

Capítulo 6

El intercambio de información de ciberseguridad y ciberdefensa en las Fuerzas Militares de Colombia*

DOI: <https://doi.org/10.25062/9786287818705.06>

Diego Edison Cabuya Padilla

Hernán Darío Ochoa Góez

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: El presente capítulo analiza los métodos actuales y propuestos para el intercambio de información en el ámbito de la ciberseguridad y la ciberdefensa, con especial énfasis en su aplicación en las Fuerzas Militares de Colombia. Se abordan, en primer lugar, los fundamentos del intercambio de información desde la perspectiva de la ciberseguridad, la ciberdefensa, la ciberinteligencia y las amenazas en redes, destacando la importancia de proteger la información clasificada en contextos operacionales y estratégicos. Posteriormente, se estudian prácticas internacionales empleadas por Fuerzas Militares de otros Estados, evidenciando modelos como el estadounidense y el brasileño, junto con sus estructuras de intercambio, clasificación, operaciones y capacidades tecnológicas. En paralelo, se analiza el sistema colombiano: su evolución normativa, institucional y doctrinal, así como los desafíos en interoperabilidad, gestión del riesgo y articulación interagencial. Como contribución central, se presenta una propuesta conceptual de método de intercambio de información cibernética, estructurada sobre seis componentes clave: marco normativo y doctrinal, criterios técnicos de clasificación, sistema nacional de intercambio, plataforma digital interoperable, gobernanza institucional y esquema de confianza compartida. La propuesta responde a la necesidad de anticiparse a amenazas emergentes, proteger infraestructuras críticas y articular los niveles estratégico, operacional y táctico de la ciberdefensa nacional.

Palabras clave: ciberdefensa, ciberinteligencia, ciberseguridad, intercambio de información cibernética, riesgos cibernéticos.

* Este capítulo de libro presenta los resultados del proyecto de investigación titulado "La Gobernanza del Ciberespacio: Desafíos y Oportunidades en procura de la autonomía y el control en el entorno Digital", vinculado a la línea de investigación Tecnología e Innovación en Defensa, del grupo de investigación "Ciberespacio, Tecnología e Innovación", de la Escuela Superior de Guerra "General Rafael Reyes Prieto", categorizado como 'C' por MinCiencias y con código de registro COL0181179. Los puntos de vista pertenecen a los autores, y no necesariamente reflejan los de las instituciones participantes.

Diego Edison Cabuya Padilla

Doctor en Ciencias del Mar con énfasis en ciberseguridad y ciberdefensa marítima, Escuela Naval de Cadetes “Almirante Padilla”, Colombia. Magíster en Gestión Logística y en Gestión de la Información. Ingeniero Electrónico. Administrador de Empresas. Profesional en Ciencias Navales. Docente e investigador, Escuela Naval de Cadetes y de la Escuela Superior de Guerra. Investigador asociado de MinCiencias

<https://orcid.org/0000-0001-5338-9943> - Contacto: diego.cabuya@esdeg.edu.co

Hernán Darío Ochoa Góez

Magíster en Ciberseguridad y Ciberdefensa, y magíster en Seguridad y Defensa Nacionales, Escuela Superior de Guerra “General Rafael Reyes Prieto”, Colombia. Profesional en Relaciones Internacionales y Estudios Políticos, Universidad Militar Nueva Granada, Colombia. Oficial de Inteligencia Naval de la Armada Nacional.

<https://orcid.org/0009-0007-8979-1521> - Contacto: hernan.ochoa@armada.mil.co

Citación APA: Cabuya Padilla, D. E. & Ochoa Góez, H. D. (2026). El intercambio de información de ciberseguridad y ciberdefensa en las Fuerzas Militares de Colombia. En C. E. Álvarez Calderón (Ed.), *El campo de batalla digital: la defensa nacional en la era algorítmica, Volumen I. (Infraestructuras de la guerra digital: computación, ciber-guerra y defensa del ciberespacio)* (pp. 379-408). Sello Editorial ESDEG.
<https://doi.org/10.25062/9786287818705.06>

EL CAMPO DE BATALLA DIGITAL: LA DEFENSA NACIONAL EN LA ERA ALGORÍTMICA

VOLUMEN I. INFRAESTRUCTURAS DE LA GUERRA DIGITAL: COMPUTACIÓN, CIBERGUERRA Y DEFENSA DEL CIBERESPACIO

ISBN IMPRESO (Obra completa): 978-628-7818-65-1

ISBN DIGITAL (Obra completa): 978-628-7818-69-9

ISBN IMPRESO Volumen I: 978-628-7818-66-8

ISBN DIGITAL Volumen I: 978-628-7818-70-5

DOI: <https://doi.org/10.25062/9786287818705>

Colección Seguridad y Defensa

Sello Editorial ESDEG

Escuela Superior de Guerra “General Rafael Reyes Prieto”

Bogotá D.C., Colombia

2026



Introducción

El ciberespacio ha desdibujado las fronteras tradicionales, y se ha consolidado como un nuevo dominio de confrontación estratégica donde los Estados y sus fuerzas militares enfrentan amenazas cibernéticas orientadas a desestabilizar sus intereses. En dicho escenario, la ciberdefensa ha sido incorporada a la agenda de seguridad nacional como responsabilidad directa de las fuerzas armadas, dadas las implicaciones operacionales, económicas, políticas y sociales de posibles ataques.

Las ciberamenazas —como el ciberespionaje, el terrorismo digital y la ciberde-lincuencia— representan riesgos transnacionales que superan incluso los conflictos armados tradicionales. Los ataques cibernéticos, difíciles de atribuir, pueden afectar gravemente la seguridad nacional y causar daños irreversibles a infraestructuras críticas (IC) y sistemas de información. En Colombia estos sistemas, particularmente los de uso militar, se hallan expuestos a riesgos crecientes, debido a la necesidad de mantener información clasificada disponible en entornos vulnerables.

Para hacer frente a este desafío, el país ha avanzado en el desarrollo de capacidades institucionales como el Comando Conjunto Cibernético (CCOCI) y el Grupo de Respuesta a Emergencias Cibernéticas (ColCERT), creados para prevenir, detectar y responder a amenazas informáticas. No obstante, persisten desafíos estructurales como la escasez de recursos, la limitada interoperabilidad entre agencias y la necesidad de fortalecer la cooperación internacional.

Conceptualmente, la respuesta nacional se apoya en tres pilares: la ciberseguridad, orientada a proteger la confidencialidad, integridad y disponibilidad de la información; la ciberdefensa, centrada en la protección de infraestructuras estratégicas, y la ciberinteligencia, enfocada en la identificación y anticipación de amenazas de origen ciberterrorista.

A pesar de estos avances, el volumen y la sensibilidad de la información que se genera y circula diariamente en el entorno de la defensa nacional hacen imperativo

montar mecanismos seguros, estructurados y ágiles para su intercambio. Según el informe *X-Force Threat Intelligence Index*, de IBM (2025), Colombia es uno de los países más vulnerables de la región frente a ciberataques, junto con Argentina, Chile y Brasil.

En respuesta, Colombia ha reforzado su marco de cooperación internacional. En 2013 suscribió un acuerdo con la Organización del Tratado del Atlántico Norte (OTAN) sobre seguridad de la información, desde 2016 participa activamente en el Foro Iberoamericano de Defensa Cibernética y en 2024 entró oficialmente al Centro de Competencia Cibernética de América Latina y el Caribe (LAC4). Todas ellas son participaciones de Colombia en contextos internacionales que promueven el intercambio de conocimientos en la materia.

Estos antecedentes evidencian la urgencia de implementar un método seguro y estandarizado de intercambio de información, alineado con las necesidades operacionales y los protocolos vigentes. La tendencia regional confirma que las Fuerzas Armadas están priorizando la inversión en capacidades de ciberseguridad, no como medida reactiva, sino como un enfoque preventivo frente a amenazas persistentes (Cornaglia & Vecelli, 2017).

En el contexto descrito, la presente investigación propone un método para optimizar el intercambio de información de ciberseguridad y ciberdefensa entre las Fuerzas Militares de Colombia. Su propósito es mejorar los procesos operacionales mediante la estandarización de mecanismos seguros y eficaces, fortalecer la base institucional de conocimiento y contribuir al desarrollo de capacidades cibernéticas alineadas con las exigencias estratégicas del país.

El objetivo central es identificar las bases de un modelo conceptual viable de intercambio de información que pueda ser adoptado operacionalmente por las Fuerzas Militares. En este marco se plantea la siguiente pregunta de investigación: ¿Qué método de intercambio de información de ciberseguridad y ciberdefensa debería adoptar Colombia para sus Fuerzas Militares?

