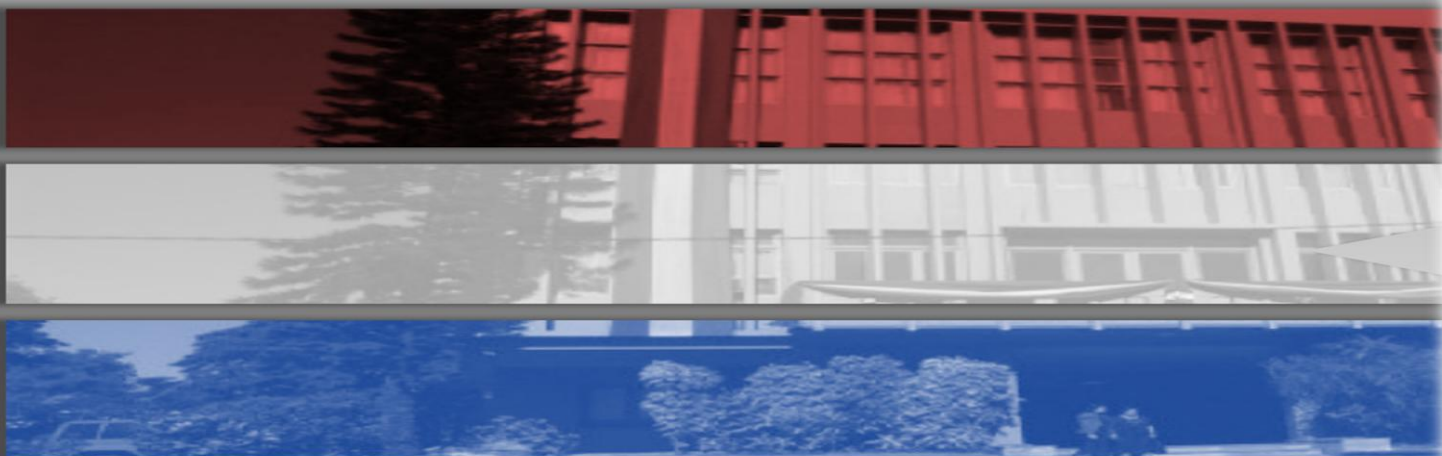




MINISTERIO DE DEFENSA NACIONAL

POLÍTICA DE CIBERDEFENSA MILITAR

2025 - 2030



GOBIERNO DEL
PARAGUAY **MINISTERIO DE**
DEFENSA
NACIONAL

mdn.gov.py



El presente documento fue actualizado, en 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. FINALIDAD.....	5
3. APLICACIÓN.....	5
4. PLANTEAMIENTOS BÁSICOS.....	6
5. OBJETIVOS ESTRATÉGICOS DE LA POLÍTICA DE CIBERDEFENSA.....	7
6. DIRECTRICES DE LOS OBJETIVOS DE LA POLÍTICA DE CIBERDEFENSA.....	8
7. RESPONSABILIDAD.....	12
8. ACTUALIZACIÓN.....	13
9. PROYECCIÓN ESTRATÉGICA EN EL ÁMBITO CIBERNÉTICO.....	13
10. DISPOSICIONES FINALES.....	14



1. INTRODUCCIÓN

La República del Paraguay transita actualmente un proceso de fortalecimiento normativo en materia de Ciberseguridad y Ciberdefensa, que evidencia la imperante necesidad de establecer una Políticas sólidas y articuladas dentro del Ministerio de Defensa Nacional y las Fuerzas Armadas de la Nación. Esta Política de Ciberdefensa constituye la respuesta a los nuevos riesgos y amenazas que el Ciberespacio genera para las capacidades de la Defensa Nacional, las cuales incluyen, entre otros elementos, la información, la infraestructura y las operaciones de defensa.

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 Ciberdefensa como componente esencial de la Doctrina de Defensa Nacional. La Ciberdefensa como concepto generalista, es el conjunto de medidas técnicas, políticas y organizativas enfocadas a proteger los sistemas de información, comunicaciones y control ante ciberataques de cualquier índole.

