
# Estrategias para la prevención de los ataques cibernéticos en el sistema de Talento Humano del Ejercito Nacional

Mayor Giovanny Ricardo Fuyo Rodríguez

Artículo para optar al título profesional:

Magister en Ciberseguridad y Ciberdefensa

Escuela Superior de Guerra “General Rafael Reyes Prieto”

Bogotá D.C., Colombia

2025

**Escuela Superior de Guerra "General Rafael Reyes Prieto"**

Bogotá D.C., Colombia

| DATOS GENERALES | | |
|---|---|---|
| Nombre del estudiante | : | Mayor Giovanny Ricardo Fuyo Rodríguez |
| Identificación | : | |
| Programa académico | : | Maestría en Ciberseguridad y Ciberdefensa |
| Tutor metodológico | : | |
| Tutor temático | : | |
| Fecha de entrega | : | |
| Extensión | : | 7.820 palabras |

**Escuela Superior de Guerra "General Rafael Reyes Prieto"**

Bogotá D.C., Colombia

# Estrategias para la prevención de los ataques cibernéticos en el sistema de Talento Humano del Ejercito Nacional

## Strategies for preventing cyberattacks in the National Army's Human Talent System

**Giovanny Fuyo Rodríguez**[1]
Escuela Superior de Guerra "General Rafael Reyes Prieto"

**Resumen:** La ciberseguridad se ha convertido en un tema de gran importancia para el ámbito militar, especialmente ante el aumento y la sofisticación de los ataques cibernéticos que amenazan las infraestructuras digitales de las Fuerzas Armadas. Estos ataques afectan directamente la comunicación, el manejo de datos sensibles y la confianza dentro de la institución. Entre las amenazas más comunes se encuentran el secuestro de información, la interrupción de servicios y la pérdida de datos críticos, todos ellos riesgos que comprometen no solo la seguridad nacional, sino también la moral del personal. Con la transformación digital, las organizaciones han adoptado nuevas tecnologías para optimizar sus procesos, pero esta modernización también ha abierto nuevas brechas de seguridad que requieren atención prioritaria. Es fundamental proteger la información mediante sistemas de encriptación, protocolos de respaldo y una formación continua en buenas prácticas de ciberseguridad. Aunque los ciberataques representan serios desafíos, también abren la oportunidad de fortalecer la infraestructura tecnológica, implementar plataformas digitales más seguras y fomentar una cultura de prevención y capacitación. Además, el trabajo conjunto con aliados estratégicos permite construir una respuesta más efectiva ante estas amenazas. En este contexto, el objetivo general de esta investigación es analizar el impacto de los ataques cibernéticos en el Sistema de Talento Humano del Ejército Nacional y proponer estrategias que permitan su prevención y mitigación. Para lograrlo, se seguirá una metodología de enfoque cualitativo y de tipo descriptivo, basada en la revisión sistemática de información relevante, que permitirá entender mejor el problema y plantear soluciones efectivas.

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

**Escuela Superior de Guerra “General Rafael Reyes Prieto”**

Bogotá D.C., Colombia

**Palabras clave:** Amenazas, Ciberseguridad, Datos Sensibles, Estrategias, Talento Humando

**Abstract:** Cybersecurity has become a topic of great importance for the military, especially given the increase and sophistication of cyberattacks that threaten the Armed Forces' digital infrastructure. These attacks directly affect communication, the handling of sensitive data, and trust within the institution. Among the most common threats are information hijacking, service interruptions, and the loss of critical data, all of which compromise not only national security but also personnel morale. With digital transformation, organizations have adopted new technologies to optimize their processes, but this modernization has also opened new security gaps that require priority attention. It is essential to protect information through encryption systems, backup protocols, and ongoing training in cybersecurity best practices. Although cyberattacks represent serious challenges, they also offer an opportunity to strengthen technological infrastructure, implement more secure digital platforms, and foster a culture of prevention and training. Furthermore, working together with strategic allies allows for a more effective response to these threats. In this context, the overall objective of this research is to analyze the impact of cyberattacks on the National Army's Human Talent System and propose strategies to prevent and mitigate them. To achieve this, a qualitative and descriptive methodology will be followed, based on the systematic review of relevant information, which will allow for a better understanding of the problem and the development of effective solutions.

**Keywords:** Threats, Cybersecurity, Sensitive Data, Strategies, Human Talent

**Escuela Superior de Guerra “General Rafael Reyes Prieto”**

Bogotá D.C., Colombia

## Introducción

La ciberseguridad se ha convertido en un tema crucial en el contexto militar global, dada la creciente amenaza de los ciberataques. En particular, las Fuerzas Armadas deben enfrentar retos significativos relacionados con la protección de su infraestructura digital, que no solo incluye sistemas de comunicaciones, sino también la gestión de datos sensibles y personales de sus miembros. Los ataques cibernéticos, como el secuestro de información, la interrupción de servicios y la pérdida de datos sensibles, son amenazas cada vez más sofisticadas que pueden afectar la operatividad y la confianza en los sistemas del Ejército Nacional. Sin embargo, cuando estos ataques se gestionan de manera efectiva, pueden ser empleados de forma benigna para mejorar la capacidad de defensa y fortalecer el sistema de talento humano de la institución.

En el contexto del avance tecnológico y la digitalización, es común pensar que las organizaciones, instituciones o empresas desempeñan un papel clave al integrar modelos tecnológicos en sus procesos productivos. Esto, motivado por el deseo de incrementar la productividad, tener un mayor control sobre los insumos, disponer de más datos para generar información estratégica a nivel gerencial y gestionar procesos que anteriormente eran manuales, lo que contribuye a reducir los errores humanos y contar con datos verificables en tiempo real desde una perspectiva administrativa (Guerra, s.f.).

En concordancia con lo anterior, es importante destacar que hoy en día, el concepto de transformación digital se ha convertido en un tema de gran relevancia para empresas,

instituciones y organizaciones a nivel global. El uso de nuevas tecnologías digitales para modificar las relaciones entre las personas, los procesos internos y las propuestas de valor es una realidad que muchas personas al frente de estos procesos han incorporado a su rutina diaria. Por otro lado, al observar el rápido avance de la adopción de tecnologías digitales en sus sectores, muchos han reconocido que el éxito de la transformación digital será crucial para determinar la competitividad futura de su empresa, institución u organización (González, 2021).

Dicho lo anterior, es importante destacar que estas nuevas tecnologías presentas unas brechas de seguridad y para hablar de ellas es necesario entonces definir qué se entiende por una brecha de seguridad, la cual se describe como un "incidente de seguridad que afecta a los datos personales". Esto puede suceder tanto por un evento provocado como por un accidente. Además, las brechas de seguridad pueden generar "destrucción, pérdida, alteración, divulgación o acceso no autorizado a datos personales" (AEPD, s.f.).

Por otro lado, el Reglamento General de Protección de Datos (RGPD), una medida clave para reforzar los derechos fundamentales de las personas en la era digital y facilitar la actividad económica, aclara las normas aplicables a empresas y organismos públicos dentro del mercado único digital (UE, 2016). Este reglamento ofrece una definición más técnica, considerando las brechas de seguridad como una "violación" que ocasiona la pérdida, alteración o destrucción ilícita o accidental de datos personales que se manejan de forma restringida.

Según la AEPD (Agencia Española de Protección de Datos), una "violación de seguridad de los datos personales" se define como "un incidente de seguridad que afecta a datos de carácter personal", independientemente de si es la consecuencia de un accidente o de una acción intencionada, y tanto si afecta a datos digitales o en formato papel. Además, estas violaciones pueden provocar "la destrucción, pérdida, alteración, comunicación o acceso no autorizado de datos personales" (AEPD, s.f.).

Ahora bien, con respecto a lo anterior, dentro de estas brechas podemos hacer referencia al secuestro de información, conocido también como ransomware, representa una de las amenazas más graves para las instituciones militares. Este tipo de ciberataque implica el cifrado de datos críticos y su posterior retención a cambio de un rescate. En el contexto militar, los datos comprometidos pueden incluir desde estrategias de operaciones hasta información personal de los miembros del Ejército. Esto no solo afecta la integridad de la información, sino que también puede tener repercusiones significativas en la seguridad nacional. Según un informe de la ONU (2018), "los ataques cibernéticos a infraestructuras críticas son una amenaza creciente para la seguridad nacional, afectando tanto la operatividad de las fuerzas armadas como la confianza pública en la protección de datos sensibles" (Naciones Unidas, 2018). El secuestro de información pone en evidencia la vulnerabilidad de las instituciones militares frente a cibercriminales organizados, lo que requiere una respuesta estratégica y constante vigilancia.

En este sentido, la protección de la información sensible del Ejército Nacional debe ser una prioridad. La implementación de sistemas de encriptación robustos, junto con una formación continua para el personal en cuanto a buenas prácticas de seguridad digital, son esenciales para mitigar el impacto de este tipo de ataques.