El intercambio de información desde la ciberseguridad, la ciberdefensa, la ciberinteligencia y las amenazas de las redes de información

La globalización y los retos del siglo XXI han introducido al ciberespacio como un nuevo dominio de confrontación, donde convergen los intereses estratégicos de los Estados y sus fuerzas militares con amenazas que buscan desestabilizar el orden institucional mediante el uso malicioso de las redes de información

(Cabuya-Padilla & Castaneda-Marroquin, 2024). En tal escenario, los sistemas de información de las Fuerzas Militares de Colombia se enfrentan a un riesgo creciente, dado que su exposición constante a redes digitales —imprescindible para asegurar la disponibilidad y actualización de información— también incrementa su vulnerabilidad. Esta información, en su mayoría, tiene carácter confidencial y es clave para el funcionamiento institucional y la seguridad nacional.

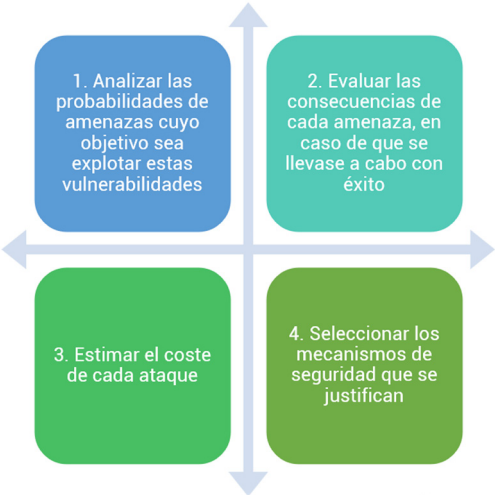
Para comprender la relevancia del ciberespacio y del intercambio seguro de información en el ámbito militar, se propone un marco conceptual que articula la ciberseguridad, la ciberdefensa y la ciberinteligencia, con el objetivo de analizar y enfrentar las amenazas que afectan directamente la integridad, disponibilidad y confidencialidad de las redes de información de las Fuerzas Militares.

La ciberinteligencia

La ciberinteligencia surge como una necesidad estratégica en un entorno intangible —el ciberespacio— que, si bien facilita las interacciones sociales y operativas, también representa un campo de riesgos latentes para la seguridad y defensa nacionales. Su función esencial es recolectar, procesar y analizar información que permita identificar actores hostiles, como ciberterroristas, sus capacidades y objetivos, para anticipar posibles ataques y proteger la infraestructura crítica del Estado.

La figura 1 ilustra las principales medidas de ciberinteligencia orientadas a identificar vulnerabilidades y desafíos en el sistema.

Figura 1. Medidas desde la ciberinteligencia para identificar las vulnerabilidades y desafíos del sistema



Fuente: elaboración propia, con base en (UIT, 2015).

Según Enrique Cubeiro (2016, pág. 50), la ciberinteligencia se sustenta en el reconocimiento del ciberespacio como la mayor fuente de datos provenientes de fuentes abiertas. Las herramientas empleadas permiten obtener información según parámetros complejos, incluso desde la web profunda, apoyando el ciclo de inteligencia mediante funciones como traducción automática, geolocalización y representación gráfica de relaciones entre identidades digitales.

Complementariamente, Gruszczak (2016) amplía esta visión al destacar que la ciberinteligencia opera sobre fuentes tanto abiertas como cerradas, lo cual reafirma su papel estratégico en la vigilancia proactiva del ciberespacio. Ante incidentes de ciberseguridad, esta disciplina resulta crucial para rastrear el origen de las amenazas, interpretar sus implicaciones y generar escenarios de respuesta que faciliten la toma de decisiones en contextos de crisis.

La ciberseguridad y la ciberdefensa

La ciberseguridad se entiende como el conjunto organizado de medidas destinadas a prevenir, evitar y minimizar potenciales daños a redes y sistemas de información propios (Ganuza, 2020). En el contexto del Estado, dicha disciplina resulta decisiva para garantizar el resguardo de la información crítica en entornos cada vez más digitalizados y expuestos a amenazas complejas y persistentes.

El Manual de Seguridad de las TIC, del Centro Criptológico Nacional, define la ciberseguridad como “las medidas para proteger la información almacenada, procesada o transmitida por los Sistemas de Información, de manera que se aseguren o garanticen la confidencialidad, integridad y disponibilidad de la información y la integridad y disponibilidad de los propios sistemas” (Centro Criptológico Nacional, 2021).

La gestión de la seguridad de los datos no se limita únicamente al plano técnico. Implica también considerar aspectos como la seguridad personal, la protección de instalaciones, la salvaguarda de documentación y la integridad de los propios sistemas TIC. La ciberseguridad, en ese sentido, adquiere un rol operativo, al asegurar el funcionamiento continuo de los sistemas de información frente a amenazas de tipo ciberterrorista o ataques deliberados.

Por su parte, la ciberdefensa se define como el uso de las “capacidades militares ante amenazas cibernéticas, ataques cibernéticos o ante actos hostiles de naturaleza cibernética que afecten la sociedad, la soberanía nacional, la independencia, la integridad territorial, el orden constitucional o los intereses nacionales” (Departamento Nacional de Planeación, 2017). Esta capacidad va más allá de la

protección pasiva de la información, al integrar una dimensión activa, estratégica y táctica en la defensa de infraestructuras críticas, redes militares y plataformas tecnológicas frente a ciberataques sofisticados.

La figura 2 presenta la clasificación de las capacidades de ciberdefensa, y destaca los distintos niveles y componentes que conforman una arquitectura de defensa efectiva en el ciberespacio.

Figura 2. Clasificación de las capacidades de la ciberdefensa



Fuente: elaboración propia, con base en Organización Tratado Atlántico Norte (OTAN, 2016).

Tipos de información en ciberseguridad y ciberdefensa

En el marco de las operaciones de ciberseguridad y ciberdefensa, es fundamental distinguir los distintos tipos de información que sirven de insumo para la toma de decisiones estratégicas y operacionales. Esta información se clasifica principalmente en dos enfoques: inteligencia cibernética y ciberinteligencia.

En primer lugar, la *inteligencia cibernética* se refiere a la información necesaria para el funcionamiento, mantenimiento y mejora de los sistemas de protección y defensa cibernética. Según el Instituto Nacional de Ciberseguridad de España (INCIBE, 2018), esta puede categorizarse en cinco tipos esenciales:

- Indicadores de compromiso (IoC): evidencias técnicas de que un sistema ha sido vulnerado o está siendo atacado, como direcciones IP maliciosas, firmas de *malware* o patrones de tráfico anómalo.
- Técnicas, Tácticas y Procedimientos (TTPs): conocimiento detallado de los métodos utilizados por los atacantes para planear y ejecutar ciberataques.
- Alertas de seguridad: notificaciones que advierten sobre vulnerabilidades activas, amenazas emergentes o campañas de ataques en curso.
- Informes de inteligencia de amenazas: análisis más elaborados sobre el contexto, motivación, capacidades y objetivos de los actores hostiles.
- Información generada automáticamente por herramientas de seguridad: datos obtenidos en tiempo real por sistemas de detección de intrusos, *firewalls* o antivirus, entre otros.

En segundo lugar, el enfoque de *ciberinteligencia* amplía el espectro de análisis al integrar la recopilación de información táctica y estratégica del ciberespacio, orientada a objetivos militares específicos. Esta incluye los mismos elementos de la inteligencia cibernética, pero los adapta y extiende según los requerimientos operacionales, y así permite anticipar movimientos del adversario, evaluar vulnerabilidades en IC y fortalecer capacidades defensivas en tiempo real.

Ambos tipos de información deben ser gestionados por plataformas automáticas de intercambio y análisis, diseñadas para procesar grandes volúmenes de datos y facilitar su distribución oportuna. Estas plataformas de inteligencia sobre amenazas deben permitir:

- La correlación de indicadores entre actores institucionales.
- El almacenamiento seguro de información crítica.
- La generación de conocimiento útil para acciones preventivas y de detección temprana.

Este tipo de arquitectura colaborativa facilita construir una red de cooperación nacional sobre amenazas cibernéticas, con miras a una respuesta coordinada, efectiva y basada en evidencia ante ataques dirigidos.

