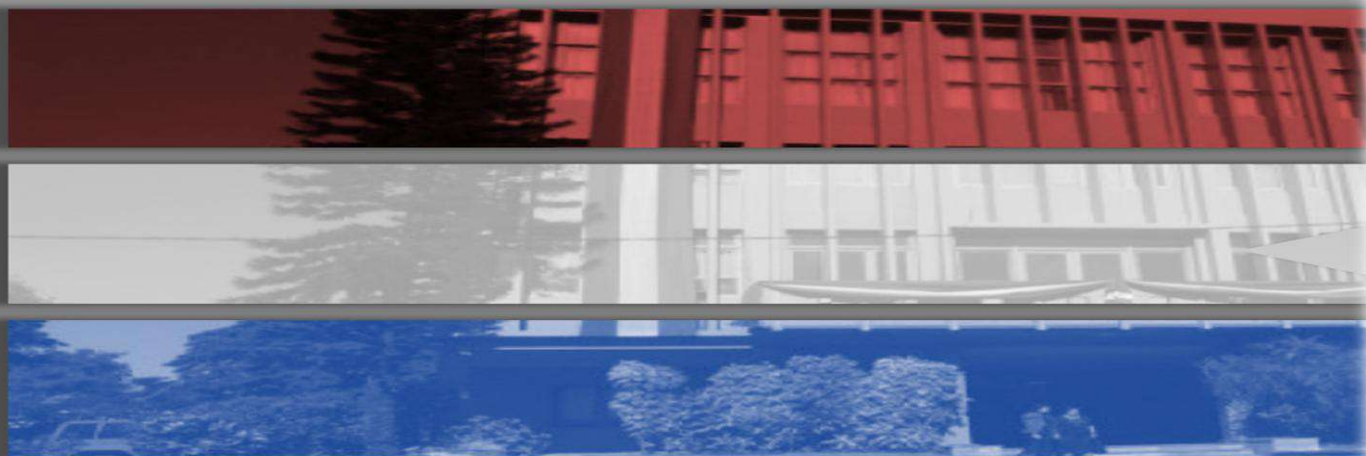




MINISTERIO DE DEFENSA NACIONAL

POLÍTICA DE CIBERSEGURIDAD MILITAR

2025 - 2028



**GOBIERNO DEL
PARAGUAY**

MINISTERIO DE
DEFENSA
NACIONAL

mdn.gov.py



El presente documento fue elaborado, por la Dirección General de Tecnologías de la Información y Comunicación del Ministerio de Defensa Nacional.

Septiembre 2025

Dirección: Avda. Mcál. López esq. Vice Presidente Sánchez y 22 de septiembre

Asunción - Paraguay

Teléfono: 021 2490000 - 1039

ciberseguridad@mdn.gov.py

www.mdn.gov.py



ÍNDICE

1. INTRODUCCIÓN	4
2. MARCO LEGAL EN MATERIA DE CIBERSEGURIDAD.....	5
3. OBJETIVOS ESTRATÉGICOS DE LA POLÍTICA DE CIBERSEGURIDAD MILITAR.....	6
4. DIRECTRICES DE LOS OBJETIVOS ESTRATÉGICOS.....	6
4. PRINCIPIOS RECTORES DE LA POLÍTICA DE CIBERSEGURIDAD MILITAR.....	7
5. COORDINACIÓN INSTITUCIONAL.....	8
6. MONITOREO, EVALUACIÓN Y ACTUALIZACIÓN	9
7. VIGENCIA, RESPONSABILIDAD Y DIFUSIÓN.....	10
8. DISPOSICIONES FINALES	11



1. INTRODUCCIÓN

La creciente digitalización de los sistemas militares, la interconectividad global y el uso extendido de tecnologías de la información han transformado el entorno estratégico de defensa. En este contexto, las amenazas cibernéticas representan desafíos cada vez más complejos y sofisticados para la soberanía nacional, la estabilidad institucional y la integridad de las Fuerzas Armadas.

La República del Paraguay transita actualmente un proceso de fortalecimiento normativo en materia de ciberseguridad, que evidencia la imperante necesidad de establecer una Política de Ciberseguridad Militar sólida y articulada dentro del Ministerio de Defensa Nacional y las Fuerzas Armadas de la Nación. Esta política representa un instrumento fundamental para la construcción de capacidades de ciberseguridad y ciberdefensa, la protección del ciberespacio nacional y el fortalecimiento de la soberanía digital, la cual debe estar acompañada del desarrollo de una doctrina específica de ciberdefensa que responda estratégicamente a los retos del entorno digital contemporáneo.