Como concepto militar, se centra en las medidas técnicas, políticas y organizativas que protegen los sistemas y redes militares de ciberataques, e incluye las capacidades de reacción y ataque propias de un conflicto armado (utilizando el ciberespacio), la protección puede extenderse a sistemas de información de terceros (civiles) que puedan resultar críticos para la nación o la misión. La Ciberdefensa se desarrolla en coherencia con la cultura de la Ciberseguridad en torno a la educación, buenas prácticas y responsabilidad en el manejo de tecnologías digitales que defina el Estado para el conjunto de los actores nacionales.

La Ciberdefensa contribuye al objetivo de prevenir que desde Paraguay se lleven a cabo acciones ilícitas en contra de otros Estados, sus habitantes o sus intereses, en el ámbito de competencia de la Defensa Nacional. La Defensa Nacional sitúa la Política de Ciberdefensa dentro del marco jurídico institucional vigente en el país, y reconoce y



respetar los tratados y acuerdos internacionales suscritos, aprobados y ratificados, sus normas, principios y costumbres.

Asimismo, se faculta y habilita a las Fuerzas Militares, a través de su órgano asesor; el Comando de Ciberdefensa, para formular y presentar propuestas estratégicas y tácticas orientadas al fortalecimiento de las capacidades operativas en el dominio cibernético.

La actualización de la Política de Ciberdefensa, aprobada por Resolución Ministerial N° 573 del 09 de octubre de 2021, 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 actualización e implementación de esta Política de Ciberdefensa 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. FINALIDAD

La Política de Ciberdefensa tiene como finalidad orientar las acciones del Ministerio de Defensa Nacional (MDN), en el ámbito de la Defensa Nacional, en el nivel estratégico operacional y táctico, para lograr los objetivos trazados en el Ciberespacio.

3. APLICACIÓN

La Política de Ciberdefensa se aplica en el ámbito de la Expresión Militar, proyectado al Poder y Potencial Nacional; así como a las instituciones y/o entidades que cooperan para las actividades de Defensa y el Desarrollo Nacional y/o Ciberdefensa.

4. PLANTEAMIENTOS BÁSICOS

La definición y determinación de los lineamientos de una Política de Ciberdefensa están orientadas a los siguientes planteamientos básicos:

- a. La Ciberdefensa está a cargo del Ministerio de Defensa Nacional y están encaminada a satisfacer las necesidades estratégicas de Defensa Nacional y proyectado al mantenimiento y consolidación de la soberanía digital.
- b. Las acciones cibernéticas defensivas, exploratorias y de defensa activa serán ejecutadas conforme a la Hipótesis de Empleo (HE) en el Ciberespacio, enmarcadas en los lineamientos estratégicos establecidos para garantizar la seguridad, resiliencia y superioridad operativa en el dominio digital.
- c. El fortalecimiento de la Ciberdefensa se sustenta principalmente en la acción coordinada y colaborativa de los actores encargados de preservar y mantener las Infraestructuras Críticas, cuya responsabilidad trasciende el ámbito del Ministerio de Defensa Nacional y se proyecta hacia todas las dimensiones del Poder Nacional.
- d. Fomentar la cooperación en la generación de inteligencia de origen cibernético relevante para la Ciberdefensa, con especial atención a las instituciones y unidades encargadas de la Defensa Nacional.
- e. El fortalecimiento de las capacidades tecnológicas del sector cibernético debe impulsarse de forma articulada y coherente con la Política de Ciencia, Tecnología e Innovación para la Defensa Nacional (C, T & I), asegurando su integración estratégica en los objetivos de seguridad y defensa del Estado
- f. La eficacia de las acciones de Ciberdefensa está directamente vinculada al marco de políticas, normas y procedimientos establecidos en materia de seguridad de la información. Este marco debe asegurar los principios de confidencialidad, disponibilidad e integridad de los datos, así como garantizar una cadena de custodia robusta y trazable.