Ciberamenazas

El ciberespacio ha redefinido las dinámicas del sistema internacional, e impulsado así el desarrollo de nuevas tecnologías y fomentado el uso masivo de internet. Sin embargo, dicha transformación ha generado nuevos desafíos de seguridad que afectan a todos los actores, en particular a los Estados. Entre tales desafíos se destacan el ciberespionaje, las operaciones de grupos terroristas, la ciberdelincuencia y la protección de infraestructuras críticas, todos ellos en expansión dentro de un entorno altamente digitalizado y deslocalizado.

Las amenazas cibernéticas dificultan la atribución de responsabilidades, debido a su capacidad para ejecutarse desde cualquier parte del mundo y a través de múltiples capas de ocultamiento. Como señaló el exfiscal Jesús Cardenal en 2019, “la comunicación en redes entre terroristas y los sabotajes informáticos son delitos que crecerán un 10.000 %” (Escuela Superior de Guerra., 2019). Esta advertencia anticipaba el crecimiento exponencial del cibercrimen y su complejidad operativa.

Los Estados son blanco habitual de ciberataques provenientes de otros actores estatales o no estatales, motivados por intereses políticos, económicos, geoestratégicos o militares. Estos ataques presentan ventajas tácticas para los ofensores: bajo costo, alto impacto potencial, baja exposición directa y dificultad para atribuirlos. Incluso, la infraestructura tecnológica de un tercer país puede ser empleada como plataforma intermedia para ejecutar el ataque, lo cual refuerza el anonimato del agresor (Villalba, & Corchado, 2017).

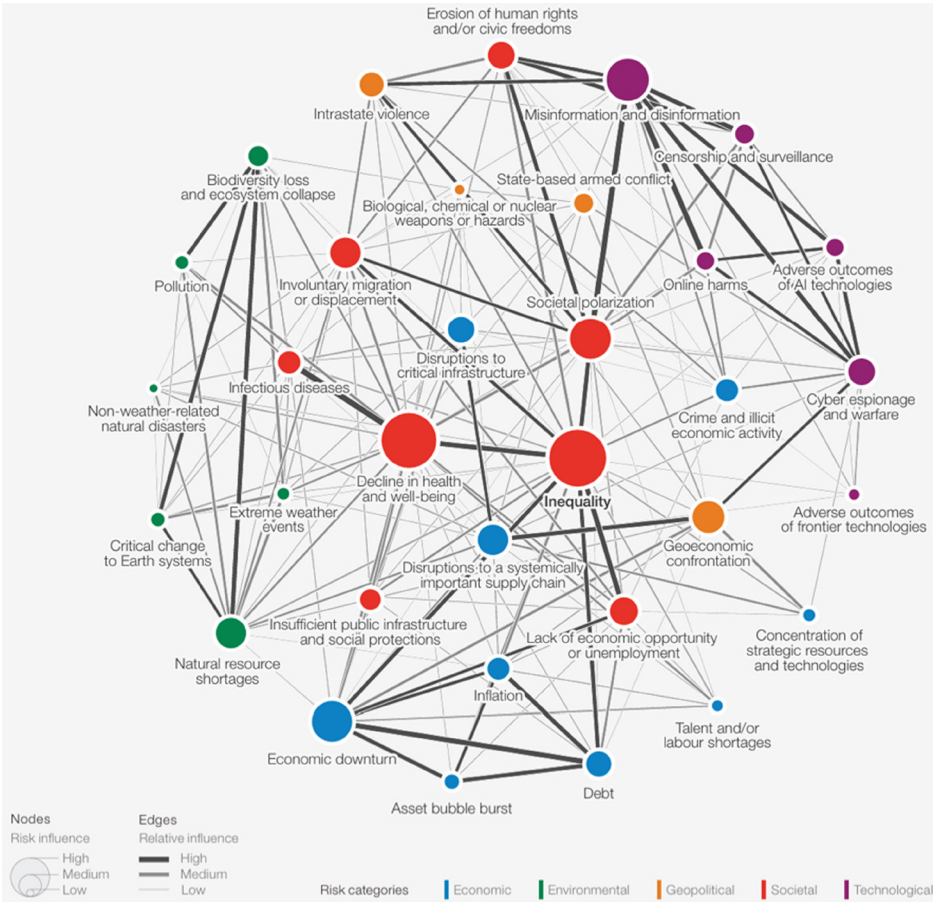
Ante el panorama descrito, la ciberseguridad y la ciberdefensa deben articular estrategias operacionales mediante el control de sistemas institucionales de información. Su objetivo es planear, anticipar, dirigir y ejecutar acciones defensivas permanentes en el ciberespacio protegiendo la confidencialidad, disponibilidad e integridad de las tecnologías de la información y la comunicación (TIC) frente a amenazas ciberterroristas.

Desde hace más de una década el World Economic Forum ha ubicado las amenazas cibernéticas y al entorno de la información entre los principales riesgos globales, junto a eventos como los desastres naturales o las crisis económicas. En su informe de 2025 se estimó que los delitos cibernéticos generan pérdidas globales anuales por más de 445 mil millones de dólares, lo que supera incluso los ingresos anuales de economías como la chilena (World Economic Forum, 2025).

El informe identifica a los ciberataques y la creciente ciberdependencia como amenazas de alta probabilidad e impacto, que ya superan en relevancia a riesgos tradicionales como el desempleo o los conflictos interestatales. En el mapa global

de interconexión de riesgos 2025 (figura 3), los ciberataques aparecen vinculados directamente con otros riesgos sistémicos: interrupciones en IC, mal uso de tecnologías y robo y fraude de datos, así como fallos en la gobernanza nacional, terrorismo y tensiones geopolíticas. Esta red de conexiones refuerza la idea de que las amenazas cibernéticas no pueden entenderse de forma aislada, sino como elementos catalizadores de crisis multidimensionales.

Figura 3. Mapa de interconexión de los riesgos



Fuente: (World Economic Forum, 2025, pág. 9).

Para que los Estados desarrollen una comprensión efectiva de las ciberamenazas deben considerar tres elementos fundamentales (Villalba, A., & Corchado, J, 2017):

- Intereses: Se refiere a los activos que pueden verse comprometidos por ciberataques, especialmente los vinculados con la seguridad y defensa nacional. Entre ellos destacan la confidencialidad, disponibilidad, trazabilidad y autenticidad de la información institucional.
- Amenazas: hace alusión a los objetivos, eventos y actividades que, ejecutadas por actores hostiles —como ciberterroristas o servicios de inteligencia hostiles—, tienen capacidad para afectar los intereses estratégicos de un Estado.
- Resiliencia: implica la capacidad de los sistemas de información para resistir, absorber y recuperarse de un ciberataque. Esto incluye tanto la ausencia de vulnerabilidades como la existencia de mecanismos de respuesta y estrategias de mitigación eficaces.

Dentro del conjunto de amenazas persistentes, el espionaje cibernético representa uno de los mayores desafíos. Este es impulsado a menudo por servicios de inteligencia extranjeros que operan al servicio de organizaciones hostiles. Dichos actores suelen disponer de abundantes recursos técnicos, humanos y financieros, así como de acceso a herramientas de ataque de procedencia diversa, muchas veces desarrolladas internamente.

Estados con regímenes autoritarios o sin controles democráticos efectivos disfrutan de mayores márgenes de maniobra en el ciberespacio. Aunque existe un consenso internacional sobre la aplicación del derecho internacional al ciberespacio, estos actores operan al margen de las normativas ejecutando operaciones ofensivas sin supervisión jurídica ni restricciones estatales. Esa ventaja táctica les permite llevar a cabo acciones altamente eficaces con bajo riesgo de atribución o represalia.

El informe conjunto del Centro Nacional de Inteligencia (CNI) y el CCN-CERT identificó cuatro vectores de ataque recurrentes en operaciones de ciberespionaje (CCN-CERT, 2008):

- Primer vector: obtención de información estratégica. Se basa en la recolección masiva y automática de datos provenientes de internet y de las comunicaciones entre nodos. El tráfico no cifrado resulta particularmente vulnerable, ya que puede ser interceptado y analizado fácilmente.
- Segundo vector: ataques dirigidos. Se ejecutan contra sistemas específicos pertenecientes a individuos u organizaciones de interés estratégico. Las herramientas de ataque son diseñadas a medida, utilizando información técnica y de ingeniería social previamente recopilada sobre la víctima.

- Tercer vector: debilitamiento de estándares técnicos. Consiste en manipular o vulnerar implementaciones criptográficas generando fallas deliberadas, que pueden ser explotadas posteriormente para comprometer la seguridad de los sistemas.
- Cuarto vector: manipulación selectiva de sistemas. Se centra en la modificación de equipos o servicios mediante la inserción de puertas traseras, alteraciones en la seguridad perimetral o configuraciones comprometidas, para así facilitar futuras intrusiones o accesos no autorizados durante fases posteriores del ataque.