Esta política busca establecer un marco estratégico para fortalecer la postura de defensa cibernética del sector Militar Paraguayo, garantizando la protección de infraestructuras críticas, el desarrollo de capacidades humanas y tecnológicas, y la integración de la ciberseguridad como componente esencial de la doctrina de defensa nacional.

La formulación de esta Política se alinea con los principios establecidos en la Política Nacional de Defensa 2019-2030, la Estrategia Nacional de Ciberseguridad 2025-2028, el Plan Estratégico 2023 - 2028 Seguridad para el Desarrollo y demás instrumentos normativos que rigen la seguridad digital del Estado Paraguayo.

En este contexto, la formulación e implementación de una Política de Ciberseguridad Militar contribuirá decisivamente al fortalecimiento de la soberanía digital del país, asegurando la defensa nacional en el ciberespacio y posicionando a



las Fuerzas Armadas como un actor estratégico, competente y comprometido con la protección de activos digitales nacionales.

2. MARCO LEGAL EN MATERIA DE CIBERSEGURIDAD Y CIBERDEFENSA DEL PARAGUAY

La legitimidad de esta política se sustenta en un conjunto de disposiciones legales, marcos estratégicos nacionales e instrumentos internacionales, asegurando su coherencia y pertinencia dentro del ordenamiento jurídico paraguayo, las cuales son:

a. Legislación Nacional

- Constitución Nacional: El Artículo 30 refiere sobre el derecho a la privacidad de las comunicaciones; base para la protección de datos e integridad de sistemas.
- Ley N° 6207/2018 - Crea el MITIC como autoridad nacional en ciberseguridad, con facultades para diseñar políticas, coordinar acciones estatales y gestionar incidentes cibernéticos.
- Ley N° 4439/2011 - Delitos Informáticos que tipifica delitos como sabotaje informático, acceso ilícito y fraude electrónico. No obstante, no existe una legislación integral sobre ciberdelitos o protección de datos personales, evidenciando una debilidad estructural que debe ser subsanada.
- Ley N° 1337/1999 y Ley N.° 5036/2013 - Defensa Nacional y Seguridad Interna Que establecen que la Defensa Nacional es el sistema de políticas del Estado para enfrentar amenazas a la soberanía, integridad y orden constitucional, lo cual incluye las amenazas digitales.
- Ley N° 6.343/19 que crea la Secretaría Nacional de Inteligencia, con competencias en inteligencia cibernética.

b. Políticas y Estratégicas Nacionales

- Política Nacional de Defensa 2019-2030: Reconoce la ciberseguridad como componente estratégico para la defensa nacional.
- Política Militar 2019 - 2030 inspirado en la Política Nacional de Defensa en el punto A Orientaciones principales, en su ítem 7: menciona La Ciberdefensa.

- Política de Ciberdefensa aprobada por Resolución N° 573/2022 del Ministerio de Defensa Nacional.
- Estrategia Nacional de Ciberseguridad 2025-2028: Establece principios rectores y acciones para fortalecer el ecosistema digital del país.
- Plan Estratégico 2023-2028 Seguridad para el Desarrollo: Eje 4: Protección de Infraestructura Crítica y Recursos Estratégicos.

3. OBJETIVOS ESTRATÉGICOS DE LA POLÍTICA DE CIBERSEGURIDAD MILITAR

La Política de Ciberseguridad Militar establece los siguientes objetivos estratégicos, orientados al fortalecimiento de la seguridad digital en el ámbito de la defensa:

- a. Proteger las Infraestructuras Críticas Militar.
- b. Fortalecer la capacidad de respuesta ante ciberataques.
- c. Impulsar la formación y especialización del personal militar.
- d. Integrar la Ciberseguridad en la Doctrina Militar.
- e. Fortalecer la cooperación interinstitucional e internacional.

4. DIRECTRICES DE LOS OBJETIVOS ESTRATÉGICOS DE LA POLÍTICA DE CIBERSEGURIDAD MILITAR.

a. Proteger las Infraestructuras Críticas Militares.

