PLANTEAMIENTO DE LA CIBERDEFENSA PARA FORTALECER LA SOBERANÍA TECNOLÓGICA Y DEFENSA NACIONAL. PARAGUAY – 2023

Dr. Edgar Ramón Mendoza Silva[1,*]

[1]Egresado del Doctorado de Desarrollo y Defensa, Universidad Metropolitana de Asunción, Asunción – Paraguay

Correo: edgarmsilva79@gmail.com

RESUMEN

La presente investigación analiza el planteamiento de la ciberdefensa como apoyo a la soberanía tecnológica y defensa nacional en Paraguay, 2023, con el propósito de aportar nuevos conocimientos en el área. El estudio se desarrolló con un enfoque descriptivo, orientado a la recolección, análisis e interpretación de datos mediante encuestas y entrevistas. Los resultados evidencian la necesidad de adoptar y adecuar doctrinas, recursos humanos, infraestructuras y equipamientos en el área de la ciberdefensa, con el objetivo de mitigar riesgos cibernéticos y concientizar sobre la importancia de la seguridad tecnológica. Asimismo, se identificó la relevancia de acompañar la transformación digital mediante la defensa nacional. La investigación concluye que los planteamientos estratégicos — políticas estatales de seguridad, estructuras tecnológicas y humanas, proyectos de seguridad, gestión de riesgos y planificación del desarrollo tecnológico — constituyen un plan de acción para fortalecer la defensa nacional y consolidar la soberanía tecnológica en Paraguay.

Palabras clave: Ciberdefensa, soberanía tecnológica, defensa nacional.

ABSTRACT

This research analyzes the role of cyber defense in strengthening technological sovereignty and national defense in Paraguay, 2023. The study was conducted with a descriptive approach, oriented toward the collection, analysis, and interpretation of data through surveys and interviews with key stakeholders in defense and information technology. The findings highlight the urgent need to adopt and adapt doctrines, human resources, infrastructures, and equipment in the field of cyber defense, with the objective of mitigating cyber risks and raising awareness of the importance of technological security. In addition, the results emphasize the relevance of accompanying the ongoing digital transformation with the implementation of a comprehensive cyber defense policy projected toward technological sovereignty and national defense. The study concludes that strategic guidelines — such as state security policies, technological and human structures, risk management, security projects, and technological development planning — constitute a coherent plan of action for national defense institutions. These measures not only support the consolidation of technological sovereignty but also contribute to the long-term strengthening of Paraguay's national defense capabilities.

Keywords: Cyber defense, technological sovereignty, national defense.

1. INTRODUCCIÓN

La presente investigación aborda el tema de la ciberdefensa en relación con la soberanía tecnológica y la defensa nacional, considerando la creciente preocupación en el ámbito de la seguridad internacional por el control y la invulnerabilidad de las infraestructuras críticas soportadas en Internet. Esta preocupación se ha intensificado a raíz de los ataques globales dirigidos a sistemas informáticos de instituciones públicas y privadas (Ocón & Gastaldi, 2019).

En el contexto nacional, la ciberdefensa se encuentra en una etapa de desarrollo doctrinario, enmarcada en las políticas del gobierno y de las instituciones responsables de la defensa nacional, con el objetivo de articular y cooperar en la construcción de un sistema de defensa cibernética (Consejo de Defensa Nacional Paraguay, 2019; Ministerio de Defensa Nacional Paraguay, 2022). La aprobación de la política de ciberdefensa exige la adecuación de recursos humanos, doctrinas, infraestructuras y equipamientos para mitigar riesgos cibernéticos, en un escenario donde el ciberespacio ha dejado de ser un dominio emergente para convertirse en un potencial teatro de guerra, obligando a revisar las nociones tradicionales de soberanía tecnológica (Bordignon, 2016; Ceballos & Maisonnave, 2020; Pohle & Thiel, 2022).

El estudio plantea la necesidad de consolidar un marco de actuación mediante estrategias y líneas de acción que fortalezcan la política de ciberdefensa y mejoren gradualmente la seguridad de las redes informáticas frente a amenazas y ciberataques. En este sentido, la ciberdefensa se configura como un componente estratégico del sistema de defensa nacional, que requiere un proceso continuo de aprendizaje y adaptación para enfrentar los desafíos emergentes de la preservación de la soberanía tecnológica (Cuenca Rótela, 2009; Sabiguero et al., 2016).