- g. En el ámbito de la Defensa Nacional, las operaciones de Ciberdefensa tienen como propósito asegurar el uso legítimo y seguro del Ciberespacio, anticipando, previniendo y neutralizando amenazas que puedan comprometer los Intereses Nacionales, y preservando así la libertad de acción estratégica.
- h. La implementación de una arquitectura de seguridad integral, acompañada del desarrollo de normativas específicas, es fundamental para garantizar el funcionamiento seguro y sostenido de las redes que respaldan las Infraestructuras Críticas (IC) bajo responsabilidad de las Fuerzas Armadas de la Nación.
- i. La Ciberdefensa debe asegurar la continuidad operativa de los servicios y actividades esenciales frente a escenarios de contingencia cibernética, garantizando la capacidad de respuesta de las Fuerzas Armadas y su proyección efectiva en las distintas dimensiones del Poder Nacional.
- j. Resulta imprescindible definir prioridades estratégicas en materia de Ciberdefensa abordando de manera integral los siguientes ejes: desarrollo doctrinario, formación y capacitación especializada, gestión eficiente del talento humano, adquisición de equipamiento tecnológico, fortalecimiento de la infraestructura, impulso a la ciencia, tecnología e innovación, protección de Infraestructuras Críticas (IC), optimización de la conectividad, aumento de la resiliencia operativa y consolidación de un marco legal robusto y actualizado.

5. OBJETIVOS ESTRATÉGICOS DE LA POLÍTICA DE CIBERDEFENSA

Los objetivos de la Política de Ciberdefensa se estructuran conforme a la visión estratégica establecida en la Política Nacional de Defensa (PND), reconociendo el Ciberespacio como un dominio operacional crítico para la seguridad nacional y que responde a la necesidad imperativa de anticipar, prevenir y neutralizar amenazas emergentes que comprometan la soberanía digital, la estabilidad institucional y la integridad del Estado. Estos objetivos son:

- a. Asegurar el uso estratégico y seguro del Ciberespacio.
- b. Asegurar la protección de Infraestructura Crítica (IC) y Recursos Estratégicos.
- c. Cooperar en la generación de Ciberinteligencia a fin de apoyar la toma de decisiones operativas y estratégicas en el ámbito del Ciberespacio.
- d. Diseñar y ejecutar programas de formación de talento humano con capacidades cibernéticas.
- e. Fortalecer las estructuras de Ciencia, Tecnología e Innovación (C, T & I), en las Fuerzas Militares, orientadas a satisfacer los requerimientos estratégicos de la Ciberdefensa.
- f. Desarrollar y mantener actualizada la Política y Doctrina de empleo de la Ciberdefensa.

6. DIRECTRICES DE LOS OBJETIVOS ESTRATÉGICOS DE LA POLÍTICA DE CIBERDEFENSA

a. Asegurar el uso estratégico y seguro del Ciberespacio.

- Integrar el Ciberespacio como componente esencial del poder militar nacional, articulando doctrinas, estructuras y tecnologías que permitan operar de manera efectiva en escenarios híbridos y multidominio.
- Contribuir a la defensa integral del territorio y la población, enfrentando amenazas como el terrorismo, el crimen organizado transnacional, el narcotráfico y los grupos armados ilegales, que utilizan el ciberespacio como plataforma de acción.
- Establecer un Consejo de Ciberdefensa, concebido e implementado con participación multisectorial de las expresiones del Poder Nacional, orientado a la formulación de políticas, la toma de decisiones estratégicas y la consolidación de capacidades en el ámbito de la defensa del Ciberespacio.
- Crear un Comando de Ciberdefensa (CCD) para llevar a cabo la coordinación e integración de la Ciberdefensa entre las FFMM, institución

Primaria de la Defensa Nacional y los entes Políticos y Estratégicos de la Defensa Nacional.

- Mantener una base de datos y establecer un canal sistémico/técnico entre el Comando de Ciberdefensa (de ser creado) y otras instituciones para el intercambio de información de incidentes en la red.
- Establecer programas y/o proyectos para garantizar la capacidad de conectividad de las redes, de manera a fortalecer la operatividad de la actividad de Comando de Ciberdefensa (CCD), Comando y Control (C2), Guerra Electrónica, Comunicaciones, Inteligencia, Equipos de Respuestas a Incidentes Cibernéticos (preventivos, detectivos y correctivos) como parte de un Comando de Ciberdefensa, a través de las FFMM y el Ministerio de Defensa Nacional.

b. Asegurar la Protección de Infraestructura Crítica y Recursos Estratégicos.