Hay que destacar también que otro tipo de ataque cibernético relevante es la interrupción de servicios, generalmente a través de ataques de denegación de servicio (DDoS). Este tipo de ataque tiene como objetivo saturar los servidores de una organización hasta dejarlos fuera de línea. En el ámbito militar, la interrupción de servicios puede afectar las comunicaciones y la capacidad de respuesta ante situaciones de emergencia, paralizando las operaciones o dificultando la toma de decisiones. Según González (2019), "la interrupción de los servicios digitales a través de ataques DDoS puede paralizar las capacidades operativas de una institución, afectando directamente la comunicación y coordinación de operaciones militares" (González, 2019). La capacidad de las fuerzas armadas para operar eficazmente depende en gran medida de la disponibilidad de sus sistemas digitales y la integridad de sus redes.

Sin embargo, la gestión adecuada de estas amenazas puede tener efectos positivos en la eficiencia del Ejército. A través de la implementación de sistemas de redundancia y la mejora de la infraestructura tecnológica, el Ejército Nacional puede fortalecer su resiliencia cibernética, aprendiendo de los ataques para prevenir futuras interrupciones. La adopción de

protocolos de respuesta rápida ante incidentes cibernéticos es un paso crucial en la creación de una infraestructura de defensa sólida.

La pérdida de datos sensibles, ya sea a través de un ataque cibernético o por errores internos, es una amenaza que pone en riesgo la privacidad de los miembros del Ejército y compromete la operatividad de las instituciones militares. En muchos casos, los datos perdidos pueden incluir información sobre la ubicación de tropas, planes de operaciones o información personal sensible de los militares. Según el Ministerio de Defensa Nacional (2019), "la pérdida de datos sensibles puede ser catastrófica para el Ejército Nacional, no solo porque compromete la seguridad, sino porque socava la confianza del personal en la protección de su información personal" (Ministerio de Defensa Nacional, 2019). Este tipo de vulnerabilidad no solo afecta la seguridad operativa, sino que también puede tener un impacto negativo en la moral del personal.

Para proteger los datos sensibles, es fundamental implementar políticas estrictas de protección de la información, que incluyan medidas como el almacenamiento seguro de datos, el uso de sistemas de respaldo confiables y protocolos de acceso restringido. La capacitación del personal en la gestión y protección de datos también es esencial para garantizar que cada miembro del Ejército comprenda la importancia de preservar la confidencialidad de la información.

A pesar de los riesgos asociados a los ciberataques, los incidentes también pueden ser utilizados de manera benigna para mejorar la infraestructura de talento humano del Ejército

Nacional. La gestión de los recursos humanos en una institución tan grande y compleja como el Ejército depende en gran medida de la efectividad de los sistemas informáticos. La capacitación continua en ciberseguridad es clave para que los miembros del Ejército comprendan los riesgos cibernéticos y adquieran las habilidades necesarias para mitigar estos peligros. González y Torres (2021) señalan que "la capacitación continua en ciberseguridad es esencial para fortalecer la resiliencia del personal militar ante posibles ciberataques, permitiéndoles detectar y mitigar riesgos antes de que causen daño" (González & Torres, 2021).

Además, la ciberseguridad puede mejorar la eficiencia de la gestión del talento humano, facilitando procesos como la asignación de tareas, la evaluación del desempeño y la planificación de las operaciones. La implementación de plataformas digitales seguras que almacenen la información sobre el personal permite que las decisiones sean más rápidas y basadas en datos confiables. Esto también contribuye a mejorar la transparencia y la eficiencia en el manejo de los recursos humanos.

En este sentido, los ciberataques representan una amenaza significativa para el Ejército Nacional, afectando la seguridad de la información y la operatividad de las fuerzas armadas. Sin embargo, cuando se gestionan adecuadamente, estos ataques pueden ser utilizados para fortalecer la infraestructura cibernética de la institución y mejorar la gestión del talento humano. La implementación de políticas de ciberseguridad, la capacitación

constante del personal y la inversión en tecnologías de protección son pasos fundamentales para garantizar que el Ejército Nacional esté preparado para enfrentar los retos del siglo XXI.

Como señala el informe de la OTAN (2020), "la colaboración internacional en materia de ciberseguridad es fundamental para compartir recursos y conocimientos, lo que fortalece la capacidad del Ejército Nacional para enfrentar las amenazas cibernéticas" (OTAN, 2020). De este modo, el Ejército puede no solo protegerse contra los ataques cibernéticos, sino también aprovechar estos desafíos para innovar y adaptarse a las nuevas realidades de la defensa nacional.

Respecto a lo anterior, se propone la siguiente pregunta de investigación: ¿Cómo afectan los ataques cibernéticos al Sistema de Talento Humano del Ejército Nacional y qué estrategias pueden reducir sus riesgos? Para responder esta pregunta inicialmente se identificaron los principales tipos de ataques cibernéticos en el Sistema de Talento Humando de la institución, seguido de ello, se hizo un análisis sobre el impacto de los ataques cibernéticos en el sistema de gestión del talento humano dentro de la institución y finalmente se proponen unas estrategias de prevención y mitigación para fortalecer la protección de los datos y la continuidad operativa del sistema.

Es de resaltar que respecto al objeto de estudio, el capítulo "Operaciones de interferencia en ciberseguridad y ciberdefensa: herramienta estratégica para la supervivencia de los Estados", publicado en el libro *Poder y estrategia* por la Escuela Superior de Guerra (ESDEG), resalta cómo las operaciones de interferencia en el ciberespacio se han convertido

en un recurso clave dentro de los conflictos contemporáneos. Estas operaciones no solo buscan neutralizar amenazas inmediatas, sino también garantizar la resiliencia digital y la capacidad de adaptación de los Estados frente a escenarios de guerra híbrida.

En este sentido, el texto enfatiza que el ciberespacio se convierte en un campo de confrontación donde lo material y lo inmaterial se entrelazan, permitiendo que actores estatales y no estatales influyan en la seguridad y en la percepción del poder. Para las Fuerzas Militares, particularmente el Ejército Nacional de Colombia, este análisis resulta pertinente, ya que integra la innovación tecnológica con la doctrina militar, orientando la construcción de capacidades que aseguren la continuidad operativa, la protección de la información crítica y la proyección estratégica en el marco de la defensa nacional (ESDEG, 2021).

Por su parte, el artículo "Ciberseguridad y ciberdefensa: pilares fundamentales de la Seguridad y Defensa Nacional", publicado por la Escuela Superior de Guerra, señala que la evolución de los conflictos hacia escenarios contemporáneos exige que los Estados transformen sus estrategias de defensa para integrar el ciberespacio como un ámbito central de acción. En el documento lo autores plantean que la conectividad y dependencia tecnológica moderna permiten no solo el flujo instantáneo de información, sino también su manipulación, infiltración o destrucción. Ante esta realidad, los Estados deben adoptar políticas de defensa robustas que incluyan la formulación de doctrina digital, estructuras organizacionales adaptadas y capacidades técnicas de ciberdefensa (Osorio et al., 2022). Esa propuesta está en consonancia con la necesidad de que el Ejército Nacional integre

doctrinalmente en su estructura militar las estrategias de protección digital (gestionando riesgos, entrenando al talento humano y dotando sistemas de resiliencia) como parte indisoluble de su misión institucional.

## Metodología

Esta investigación se llevará a cabo utilizando un enfoque cualitativo de carácter descriptivo, con el objetivo de analizar las amenazas cibernéticas que afectan al sistema de talento humano del Ejército Nacional. Como parte de la metodología, se realizará una revisión sistemática de literatura, una técnica ampliamente empleada en la investigación académica que, según Kitchenham y Carters (2007), tiene como fin recopilar y sintetizar la evidencia existente sobre un tema específico. En el contexto de este estudio, dicha evidencia se referirá a las amenazas cibernéticas que impactan los sistemas de gestión de talento humano en las instituciones militares.

El proceso de revisión sistemática se llevará a cabo en tres fases fundamentales, siguiendo el marco propuesto por Keele (2007). La primera fase será la planificación de la revisión, en la que se definirá el objetivo, los criterios de inclusión y exclusión, y la estrategia para la búsqueda de fuentes. En esta fase se establecerán las bases metodológicas que guiarán la selección de los documentos y la delimitación del alcance de la investigación. La fase de ejecución implicará la recolección activa de la literatura pertinente, evaluando la calidad de las fuentes y asegurando que cada documento seleccionado sea relevante y esté alineado con los objetivos del estudio. Finalmente, en la fase de análisis, se procederá a evaluar la

información recopilada, realizando una síntesis de los hallazgos y destacando los patrones recurrentes, tendencias y brechas existentes en la literatura respecto a las amenazas cibernéticas en el ámbito militar.