2. MARCO TEÓRICO

La inserción de las Tecnologías de la Información y Comunicación (TIC) en el ámbito castrense de las Fuerzas Armadas de la Nación, conforme al *Manual Especial ME 55-400: Fundamentos de Introducción a las TIC* (2019), ha traído consigo tanto avances como dificultades. Entre los principales desafíos se destacan los ciberataques, aunque no constituyen el único riesgo. También se identifican amenazas vinculadas a daños en equipos informáticos, fallas en redes, errores humanos involuntarios, catástrofes naturales, pandemias y otros hechos que pueden ocasionar pérdidas significativas en el ecosistema digital.

El impacto de las TIC trasciende el ámbito militar y se proyecta en las dimensiones social, económica, política y cultural. En el contexto de la globalización, la información circula sin barreras geográficas y se caracteriza por su inmaterialidad, instantaneidad, interactividad y capacidad multimedia. Este fenómeno refleja una época de innovaciones profundas que transforman la realidad en todas sus dimensiones.

Para enfrentar estos retos, resulta indispensable fortalecer los recursos humanos. Cohen (2002) señala que la formación de capital humano es un proceso complejo, donde la motivación del estudiante constituye el factor clave para alcanzar los objetivos de aprendizaje. En el ámbito militar, este principio se mantiene vigente: la carrera castrense exige disciplina y disposición para aprender, con el fin de desarrollar las competencias necesarias para la defensa nacional.

La gestión tecnológica constituye un eje fundamental para el desarrollo de capacidades estratégicas en defensa y soberanía digital, ya que permite articular procesos de innovación, planificación y aprovechamiento de recursos tecnológicos en beneficio de la seguridad nacional. En este sentido, diversos estudios destacan que la gestión tecnológica es clave para consolidar políticas de soberanía digital y fortalecer la capacidad de respuesta frente a amenazas emergentes (Britos, Hernández, & Álvarez, 1998).

La ciberdefensa, en este contexto, se configura como un elemento estratégico para el fortalecimiento de la soberanía tecnológica y la defensa nacional. La *Política de Ciberdefensa* (Ministerio de Defensa Nacional, 2021) establece que la ciberdefensa y la ciberseguridad forman parte de un sistema integrado, cuyo propósito es mitigar riesgos cibernéticos y garantizar la seguridad del Estado. El *Plan Nacional de Ciberseguridad* (2017) reconoce que la ciberseguridad actúa de manera transversal en todos los niveles, con un enfoque preventivo orientado a la protección de la información. Asimismo, la *Política Nacional de Defensa 2019–2030* (Ministerio de Defensa Nacional, 2019) subraya que la ciberdefensa constituye un componente esencial de la defensa nacional, con capacidades ofensivas, defensivas y exploratorias, proyectadas hacia escenarios de operaciones militares.

Este marco doctrinario enfatiza que la protección del ciberespacio requiere el compromiso de la sociedad en su conjunto. La responsabilidad individual y colectiva resulta indispensable para salvaguardar las infraestructuras críticas nacionales, consolidando así la soberanía tecnológica.

En el ámbito de la soberanía tecnológica, el Ministerio de Tecnologías de la Información y Comunicación (MITIC) y la Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs), con apoyo del Banco Interamericano de Desarrollo (BID) y la consultora Networld Consulting, impulsaron en 2018 el proyecto de diseño y despliegue de un Centro de Datos en Paraguay. El proyecto contempló una infraestructura con topología Tier III y una vida útil estimada de 20 años, destinada a centralizar servicios actuales y futuros de la SENATICs. En 2020, mediante la *Adenda N° I* al contrato de usufructo entre el MITIC y el Ministerio de Defensa Nacional, se establecieron contraprestaciones específicas, como la instalación de alambrado perimetral, espacios para el Comando de Ciberdefensa en el nuevo centro de datos, construcción de casetas y provisión de equipos de teleconferencia. Estas acciones reflejan la articulación institucional en torno a la soberanía tecnológica y la defensa nacional.

La transmisión de datos mediante fibra óptica constituye otro pilar estratégico para reducir la brecha digital en Paraguay. El MITIC y la SENATICs culminaron en 2020 la primera etapa de la Red Nacional de Fibra Óptica, denominada "última milla", que conecta ciudades clave como Asunción, Ciudad del Este y Encarnación. La red troncal se integró con infraestructuras de instituciones estatales como la Administración Nacional de Electricidad (ANDE), la Compañía Paraguaya de Comunicaciones (COPACO), el Ministerio de Hacienda y el Ministerio del Interior, aunque inicialmente no incluyó al Ministerio de Defensa Nacional.

