

CONGRESO DE LA REPÚBLICA
ÁREA DE TRÁMITE DOCUMENTARIO
REPÚBLICA**RECIBIDO**PROYECTO DE LEY N°
13233/2025-CR RU 2132719

18 NOVIEMBRE 2025 04:20 p. m.

FIRMADO DIGITALMENTE: EBOHORQUEZ

**LEY QUE CREA EL SISTEMA DE DEFENSA DE
CIBERSEGURIDAD DE LA SOBERANIA
DIGITAL POR LAS FUERZAS ARMADAS DEL
PERÚ**

A iniciativa del **CONGRESISTA ESDRAS RICARDO MEDINA MINAYA**, miembro del Grupo Parlamentario **RENOVACIÓN POPULAR**, en ejercicio del derecho de iniciativa legislativa que les confiere el artículo 107° de la Constitución Política del Perú y de conformidad con los artículos 75° y 76° del Reglamento del Congreso de la República, proponen la siguiente iniciativa legislativa:

**LEY QUE CREA EL SISTEMA DE DEFENSA DE CIBERSEGURIDAD DE LA
SOBERANIA DIGITAL POR LAS FUERZAS ARMADAS DEL PERÚ****I. FÓRMULA LEGAL****Artículo 1°: Objeto de la Ley**

La presente ley tiene como objeto reconocer la ciberseguridad y la protección de la información tecnológica como elementos esenciales de la defensa nacional, en defensa de su autonomía y protección de su soberanía digital, crea el sistema de defensa de ciberseguridad y especializar las funciones de las Fuerzas Armadas en el ámbito de la inteligencia y las operaciones en el ciberespacio, y establecer directrices claras para la adquisición, interconexión y estandarización de sistemas digitales y redes de vigilancia. Así como la modificación del Artículo 5 de la Ley N° 30999 (Ley de Ciberdefensa) y por consiguiente su modificatoria del reglamento.

Artículo 2°: Soberanía digital

Se reconoce la soberanía digital como un componente esencial de la seguridad nacional, la cual debe ser compatible con un mercado abierto y el intercambio de información, con el fin de fortalecer la capacidad cibernética del país y garantizar la protección de sus activos digitales, infraestructura crítica y ciudadanos frente a ciberamenazas nacionales y extranjeras.

Artículo 3°: Ciberdefensa

Para efectos de esta ley, se entiende por ciberdefensa el conjunto de conocimientos, habilidades, recursos y capacidades destinados a realizar operaciones en y a través del ciberespacio, con el objetivo de garantizar la protección, seguridad y uso eficiente de dicho dominio para las Fuerzas Armadas del Perú, así como de sus infraestructuras críticas y bienes de interés estratégico.

Artículo 4º: Atribuciones

Las atribuciones conferidas al sistema de defensa de ciberseguridad, conforme a la Ley N° 30999, Ley de Ciberdefensa, son esenciales para la protección de infraestructuras críticas y la ejecución de operaciones defensivas en el ciberespacio. Estas atribuciones incluyen, pero no se limitan a:

- a) Planificar, organizar, coordinar y ejecutar operaciones de ciberdefensa pasiva y activa, de acuerdo con las necesidades de la seguridad nacional.
- b) Implementar acciones de vigilancia, análisis de riesgos y respuesta ante incidentes de seguridad informática y ciberataques.
- c) Desarrollar e implementar tecnologías avanzadas de protección de datos, software, sistemas informáticos y redes integradas de comunicaciones.
- d) Supervisar la interconexión y estandarización de sistemas digitales y redes de comunicaciones en el ámbito de las Fuerzas Armadas.
- e) Promover y liderar proyectos de innovación tecnológica en el ámbito de la ciberseguridad, incluyendo la inteligencia artificial, la automatización y la robótica, con aplicaciones directas en la defensa nacional.
- f) Fomentar la colaboración con instituciones académicas y centros de investigación, a fin de desarrollar soluciones tecnológicas de vanguardia para la defensa cibernética.
- g) Impulsar la industria nacional de ciberseguridad, promoviendo la transferencia de tecnología y el fortalecimiento de capacidades locales en el sector.