- Establecer los criterios de riesgo de los activos críticos de información, mitigando los riesgos para las infraestructuras críticas, de interés para la Defensa Nacional y su proyección a la soberanía digital.
- Establecer las estrategias y las estructuras adecuadas que permitan dirigir, coordinar y supervisar las Infraestructuras Críticas (IC), a cargo de las FFAA de la Nación.
- Crear y estandarizar procesos de seguridad de la información de las Infraestructuras Críticas (IC) y de interés para la Defensa Nacional y la soberanía digital.
- Establecer un Plan de Contingencia y continuidad de las Infraestructuras Críticas (IC).
- Realizar intercambios doctrinarios para la preservación de Infraestructuras Críticas (IC).

- Cooperar con otros órganos o entes de Ciberdefensa.

c. Cooperar en la generación de Ciberinteligencia a fin de apoyar la toma de decisiones operativas y estratégicas en el ámbito del Ciberespacio.

- Crear estructuras de Ciberinteligencia, según lo necesiten las instituciones y/o unidades de inteligencia de las FFAA, para aplicar métodos científicos y sistemáticos, buscando extraer y analizar datos de la fuente Cibernética, produciendo conocimiento de interés para la Ciberdefensa.
- Establecer un canal sistémico y técnico entre los órganos de Ciberdefensa y de inteligencia de las FFAA.
- Contribuir a la formación de la conciencia situacional necesaria para las actividades de inteligencia en apoyo a la Defensa y el Desarrollo Nacional.

d. Diseñar y ejecutar programas de formación de talento humano con capacidades cibernéticas.

- Identificar, registrar y seleccionar personal con habilidades o destrezas, existentes en los entornos internos y externos de las FFAA, para integrar un Comando de Ciberdefensa.
- Proyectar la participación del personal involucrado en la Ciberdefensa realizando cursos, pasantías, congresos, seminarios, simposios, ejercicios de simulación conjunto y otras actividades relacionadas en nuestro país y en el extranjero.
- Representar al Paraguay en el Foro Iberoamericano de Ciberdefensa.
- Preparar Planes y programas de entrenamiento, ejercicios de simulación en la Operaciones Conjuntas de Ciberdefensa
- Fortalecer los lazos de cooperación con los países en materia de Ciberdefensa.

- Realizar intercambios doctrinarios para la preservación de Infraestructuras Críticas (IC).
 - Impulsar la firma de convenios de cooperación de Ciberdefensa.
 - Promover desarrollo de capacidades propias en materia de Ciberseguridad y Ciberdefensa para preservar la soberanía digital y tecnológica.
 - Realizar eventos periódicos que permitan la presentación y discusión de temas relevantes en áreas de interés para el sector cibernético, a ser organizado y dirigido por el Comando de Ciberdefensa, para unificar criterios, nivelar y actualizar el conocimiento.
 - Incluir el contenido de Ciberdefensa al plan de estudios de los cursos en todos los niveles de las instituciones educativas de las FFAA.
 - Promover la realización de una campaña de sensibilización y concientización en Ciberdefensa.
- e. Fortalecer las estructuras de Ciencia, Tecnología e Innovación (C, T & I) en las Fuerzas Militares, orientadas a satisfacer los requerimientos estratégicos de la Ciberdefensa.**
- Crear programas a cargo del MDN, en asociación con el MITIC que aborden la doble característica (empleo civil y militar) de las tecnologías de información y comunicación (TIC) empleadas en el área cibernética, para fortalecer la participación del sector industrial en las fases de proyectos de interés de la Ciberdefensa.
 - Adaptar las estructuras de la Ciencia, Tecnología e Innovación (C, T & I) de las Fuerzas Singulares y Direcciones Generales, para implementar las actividades de investigación y desarrollo, a fin de satisfacer las necesidades de la Ciberdefensa
 - Crear un Comité permanente compuesto por representantes del Ministerio de Defensa Nacional e invitados, otros ministerios y agencias de financiamiento



para intensificar y explorar nuevas oportunidades de cooperación en C, T & I en las áreas de interés del Sistema de Ciberdefensa.

f. Desarrollar y mantener actualizada la Política y Doctrina de empleo de la Ciberdefensa