Dentro del contexto específico de este estudio, se prestará especial atención a las principales amenazas cibernéticas que afectan al sistema de talento humano, tales como el secuestro de información, la interrupción de servicios esenciales y la pérdida de datos sensibles. Estos riesgos no solo comprometen la información crítica de la institución, sino que también tienen repercusiones directas en la seguridad, el bienestar y la eficiencia operativa del personal militar. Según diversos estudios, la exposición inadecuada a vulnerabilidades digitales puede facilitar el acceso no autorizado a datos personales y profesionales de los miembros del Ejército, lo que podría resultar en pérdidas sustanciales en términos de confianza institucional y operacional (McAfee, 2018; Symantec, 2020).

La literatura también destaca que las organizaciones militares, al igual que otras instituciones que gestionan información confidencial, deben implementar mecanismos de seguridad robustos para mitigar los riesgos asociados a los ciberataques. Las estrategias de protección deben abarcar tanto las infraestructuras tecnológicas como las prácticas de seguridad cibernética a nivel individual y organizacional. Entre las medidas recomendadas se encuentran el cifrado de datos, la autenticación multifactor, la capacitación continua del personal sobre amenazas cibernéticas y la adopción de tecnologías de detección de intrusiones (Kaspersky, 2019; Talbot, 2019). Estas medidas no solo protegen los sistemas de

información, sino que también contribuyen a mantener la integridad de los procesos de selección, formación y administración del talento humano dentro del Ejército.

Para garantizar la validez y relevancia de los hallazgos, se establecerán criterios rigurosos de inclusión y exclusión en la selección de las fuentes documentales. Estos criterios permitirán asegurar que las fuentes seleccionadas sean de alta calidad, pertinentes y representativas del estado actual del conocimiento en el campo de la ciberseguridad en el ámbito militar. Se dará prioridad a estudios publicados en revistas académicas especializadas, informes de organismos internacionales de seguridad, y documentos técnicos de instituciones de referencia en ciberseguridad (como la Agencia Nacional de Ciberseguridad de los Estados Unidos, o la Unión Europea). De acuerdo con la metodología propuesta por Petticrew y Roberts (2006), se aplicará un enfoque sistemático para evaluar la fiabilidad y la relevancia de cada fuente antes de su inclusión en la revisión.

El análisis exhaustivo de los documentos seleccionados permitirá identificar las mejores prácticas, lecciones aprendidas y lagunas en la literatura existente en relación con las amenazas cibernéticas en el contexto de la gestión del talento humano en el Ejército Nacional. Este enfoque analítico permitirá no solo comprender las amenazas cibernéticas actuales, sino también proponer recomendaciones para mejorar las estrategias de protección, fortaleciendo las capacidades defensivas de la institución y asegurando la integridad y disponibilidad de los sistemas de información relacionados con el personal militar.

# Principales tipos de ataques cibernéticos que afectan al Sistema de Talento Humano del Ejército Nacional

El ciberespacio ha surgido en las últimas décadas como un nuevo dominio estratégico de influencia y confrontación, al mismo nivel que los dominios terrestre, marítimo, aéreo y espacial. Según Hughes (2010) y Dobbins et al. (2015), este entorno no solo reconfigura las dinámicas de conflicto y defensa tradicionales, sino que también plantea nuevos desafíos para la seguridad nacional, al ser un espacio en el que las amenazas pueden materializarse de manera instantánea y asimétrica. Ahora, como escenario operacional, el ciberespacio está definido por el Departamento de Defensa de los Estados Unidos (2006) como "un entorno operativo caracterizado por el uso de la electrónica y el espectro electromagnético para generar, almacenar, modificar, intercambiar y explotar información mediante sistemas interconectados y conectados a Internet, junto con sus infraestructuras asociadas". Esta definición subraya el carácter tecnológico y transfronterizo del ciberespacio, en donde las interacciones no se limitan por las fronteras físicas ni los marcos legales tradicionales.

Una de las características más relevantes del ciberespacio es su naturaleza no física: no existe en un espacio tangible, sino en redes de información que dependen de infraestructuras físicas, pero que trascienden las limitaciones geográficas. Además, es un espacio altamente dinámico, en constante transformación, moldeado por la innovación tecnológica y la creatividad humana (Nye, 2010). A diferencia de los espacios convencionales, el ciberespacio permite la participación activa tanto de actores estatales

como de actores no estatales como empresas privadas, organizaciones criminales, grupos terroristas, comunidades de hackers, e incluso individuos, quienes pueden ejercer influencia significativa en el ámbito global. Este bajo umbral de acceso altera profundamente la lógica tradicional de la seguridad internacional, donde antes la posesión de recursos materiales determinaba la capacidad de un actor de influir en el sistema internacional (Nye, 2004).

La accesibilidad del ciberespacio, combinada con su bajo costo de entrada y la dificultad para atribuir de manera certera los ataques, ha permitido la proliferación de amenazas de múltiples orígenes. La atribución en el ciberespacio se convierte en un problema crítico, dado que los atacantes pueden ocultar su identidad, operar a través de terceros países y explotar vulnerabilidades de sistemas sin necesidad de un despliegue físico de fuerzas. En este sentido, Nye (2010) advierte que el poder en el ciberespacio no depende únicamente de la posesión de tecnología avanzada, sino también de la capacidad de adaptarse rápidamente a las nuevas condiciones, explotar información y proteger la propia infraestructura digital.

En este escenario, los ciberataques constituyen una de las principales amenazas contemporáneas, afectando no solo la infraestructura crítica de los Estados, sino también su capital humano, las operaciones militares, los sistemas financieros, y las estructuras políticas y sociales. La multiplicidad de actores que operan en el ciberespacio desde Estados Nación hasta individuos aislados, complica la elaboración de estrategias de defensa y respuesta efectiva. De acuerdo con Klimburg y Healey (2012), esta realidad demanda un enfoque

integral de ciberseguridad que combine capacidades técnicas, jurídicas, diplomáticas y militares.

Además, el ciberespacio rompe los esquemas tradicionales de poder jerárquico. En los dominios clásicos de conflicto, los Estados más poderosos podían imponer su voluntad a través de medios materiales superiores (armas, ejército, territorio). En cambio, en el ciberespacio, el conocimiento técnico y la innovación se convierten en multiplicadores de poder, permitiendo que actores más pequeños y flexibles desafíen a Estados más grandes y poderosos (Klimburg, 2012). Incluso un individuo con habilidades avanzadas puede comprometer sistemas de alta seguridad, como han demostrado múltiples incidentes a lo largo de las últimas dos décadas.

Esta dispersión del poder en el ciberespacio tiene implicaciones profundas para la gestión de riesgos y la formulación de políticas de seguridad. Según Nye (2010), la "revolución de la información" está redistribuyendo el poder no solo entre Estados, sino también entre Estados y actores no estatales, modificando las reglas del juego en las relaciones internacionales. La competencia por el control de la información, el acceso a infraestructuras críticas y la capacidad de defender los propios sistemas se ha convertido en un componente central de la seguridad nacional.

Desde esta perspectiva, resulta importante reconocer que los ataques cibernéticos afectan no solo los sistemas tecnológicos, sino también los sistemas humanos, incluyendo el talento humano estratégico de las organizaciones, como sucede en el caso del Ejército

Nacional. La protección de datos personales, la integridad de los sistemas de información del personal y la continuidad de los procesos de gestión del talento humano son objetivos prioritarios para garantizar la resiliencia institucional frente a amenazas cibernéticas. La capacidad de prevenir, detectar, responder y recuperarse de un ciberataque no solo requiere soluciones tecnológicas, sino también la capacitación constante del personal, la formulación de políticas claras, y la cooperación interinstitucional.

Finalmente, en este entorno de incertidumbre permanente, la construcción de capacidades cibernéticas defensivas y ofensivas, así como el fortalecimiento de la resiliencia organizacional, se presentan como ejes fundamentales para enfrentar los riesgos asociados al ciberespacio. De este modo, la propuesta de estrategias de prevención y mitigación de ataques cibernéticos al sistema de talento humano del Ejército Nacional debe partir de una comprensión profunda de la naturaleza del ciberespacio, la tipología de actores involucrados, las dinámicas de poder que se configuran en este entorno y la necesidad de proteger no solo las infraestructuras, sino también el capital humano institucional.

La digitalización de las organizaciones y el almacenamiento de datos en línea han incrementado significativamente los delitos informáticos. En este contexto, la seguridad informática se ha convertido en un tema crucial para las organizaciones, que ahora deben incorporar medidas de protección en sus agendas. Esto implica realizar inversiones en equipos especializados, sistemas informáticos y ciberseguridad según el Reporte de Ciberseguridad Entel Ocean 2021-2022.

Este tema adquiere gran relevancia, ya que no solo la información de la organización está en riesgo, sino también los datos personales de sus empleados. Es aquí donde el área de Recursos Humanos debe poner especial atención, reforzando los protocolos de seguridad para proteger tanto los datos corporativos como los personales.

El ciberdelito se refiere a cualquier actividad delictiva realizada mediante dispositivos electrónicos y redes informáticas a través de internet. Los ciberataques varían desde el robo de identidad y datos hasta fraudes en línea, phishing, malware, entre otros. El impacto y el costo de un ciberataque en una organización dependen directamente de su tamaño. Las empresas pueden no ser conscientes de un ciberdelito o elegir no divulgarlo públicamente. Sin embargo, si dicho ataque afecta el servicio, la reputación de la marca o implica consecuencias legales, debe ser informado.