Dada la creciente sofisticación y el impacto potencial de los ciberataques, varios Estados han incorporado explícitamente las operaciones cibernéticas como parte fundamental de su estrategia militar. Dichas acciones, ejecutadas tanto por actores estatales como por organizaciones criminales cibernéticas, tienen como propósito interferir en el desarrollo de operaciones militares convencionales o afectar infraestructuras críticas del adversario.

Los programas de ciberataques —por su naturaleza indirecta— están diseñados para inutilizar redes de comunicaciones, paralizar infraestructuras logísticas o comprometer sistemas esenciales como los de salud pública y respuesta a emergencias. En tales casos, aunque el ataque no se realiza mediante medios cinéticos, sus efectos son directos y estratégicos (Villalba & Corchado, 2017).

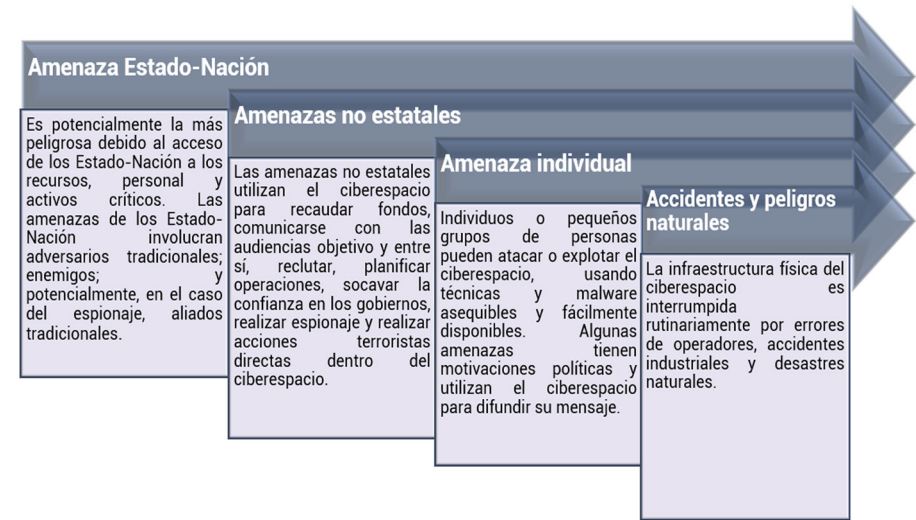
En el caso de Colombia, se han clasificado los desafíos cibernéticos en cuatro grandes categorías, según el enfoque adoptado en cooperación con el Gobierno de Estados Unidos (2018):

- Amenazas y anonimato: Dificultades para identificar con precisión a los actores hostiles y atribuir responsabilidades.
- Geografía: Limitaciones impuestas por la distribución territorial y la cobertura de infraestructura digital.
- Tecnología: Brechas tecnológicas que impiden una respuesta eficaz y autónoma.
- Infraestructura pública e industria privada: Necesidad de coordinación entre sectores críticos que comparten la responsabilidad de la seguridad cibernética.

Estos elementos se integran en la figura 4, la cual sintetiza los desafíos principales que enfrentan las Fuerzas Militares de Colombia en el entorno cibernético.

Esta clasificación permite priorizar capacidades, orientar recursos y definir estrategias diferenciadas según el tipo de riesgo identificado.

Figura 4. Clasificación de desafíos cibernéticos



Fuente: Elaboración propia, con base en (Gobierno de Estados Unidos de América, 2018).

En síntesis, el intercambio de información en las Fuerzas Militares de Colombia requiere una integración articulada entre ciberseguridad, ciberdefensa y ciberinteligencia, concebidas como capacidades complementarias frente a amenazas persistentes y en evolución. La identificación temprana de actores maliciosos, vulnerabilidades críticas y vectores de ataque, junto con el despliegue de tecnologías especializadas y plataformas seguras, resulta decisiva para anticipar, mitigar y neutralizar incidentes cibernéticos. Una adecuada gestión de la información clasificada y operativa no solo refuerza la protección de la infraestructura crítica nacional, sino que también fortalece la postura estratégica del país en el escenario global de confrontación digital.

Sistemas de intercambio de información cibernética utilizados por los Estados

Tomando en cuenta que los ciberataques afectan directamente la estabilidad y desarrollo de los Estados, muchos gobiernos ya han implementado capacidades

para llevar a cabo operaciones y estrategias desde sus fuerzas militares en el ciberespacio. Los cibercriminales operan con el objetivo de destruir o inutilizar las redes de información de las instituciones para usarla a su favor o hacer inaccesible su información.

Las Fuerzas Militares de Estados son instituciones que manejan una gran cantidad de información confidencial, y de ello depende el éxito de las operaciones que tienen como fin la garantía de la Seguridad y Defensa Nacionales. Por tal motivo, desde el Ministerio de Defensa Nacional de cada estado deben adoptarse medidas orientadas a proteger, monitorizar, analizar, detectar y responder a los ataques encaminados a dañar o comprometer las redes o los sistemas de información.

Con el fin de examinar las falencias existentes en el método de intercambio de información de las Fuerzas Militares de Colombia, en las siguientes páginas se hace un análisis comparado entre los sistemas de información de otros Estados y el sistema que usan las Fuerzas Militares de Colombia, a fin de tomar dichos casos como lecciones aprendidas.

Modelos internacionales de intercambio de información cibernética en las Fuerzas Armadas

En el actual escenario geopolítico, el ciberespacio se ha vuelto un nuevo dominio de confrontación estratégica. Ante el aumento de incidentes cibernéticos a gran escala, los Estados han activado mecanismos de alerta y han reforzado el papel de sus fuerzas armadas priorizando la capacidad para identificar, contener y responder a amenazas emergentes. En ese contexto, el intercambio seguro de información sensible constituye un componente crítico para lograr los objetivos estratégicos nacionales (Saz, 2016).

Los servicios de inteligencia son clave en la defensa frente a ataques cibernéticos, los cuales pueden afectar IC y desestabilizar sistemas políticos o económicos. La creciente vulnerabilidad digital exige plataformas tecnológicas robustas, redes intrínsecamente seguras y capacidades especializadas dentro de las estructuras militares para garantizar una respuesta oportuna y eficaz.

El intercambio de información en el ámbito de la inteligencia militar exige protocolos estrictos de seguridad que garanticen la protección de datos sensibles. A nivel internacional, las doctrinas de inteligencia varían: mientras en Europa el énfasis está en la obtención y análisis de datos para generar conocimiento estratégico, en América Latina persiste cierta ambigüedad conceptual entre los términos "información" e "inteligencia". En Estados Unidos, el concepto de inteligencia ha sido estandarizado desde finales del siglo XX, influenciado por su evolución doctrinal

en las distintas ramas de sus fuerzas armadas, y formalizado en agencias como el CNI español, anteriormente conocido como CESID (Sainz, 2012).

La eficacia en la toma de decisiones operacionales depende en gran medida del flujo oportuno y seguro de información hacia los niveles de mando. En el contexto actual, el ciberespacio se ha consolidado como el medio idóneo para la transmisión de datos estratégicos, lo cual exige que los sistemas de inteligencia operen de manera articulada desde el nivel táctico. Sin garantías de seguridad en la información, el éxito de una operación puede verse comprometido seriamente.

Según datos de la Organización de Estados Americanos (OEA, 2019), el manejo de información clasificada en los Estados es altamente reservado. Aunque existen acuerdos bilaterales y multilaterales, los mecanismos específicos para el intercambio no se hacen públicos, dada su naturaleza crítica y el alto riesgo asociado a su exposición.

A pesar de los esfuerzos por adoptar una Estrategia de Seguridad Cibernética común, la respuesta de los Estados miembros frente a la delincuencia cibernética sigue siendo desigual. La mayoría reconoce el impacto negativo de las amenazas cibernéticas sobre las capacidades de defensa, pero enfrenta limitaciones estructurales.

En América Latina, dos factores son en especial críticos: la escasez de recursos dedicados a fortalecer las capacidades de ciberseguridad y la falta de personal especializado con experiencia práctica para implementar políticas eficaces (OEA, 2019).

Los países que han logrado avances significativos en materia de seguridad cibernética han invertido sostenidamente en el desarrollo de plataformas seguras, redes intranet robustas y personal capacitado en ciberdefensa. La OEA, por su parte, promueve programas de intercambio de buenas prácticas entre sus Estados miembros, orientados a fortalecer los sistemas nacionales y garantizar la circulación segura de información sensible dentro de las instituciones gubernamentales.

