegura un proceso robusto de autenticación y confirma la identidad de quienes participan en el protocolo ESP. En tercer lugar, el tratamiento y almacenamiento seguro de la información, mediante cifrado avanzado y segmentación de datos, garantiza que los expedientes digitales se preserven bajo altos estándares de confidencialidad, integridad y disponibilidad.

Esta creación de un sistema de auditoría continua, apoyado en plataformas SIEM y en prácticas de Red Team/Blue Team, constituye un mecanismo indispensable para anticipar amenazas y responder a incidentes de ciberseguridad en tiempo real. Adicionalmente la cultura organizacional en ciberseguridad, promovida a través de la

capacitación en ciberhigiene y campañas de sensibilización, es un elemento clave para mitigar riesgos asociados a la ingeniería social y a la manipulación de credenciales.

La gobernanza del protocolo, sustentada en la articulación entre el Comando de Apoyo de Contrainteligencia Militar, la Dirección de Telemática, los centros de protección de datos y las unidades operativas, garantiza la sostenibilidad y legitimidad del modelo.

La implementación del protocolo propuesto no solo responde a necesidades operativas inmediatas, sino que también proyecta al Ejército Nacional hacia un escenario estratégico de modernización y alineación con estándares internacionales de ciberseguridad y ciberdefensa, consolidando así la confianza institucional y la resiliencia frente a amenazas emergentes.

Referencias

Asamblea Nacional Constituyente. (1991). Constitución Política de Colombia 1991. Bogotá, Colombia.

CEInterim. (2024, septiembre 27). *Comparación de las normas de ciberseguridad: EE. UU., Europa y Oriente Medio*. CE Interim. (2024, septiembre 27). *Comparación de las normas de ciberseguridad: EE. UU., Europa y Oriente Medio*. https://ceinterim.com/es/ciberseguridad-normas-ee-uu-europa-oriente-medio/?

Comando General de las Fuerzas Militares de Colombia. (2021, 19 de agosto). Civiles y militares validarán su identidad en línea para ingresar a las guarniciones en todo el país. https://www.cgfm.mil.co/es/multimedia/noticias/civiles-y-militares-validaran-su-identidad-en-linea-para-ingresar-las

Comisión Europea. (2017). European interoperability framework – implementation strategy. Publications Office of the European Union. https://doi.org/10.2799/78681

Congreso de Colombia. (2012). Ley 1581 de 2012: Protección de datos personales. Diario Oficial de la República de Colombia.

Congreso de la República de Colombia. (17 de abril de 2013). *Ley 1621 de 2013*. Función Pública — Gestor Normativo. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=52706

Contraloría General de la República de Colombia. (2022). *Misión y visión*. https://www.contraloria.gov.co/web/guest/mision-y-vision

Ejército Nacional de Colombia, (2017). *Actualización de datos estudio de seguridad personal funcionario público o contratista.* Ministerio de Defensa Nacional Comando General Fuerzas Militares Ejército Nacional Departamento de Inteligencia y Contrainteligencia [Documento Reservado].

Ejército Nacional de Colombia, (2022) Procedimiento definición situación militar, Proceso de Reclutamiento. [Documento reservado].

Ejército Nacional de Colombia. (2022). *Por presunta suplantación fue capturado un sujeto que pretendía ingresar a la Brigada 11 del Ejército*. https://www.ejercito.mil.co/por-presunta-suplantacion-fue-capturado-un-sujeto-que-pretendia-ingresar-a-la-brigada-11-del-ejercito/

Ejército Nacional de Colombia. (2023). MCE 3-37.33 Seguridad Militar.

Ejército Nacional de Colombia. (2023). *Redes de estafadores suplantan identidad de funcionarios del Ejército Nacional*. https://www.ejercito.mil.co/redes-de-estafadores-suplantan-identidad-de-funcionarios-del-ejercito-nacional/

Espitia-Cubillos, A. A., Agudelo-Calderón, J. A., & Ramírez-Contreras, T. (2021). Percepciones sobre innovaciones tecnológicas en el Ejército colombiano.

Revista Logos Ciencia & Tecnología, 13(2), 85–102. https://doi.org/10.22335/rlct.v13i2.1408

European Union. (2017). ISA²: New European Interoperability Framework—Promoting seamless services and data flows for European public administrations. https://doi.org/10.2799/360327

González, P. L. (2021). *Identidad digital*. Wolters Kluwer España. https://www.marcialpons.es/media/pdf/identidad.pdf

Herrera Guzmán, E. (2025). Inteligencia artificial y ciberseguridad: Transformación digital de la seguridad nacional en el siglo XXI / Artificial intelligence and cybersecurity: Digital transformation of national security in the 21st century. Revista Inclusiones – Revista de Humanidades y Ciencias Sociales, 12(3), 1–20. https://doi.org/10.58210/ri3639

Ho, A. (2022). Identidad digital. *Revista Ratio Legis*, *2*(4), 137–147. https://doi.org/10.61311/2953-2965.51

Hoffman, F. G. (2021). Hybrid Warfare and the Future of Conflict. Center for Strategic and International Studies (CSIS).