Un ciberataque puede ser devastador para una pequeña empresa, causar grandes pérdidas a una mediana y afectar seriamente la reputación de una gran empresa. En América Latina, los ciberataques han ido en aumento cada año. En 2022, países como Chile, Perú, México, Brasil y Colombia fueron los más afectados, siendo las industrias de retail, banca y energía las principales víctimas.

**Tipos de cibercrimen más comunes:**

- Phishing: Consiste en correos electrónicos o mensajes falsos que se hacen pasar por la empresa, engañando a los empleados para que proporcionen contraseñas y datos financieros.
- Ransomware: Se trata de un ataque en el que los archivos de la organización son cifrados, exigiéndose un pago para desbloquearlos. Si no se paga, la información puede perderse o ser publicada. Este es uno de los ataques más comunes, y en 2022, aproximadamente el 60% de las empresas fueron víctimas de uno.
- Ataques de ingeniería social: Manipulación de empleados para obtener información confidencial o vulnerar la seguridad de la empresa, aprovechando la confianza y la autoridad.
- Malware: Distribución de software malicioso a través de descargas en línea. Puede estar presente en correos electrónicos o dispositivos, y tiene la capacidad de robar datos, monitorear actividades y causar daños significativos.
- Ataques a dispositivos IoT: Con la creciente utilización del Internet de las Cosas (IoT), más empresas están expuestas a ataques cibernéticos si estos dispositivos no están debidamente asegurados, lo que podría permitir a los atacantes acceder a la red empresarial (Sopra, 2022).

El área de Recursos Humanos (RRHH) de cualquier empresa o institución ya sea pública o privada, desempeña un papel fundamental en la seguridad de la información dentro

de la organización. Su responsabilidad incluye garantizar la confianza, disponibilidad e integridad de los datos tanto de la empresa como de sus empleados. Por ello, es crucial que trabaje de manera estrecha con los equipos de ciberseguridad de la empresa. Una de las tareas clave de RRHH y ciberseguridad es evaluar conjuntamente los riesgos a los que podría enfrentarse la organización en la red. Será fundamental contar con una infraestructura digital adecuada, herramientas de seguridad y programas de capacitación que ayuden a identificar las amenazas cibernéticas (AdelantTa, 2024).

Por lo anterior, también las empresas son sensibles de que se cometan errores humanos en ciberseguridad, según un informe del Foro Económico Mundial de 2022, el 95% de los incidentes de ciberseguridad se originan por errores humanos, lo que resalta la necesidad de políticas estrictas y capacitación continua para reducir estos riesgos. Aunque se cuente con las mejores soluciones técnicas, el comportamiento de los empleados sigue siendo el eslabón más vulnerable en la cadena de seguridad. En el entorno actual, donde la digitalización y el trabajo a distancia son cada vez más comunes, los errores humanos en ciberseguridad se han convertido en una de las principales amenazas para las empresas. Un simple descuido, como permitir que un familiar use un dispositivo de trabajo o enviar un correo a la dirección equivocada, puede generar incidentes graves (World Economic Forum, 2022)

En concordancia con lo anterior, los errores más frecuentes cometidos por los empleados que afectan la ciberseguridad de las empresas incluyen:

- *Acceso no autorizado:* Permitir que personas no autorizadas utilicen dispositivos de trabajo representa un riesgo significativo para la seguridad de la información y la protección de datos sensibles. Esto puede tener consecuencias graves, como:
- *Exposición de datos sensibles:* Si alguien no autorizado accede a un dispositivo con información confidencial, esta puede ser vista, copiada o robada.
- *Vulnerabilidad a ciberataques:* Un usuario no autorizado podría instalar software malicioso, comprometiendo la seguridad del dispositivo y la red. Esto podría generar ataques más graves.
- *Incumplimiento normativo:* Muchos sectores tienen regulaciones estrictas sobre quién puede acceder a ciertos datos. Permitir el acceso no autorizado podría resultar en violaciones de estas normativas, lo que podría generar multas, sanciones y daños a la reputación de la empresa.

Además de lo anterior, hay que resaltar que la exposición a datos sensibles, también juega un papel fundamental a la hora de identificar riesgos toda vez que cuando una persona no autorizada accede a un dispositivo de trabajo, la exposición a datos sensibles es una de las principales amenazas. Algunos ejemplos incluyen:

- *Datos personales de clientes:* La información personal, como nombres, direcciones, números de identificación, detalles de tarjetas de crédito o

información médica, es altamente valiosa. Su exposición puede llevar a fraudes, robos de identidad o venta en mercados ilegales.

- *Información financiera:* Datos como estados financieros, presupuestos, información bancaria y registros de transacciones pueden ser utilizados para fraudes financieros, manipulación de operaciones, entre otros.
- *Propiedad intelectual:* La información sobre productos en desarrollo, estrategias de mercado, investigaciones y diseños exclusivos es vital para mantener la competitividad de una empresa. Su exposición puede ocasionar la pérdida de ventajas competitivas y daño irreparable a la posición en el mercado.
- *Consecuencias legales y regulatorias:* La exposición de datos sensibles puede violar regulaciones como el Reglamento General de Protección de Datos (GDPR), lo que podría resultar en multas y daños a la reputación de la empresa.

Además de lo descrito anteriormente, la reutilización de contraseñas en múltiples sitios puede poner en peligro varios servicios en caso de una filtración de dato, un ejemplo de ello es que si una contraseña utilizada para acceder al correo corporativo es filtrada en la dark web, un atacante podría usarla para acceder a otros sistemas de la empresa. En complemento, existe un coste de una filtración de datos que de conformidad con lo arrojado en el informe "Cost of a Data Breach 2023" de IBM, el costo promedio de una filtración de datos en 2023 fue de 4.45 millones de dólares, lo que representa un aumento del 15% en tres

años. Además de las pérdidas financieras, las violaciones de datos pueden dañar irreparablemente la reputación de una empresa (Crouse, 2023).

Otro aspecto que es importante mencionar es la exposición de interfaces remotas, aunque hay que decir también que la administración remota de sistemas es una herramienta útil para el trabajo a distancia y la gestión de infraestructura, también plantea riesgos para la seguridad, algunos de estos riesgos incluyen algunos de los que ya se mencionaron anteriormente como el acceso no autorizado, si las interfaces remotas no están adecuadamente protegidas, pueden ser blanco de ataques para obtener acceso no autorizado a sistemas críticos.

La exposición de credenciales, es decir que las credenciales de administración remota pueden ser capturadas o comprometidas si no se protegen adecuadamente; los ataques de intermediario (Man-in-the-Middle), esto quiere decir que sin cifrado adecuado, las comunicaciones remotas pueden ser interceptadas y manipuladas por atacantes, además, un software desactualizado puede tener vulnerabilidades que, si no se actualizan, pueden ser explotadas y finalmente que se hagan configuraciones incorrectas, en este aspecto una administración remota mal configurada puede abrir la puerta a accesos no deseados o permitir operaciones inseguras (He, Xu y Zhang, 2015).

En términos más precisos, los ciberataques son intentos de acceder, robar, modificar o destruir datos sensibles o dañar una red a través de un acceso no autorizado. Según CheckPoint, estos ataques aumentaron un 50% a nivel mundial en 2021 en comparación con

el año anterior. Estas amenazas están diseñadas para causar perjuicios a las empresas, e incluso a veces a países enteros, como parte de la ciberguerra. A continuación, en la siguiente tabla se presentan algunos de los tipos de ciberataques más comunes

**Tabla 1**

Tipos de ciberataques

| Tipo de ciberataque | Descripción | Impacto principal |
|---|---|---|
| **Denegación de servicio (DoS/DDoS)** | El DoS busca cerrar un sitio web mediante tráfico masivo; el DDoS utiliza múltiples dispositivos para generar aún más tráfico y colapsar la red. | Inaccesibilidad de servicios web, afectación operativa y pérdidas económicas. |
| **Malware** | Software malicioso como virus, gusanos o spyware que se introduce en la red aprovechando vulnerabilidades. | Robo, daño o pérdida de datos; afectación a la integridad de sistemas. |
| **Phishing** | Engaño a usuarios para que revelen datos sensibles mediante correos, llamadas o mensajes que simulan ser de entidades legítimas. | Robo de credenciales, fraudes financieros y suplantación de identidad. |
| **Inyección SQL** | Inserción de código malicioso en consultas SQL para acceder a bases de datos sin autorización. | Exposición de información confidencial, como datos personales y financieros. |
| **Amenaza interna** | Empleados o ex empleados que usan su acceso autorizado para causar daño. | Filtración de información, daños reputacionales y pérdidas económicas. |

Nota: Elaboración propia con datos de (Jaimovich, 2024)

De la tabla anterior, es importante resaltar que el Ejército Nacional enfrenta amenazas digitales que van más allá de los riesgos típicos de instituciones civiles. Cada tipo de ciberataque expuesto en el cuadro tiene implicaciones estratégicas que pueden afectar directamente tanto la operatividad como el bienestar del personal militar.