Los grupos de delincuencia organizada continúan ampliando sus propias capacidades cibernéticas, mientras los colectivos de *hackers* incrementan su número y nivel de sofisticación. Esta evolución plantea un reto creciente para los Estados, que deben reforzar sus mecanismos de coordinación e intercambio de información con agencias de seguridad, proveedores de servicios de internet y actores del sector privado. Desmantelar redes ilícitas requiere inteligencia técnica especializada, conocimiento profundo de los métodos de operación y control sobre los canales financieros utilizados por los ciberdelincuentes (OEA, 2019).

En este escenario, entender el ciberespacio como un nuevo campo geopolítico de batalla se vuelve esencial para el éxito de las operaciones militares. Por ello, numerosos Estados han ido creando estructuras militares especializadas —cibercomandos— integradas a sus fuerzas armadas, a fin de actuar de forma coordinada en este dominio intangible.

España constituye un ejemplo destacado. Sus fuerzas armadas han sido objeto de agresiones cibernéticas dirigidas a comprometer servicios críticos, lo que impulsó el desarrollo de estrategias nacionales orientadas a enfrentar los riesgos asociados al uso del ciberespacio. La ciberseguridad fue incorporada como un eje fundamental de la política de seguridad nacional ampliando el concepto tradicional de seguridad más allá del ámbito militar y policial para abordar nuevas amenazas de carácter digital (Ministerio de Defensa de España, 2013).

El Servicio de Inteligencia de España desempeña un papel clave en este esfuerzo proporcionando elementos de análisis para la toma de decisiones estratégicas en ciberseguridad. Sus funciones incluyen la obtención y tratamiento de información tanto en territorio nacional como en cooperación con servicios extranjeros, lo cual resulta indispensable, dada la naturaleza transnacional de las (Villalba, A., & Corchado, J, 2017, pág. 101).

Por su parte, la Oficina Nacional de Seguridad (ONS), como autoridad responsable de la protección de información clasificada, vela por el cumplimiento de normativas relacionadas con el resguardo de datos sensibles en contextos nacionales e internacionales. En materia de ciberseguridad, esta oficina colabora activamente en la protección de sistemas críticos y activos estratégicos frente a amenazas digitales (Ministerio de Defensa de España, 2013).

El Mando Conjunto de Ciberdefensa español, además de garantizar la seguridad de las redes militares, desarrolla capacidades ofensivas y defensivas, incluyendo acciones preventivas, reactivas, de alerta temprana y de explotación del entorno digital, con el fin de generar superioridad informacional en el ciberespacio (Ministerio de defensa España, 2014).

En ese contexto, el traspaso de información entre fuerzas militares requiere comprender y aplicar principios de inteligencia que aseguren la reserva y el manejo adecuado de la información crítica. Aunque muchos de estos métodos son clasificados, existen modelos de cooperación internacional que permiten compartir conocimientos y capacidades en escenarios conjuntos, y fortalecer así las operaciones militares y la defensa cibernética cooperativa.

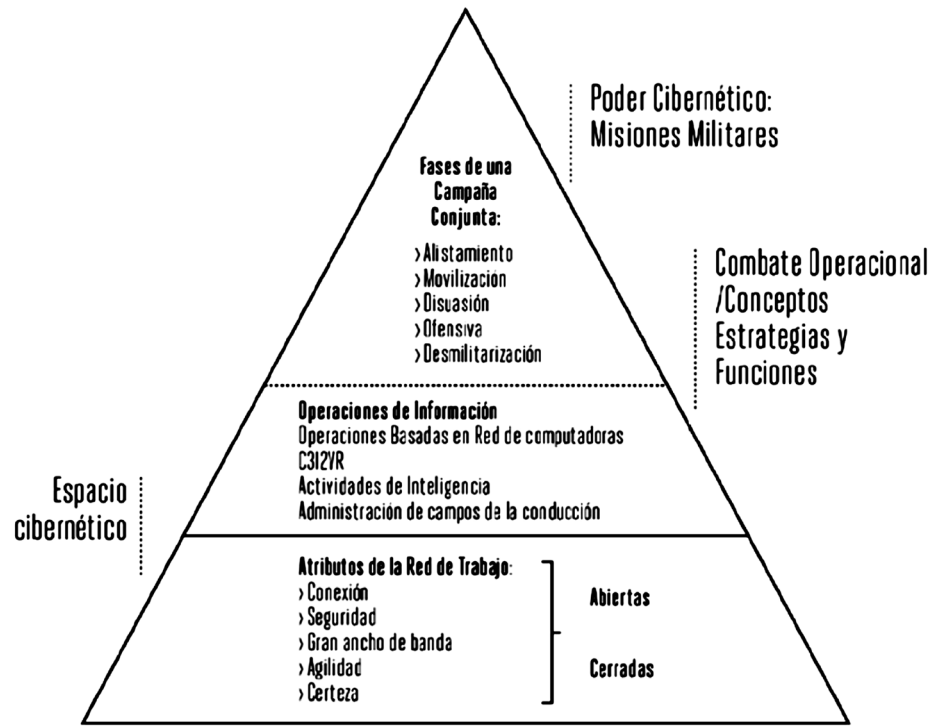
El éxito del intercambio de información interagencial radica en garantizar su seguridad, clasificación adecuada y control sobre los posibles vectores internos de riesgo. La mitigación de amenazas internas —como filtraciones o infiltraciones— requiere no solo medidas técnicas, sino también el fortalecimiento de la lealtad institucional y la gestión estratégica del talento humano. Estos esfuerzos deben acompañarse del desarrollo continuo de plataformas tecnológicas y métodos seguros de intercambio de datos (Becerra, 2019).

En el caso de Estados Unidos, la doctrina operacional en el ciberespacio está formalizada en la *Joint Publication 3-12: Cyberspace Operations* (2018), que integra dicho dominio en las operaciones conjuntas. Esa doctrina distingue tres tipos de operaciones: ofensivas (OCO), defensivas (DCO) y defensa de la red de información del Departamento de Defensa (DODIN). Las OCO buscan proyectar poder a través del espacio cibernético; las DCO están orientadas a proteger las redes propias o aliadas, y las operaciones DODIN se centran en el diseño, operación y protección de las redes del Departamento de Defensa, para asegurar la integridad, disponibilidad, confidencialidad y autenticidad de los sistemas de información (Joint Force Development, 2018).

En contraste, América Latina enfrenta importantes desafíos estructurales. Según el Banco Interamericano de Desarrollo (BID), el 80 % de los países carecen de una estrategia nacional de ciberseguridad (BID, 2016; Cabuya-Padilla & Castaneda-Marroquin, 2024). Brasil ha sido una excepción relativa, al avanzar en el diseño de una política nacional impulsada por amenazas crecientes. Sin embargo, enfrenta obstáculos en la definición de prioridades y en la implementación efectiva de sus lineamientos estratégicos (Diniz et al., 2014).

A nivel doctrinal, las Fuerzas Militares suelen estructurar su poder cibernético en tres niveles jerárquicos, como se observa en la figura 5. En la base del triángulo se encuentran las redes abiertas y cerradas, junto con capacidades de conectividad segura, resiliencia y alto rendimiento. El nivel intermedio comprende las funciones operacionales, estrategias y acciones como las operaciones de redes computacionales (en inglés, NCO, por las iniciales de Network Computer Operations) y las operaciones de información. En la cúspide se ubican las misiones militares articuladas con el empleo del poder cibernético en todas las fases de una campaña (De Vergara, E., & Trama, G, 2017, pág. 141).

Figura 5. Estructura del poder cibernético militar



Fuente: De Vergara y Trama (2017, p. 141).

Los sistemas cibernéticos militares pueden clasificarse como abiertos o cerrados. Los sistemas abiertos permiten el acceso a través de credenciales y suelen estar conectados a infraestructuras comerciales. Su seguridad depende del cifrado, autenticación y uso de herramientas de protección, pero su exposición a redes públicas los hace inherentemente más vulnerables. Por tal motivo, muchas fuerzas armadas trabajan en el desarrollo de soluciones propias con mayores garantías de control.

En contraste, los sistemas cerrados están restringidos a nodos autorizados y operan de forma aislada, sin conexión con redes abiertas. Aunque no todos los Estados han implementado plenamente este modelo —como es el caso de Argentina—, su uso garantiza mayores niveles de seguridad, disponibilidad y confiabilidad de la información transmitida. Sin embargo, no están exentos de riesgos: siguen siendo susceptibles a infecciones por medios físicos, como dispositivos USB contaminados (De Vergara & Trama, 2017, p. 142).