Este proyecto busca consolidar una red única, soberana y robusta, capaz de responder a las demandas actuales de seguridad y estabilidad. Además de la instalación de equipos de última generación, se contemplaron tareas de mantenimiento, actualización y ampliación de la infraestructura existente, con el objetivo de garantizar calidad en la conectividad y fomentar una cultura de colaboración interinstitucional.

3. METODOLOGÍA

La presente investigación se desarrolló bajo un enfoque cualitativo, orientado a comprender las percepciones y experiencias de actores institucionales vinculados a la defensa nacional y la soberanía tecnológica. Se emplearon entrevistas semiestructuradas y encuestas como técnicas principales de recolección de datos, lo que permitió obtener información relevante sobre las políticas, proyectos y desafíos en torno a la ciberdefensa.

El diseño metodológico se estructuró en fases sucesivas: definición del problema, formulación de objetivos, selección de técnicas de recolección de información, análisis de resultados y elaboración de conclusiones. Este proceso se fundamenta en los lineamientos clásicos de la investigación científica, que destacan la importancia de la rigurosidad y la sistematicidad en cada etapa (Hernández, Fernández, & Baptista, 2014).

La población de estudio estuvo conformada por representantes de instituciones responsables de la defensa nacional y de la gestión tecnológica en Paraguay. La muestra, de carácter intencional, incluyó a un número de hasta 19 actores estratégicos del Ministerio de Defensa Nacional, del Ministerio de Tecnologías de la Información y Comunicación (MITIC) y del Comando Conjunto de Ciberdefensa.

El análisis de los datos se realizó mediante técnicas de categorización y triangulación, lo que permitió contrastar la información obtenida en entrevistas y encuestas con los documentos oficiales y las políticas vigentes. Este procedimiento garantizó la validez y confiabilidad de los hallazgos, asegurando que las conclusiones reflejen de manera fiel la realidad estudiada.

4. RESULTADOS Y DISCUSIÓN

Los hallazgos obtenidos a partir de entrevistas y encuestas permiten identificar dimensiones estratégicas vinculadas a la ciberdefensa y la soberanía tecnológica. Las respuestas abiertas reflejan una orientación hacia el fortalecimiento de competencias mediante alianzas en el marco de la transformación digital, lo que evidencia una conciencia institucional sobre la necesidad de anticiparse a amenazas emergentes, en concordancia con la *Política Nacional de Defensa 2019–2030*. Asimismo, se destacó la importancia de aplicar políticas y estándares técnicos en las adquisiciones públicas de equipos, software, hardware y licencias legales, con el fin de mitigar vulnerabilidades y consolidar la seguridad digital, tal como lo establece la normativa vigente.

El análisis de los cuestionarios semiestructurados permitió organizar los resultados en torno a cuatro dimensiones principales. En el plano del planeamiento estratégico (Figura 1), los directores priorizaron funciones de previsión y organización, lo que sugiere una visión institucional de largo plazo orientada al desarrollo tecnológico. En contraste, los jefes enfatizaron la infraestructura y los sistemas de información, mostrando un enfoque más operativo y pragmático. Una minoría de ambos grupos introdujo la necesidad de fortalecer la soberanía tecnológica desde una perspectiva política, lo que aporta un matiz relevante al vincular la ciberdefensa con la seguridad nacional. Estos hallazgos confirman que los fundamentos teóricos constituyen pilares esenciales para proyectar la seguridad cibernética y la soberanía tecnológica, en línea con lo señalado por Castells (2009) sobre el poder de la comunicación en la era digital.

En relación con el nivel de empoderamiento institucional (Figura 2), los directores lo calificaron

Figura 1. *Planeamiento estratégico.*

como regular, mientras que los jefes lo consideraron deficiente. Esta diferencia se explica por el desconocimiento tecnológico señalado por los directores y la falta de inversión en recursos humanos y materiales mencionada por los jefes. El hallazgo refleja una brecha significativa en la capacidad institucional para afrontar la transformación digital, coincidiendo con las advertencias del *Plan Nacional de Ciberseguridad*, que subraya la insuficiencia de recursos para enfrentar amenazas emergentes.