1. **DoS/DDoS:** Los ataques de denegación de servicio, especialmente los DDoS de alto volumen y corta duración, representan una amenaza capaz de paralizar sistemas clave con una eficacia devastadora. En 2025, Cloudflare bloqueó ataques récord de hasta 7.3 Tbps, lanzados en ráfagas de tráfico de apenas 45 segundos, lo que evidencia la velocidad y potencia de estas agresiones y la necesidad de defensas automatizadas permanentes. Para las Fuerzas Armadas, esto subraya la urgencia de contar con redes resilientes y respuestas rápidas que protejan los canales de mando y comunicación crítica (Cloudflare. 2025).
2. **Malware:** El software malicioso sigue siendo una puerta de entrada peligrosa para infiltraciones y sabotajes. Históricamente, ciberataques como *Stuxnet* han demostrado el potencial destructivo de estas amenazas en entornos militares. Aunque no se consignó aquí, se reconoce ampliamente el impacto de tales ataques en infraestructuras estratégicas.
3. **Phishing (incluyendo spear phishing):** Este ataque se basa en la manipulación psicológica para extraer información confidencial. El grupo ruso Fancy Bear, por ejemplo, utilizó spear phishing para acceder a correos del equipo de campaña de Hillary Clinton en 2016. En el ejército, altos mandos o personal administrativo pueden convertirse en blanco, lo que resalta la necesidad de formación continua en ciberseguridad y protocolos claros ante enlaces o comunicaciones sospechosas (Wilson, 2019).

4. **Inyección SQL:** Aunque menos visible, este tipo de ataque representa un riesgo en sistemas de información militar que gestionan datos logísticos o de personal. La manipulación de consultas SQL puede exponer información confidencial crítica, como datos de operaciones o movimiento de tropas. La protección de estas bases de datos requiere especial atención.
5. **Amenaza interna:** El riesgo interno (personas autorizadas que actúan maliciosamente) puede vulnerar incluso los sistemas más seguros. En contextos militares, donde la confianza y la disciplina son esenciales, la existencia de brechas internas es especialmente delicada. La institución debe fortalecer no solo sus protocolos técnicos, sino también su cultura de integridad y monitoreo (Satter, Donn y Day, 2017).

Teniendo en cuenta lo anterior, es esencial que Recursos Humanos entregue a los empleados documentos sobre las políticas de ciberseguridad para garantizar la protección de la información y evitar el mal uso de los datos personales. Estos documentos deben ser firmados por los empleados al momento de su contratación. Dado que RRHH maneja una gran cantidad de datos sensibles, como información financiera y personal de los empleados, es importante que el personal de esta área reciba capacitación constante. Además, es recomendable que se organicen cursos y talleres que ayuden a los colaboradores a desempeñar sus funciones con bajos riesgos en términos de ciberseguridad (Greenlee, 2023)

A pesar de la creciente importancia de la ciberseguridad, menos del 41% de las empresas implementan políticas efectivas de protección y actualizan sus sistemas y software. Esto las deja vulnerables a posibles ciberataques. Actuar rápidamente es esencial, ya que menos del 16% de los ataques son corregidos en un corto período, lo que incrementa los riesgos para las empresas. Una gestión ágil de los incidentes cibernéticos puede reducir significativamente los daños y los costos asociados. Es crucial que las empresas busquen herramientas y recursos adaptados a sus necesidades para fomentar la conciencia sobre la ciberseguridad, tanto en el entorno presencial como remoto. La protección de los datos hoy será un alivio en el futuro, tanto para las organizaciones como para sus empleados.

En el caso del Ejército Nacional, esta realidad adquiere un matiz aún más crítico, es decir, si en el sector empresarial como se mencionó anteriormente, menos del 41% de las organizaciones implementa políticas efectivas de protección y actualización de sistemas, se puede dimensionar el riesgo que enfrentan instituciones estratégicas como las Fuerzas Militares, donde la información que se gestiona no solo es sensible, sino vital para la seguridad nacional. La falta de protocolos de ciberseguridad sólidos y en constante actualización puede dejar expuesto al Sistema de Talento Humano a ataques como el secuestro de datos, la filtración de información personal del personal militar o la interrupción de plataformas que soportan la gestión administrativa.

Según el informe *SecOps by the Numbers: 30 Cybersecurity Stats That Matter*, en 2023 el tiempo medio para responder a un incidente de seguridad (MTTR) entre

organizaciones que utilizan inteligencia artificial y automatización fue de 58 minutos, mientras que las que emplean mecanismos tradicionales tardaron 2.3 días en promedio (ReliaQuest. 2024)

Estos datos sugieren que una respuesta lenta, como la que emplean muchos sectores sin herramientas avanzadas (2.3 días o más), sería inadecuada en un entorno militar donde la seguridad y la continuidad operativa son esenciales. Para el Ejército Nacional, una demora en reaccionar ante un ciberataque no solo podría comprometer datos sensibles y procesos fundamentales, sino también poner en riesgo la vida del personal y la defensa nacional.

Por tanto, es imperativo implementar una estructura de ciberseguridad ágil y especializada, que incorpore sistemas automatizados de detección y respuesta inmediata. Solo de esta manera se puede garantizar la protección efectiva de la información, el talento humano y la misión institucional en un entorno digital insidioso.

Por tanto, la implementación de herramientas y recursos tecnológicos adaptados a las necesidades del Ejército Nacional se vuelve indispensable. No se trata únicamente de invertir en sistemas de protección, sino también de generar conciencia en todos los niveles jerárquicos de la institución sobre la importancia de la ciberseguridad, fomentando una cultura de prevención tanto en el trabajo presencial como en los escenarios remotos. De esta manera, se garantiza no solo la protección de datos sensibles, sino también la continuidad operativa y la confianza del personal militar en la gestión de su información. En última

instancia, fortalecer la ciberseguridad hoy representa un alivio y una garantía de estabilidad institucional en el futuro.

### *Protocolos a seguir por Recursos Humanos*

Para mitigar estos riesgos, es esencial implementar políticas de acceso rigurosas, utilizar autenticación multifactor y capacitar a los usuarios en prácticas de seguridad.

**Tabla 2**

Medidas para mitigar el riesgo

| **Acción** | **Descripción** |
|---|---|
| **Monitoreo continuo** | Supervisar dispositivos y sistemas en tiempo real para detectar accesos no autorizados de manera temprana. |
| **Resguardo de equipos** | Asegurar que los dispositivos usados en teletrabajo tengan medidas de seguridad (antivirus, firewalls, cifrado) y copias de seguridad de la información. |
| **Inventarios de información sensible** | Mantener un registro actualizado de los datos confidenciales y sus ubicaciones (nube, dispositivos, áreas internas). |
| **Accesos únicos** | RRHH debe registrar a las personas con permisos especiales para acceder a información confidencial. |
| **Accesos generales** | Monitorear cambios de contraseñas de empleados y validar que no superen las políticas de seguridad establecidas. |
| **Monitoreo de usuarios con privilegios** | Supervisar el uso de dispositivos e información por parte de empleados con accesos especiales para evitar riesgos de mal uso. |
| **Concientización** | Implementar programas de capacitación en ciberseguridad, difusión de políticas y formación en detección de amenazas. |
| **Controles de acceso y auditorías** | Aplicar controles estrictos, cifrado de datos, políticas claras de acceso y auditorías periódicas para prevenir fugas o accesos indebidos. |

*Nota*: Elaboración propia

En complemento del cuadro anterior, es fundamental seguir buenas prácticas de seguridad, como:

- Utilizar contraseñas únicas para cada cuenta o servicio.
- Implementar autenticación multifactor (MFA) para añadir una capa adicional de seguridad.
- Utilizar gestores de contraseñas que generen y almacenen contraseñas fuertes y únicas.
- Educar a los empleados sobre la importancia de la seguridad de contraseñas y las mejores prácticas.

## Impacto de los ataques en la seguridad de la información y la gestión del talento humano dentro del Ejército Nacional

En el contexto actual, la transformación digital se ha posicionado como un tema central para empresas, instituciones y organizaciones a nivel global, pues la incorporación de tecnologías digitales con el propósito de modificar la interacción entre las personas, los procesos internos y las propuestas de valor, se ha convertido en una práctica habitual para muchos líderes organizacionales. En virtud de ello, al observar el vertiginoso avance del uso de estas tecnologías en cada uno de los sectores, se ha comprendido que la competitividad futura de las entidades dependerá en buena medida del éxito con que logren adoptar la transformación digital (González, 2021). En este sentido, resulta fundamental abordar el fenómeno de la cuarta revolución industrial, resaltando que esta se encuentra caracterizada

por la convergencia de tecnologías digitales que están borrando las fronteras entre los ámbitos físico, digital y biológico. Elementos como la inteligencia artificial, los vehículos autónomos, el internet de las cosas, el aprendizaje automático, los drones, el reconocimiento facial, la impresión 3D, el Big Data, la biología sintética y la ecología industrial, entre otros, ya forman parte del entorno cotidiano y están transformando radicalmente la manera en que vivimos, trabajamos y nos relacionamos.