En contextos como el de Estados Unidos, los sistemas *Secret Internet Protocol Router Network* (SIPRNet) y *Secure Telephone Units* (STU) son ejemplos de redes militares cerradas que permiten el control total sobre el acceso, el tráfico y los nodos. Dichos sistemas no solo garantizan un uso seguro y eficiente de la información, sino que también contribuyen de forma decisiva al éxito de las operaciones militares mediante su resiliencia y confiabilidad (Kramer, 2009).

En conjunto, los modelos internacionales revisados evidencian que el intercambio de información cibernética en el ámbito militar requiere estructuras técnicas robustas, protocolos interoperables y marcos doctrinales sólidos. La seguridad, la clasificación, la cooperación interagencial y el dominio del ciberespacio como entorno operacional emergen como factores determinantes en la construcción de capacidades estratégicas que permitan anticipar y neutralizar amenazas en escenarios complejos y dinámicos.

Sistema de intercambio de información de las Fuerzas Militares de Colombia

En la actual sociedad de la información, los sistemas digitales y las estrategias orientadas a proteger los activos estratégicos de las organizaciones son fundamentales. La protección de la confidencialidad de la información no solo afecta al ámbito militar, sino también a sectores como la economía, la política, la educación y las comunicaciones.

Colombia ha registrado avances importantes en materia de tecnologías de la información y las telecomunicaciones, lo que ha exigido una rápida adaptación institucional para garantizar la seguridad nacional. En dicho proceso, las Fuerzas Militares han unificado esfuerzos para prevenir, controlar y neutralizar amenazas en el ciberespacio.

Como señala Niño (2015), el uso coherente de las tecnologías debe responder a una alineación entre los intereses nacionales e internacionales. En ese marco, se han establecido normas para prevenir el uso indebido de los recursos tecnológicos, en línea con principios de seguridad digital.

En 2011 el Gobierno colombiano expidió el primer documento CONPES en ciberseguridad y ciberdefensa, lo que dio origen a entidades clave, como el Grupo de Respuesta a Emergencias Cibernéticas (ColCERT) y el Comando Conjunto Cibernético (CCOCI). Este último, bajo el mando del Ministerio de Defensa Nacional, tiene la misión de prevenir, detectar, neutralizar, analizar y responder ante amenazas informáticas que comprometan la seguridad del Estado. Además, cada Fuerza

—Ejército, Armada y Fuerza Aeroespacial— ha desarrollado capacidades propias en ciberdefensa, complementadas por el Centro Cibernético Policial en el ámbito de la ciudadanía (CONPES 3701).

El desarrollo institucional prosiguió con la creación de Unidades Cibernéticas específicas en cada Fuerza, desde donde el CCOCI coordina operaciones de ciberdefensa según el tipo de amenaza y el rol funcional de cada componente. Este enfoque fue consolidado en el Plan Nacional de Desarrollo 2014-2018 (Departamento Nacional de Planeación, 2014). En 2016 el CONPES 3854 —Política Nacional de Seguridad Digital— incorporó la gestión del riesgo como un eje estratégico determinando principios y dimensiones que permiten fortalecer la capacidad de respuesta de actores públicos y privados ante amenazas digitales (Comando Conjunto Cibernético, 2017, págs. 11-12).

Los destacamentos militares trabajan de forma continua en la identificación de riesgos, la corrección de fallas y la reacción ante agresiones, especialmente en los entornos intranet de sus unidades. Alineados con la Resolución 57/53 de la ONU, Colombia ha adoptado criterios internacionales para el uso legítimo y seguro de las TIC (OEA, 2019, págs. 1-2).

La acción conjunta de las Fuerzas Militares en ciberdefensa es clave para neutralizar amenazas que ponen en riesgo la seguridad nacional y el desarrollo del país. En ese contexto, la gestión del riesgo, la anticipación de incidentes y la percepción ciudadana sobre la seguridad son factores decisivos, incluso si ello implica restricciones a ciertas libertades en aras de proteger infraestructuras críticas (IC) (Becerra, 2019).

En cuanto al intercambio de información, se han definido lineamientos estratégicos que incluyen: procesos de clasificación y compartición a nivel operativo y táctico; una taxonomía estandarizada para el manejo de datos cibernéticos, y el desarrollo de una plataforma tecnológica que permita la transferencia segura y en tiempo real de información entre actores clave del ecosistema de ciberdefensa.

La creciente amenaza en el ciberespacio proviene de actores estatales y no estatales que persiguen objetivos como espionaje, sabotaje, terrorismo o criminalidad organizada. De acuerdo con cifras oficiales, el cibercrimen en Colombia aumentó en el 34 % a lo largo del último año, con más de 60.000 denuncias registradas y más de 30.000 incidentes reportados (Presidencia de la República de Colombia, 2018, pág. 29).

En conclusión, Colombia sí ha avanzado significativamente en la consolidación de un sistema de intercambio de información cibernética en el sector defensa,

al articular políticas públicas, capacidades operativas y estructuras técnicas especializadas. Sin embargo, la evolución constante del entorno digital exige continuar fortaleciendo la interoperabilidad entre actores, la estandarización de procedimientos y la adopción de tecnologías seguras que permitan anticipar, mitigar y responder de forma eficaz a las amenazas en el ciberespacio.

Método de intercambio de información cibernética para las Fuerzas Militares de Colombia

Uno de los indicadores clave de la preparación cibernética de un país es su capacidad para establecer mecanismos seguros y sostenibles de intercambio de información entre el Estado, la industria y otros actores estratégicos. Dichas capacidades son fundamentales para identificar, evaluar y responder a ciberataques que puedan afectar sectores críticos como las telecomunicaciones, el comercio o la defensa (Hathway, 2015, pág. 18).

Existen al menos cuatro modelos reconocidos de intercambio de información, liderados: 1) por el Gobierno; 2) por la industria; 3) por organizaciones sin ánimo de lucro, y 4) modelos híbridos, que integran sectores gubernamentales, académicos y privados. Cada uno presenta desafíos únicos, como el equilibrio entre rapidez en el intercambio, confidencialidad de los datos, respeto por las libertades civiles y sostenibilidad operativa. No obstante, todos requieren dos factores esenciales para su éxito: confianza institucional y claridad en los roles, responsabilidades y objetivos (Hathaway, 2010).

Para que estos esquemas sean efectivos, debe definirse con precisión qué información debe compartirse, quién tiene acceso, y qué medidas deben adoptarse para proteger los datos una vez divulgados. La complejidad aumenta cuando los miembros del sistema son Estados soberanos con distintas prioridades de seguridad (Hathway, 2015, pág. 19). En el caso colombiano, resulta indispensable contar con mecanismos formales y procedimientos acordes con la normativa nacional que permitan establecer responsabilidades claras, aplicar sanciones cuando sea necesario y garantizar la integridad de la información transmitida en el sistema de comunicaciones del sector defensa.

La protección de las tecnologías de la información y las comunicaciones (TIC) en el teatro de operaciones del ciberespacio requiere la integración efectiva entre ciberseguridad, ciberdefensa y ciberinteligencia. Esta sinergia permite anticipar, planear, dirigir y ejecutar acciones coordinadas frente a amenazas terroristas y

otras formas de agresión digital. Dado que las amenazas cibernéticas afectan directamente la estabilidad de los Estados y la resiliencia de sus instituciones, es imprescindible tener la capacidad para anticipar y neutralizar incidentes críticos mediante mecanismos de seguridad estructurados (Sancho, 2018). La globalización y la convergencia tecnológica han intensificado la frecuencia, sofisticación y alcance de los ataques, y ello evidencia la necesidad de adoptar modelos más robustos de protección de la infraestructura nacional.

Para consolidar una verdadera capacidad de colaboración e intercambio de información, es indispensable estandarizar los sistemas empleados, para así facilitar una articulación eficiente entre las entidades responsables de la seguridad y defensa del país.

En tal sentido, la protección de infraestructuras críticas debe apoyarse en sistemas capaces de anticipar riesgos mediante la recolección y análisis de datos de múltiples fuentes. Las amenazas actuales ya no pueden ser enfrentadas con métodos tradicionales: requieren plataformas avanzadas que detecten señales tempranas dispersas y permitan activar mecanismos de respuesta y recuperación ágiles y eficaces (Escuela Superior de Guerra., 2019).