- Cooperar para la elaboración de la Política Nacional de Ciberdefensa.
- Mantener actualizada la Política de Ciberdefensa en línea con la Política de Defensa Nacional (cuando esté en vigencia).
- Definir atribuciones y responsabilidades para el ejercicio de actividades relacionadas con la Ciberdefensa.
- Elaborar propuestas para la creación y adaptación de legislación, para apoyar las actividades de Ciberdefensa.
- Revisar los planes de Hipótesis de Empleo (HE) para considerar acciones en el Ciberespacio.
- Crear la Doctrina de Ciberdefensa.
- Promover intercambios doctrinarios, normativos y técnicos con instituciones civiles y militares, nacionales y de países amigos.
- Insertar la Ciberdefensa en ejercicios de simulación de combate y Operaciones Conjuntas.
- Crear un sistema de gestión del conocimiento de las lecciones aprendidas para la composición y actualización de la doctrina de Ciberdefensa.

7. RESPONSABILIDADES

El Comandante de las Fuerzas Militares (FFMM), mediante la creación y operación de un Comando de Ciberdefensa (CCD), asumirá la responsabilidad de asesorar a los



niveles Político y Estratégico de la Defensa Nacional en materia de implementación, conducción y supervisión de la Ciberdefensa. Esta función tiene como propósito fortalecer, asegurar y alcanzar niveles óptimos de seguridad y resiliencia en el Ciberespacio, en concordancia con los intereses nacionales y los desafíos del entorno digital.

8. ACTUALIZACIÓN

Durante el período 2025-2030, esta Política será objeto de revisión y actualización periódica por parte del Ministerio de Defensa Nacional, ya sea por iniciativa propia o en respuesta a propuestas formuladas por las Fuerzas Armadas de la Nación. Este proceso garantizará su adecuación continua frente a los avances tecnológicos, los desafíos emergentes en materia de seguridad y las prioridades estratégicas del Estado en el ámbito de la Defensa Nacional.

9. PROYECCIÓN ESTRATÉGICA EN EL ÁMBITO CIBERNÉTICO

Con miras a fortalecer la postura nacional en el Ciberespacio durante el período 2025-2030, se establece como prioridad contar con los siguientes elementos estructurales, doctrinarios y operativos:

- **Política de Ciberdefensa** que establezca los principios rectores, objetivos y líneas de acción para la defensa activa en el entorno digital.
- **Política de Ciberseguridad** orientada a la protección integral de activos digitales, sistemas de información y servicios esenciales frente a amenazas cibernéticas.
- **Doctrina de Ciberdefensa** que articule conceptos operativos, tácticos y estratégicos para la conducción de operaciones en el Ciberespacio.
- **Plan de Ciberdefensa** que operacionalice la política y doctrina mediante programas, metas y recursos asignados.



- **Plan de Protección de Infraestructuras Críticas (IC)** enfocado en identificar, priorizar y resguardar los sistemas vitales para el funcionamiento del Estado.
- **Un Comando de Ciberdefensa** como órgano especializado para la planificación, ejecución y coordinación de acciones de defensa cibernética en el ámbito conjunto.
- **Optimización de la estructura organizacional** asegurando una arquitectura funcional, interoperable y adaptable a los desafíos emergentes.
- **Optimización de la tecnología** mediante la incorporación de capacidades avanzadas de detección, respuesta, inteligencia artificial y automatización.
- **Formación y capacitación especializada de Cibersoldados**, con perfiles técnicos, tácticos y estratégicos que respondan a los requerimientos operativos del entorno digital.

10. DISPOSICIONES FINALES

Esta Política de Ciberdefensa Militar, tiene carácter obligatorio para las Instituciones con responsabilidad primaria o complementaria para la Defensa Nacional, así como para aquellas de base para la Defensa de nuestros Intereses Vitales y Recursos Estratégicos. Se constituye en referencia para los demás entes públicos del Estado en temas transversales de Defensa de los Intereses Vitales y Recursos Estratégicos del País.

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, fortaleciendo la defensa integral del territorio paraguay con una postura firme, soberana y proactiva ante los desafíos contemporáneos en el Ciberespacio.

La actualización de esta Política de Ciberdefensa Militar entra en vigencia a partir de la divulgación de la Resolución respectiva, hasta el año 2030, inclusive.



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