En el contexto contemporáneo de transformación digital, el Ejército Nacional, al igual que muchas organizaciones de carácter público y privado, enfrenta nuevos desafíos derivados de la adopción acelerada de tecnologías digitales sin una evaluación rigurosa del nivel de madurez tecnológica ni de las capacidades del talento humano. Este fenómeno genera lo que puede denominarse *riesgos de oportunidad incierta*, pues la incorporación de tecnologías sin planificación estratégica ni personal calificado conlleva vulnerabilidades críticas en los sistemas de información y en la operatividad institucional (Rodríguez, 2020).

Es de resaltar que en instituciones como el Ejército Nacional, donde la información se constituye como un activo estratégico vital para la seguridad y defensa nacional, la materialización de ciberataques representa un riesgo no solo tecnológico, sino operativo y estructural. Por lo anterior, hay que mencionar un tema que es muy importante como las brechas de seguridad digital que representan un impacto en la seguridad y que pueden comprometer la integridad, confidencialidad y disponibilidad de datos altamente sensibles, tales como planes operacionales, datos biométricos, ubicación de tropas o información de

inteligencia. Esto afecta directamente la capacidad de reacción, planificación táctica y toma de decisiones estratégicas, pilares fundamentales del poder militar moderno (Mozo & Ardila, 2022).

Por ello, uno de los principales retos en este escenario es el fortalecimiento de las capacidades humanas en ciberseguridad dentro del Ejército Nacional. La falta de personal calificado para enfrentar amenazas persistentes, como el *ransomware*, las denegaciones de servicio (*DoS*) o los ataques de tipo *phishing*, limita la respuesta institucional ante incidentes críticos. Además, la transformación de los esquemas de trabajo (que incluyen modalidades híbridas, trabajo remoto y digitalización de procesos administrativos) ha dejado obsoletas muchas de las medidas tradicionales de protección de la información (Arroyo, 2021).

En el contexto colombiano, las estadísticas recientes evidencian la magnitud de la amenaza cibernética pues según datos del Ministerio de las Tecnologías de la Información (TIC) y el ColCERT (Equipo de Respuesta a Emergencias Cibernéticas de Colombia) en tan solo un mes y medio, se recibieron 36 reportes de ataques, siendo la suplantación de sitios web (19 casos) y de dominios de correo electrónico (8 casos) las modalidades más frecuentes (MinTIC, 2023). Estos hechos reflejan la urgencia de contar con mecanismos de monitoreo y alerta temprana más robustos dentro de las instituciones estatales, incluyendo al Ejército Nacional, cuya información sensible de personal y operaciones resulta un blanco estratégico de alto valor.

Por su parte, el Centro Cibernético Policial (CCP) ha consolidado un papel protagónico en la gestión de incidentes cibernéticos a través de su CAI Virtual que es un canal habilitado para recibir denuncias ciudadanas 24/7. El CCP reportó que en 2022 se registraron 54.121 denuncias por delitos cibernéticos, lo que representó un incremento del 79% respecto al año 2021. Las modalidades más comunes fueron el fraude bancario y la suplantación de identidad (Impacto TIC, 2022). Estos datos confirman que los ataques digitales no solo afectan a individuos y empresas privadas, sino también a las instituciones públicas y militares, donde la confianza y la integridad de la información son vitales para la seguridad nacional.

El impacto de los ciberataques sobre la gestión del talento humano se manifiesta en varios niveles. En primer lugar, se requiere un perfil profesional con competencias técnicas avanzadas en seguridad informática, gestión de riesgos y respuesta a incidentes. Sin embargo, el déficit de formación y capacitación especializada genera una brecha estructural, impidiendo el desarrollo de una cultura institucional orientada a la ciberdefensa. En segundo lugar, la carga emocional y cognitiva que enfrentan los funcionarios responsables de mitigar ciberincidentes afecta su bienestar laboral, generando estrés, fatiga decisional y sobrecarga operativa, elementos que también deben ser gestionados desde el enfoque del talento humano (González, 2021).

En complemento de lo anterior, las políticas de ciberseguridad adoptadas por las instituciones armadas en Colombia han avanzado con iniciativas como la Directiva de

Seguridad de la Información 00221 de 2017, la cual establece responsabilidades en materia de seguridad digital dentro del Ejército Nacional. Sin embargo, su implementación ha sido desigual y muchas veces insuficiente para enfrentar amenazas de alta complejidad. Esto ha llevado a que algunos ataques hayan comprometido datos institucionales, obligando a reconfigurar redes, suspender servicios o incluso modificar operaciones en curso (Ministerio de Defensa Nacional, 2017).

Por lo tanto, resulta importante adoptar un enfoque de seguridad basada en el conocimiento, en el que se promueva la formación continua del personal, el fortalecimiento de capacidades técnicas, y la sensibilización de todos los niveles jerárquicos frente a los riesgos digitales. La seguridad no debe asumirse como una configuración predeterminada, sino como una práctica dinámica, transversal y sostenible dentro del ecosistema institucional (Ambit, 2022).

Es de destacar que los ataques a la seguridad de la información en el Ejército Nacional no solo comprometen infraestructuras digitales, sino que también ponen en evidencia la necesidad urgente de fortalecer la gestión estratégica del talento humano como eje central de la ciberdefensa. La combinación entre tecnología, educación y cultura organizacional será clave para reducir vulnerabilidades, responder de manera efectiva y mantener la soberanía digital institucional.

## Estrategias de prevención y mitigación para fortalecer la protección de los datos y la continuidad operativa del sistema

La protección de los datos y la continuidad operativa en el Sistema de Talento Humano del Ejército Nacional de Colombia exige una estrategia integral que articule aspectos tecnológicos, organizacionales y humanos. La complejidad del entorno digital contemporáneo, sumada a la criticidad de la información que gestiona esta fuerza pública, hace imperativa la implementación de medidas sólidas de ciberseguridad.

Tan es así que hacia 2030, los conflictos armados tradicionales estarán profundamente interconectados con el ciberespacio y las operaciones híbridas (que combinan acciones convencionales, irregulares y cibernéticas) serán el modelo dominante de confrontación. En este sentido, actores estatales y no estatales emplearán ciberataques coordinados con operaciones físicas para desestabilizar a sus adversarios, paralizar infraestructuras críticas, desinformar a la población y degradar la moral de las fuerzas armadas. En este escenario, los ejércitos que no integren la ciberdefensa como parte sustantiva de su doctrina quedarán en una posición de desventaja estratégica.

Colombia, por su ubicación geopolítica y sus retos de seguridad interna, podría enfrentar hacia 2030 conflictos que combinen:

- Ataques a infraestructuras críticas (energía, telecomunicaciones, transporte militar).
- Campañas de desinformación dirigidas a socavar la legitimidad institucional y la moral de la tropa.
- Exfiltración de datos sensibles del talento humano militar, incluyendo identidad, ubicación y operaciones.

- Amenazas internas y actores criminales que aprovechen vulnerabilidades digitales para debilitar la seguridad nacional.

Sin embargo para afrontar estas amenazas, a continuación, se abordan las estrategias más efectivas para prevenir y mitigar los riesgos asociados a los ciberataques, tomando como base buenas prácticas nacionales e internacionales, así como recomendaciones especializadas en ciberdefensa gubernamental.

1. **Fortalecimiento del modelo de seguridad de la información:** Una primera línea de defensa es la consolidación de un modelo robusto de gestión de la seguridad de la información (SGSI), alineado con estándares como la ISO/IEC 27001, que permite establecer políticas, procedimientos y controles técnicos que aseguren la confidencialidad, integridad y disponibilidad de los datos. Este modelo debe ser aplicado transversalmente en todas las unidades responsables de la gestión del talento humano, garantizando así una respuesta homogénea y eficiente frente a posibles amenazas (ICONTEC, 2020).

   Además, debe incorporarse un enfoque de análisis de riesgos periódicos que identifique vulnerabilidades tanto técnicas como organizacionales. La gestión de estos riesgos debe permitir tomar decisiones fundamentadas respecto a la priorización de inversiones en seguridad, la adopción de tecnologías específicas o el rediseño de procesos sensibles.