Artículo 5º: Responsabilidades

Las principales responsabilidades del sistema de defensa de ciberseguridad de las Fuerzas Armadas del Perú incluyen:

- a) Analizar y gestionar "smart data" (datos inteligentes) para la generación de inteligencia estratégica, apoyando la toma de decisiones en tiempo real.
- b) Desarrollar y aplicar normativas y programas de protección contra actividades delictivas cibernéticas, como la piratería informática y el robo de datos.
- c) Supervisar la interoperabilidad de los sistemas hombre-máquina y las infraestructuras críticas, garantizando su eficiencia y resiliencia ante ciberamenazas.
- d) Coordinar con el Ministerio de Trabajo, las industrias de Tecnologías de la Información y Comunicaciones (TIC), y el ecosistema de startups tecnológicas para promover la innovación en ciberseguridad y fomentar la colaboración público-privada en el desarrollo de soluciones tecnológicas.

Artículo 6º: Modificación del Artículo 5 de la Ley N° 30999 (Ley de Ciberdefensa)

Se propone modificar el Artículo 5 de la ley, específicamente en lo relativo a los órganos ejecutores. El texto modificado quedaría como sigue:

“Artículo 5. Órganos ejecutores

Las Fuerzas Armadas, compuestas por el Ejército, la Marina de Guerra, la Fuerza Aérea, **Operaciones Tecnológicas**, y el Comando Conjunto de las Fuerzas Armadas, son las instituciones con la calidad de órganos ejecutores del Ministerio de Defensa.”

DISPOSICIONES COMPLEMENTARIAS

Primera. La Presidencia del Consejo de Ministros, en coordinación con el Ministerio de Defensa, aprobará el Reglamento de la presente ley, en un plazo máximo de noventa (90) días, contados a partir del día siguiente de su publicación en el Diario Oficial El Peruano. El reglamento deberá establecer los procedimientos específicos para la implementación de la Fuerza de Ciberespacio e Información, la asignación de recursos y la regulación de las operaciones cibernéticas conforme a la normativa nacional e internacional.

3

Lima, Noviembre de 2025



Firmado digitalmente por:
TRIGOZO REÁTEGUI Cheryl
FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 18/11/2025 12:31:47-0500



Firmado digitalmente por:
MEDINA MINAYA Esdras
Ricardo FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 04/11/2025 14:47:53-0500



Firmado digitalmente por:
JAUREGUI MARTINEZ DE
AGUAYO Maria De Los Milagros
Jackeline FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 18/11/2025 10:19:39-0500



Firmado digitalmente por:
CICCIA VASQUEZ Miguel
Angel FAU 20161749126 hard
Motivo: Soy el autor del documento
Fecha: 18/11/2025 11:09:43-0500



Firmado digitalmente por:
ZEBALLOS APONTE Jorge
Arturo FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 18/11/2025 12:21:00-0500



Firmado digitalmente por:
BAZAN CALDERON Diego
Alonso Fernando FAU 20161749126
soft
Motivo: Soy el autor del documento
Fecha: 18/11/2025 11:44:46-0500



Firmado digitalmente por:
YARROW LUMBRERAS Norma
Martina FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 12/11/2025 15:50:55-0500



Firmado digitalmente por:
YARROW LUMBRERAS Norma
Martina FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 12/11/2025 15:50:42-0500



II. EXPOSICIÓN DE MOTIVOS

La irrupción acelerada de las Tecnologías de la Información y la Comunicación (TIC) en el ámbito militar ha cambiado la concepción tradicional de defensa nacional e introducido el concepto de 'guerra cibernética'. Esto ha llevado a la necesidad de la formación de una institución especializada encargada de la ciberseguridad, la inteligencia digital y las operaciones, que garantizará la protección y soberanía digital del estado y salvaguardará infraestructuras críticas estatales y privadas.¹