- Asegurar la resiliencia de sistemas informáticos, redes de comunicación, centros de comando y plataformas operativas militares frente a ciberamenazas.
- Establecer protocolos de contingencia, recuperación y respuesta ante incidentes cibernéticos que afecten activos estratégicos.

b. Fortalecer la capacidad de respuesta ante ciberataques.

- Desarrollar capacidades operativas de vigilancia, detección, análisis y neutralización de ataques informáticos.
- Implementar sistemas de monitoreo continuo y centros de operaciones cibernéticas (Cyber-COCs) dentro de las Fuerzas Armadas.

c. Impulsar la formación y especialización del personal militar.

- Fomentar programas de capacitación técnica y táctica en Ciberseguridad para oficiales, suboficiales y especialistas.
- Establecer alianzas con universidades, academias militares y entidades internacionales para la profesionalización en el área de Ciberseguridad y Ciberdefensa.

d. Integrar la Ciberseguridad en la Doctrina Militar

- Incorporar la Ciberseguridad como eje transversal en la planificación estratégica, entrenamiento y operaciones militares.
- Reconocer el Ciberespacio como un dominio operacional junto con la tierra, el aire, el mar y el espacio.

e. Fortalecer la cooperación interinstitucional e internacional

- Promover sinergias con entidades civiles, gubernamentales y organismos internacionales para una defensa digital colaborativa.
- Participar activamente en ejercicios conjuntos y redes de intercambio de información cibernética.

5. PRINCIPIOS RECTORES DE LA POLÍTICA DE CIBERSEGURIDAD MILITAR

La Política de Ciberseguridad Militar se basa en principios fundamentales que orientan su implementación y aseguran su coherencia institucional:

a. Seguridad Integral

La protección de los sistemas militares debe considerar aspectos físicos, digitales y humanos, garantizando una defensa holística ante amenazas multidimensionales manteniendo la soberanía tecnológica y operativa.



b. Soberanía Tecnológica

El principio de soberanía tecnológica implica que Paraguay controle, administre y desarrolle sus propios sistemas digitales, minimizando la exposición y dependencia de proveedores tecnológicos extranjeros, especialmente en sectores sensibles como la Defensa Nacional, la Ciberseguridad y las Comunicaciones Estratégicas.

c. Interoperabilidad

Capacidades tecnológicas compatibles con otras fuerzas y organismos, facilitando la coordinación en operaciones conjuntas y sistemas de intercambio seguro de información, optimizando recursos tecnológicos y humanos para enfrentar desafíos complejos en escenarios cada vez más interconectados.

d. Integración de la Ciberseguridad y Ciberdefensa en la Doctrina Militar

La Ciberseguridad en conjunto con la ciberdefensa se integra en la planificación estratégica, entrenamiento y operaciones militares como eje transversal. Y se reconoce al ciberespacio como un dominio operacional junto a terrestre, aéreo, marítimo y espacial.

e. Cooperación interinstitucional e internacional.

Se busca sinergias con entidades civiles, gubernamentales y organismos internacionales para una defensa digital colaborativa. Participando activamente en ejercicios conjuntos y redes de intercambio de información cibernética.

6. COORDINACIÓN INSTITUCIONAL

La implementación de la Política de Ciberseguridad Militar requiere un enfoque colaborativo entre el Ministerio de Defensa Nacional y el Comando de las Fuerzas Militares que articule esfuerzos con diferentes organismos del Estado y actores internacionales. La coordinación garantiza una respuesta integral, eficaz y sostenida frente a amenazas cibernéticas.

a. Ministerio de Defensa Nacional

- Encargado de liderar la formulación, ejecución y supervisión de esta política en el ámbito militar.
- Coordina con el Comando de las FFMM (Comando de Ciberdefensa) asuntos técnicos, operativos y estratégicos de ciberdefensa y ciberseguridad.

b. Comando de las FFMM /Comando Ciberdefensa.

- El Comando de las FFMM a través de un Comando de Ciberdefensa (CCD), será el responsable de asesorar al Ministro de Defensa Nacional sobre la implementación y gestión de la Ciberseguridad y Ciberdefensa en el Ciberespacio.
- Facilita el intercambio de información con organismos del Estado como la Secretaria Nacional de Inteligencia (SNI) y el Ministerio de Tecnologías de la Información y Comunicación (MITIC).