Hurtado Martos, J. Á. (2020). *La identidad digital, una herramienta para el desarrollo sostenible*. RAYDEM.

https://www.uco.es/docencia_derecho/index.php/RAYDEM/article/viewFile/219/272

International Organization for Standardization. (2023a). ISO/IEC 27037:2023 Guidelines for identification, collection, acquisition and preservation of digital evidence.

Migración Colombia. (s. f.). *Misión y visión*. https://www.migracioncolombia.gov.co/entidad/mision-y-vision

Muñoz Medina, L. (15 de mayo de 2025). *Corrupción en el Ejército: estos son los detalles de un esquema de extorsión que afectó a 37 soldados*. *Infobae.* https://www.infobae.com/colombia/2025/05/15/corrupcion-en-el-ejercito-estos-son-los-detalles-de-un-esquema-de-extorsion-que-afecto-a-37-soldados/

National Institute of Standards and Technology. (2020). Digital identity guidelines (NIST Special Publication 800-63-3). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-63-3

NATO Cooperative Cyber Defence Centre of Excellence. (2016). NATO CCDCOE strategy on cyber defence. Tallinn: CCDCOE Publications.

NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). (2023). Strategy and Doctrine in Cyberspace: Annual Report 2023. Tallinn: CCDCOE Publications

National Institute of Standards and Technology. (2017). NIST Special Publication 800-63-3: Digital Identity Guidelines. U.S. Department of Commerce.

National Institute of Standards and Technology. (2020). SP 800-207: Zero Trust Architecture. U.S. Department of Commerce.

National Institute of Standards and Technology. (2024). Cybersecurity Framework (CSF) 2.0. U.S. Department of Commerce.

OECD. (2011). *Digital identity management for natural persons: Enabling innovation and trust in the internet economy – Guidance for government policy makers* (OECD Digital Economy Papers, No. 186). [OCDE] Publishing. https://doi.org/10.1787/5kg1zqsm3pns-en

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

Policía Nacional de Colombia. (2024). *Dirección de Investigación Criminal e Interpol (DIJIN)*. https://www.policia.gov.co/jefatura-nacional-del-servicio-de-policia/dijin

Presidencia de la República. (2022). Directiva 02 de 2022: Lineamientos de la Presidencia de la República en materia de seguridad digital. Bogotá, Colombia.

Presidente de la República. (2015). Decreto 1070 de 2015: Sector Administrativo de Defensa. Diario Oficial de la República de Colombia.

Procuraduría General de la Nación de Colombia. (2024). *Misión y visión*. https://www.procuraduria.gov.co/procuraduria/conozca-entidad/Pages/mision-vision.aspx

Registraduría Nacional del Estado Civil. (2025). *Registro Civil e Identificación*. https://www.registraduria.gov.co/-Registro-Civil-e-Identificacion-798-.html

Remolina Angarita, N. (2022). Responsabilidad por el tratamiento de los datos personales de clientes, empleados, proveedores y terceros. SSRN. http://ssrn.com/abstract=5834

Rodríguez Sevilla, D. M. (2025, 24 de septiembre). *Por espionaje, detuvieron a dos militares y a una falsa oficial: intentaban acceder a datos estratégicos sobre el presidente Gustavo Petro*. Infobae. https://www.infobae.com/colombia/2025/09/24/detienen-a-dos-militares-y-una-falsa-oficial-por-intentar-acceder-a-datos-estrategicos-sobre-gustavo-petro-estas-son-las-identidades/

Salazar-Escorcia, L. S. (2020). Investigación cualitativa: Una respuesta a las investigaciones sociales educativas. *CIENCIAMATRIA: Revista Interdisciplinaria de Humanidades, Educación, Ciencia y Tecnología, 6*(11), 138–153. https://dialnet.unirioja.es/servlet/articulo?codigo=7390995

Vargas Borbúa, R., Reyes Chicango, R. P., & Recalde Herrera, L. (2017). Ciberdefensa y ciberseguridad, más allá del mundo virtual: Modelo ecuatoriano de gobernanza en ciberdefensa. *URVIO: Revista Latinoamericana de Estudios de Seguridad*, (20), 31–45. DOI: http://dx.doi.org/10.17141/urvio.20.2017.2571