2. **Segmentación y control de acceso a la información:** Una estrategia clave en la protección de datos es la segmentación lógica de redes y la gestión granular de permisos. Esto implica que no todos los usuarios dentro del sistema tengan acceso indiscriminado a toda la información, sino que se delimiten privilegios conforme al principio de menor privilegio (least privilege). En el caso del Ejército Nacional, donde se manejan perfiles sensibles, historias clínicas, información patrimonial y trayectoria de los efectivos, el acceso debe ser limitado y monitoreado de forma continua (Sánchez et al., 2022). Esta segmentación debe complementarse con herramientas de autenticación multifactor (MFA), contraseñas robustas, cifrado de datos en reposo y en tránsito, así como la implementación de políticas de sesión seguras (tiempos de inactividad, cierres automáticos y monitoreo de accesos sospechosos).
3. **Actualización tecnológica y sistemas de detección de amenazas:** La actualización permanente de software, sistemas operativos y firmware constituye una práctica básica pero crítica. Muchos ataques exitosos se producen por vulnerabilidades conocidas no corregidas. Por tanto, el Ejército debe implementar procesos automatizados de gestión de parches, así como soluciones de detección y respuesta ante amenazas (EDR – Endpoint Detection and Response) que analicen comportamientos anómalos en tiempo real (Arbeláez, 2023). De igual forma, los sistemas de información que soportan el talento humano deben incluir firewalls avanzados, sistemas de prevención de intrusos (IPS), y SIEM (Security Information

and Event Management) para correlacionar eventos y generar alertas tempranas que permitan una reacción inmediata frente a ataques como el ransomware o el phishing dirigido.

4. **Cultura organizacional y formación continua:** Un eslabón fundamental en la estrategia de prevención es el factor humano. Se ha demostrado que una alta proporción de incidentes de seguridad ocurren por errores humanos, negligencia o desconocimiento de los usuarios (ENISA, 2023). Por ello, es crucial establecer una cultura organizacional de ciberseguridad, acompañada de campañas pedagógicas constantes. El Ejército Nacional debe estructurar programas de formación diferenciada: desde entrenamientos básicos para todo el personal administrativo hasta capacitaciones especializadas en ciberseguridad para los encargados de TI. Deben incluirse simulacros de respuesta ante ataques, talleres de manejo de incidentes, y formación en detección de correos maliciosos, suplantación de identidad, ingeniería social, entre otros (Mendoza & Rodríguez, 2022). Una estrategia efectiva es la gamificación del aprendizaje, mediante herramientas que simulen amenazas reales y evalúen la capacidad de reacción del personal. Esto no solo fortalece la conciencia situacional, sino que permite monitorear el progreso y corregir errores recurrentes.
5. **Plan de continuidad operativa y recuperación ante desastres:** La continuidad del sistema en caso de incidente requiere de planes estructurados de recuperación que estén actualizados y probados. En este sentido, debe existir un Plan de Continuidad del Negocio (BCP) y un Plan de Recuperación ante Desastres (DRP) adaptados al

sistema de talento humano. Estos documentos deben definir roles, tiempos de respuesta, responsables y procedimientos para restaurar los servicios críticos ante diferentes escenarios de ataque (MinDefensa, 2021). Es recomendable la implementación de centros de respaldo geográficamente distribuidos, con capacidad para asumir la operación de manera inmediata, y con respaldos automáticos cifrados y verificados periódicamente. Asimismo, los sistemas deben contar con redundancia de servidores, mecanismos de failover y monitoreo de rendimiento constante.

6. **Gobernanza, auditoría y cumplimiento normativo:** La estrategia de prevención debe estar sostenida por una estructura de gobernanza clara, con responsabilidades definidas, canales de reporte y rendición de cuentas. Es importante que el Ejército cuente con un Comité de Seguridad de la Información, que tome decisiones estratégicas, supervise incidentes y valide inversiones en ciberseguridad. La auditoría periódica, tanto interna como externa, permite asegurar el cumplimiento de estándares y detectar posibles brechas. Asimismo, es indispensable el alineamiento con el Marco Nacional de Ciberseguridad del Ministerio TIC y con lo establecido por el Documento CONPES 3995 de 2020, que orienta la política nacional en materia de ciberseguridad y ciberdefensa (MinTIC, 2020). Estas auditorías también deben incluir el cumplimiento de las normas de protección de datos personales, particularmente la Ley 1581 de 2012, garantizando el adecuado tratamiento de la información sensible que se encuentra en poder del Ejército.

7. **Colaboración interinstitucional e inteligencia de amenazas:** La ciberseguridad en el sector defensa no puede abordarse de forma aislada. El Ejército Nacional debe fomentar la colaboración interinstitucional con otras ramas de la Fuerza Pública, organismos de inteligencia, entidades del Estado y actores internacionales. Esta cooperación permite el intercambio de información sobre amenazas, la detección temprana de actores maliciosos y la adopción de buenas prácticas conjuntas (González & Trujillo, 2022). En este contexto, se destaca la importancia de participar activamente en redes de inteligencia de amenazas (Threat Intelligence Sharing) y en foros de ciberseguridad regional como el CSIRT gubernamental de Colombia. Además, se debe promover la articulación con el Centro Cibernético Policial, que ya cuenta con experiencia en manejo de incidentes cibernéticos en el sector público.
8. **Innovación y resiliencia digital:** Por último, la estrategia debe apuntar a la resiliencia digital, entendida como la capacidad del sistema de talento humano para resistir, adaptarse y recuperarse de los ataques cibernéticos sin perder su operatividad. Para ello, se debe fomentar una cultura de innovación permanente, en la que se evalúe la adopción de tecnologías como inteligencia artificial, blockchain para trazabilidad de datos y automatización de respuestas ante incidentes (Caballero & Díaz, 2021). El fortalecimiento de laboratorios de ciberdefensa dentro del Ejército, así como la creación de alianzas con universidades, centros de investigación y empresas tecnológicas, puede aportar a una visión prospectiva que anticipe nuevas amenazas y prepare mejor al sistema.

**Tabla 3**

Matriz Estratégica de Protección de Datos y Continuidad Operativa en el Sistema de Talento Humano del Ejército Nacional

| Ejes Estratégicos | Acciones Propuestas | Impacto Esperado |
|---|---|---|
| **Fortalecimiento del modelo de seguridad de la información (SGSI)** | Implementar políticas y controles bajo ISO/IEC 27001; realizar análisis de riesgos periódicos; priorizar inversiones en seguridad. | Asegurar la confidencialidad, integridad y disponibilidad de la información; decisiones basadas en riesgos. |
| **Segmentación y control de acceso** | Definir privilegios según el principio de menor privilegio; aplicar autenticación multifactor, cifrado de datos y monitoreo constante. | Reducción de accesos indebidos y protección de información sensible (ej. datos patrimoniales, historias clínicas, trayectoria del personal). |
| **Actualización tecnológica y detección de amenazas** | Automatizar gestión de parches; implementar EDR, SIEM, firewalls e IPS. | Prevención de ataques basados en vulnerabilidades; respuesta temprana a ransomware y phishing dirigido. |
| **Cultura organizacional y formación continua** | Programas de capacitación diferenciados; simulacros de ciberataques; gamificación del aprendizaje. | Disminución de errores humanos; mayor conciencia situacional en el personal. |
| **Plan de continuidad operativa y recuperación ante desastres (BCP/DRP)** | Elaborar y probar planes de continuidad; implementar respaldos cifrados, redundancia y failover. | Capacidad de restablecer servicios críticos rápidamente tras un incidente. |
| **Gobernanza y cumplimiento normativo** | Crear Comité de Seguridad de la Información; realizar auditorías internas y externas; alinearse con CONPES 3995/2020 y Ley 1581/2012. | Transparencia, rendición de cuentas y cumplimiento normativo nacional e internacional. |
| **Colaboración interinstitucional e inteligencia de amenazas** | Articulación con Fuerza Pública, MinTIC, CSIRT y Centro Cibernético Policial; participación en redes internacionales de inteligencia. | Fortalecimiento de la ciberdefensa nacional y capacidad de anticipación de amenazas. |

| | | |
|---|---|---|
| **Innovación y resiliencia digital** | Evaluar uso de IA, blockchain y automatización de respuestas; alianzas con universidades y centros de investigación. | Mayor resiliencia y adaptación a amenazas emergentes; desarrollo de laboratorios de ciberdefensa propios. |

*Nota:* Elaboración propia

En síntesis, la implementación de esta matriz estratégica proporciona un marco de referencia para gestionar los riesgos asociados a la ciberseguridad y la continuidad operativa en el Sistema de Talento Humano. Al articular acciones tecnológicas, formativas y de gobernanza, la institución fortalece la protección de datos sensibles, asegura la operatividad de procesos críticos y promueve una cultura organizacional orientada a la resiliencia, la innovación y el cumplimiento normativo, consolidando así su capacidad de respuesta ante amenazas y eventos imprevistos.

## Conclusiones

El estudio desarrollado evidencia que el ciberespacio se ha consolidado como un escenario estratégico de confrontación en el que los Estados y sus instituciones enfrentan amenazas constantes. Para el Ejército Nacional de Colombia, el Sistema de Talento Humano representa un activo crítico cuya vulneración puede comprometer no solo la operatividad de la institución, sino también la confianza, moral y bienestar de su personal. A partir del análisis de los tipos de ataques, su impacto en la gestión de la información y las estrategias de

mitigación, se presentan las siguientes conclusiones, que buscan integrar hallazgos técnicos, organizacionales y humanos en una visión integral de la ciberseguridad militar.