7. MONITOREO, EVALUACIÓN Y ACTUALIZACIÓN.

El monitoreo, la evaluación y actualización de la Política de Ciberseguridad Militar son componentes esenciales para garantizar su efectividad operativa, su alineación con los objetivos estratégicos, y su adaptación ante nuevas amenazas tecnológicas. Teniendo en cuenta los siguientes indicadores de desempeño:

b. Monitoreo

- Grado de implementación de medidas de protección en sistemas militares establecidas en la estrategia militar de Ciberseguridad Y Ciberdefensa.
- Número de incidentes cibernéticos reportados, mitigados y resueltos.
- Porcentaje de personal capacitado en Ciberseguridad por unidad militar.
- Nivel de interoperabilidad con actores institucionales y aliados internacionales.

b. Evaluación (Auditorías Técnicas)

- Evaluaciones periódicas (semestrales o anuales) del estado de los sistemas, redes, logros, desafíos y mecanismos de Ciberseguridad y Ciberdefensa.



- Auditorías internas realizadas por entidades de control y cooperación técnica.

c) Actualización

- Establecimiento de un ciclo de actualización cada 3 años que contemple; Incorporación de nuevas tecnologías y amenazas emergentes, actualización de objetivos, principios y estrategias según contexto geopolítico.
- Consultas a expertos, unidades técnicas, organismos gubernamentales en el proceso de actualización que establece los elementos institucionales para la vigencia, implementación y revisión de la política.

8. VIGENCIA, RESPONSABILIDAD Y DIFUSIÓN.

Se define las condiciones de entrada en vigor, asignación de responsabilidades y mecanismos de revisión de la Política de Ciberseguridad Militar del Paraguay.

a. Vigencia e implementación

- La política entrará en vigor a partir de su aprobación por el Ministerio de Defensa Nacional.
- Su implementación será progresiva, conforme a las capacidades operativas, presupuestarias y normativas de las Fuerzas Armadas.

b. Responsabilidades institucionales

- El Ministerio de Defensa Nacional será el órgano rector.
- Las Fuerzas Armadas deberán adecuar sus estructuras, planes y procedimientos para cumplir lo establecido.
- Las instituciones mencionadas más arriba (MDN y FFMM) deberán coordinar con la Secretaría Nacional de Inteligencia y el MITIC el apoyo técnico y estratégico necesario para el cumplimiento de los objetivos propuestos.

c. Difusión y sensibilización

- La política será divulgada a todo el personal militar mediante canales oficiales, capacitaciones y materiales informativos.



- Se promoverá la cultura de seguridad digital en todos los niveles institucionales.

9. Disposiciones Finales

La Política de Ciberseguridad Militar representa un pilar estratégico esencial para la Defensa Nacional en el siglo XXI. Su enfoque integral, escalonado y colaborativo articula con precisión los niveles político, estratégico y táctico, conectando el diseño normativo con la ejecución operativa en todos los dominios. Esta política no sólo responde al incremento de amenazas en el entorno digital, sino que también posiciona al Estado Paraguayo con una postura firme, soberana y proactiva ante los desafíos contemporáneos del Ciberespacio.

Su implementación requiere la sincronización efectiva de las Fuerzas Armadas con organismos estatales, actores del sector privado y socios internacionales, consolidando una gobernanza ciber estratégica que trasciende lo meramente técnico. A través de ejes como la innovación tecnológica, la capacitación especializada, la creación de unidades de élite y la cooperación institucional, se configura una arquitectura de defensa digital resiliente, adaptativa y capaz de ejercer disuasión ante amenazas cibernéticas.

Esta política no sólo preserva los activos estratégicos y la Infraestructura Crítica del país, sino que amplía el rol de las Fuerzas Armadas como actor relevante dentro del ecosistema nacional de Ciberseguridad, fortaleciendo la defensa integral del territorio paraguayo en el dominio virtual. En suma, constituye un instrumento de soberanía digital y seguridad nacional, alineado con los principios democráticos y los estándares internacionales, indispensable para proyectar a la República del Paraguay como un Estado frente a los desafíos del entorno global.



MINISTERIO DE DEFENSA NACIONAL

DIRECCIÓN GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

DIRECCIÓN DE CIBERSEGURIDAD

Avenida Mariscal López esquina Vicepresidente Sánchez y 22 de septiembre

Asunción, Paraguay

595 21 2490 000 - 1039

ciberseguridad@mdn.gov.py

www.mdn.gov.py