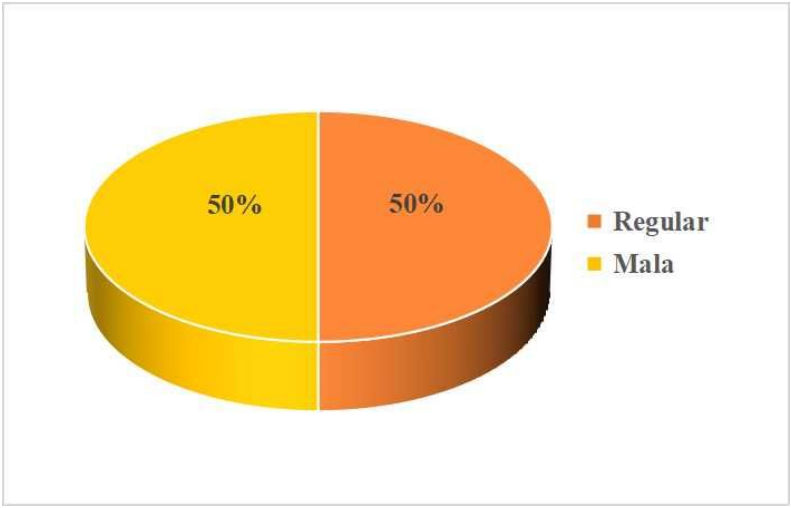

Figura 2. *Nivel de empoderamiento.*

Respecto a la infraestructura (Figura 3), los directores valoraron la disponibilidad física existente, pero los jefes subrayaron la necesidad de contar con personal especializado en ciberdefensa. Este contraste evidencia que la infraestructura tecnológica, aunque necesaria, resulta insuficiente sin capital humano capacitado, reafirmando lo señalado por Cohen sobre la centralidad de la formación en la implementación de la ciberdefensa y la garantía de soberanía tecnológica.

En cuanto a la implementación de la soberanía tecnológica (Figura 4), los directores la vincularon con la seguridad del Estado, mientras que los jefes la relacionaron con el avance tecnológico global. Una minoría destacó la protección de comunicaciones y activos críticos, aportando una visión integral que conecta la ciberdefensa con la preservación de infraestructuras estratégicas. Estos hallazgos

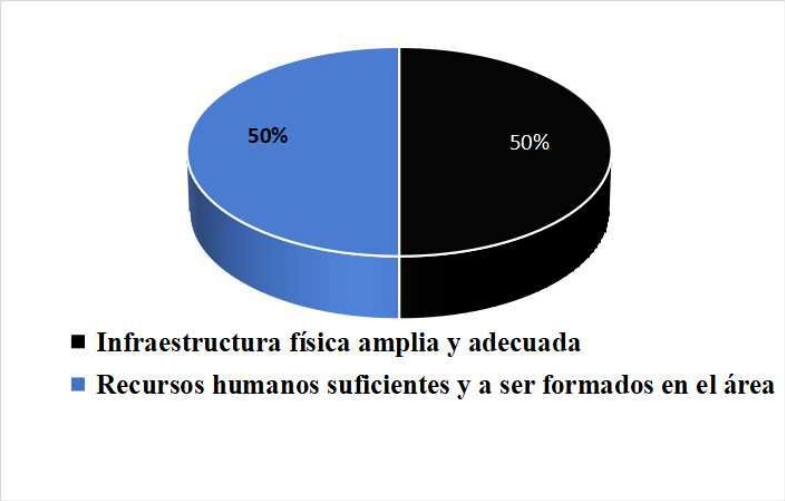

Figura 3. *Infraestructura.*

confirman que la ciberdefensa no solo constituye un mecanismo de protección, sino también un instrumento para garantizar la soberanía tecnológica y la defensa nacional, en concordancia con la *Política de Ciberdefensa*.