Del primer apartado se puede concluir que los ciberataques más recurrentes, tales como el phishing, el malware, los ataques de denegación de servicio (DoS/DDoS), la inyección SQL y las amenazas internas, constituyen riesgos directos para la estabilidad y la operatividad del Sistema de Talento Humano. Estas modalidades no se limitan a comprometer la infraestructura tecnológica, sino que buscan específicamente vulnerar la información sensible del personal militar, lo cual afecta la integridad, confidencialidad y disponibilidad de los datos. La facilidad de acceso al ciberespacio, la dificultad para atribuir responsabilidades y la capacidad de actores no estatales para generar daños significativos convierten al Ejército en un objetivo estratégico. De este modo, se concluye que los ataques cibernéticos deben ser comprendidos no solo como un fenómeno tecnológico, sino también como un factor de riesgo operacional y estratégico que exige respuestas adaptativas, constantes y sostenidas en el tiempo.

Frente al apartado de los impactos de los ataques en la seguridad de la información es importante decir que ese impacto trasciende lo meramente tecnológico y alcanza directamente la gestión del talento humano, al poner en riesgo datos personales, historias clínicas, información patrimonial y trayectorias profesionales de los miembros de la institución. La pérdida, manipulación o filtración de esta información compromete la confianza institucional, afecta la moral de la tropa, disminuye la disciplina interna y puede

repercutir en la continuidad de operaciones estratégicas. Además, la falta de protocolos claros y de personal especializado incrementa la vulnerabilidad ante incidentes de alta complejidad, generando sobrecarga operativa y estrés en quienes tienen la responsabilidad de dar respuesta. En consecuencia, se concluye que la ciberseguridad no debe abordarse únicamente como una cuestión de protección de infraestructuras digitales, sino como un pilar esencial en la protección del capital humano militar, cuya estabilidad y confianza son fundamentales para el cumplimiento de la misión institucional.

Respecto al apartado de las estrategias de prevención, hay que decir que el análisis confirma que las estrategias propuestas son indispensables para enfrentar los retos que plantea el ciberespacio. Medidas como el fortalecimiento del modelo de seguridad de la información (SGSI) bajo estándares internacionales, la segmentación y control de accesos, la actualización tecnológica permanente y la detección temprana de amenazas constituyen una base sólida para la protección de los datos. Sin embargo, estas medidas técnicas deben complementarse con la creación de una cultura organizacional de ciberseguridad que promueva la capacitación constante, la concienciación en todos los niveles jerárquicos y la preparación frente a escenarios de ataque. De igual manera, la articulación entre el área de Recursos Humanos y los equipos especializados en ciberdefensa es esencial para asegurar que las medidas implementadas trasciendan lo técnico y se conviertan en prácticas institucionales integrales. Solo mediante esta gestión multidimensional será posible garantizar la resiliencia digital, la continuidad operativa y la protección estratégica de la información del personal militar.

En síntesis, los hallazgos de esta investigación confirman que el Sistema de Talento Humano del Ejército Nacional es un objetivo de alto valor en el ciberespacio, donde los ataques cibernéticos ponen en riesgo tanto la infraestructura digital como el capital humano de la institución. La identificación de las principales amenazas, el análisis de sus impactos y la formulación de estrategias de prevención y mitigación permiten concluir que la ciberseguridad no es un componente accesorio, sino un eje estructural de la seguridad y defensa nacional. Fortalecer las capacidades técnicas, humanas y organizacionales, junto con la articulación interinstitucional, resulta indispensable para anticipar, enfrentar y superar los desafíos emergentes de un entorno digital cada vez más hostil. De esta manera, la institución podrá garantizar la protección de sus miembros, la continuidad de sus procesos estratégicos y la consolidación de su soberanía en el ámbito digital.

## Referencias (APA séptima edición)

Centro Criptológico Nacional. (2021). Guía CCN-STIC 819. Gestión de incidentes de ciberseguridad. https://www.ccn-cert.cni.es/publicaciones/guias-ccn-stic.html

Cloudflare. (2025). Cloudflare mitigates one of the largest DDoS attacks on record. Cloudflare. https://blog.cloudflare.com/tag/ddos/

Departamento de Defensa de los Estados Unidos de América. (2006). National Military Strategy for Cyberspace Operations. https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf

Dobbins, J., McGinn, J. G., Crane, K., Jones, S. G., Lal, R., Rathmell, A., & Swanger, R. D. (2015). America's Role in Nation-Building: From Germany to Iraq. RAND Corporation. https://www.jstor.org/stable/10.7249/mr1753rc

ENISA. (2022). Threat Landscape for Ransomware Attacks. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications

Foro Económico Mundial. (2022). Global Cybersecurity Outlook 2022. World Economic Forum. https://www.weforum.org/reports/global-cybersecurity-outlook-2022

González, M. (2019). Ciberseguridad en el ámbito militar: riesgos y medidas preventivas. Bogotá: Editorial Defensa.

González, M., & Torres, J. (2021). Estrategias de formación en ciberseguridad en las fuerzas armadas. Bogotá: Ministerio de Defensa.

Guerra, R. (s.f.). Digitalización del Recurso Humano. Gestión Humana. https://revistaempresarial.com/gestion-humana/digitalizacion-del-recurso-humano/

Hernández, F., & Martínez, C. (2020). Ciberseguridad en el Ejército Nacional: Desafíos y estrategias. Bogotá: Ministerio de Defensa.

Hughes, J. (2010). The Military's Role in Cybersecurity: A Policy Framework. Center for Strategic and International Studies.

Hughes, R. (2010). Cyberpower in strategic affairs. Routledge.

IBM Security. (2023). Cost of a Data Breach Report 2023. IBM. https://www.ibm.com/reports/data-breach

Impacto TIC. (2022, 26 de julio). *Ciberseguridad en Colombia: Riesgos a los que se enfrenta el país*. Impacto TIC. https://impactotic.co/ciber-seguridad/ciberseguridad-en-colombia-riesgos-a-los-que-se-enfrenta-el-pais/

Instituto Nacional de Ciberseguridad (INCIBE). (2023). Guía de continuidad de negocio y gestión de crisis para organizaciones. https://www.incibe.es

Jaimovich, D. (2024). Tipos de ciberataques más comunes y cómo prevenirlos. Forbes Colombia. https://forbes.co

Keele, S. (2007). Guidelines for performing systematic literature reviews in software engineering. EBSE Technical Report. https://www.cs.auckland.ac.nz/~ian/SE751A/Handouts/SLRGuidelines.pdf

Kitchenham, B., & Charters, S. (2007). Guidelines for performing systematic literature reviews in software engineering. EBSE Technical Report, Keele University. https://www.elsevier.com/__data/promis_misc/525444systematicreviewsguide.pdf

Klimburg, A., & Healey, J. (2012). Strategic cooperation in cyberspace: New avenues for U.S.-Japan alliance. Center for a New American Security. https://www.cnas.org/publications/reports/strategic-cooperation-in-cyberspace

Ministerio de Defensa Nacional. (2019). Informe sobre la modernización de la infraestructura tecnológica en el Ejército Nacional. Bogotá: Ministerio de Defensa.

MinTIC. (2023, 9 de junio). *ColCERT recibió 36 reportes de ataques cibernéticos en mes y medio*. Ministerio de Tecnologías de la Información y las Comunicaciones. https://mintic.gov.co/portal/715/w3-article-273464.html

Naciones Unidas. (2018). La ciberseguridad y su impacto en la defensa nacional. Nueva York: Naciones Unidas.

North Atlantic Treaty Organization – OTAN. (2020). La ciberseguridad en la defensa: buenas prácticas y cooperación internacional. Bruselas: OTAN.

Nye, J. S. (2004). Soft power: The means to success in world politics. Public Affairs.

Nye, J. S. (2010). Cyber power. Harvard Kennedy School. https://www.belfercenter.org/publication/cyber-power

OAS – Organización de los Estados Americanos, & BID – Banco Interamericano de Desarrollo. (2020). Ciberseguridad: Riesgos, avances y el camino a seguir en América Latina y el Caribe. https://publications.iadb.org/es/ciberseguridad-riesgos-avances-y-el-camino-seguir-en-america-latina-y-el-caribe

Pérez, R. (2020). Estrategias de ciberdefensa en las Fuerzas Armadas. Revista Militar, 34(4), 150–162.

Sánchez, J., & Pérez, R. (2020). Impacto psicológico de los ataques cibernéticos en los miembros del Ejército. Revista Militar, 34(2), 112–130.

Talana. (2023). Recursos Humanos y problemas de ciberseguridad en empresas. Talana Blog. https://web.talana.com/blog/recursos-humanos-y-problemas-de-ciberseguridad-en-empresas

Vásquez, S. (2021). La protección de datos sensibles en las Fuerzas Armadas. Bogotá: Editorial Seguridad.