El Ministerio de Defensa Nacional requiere una plataforma especializada para el intercambio de información cibernética que permita consolidar el conocimiento sobre amenazas que afectan la ciberseguridad y la ciberdefensa institucional. Esta plataforma debe facilitar la identificación de ataques que comprometan redes, sistemas y activos críticos, y permitir que se ajusten medidas de protección, mejorar la capacidad de monitoreo y promover acciones preventivas entre administradores y usuarios.

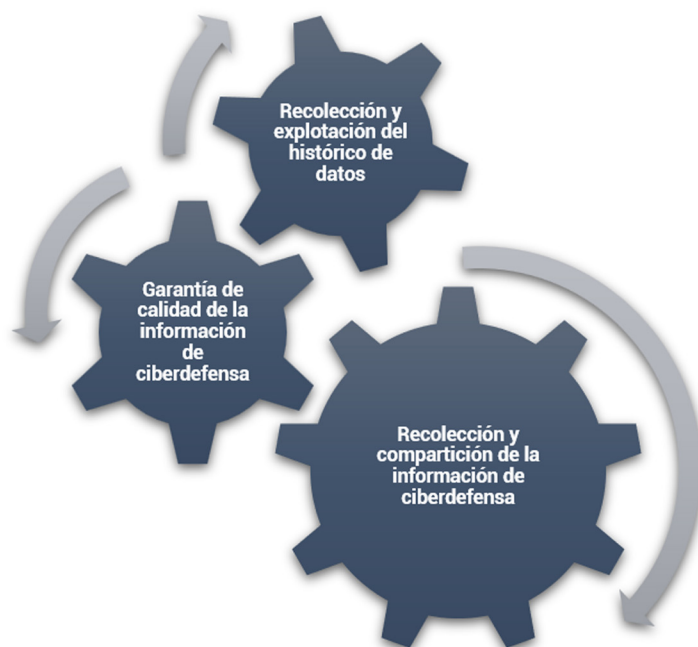
Un sistema de intercambio eficaz fortalecería la articulación entre organismos del sector defensa generando capacidades conjuntas para emitir alertas tempranas, compartir indicadores de compromiso y sistematizar lecciones aprendidas frente a amenazas comunes. En ausencia de dicha plataforma interagencial se reduce la capacidad de anticipación ante riesgos ya detectados por otras fuerzas, y se debilita, por tanto, la respuesta nacional frente al cibercrimen.

La gestión del riesgo cibernético debe entenderse como una responsabilidad colectiva del Estado, que implique cooperación nacional e internacional bajo el principio de responsabilidad compartida. Ello permitiría acciones articuladas y transnacionales frente a actores maliciosos cada vez más sofisticados.

Esta capacidad de colaboración debe ser inherente a toda organización de ciberdefensa. Para ello, se requiere una infraestructura que facilite el intercambio de información técnica y operativa mediante servicios de mensajería segura,

videoconferencia, chats especializados y herramientas colaborativas como pizarras digitales. La información compartida debe cumplir estándares de calidad, lo que incluye datos sobre vulnerabilidades, amenazas, incidentes, riesgos, activos y medidas implementadas, todo bajo formatos estructurados que optimicen su análisis y uso estratégico (Escuela Superior de Guerra, 2019). La figura 6 incorpora esta complejidad en el marco de la capacidad de las organizaciones de seguridad de los sistemas de información.

Figura 6. *Capacidad de las organizaciones de seguridad de los sistemas de información*



Fuente: elaboración propia (Escuela Superior de Guerra, 2019).

La interoperabilidad es un componente esencial en los sistemas de intercambio de información cibernética. Permite garantizar la confidencialidad, integridad, disponibilidad, autenticación y no repudio de los datos; reduce los tiempos de respuesta, y mejora la seguridad mediante la coordinación entre múltiples organismos. Además, favorece el conocimiento situacional compartido, optimiza recursos y permite sincronizar actividades de ciberdefensa en tiempo real (Escuela Superior de Guerra, 2019, págs. 14-15).

En línea con este enfoque, las políticas de defensa de Colombia vienen enfatizando la importancia de fortalecer las alianzas internacionales en materia de

seguridad. Colombia ha buscado consolidarse como socio estratégico de la OTAN y de Estados Unidos promoviendo el intercambio de conocimientos en áreas clave como inteligencia, operaciones militares, lucha contrainsurgente, narcotráfico y gestión de riesgos.

Este esfuerzo también incluye la mejora continua en capacidades logísticas, estándares interoperables y doctrinas en ciberdefensa. Para eso se requiere una formación constante del personal militar, así como el desarrollo de operaciones combinadas que aseguren una mayor integración con fuerzas aliadas. Como parte de dicha estrategia, se renovó el programa de cooperación *Individual Partnership Cooperation Program* (IPCP), con énfasis en desminado, ciberdefensa y combate al crimen organizado (Presidencia de la República de Colombia, 2018, págs. 51-52).

Finalmente, la seguridad técnica de los sistemas utilizados es un aspecto crítico. La protección de los sistemas operativos, a menudo expuestos a riesgos y vulnerabilidades, debe ser abordada desde un enfoque preventivo, que garantice su integridad y minimice la posibilidad de modificaciones maliciosas o fallas que comprometan la seguridad de la información intercambiada.

Con base en los modelos internacionales analizados, las necesidades específicas del entorno estratégico colombiano, junto con las capacidades ya existentes en materia de ciberdefensa, se propone un modelo híbrido adaptado a las Fuerzas Militares de Colombia, con los siguientes elementos clave:

- Modelo base propuesto:
 - o Modelo híbrido colaborativo, articulado entre el Ministerio de Defensa Nacional, la industria nacional, el sector académico y aliados estratégicos internacionales, para garantizar sinergias, confianza y capacidades sostenibles.
- Componentes estructurales del sistema:
 - o Plataforma nacional segura de intercambio de información cibernética (con estándar STIX/TAXII), que integre:
 - Las Unidades Cibernéticas de cada Fuerza.
 - El Comando Conjunto Cibernético (CCOCI).
 - El Centro Cibernético Policial.
 - El CSIRT Defensa.
 - Las entidades civiles con funciones críticas (por ejemplo, infraestructura crítica energética o de comunicaciones).

- o Sistemas interoperables con capacidades de:
 - Clasificación automática de información.
 - Compartición de alertas tempranas.
 - Indicadores de compromiso (IoC) y análisis de amenazas en tiempo real.
 - Canal seguro para lecciones aprendidas.
- Principios de funcionamiento:
 - o Confianza mutua institucional: mediante acuerdos interinstitucionales de cooperación y confidencialidad.
 - o Criterios comunes de clasificación y taxonomía de información cibernética.
 - o Responsabilidad compartida en la gestión del riesgo cibernético.
 - o Interoperabilidad con aliados estratégicos: como la OTAN y Estados Unidos, asegurando estándares compatibles para operaciones combinadas.
- Capacidades clave que debe garantizar:
 - o Protección de información clasificada y crítica.
 - o Coordinación en tiempo real en caso de incidentes.
 - o Mejora de la conciencia situacional cibernética conjunta.
 - o Fortalecimiento de la anticipación, reacción y resiliencia institucional.
- Requisitos para su implementación:
 - o Desarrollo normativo y técnico para garantizar confidencialidad, autenticación, disponibilidad y no repudio.
 - o Capacitación continua del personal militar y técnico.
 - o Inversión sostenida en plataformas, redes seguras e infraestructura crítica.
 - o Inclusión del componente de ciberinteligencia en el ciclo de planeamiento militar.

Esta propuesta busca equilibrar la necesidad de proteger la información sensible con la urgencia de compartir datos clave entre organismos de seguridad y defensa para neutralizar amenazas cibernéticas de forma oportuna, anticipada y coordinada. Así, Colombia avanzaría hacia un modelo integral de ciberdefensa colaborativa en el ámbito militar.

Figura 7. Esquema general de las bases del modelo conceptual propuesto

**Propuesta de método de intercambio de información de
ciberseguridad y ciberdefensa para las Fuerzas Militares de Colombia**

- Adoptar un modelo híbrido de intercambio de información
- Plataforma tecnológica interoperable
- Clasificación de la información según estándares establecidos
- Garantía de seguridad y confianza en el intercambio
- Colaboración en tiempo real frente a incidentes
- Colaboración en tiempo real frente a incidentes



Fuente: elaboración propia.