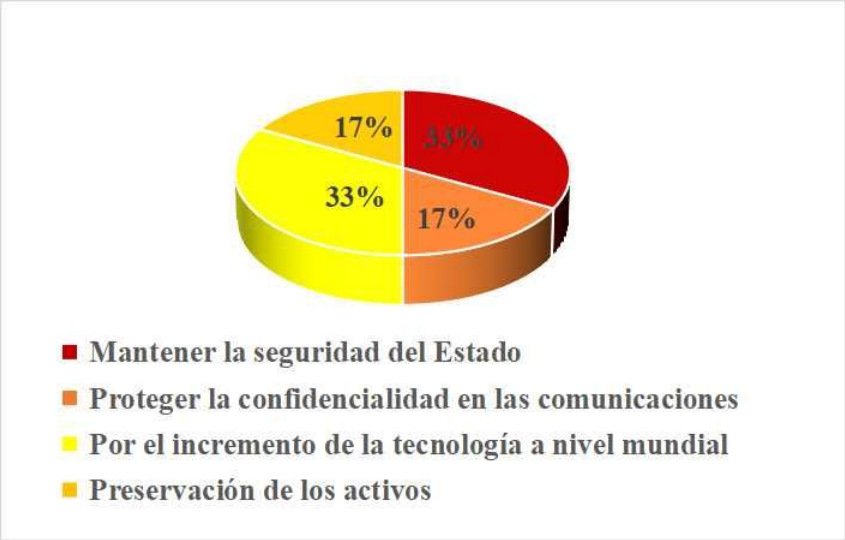

Figura 4. *Implementación de la soberanía tecnológica.*

En conjunto, los resultados evidencian la necesidad de fortalecer la articulación institucional entre organismos de defensa y entidades tecnológicas, promoviendo políticas públicas que aseguren inversiones sostenidas en infraestructura y capacitación. La formación continua en ciberdefensa y la implementación de estándares técnicos obligatorios en las adquisiciones públicas de TIC se perfilan como medidas prioritarias para consolidar la seguridad digital. Estas recomendaciones coinciden con la visión de Castells (2009), quien sostiene que el poder contemporáneo se ejerce a través de la gestión de la información y la comunicación.

5. CONCLUSIONES

Este estudio evidenció la relevancia de la ciberdefensa para la soberanía tecnológica y la defensa nacional, destacando su papel estratégico en la preservación de infraestructuras críticas y en el fortalecimiento de las Fuerzas Armadas en el ámbito digital. Los hallazgos confirmaron la necesidad de políticas claras, infraestructura adecuada y recursos humanos capacitados, en concordancia con el marco doctrinario nacional. La investigación aporta al conocimiento científico al caracterizar el ambiente cibernético de la defensa nacional y al vincular los resultados con teorías sobre capital humano y poder de la información. Se reafirma que la ciberdefensa no es solo técnica, sino también social y política.

Entre las limitaciones se reconoce el tamaño reducido de la muestra y el enfoque en actores institucionales, lo que restringe la generalización.

Futuras investigaciones deberían ampliar la población, realizar comparaciones regionales y analizar la relación entre inversión tecnológica y efectividad en la defensa cibernética.

En síntesis, la ciberdefensa debe consolidarse como un eje estratégico de la soberanía tecnológica, mediante diagnósticos institucionales, políticas de continuidad y programas de formación que fortalezcan la capacidad nacional frente a amenazas emergentes.

REFERENCIAS

Britos, B. C., Hernández, G., & Álvarez, A. (1998). Gestión tecnológica y desarrollo sostenible y solidario en los países latinoamericanos: Experiencia cubana. *Revista Espacios, 19*(2). https://www.revistaespacios.com/a98v19n02/40981902.html

Bordignon, F. R. A. (2016). Soberanía tecnológica y educación: una dupla indisoluble. *Centro de Investigación, Docencia y Extensión en Tecnologías de la Información y las Comunicaciones (CIDETIC)*, 79–102.

Castells, M. (2009). *Comunicación y poder*. Madrid: Alianza Editorial.

Ceballos, L., & Maisonnave, M. et al. (2020). Soberanía tecnológica digital en Latinoamérica. *Propuestas para el Desarrollo*. http://www.propuestasparaeldesarrollo.com

Consejo de Defensa Nacional Paraguay. (2019). *Política de Defensa Nacional 2019–2030*. Ministerio de Defensa Nacional. https://mdn.gov.py/wp-content/uploads/2023/09/Politica_de_Defensa_Nacional_2019-2030.pdf

Cuenca Rótela, C. (2009). *Reflexiones sobre Política y Estrategia: Desarrollo, Seguridad y Defensa*. Asunción: Editorial Don Bosco.

Hernández, S., Fernández, C., & Baptista, P. (2014). *Metodología de la Investigación* (6ª ed.). México: McGraw-Hill Education.

Ministerio de Defensa Nacional Paraguay. (2022). *Libro Blanco de la Defensa*. https://onedrive.live.com

Ocón, A., & Gastaldi, S. (2019). Ciberespacio y Defensa Nacional: una reflexión sobre el dilema libertad-seguridad en el ejercicio de la soberanía. *Repositorio Digital de las Fuerzas Armadas*, 88–109. http://www.cefadigital.edu.ar

Pohle, J., & Thiel, T. (2022). Soberanía digital. *Revista Latinoamericana de Economía y Sociedad Digital, 1*. https://revistalatam.digital/article/22tr03/?pdf=3409

Sabiguero, A., et al. (2016). Relaciones entre soberanía y tecnología en los tiempos de Internet. *Revista de la Facultad de Derecho, 41*, 259–286. http://www.scielo.edu.uy/pdf/rfd/n41/n41a11.pdf