Conclusiones

Las amenazas cibernéticas han evolucionado en complejidad y volumen, hasta convertirse en un desafío crítico para la seguridad nacional de Colombia. El crecimiento acelerado de estas amenazas y su vinculación con el uso de nuevas tecnologías representan un riesgo directo para las Fuerzas Militares, cuyas capacidades dependen cada vez más de sistemas tecnológicos para la navegación, armamento, transporte, información y comunicaciones.

La vulnerabilidad de las infraestructuras y redes críticas no solo compromete la seguridad y defensa del país, sino que también impone costos económicos significativos y afecta la estabilidad social. Por ello, resulta decisivo alinear las agendas de seguridad nacional y económica, y reconocer la ciberseguridad como un pilar para la protección del crecimiento digital y del desarrollo estratégico nacional.

Uno de los retos centrales de la ciberdefensa es garantizar el funcionamiento estable de la sociedad en el entorno digital generando condiciones de confianza suficientes para la integración segura de tecnologías como el Internet de las Cosas (IoT). Esta confianza es clave para el aprovechamiento del potencial del ciberespacio en la vida cotidiana, tanto en el ámbito civil como en el militar.

La ciudadanía, en su interacción diaria con plataformas digitales, enfrenta múltiples vulnerabilidades. Su capacidad de respuesta es limitada, lo que justifica la necesidad de implementar iniciativas pedagógicas que promuevan la conciencia cibernética, el uso responsable de la tecnología y la protección de la información personal ante ataques como el robo de contraseñas, el espionaje en redes o la infiltración de *software* malicioso.

Para proteger las infraestructuras críticas del país, resulta prioritario transformar el enfoque actual de gestión de datos desarrollando sistemas resilientes capaces de anticiparse a los riesgos. Esto requiere una arquitectura flexible y adaptativa frente al carácter dinámico del ciberespacio, lo que implica integrar la seguridad civil y militar bajo una estrategia nacional unificada.

Finalmente, se concluye que Colombia debe adoptar un modelo híbrido de intercambio de información cibernética, basado en una plataforma tecnológica interoperable que articule a las Fuerzas Militares con organismos civiles y aliados internacionales. Este modelo debe combinar elementos gubernamentales, industriales y académicos, garantizar estándares de clasificación, seguridad y confianza, y promover la colaboración en tiempo real frente a incidentes. La interoperabilidad, la gestión del riesgo y la anticipación a las amenazas deben ser los principios rectores para consolidar esta capacidad estratégica nacional.

Referencias

- Becerra, J. (2019). La Seguridad en el Ciberespacio Un desafío para Colombia. En G. Medina, *La Seguridad*. Bogotá.
- Banco Interamericano de Desarrollo [BID]. (2016). *Ciberseguridad: ¿Estamos preparados en América Latina y el Caribe*. Banco Interamericano de Desarrollo.
- Cabuya-Padilla, D., & Castaneda-Marroquin, C. (2024). Marco de referencia para el modelamiento y simulación de la ciberdefensa marítima - MARCIM: estado del arte y metodología. *DYNA*, 169-179. doi:10.15446/dyna.v91n231.109774
- Cabuya-Padilla, D., Alvarado Carvajal, C., Carrascal Ortiz, R., Riola Rodríguez, J., Fajardo-Toro, C., & Escandon Bernal, S. (2022). Ciberseguridad y ciberdefensa marítima: análisis bibliométrico años 1990-2021. *RISTI - Revista Iberica de Sistemas e Tecnologias de Informação*, 197-210.
- Cabuya-Padilla, D., Díaz-López, D., Martínez-Páez, J., Hernández, L., & Castaneda-Marroquin, C. (2025). SERDUX-MARCIM: Maritime Cyberattack simulation using Dynamic Modeling, Compartmental Models in Epidemiology and Agent-based Modeling. *International Journal of Information Security*, 122.
- CCN-CERT. (2008). *Sistema de alerta temprana*. Centro Criptológico Nacional Español y Centro Nacional de Inteligencia de España.
- Centro Criptológico Nacional. (2021). *Guía de Seguridad de las TIC CCN-STIC 201*. Centro Criptológico Nacional.
- Comando Conjunto Cibernético. (2017). *Plan Nacional de Protección y Defensa para la Infraestructura Crítica Cibernética de Colombia*. Comando General de las Fuerzas Militares.
- Cornaglia, S., & Vecelli, A. (2017). La ciberdefensa y su regulación legal en Argentina (2006-2015). *URVIO - Revista Latinoamericana de Estudios de Seguridad*.
- Cubeiro, E. (2016). Ciberinteligencia. En A. Díaz, *Conceptos Fundamentales de Inteligencia*. Tirant lo Blanch.
- De Vergara, E., & Trama, G. (2017). *Operaciones militares cibernéticas*. Escuela Superior de Guerra Conjunta de las Fuerzas Armadas.
- Departamento Nacional de Planeación. (2014). *Plan Nacional de Desarrollo 2014-2018*. Presidencia de la República de Colombia.
- Departamento Nacional de Planeación. (2017). *CONPES 3854 - Política Nacional de Seguridad Digital*. Bogotá.
- Diniz, G., Muggah, R., y Misha, G. (2014). Deconstructing cyber security in Brazil: Threats and responses. *Strategic Paper 11*, 3-32.
- Escuela Superior de Guerra. (2019). Ciberseguridad y ciberdefensa UD1. Introducción a la Ciberdefensa.
- Escuela Superior de Guerra. (2019). Fundamentos de Ciberdefensa: documentación técnica.
- Escuela Superior de Guerra. (2019). Ciberseguridad y Ciberdefensa UD2. Capacidades de ciberseguridad y Ciberdefensa.
- Ganuza, N. (2020). Guía de ciberdefensa: orientaciones para el diseño, planeamiento, implantación y desarrollo de una ciberdefensa militar. Junta Interamericana de Defensa.

- Gobierno de Estados Unidos de América. (2018). *Cyberspace Operations* - Joint Publication 3-12.
- Gruszczak, A. (2016). *Intelligence security in the European Union*. Springer <https://link.springer.com/book/10.1057/978-1-137-45512-3>
- Hathaway, M. (2010). *Why Successful Partnerships are Critical for Promoting Cybersecurity*. The New Muga Internet.
- Hathway, M. (2015). *Índice de preparación cibernética 2.0: Un plan para la preparación cibernética: Una línea de base y un índice*. Potomac Institute for Policy Studies.
- IBM. (2025). *X-Force Threat Intelligence Index*. IBM.
- INCIBE. (2018). *Memorias Cybersecurity Summer Botcamp*.
- Joint Force Development. (2018). *Joint Publication 3-12: Cyberspace Operations*.
- Kramer, F. (2009). *Cyberpower and National Security*. National Defense University Press and Potomac Books.
- Ministerio de Defensa de España. (2013). *Estrategia de Seguridad Nacional. Un proyecto compartido*.
- Ministerio de defensa España. (2014). *MCCD-RD872 - Organización FAS*. Ministerio de defensa España.
- Moreno, L. (2017). *Seguridad de la Información y tendencias estratégicas de ciberseguridad*. Sala de prensa. Escuela Militar de Cadetes "General José María Córdova".
- Niño, F. (2015). *Concepto de Ciberseguridad organizacional*. Universidad Militar Nueva Granada.
- Organización de Estados Americanos [OEA]. (2019). La OEA y AWS presentan un "White Paper" para fortalecer la capacidad de seguridad cibernética en las Américas a través del marco de seguridad cibernética del NIST.
- Organización de Naciones Unidas [ONU]. (1999). Asamblea General de las Naciones Unidas del 4 de enero de 1999.
- OTAN. (2016). NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit. Warsaw Summit.
- Presidencia de la República de Colombia. (2018). *Política de Defensa y Seguridad PDS - Para la Legalidad, el Emprendimiento y la Equidad*.
- Sainz, J. (2012). *Inteligencia Táctica*. Universidad Complutense de Madrid.
- Sancho, C. (2018). Ciberinteligencia: Contextualización, aproximación conceptual, características y desafíos. Centro de Investigaciones y Estudios estratégicos, Cuaderno de trabajo N°1.
- Saz, M. (2016). *Conferencia: Operaciones Militares en el Ciberespacio*.
- UIT. (2015). *Medición de la Sociedad de la Información*. UIT.
- Villalba, A., & Corchado, J. (2017). Análisis de las ciberamenazas. En *Cuadernos de estrategia* (pp. 97-138). Ministerio de Defensa España.
- World Economic Forum. (2025). *The Global Risks Report*. <https://www.weforum.org/publications/global-risks-report-2025/>
- Zhaoyang, D. (2014). *Smart Grid Cyber Security*.