Refiriéndose al contexto más amplio de la competencia estratégica global y la nueva configuración geopolítica, la rivalidad digital entre China y EE. UU. se refleja en el ciberespionaje a gran escala, el tráfico de influencia a nivel global y las adquisiciones de microcomponentes de defensa (por ejemplo, NVIDIA), o en la captura de la Taiwan Semiconductor Manufacturing Company Limited, que es la clave de la producción global de componentes digitales.² La República Popular de China ha fortalecido y consolidado su posición como superpotencia de ciberespionaje al aumentar las inversiones en redes 5G, inteligencia artificial y sistemas de vigilancia.

La implicación de actores no estatales —el caso de los hackers rusos que en 2022 intrusaron en la Dirección General de Inteligencia del Ministerio del Interior (DIGIMIN) debido a la falta de cifrado de datos, por ejemplo— muestra las debilidades de los sistemas del estado ante las amenazas cibernéticas organizadas.

La doctrina de ciberseguridad en términos de confidencialidad, integridad y disponibilidad argumenta la necesidad de una estructura única y centralizada para la integración estratégica, activa y pasiva, y especializada de la geoinformación. El Comando Conjunto Proporciona Principalmente Defensa en Tierra, Mar y Aire. Ahora se requiere extender el alcance con una doctrina específica para el dominio cibernético que incluya:

¹ <https://www.redalyc.org/journal/531/53169476007/html/>

² <https://elpais.com/tecnologia/2025-02-27/china-se-consolida-como-la-gran-superpotencia-del-ciberespionaje.html>



- Un Comando de Inteligencia Estratégica, encargado de ciberinteligencia, guerra electrónica y operaciones psicológicas.
- Un Comando Técnico de la Información, que gestione comunicaciones seguras, informática forense y ciberoperaciones pasivas.
- Un Centro de Geoinformación, soporte multidisciplinario en teledetección, geopolítica y análisis de infraestructuras críticas.

Así lo demuestra la implementación de un sistema para el desarrollo de capacidades de ciberdefensa por parte de la Marina de Guerra del Perú³, evidencia la viabilidad técnica de este modelo. Más allá de esto, estudios comparativos entre China y Estados Unidos muestran que la concentración de unidades de ciberdefensa mejora la defensa nacional y fomenta la innovación industrial en TIC.

- En un entorno cada vez más interconectado y competitivo, el legislador tiene la responsabilidad de dotar al Estado peruano de una normativa visionaria que:
- Reconozca formalmente la protección del entorno digital como parte de la soberanía nacional.
- Reconfigure las competencias de las Fuerzas Armadas para integrar operaciones en el ciberespacio.
- Garantice la defensa de los derechos fundamentales y neurológicos de la población frente a ciberataques y operaciones de influencia.

De esta manera, la presente ley consolidará la Unidad Orgánica de Operaciones Digitales como garante de la seguridad digital del país, alineándose con las mejores prácticas internacionales y fortaleciendo la capacidad de respuesta frente a amenazas emergentes.

³ <https://www.gob.pe/institucion/mindef/noticias/1236491-marina-de-guerra-contara-con-plataforma-para-el-desarrollo-de-capacidades-ciberneticas-en-ciberseguridad-y-ciberdefensa>



2.1. Necesidad de una Unidad Especializada en "operaciones tecnológicas"

Contar con la capacidad de gestionar y contrarrestar estas amenazas exige la integración de ciberdefensa, ciber inteligencia y operaciones electrónicas en una unidad especializada. Debido a la velocidad con que los ataques cibernéticos se pueden generar y escalar, esta unidad debe tener la capacidad de ejecutar de forma coordinada, en tiempo real, acciones cibernéticas defensivas y ofensivas. A continuación, se explican las razones que hacen que esta unidad especializada tenga carácter prioritario:

- Coordinación Eficaz en Tiempo Real: La respuesta a las amenazas cibernéticas debe ser inmediata. Los ataques cibernéticos se concentran en magnitudes y velocidades que pueden fácilmente superar los sistemas de defensa tradicionales. La integración de sistemas especializados en la tecnología de las operaciones a las Fuerzas Armadas permitirá la asignación y el despliegue coordinado de los recursos tecnológicos y humanos necesarios para mantener la defensa en el nivel requerido, asegurando así la velocidad y precisión de la respuesta ante un incidente.
- Capacidades Integradas en Ciberdefensa y Ciber inteligencia: La participación en operaciones en el ciberespacio exige la integración de la cobertura protectora de infraestructuras operativas y la cobertura operativa de ciberespacio con aviso anticipado y conocimiento de amenazas estridentes superadas. Una unidad especializada poseerá las funciones de análisis de ciber inteligencia, identificación de puntos débiles estratégicos, vigilancia avanzada de redes y pronóstico de ataques. Esto es crítico en la prevención y mitigación de riesgos antes de que se escalen a amenazas reales.
- Operaciones Ofensivas y Defensivas: La existencia de un componente dedicado exclusivamente a operaciones tecnológicas facilitará la ejecución de las operaciones de ataque y defensa en la seguridad del ciberespacio. Con esta orquestación, el país podrá asegurar una red de defensas y mantener una posición sostenible en el ciberespacio, con la capacidad de lanzar operaciones de manera preventiva y reactiva para



defender y atacar amenazas a la red.

- Resiliencia y Sostenibilidad del Estado: La existencia de una unidad especializada garantizará que la ciberdefensa minimice los efectos de violaciones críticas de seguridad, permitiendo una respuesta ciberdefensiva resiliente y planificada y la recuperación ante la guerra operativa inducida técnicamente. Esto asegurará que el estado peruano sea resiliente y minimice el impacto de amenazas cibernéticas altamente disruptivas a la seguridad nacional y la infraestructura crítica.

2.2. Vulnerabilidades nacionales y casos emblemáticos

Ataque del grupo Conti a la Dirección General de Inteligencia del Ministerio del Interior (DIGIMIN) el 29 de abril de 2022, exfiltrando 9,4 GB de datos clasificados como "secretos" debido a redes sin cifrado.⁴

Investigación de un presunto incidente en Telefónica Perú en junio de 2025, con 1 000 000 de registros de clientes peruanos publicados en un foro por el grupo "Dedale".⁵

Incidente de ransomware contra BDO Perú en agosto de 2025, atribuido al grupo incransom, con acceso a datos sensibles de personal directivo y clientes, incluyendo firmas electrónicas y documentos contables.⁶

Un informe revela que los grupos de hackers vinculados al país asiático aumentaron un 150% su actividad en 2024, mientras que los de Corea del Norte acaba de apropiarse 1.500 millones de dólares con un solo golpe⁷

7

2.3. Evolución de las amenazas y el contexto global

⁴ <https://rpp.pe/tecnologia/mas-tecnologia/hackers-rusos-atacan-al-servicio-de-inteligencia-peruano-y-exigen-millonaria-recompensa-noticia-1405437>

⁵ <https://www.reuters.com/business/media-telecom/telefonica-investigates-potential-cyberattack-after-release-data-peru-2025-06-03/>

⁶ <https://www.dexpose.io/incransom-targets-bdo-peru-in-ransomware-attack/>

⁷ <https://elpais.com/tecnologia/2025-02-27/china-se-consolida-como-la-gran-superpotencia-del-ciberespionaje.html>

En las últimas décadas, el cibercrimen y las ciberamenazas no sólo han aumentado de volumen, sino también en complejidad. Los ciberataques han sido ejecutados y provocados por actores estatales y no estatales, y han sido lo suficientemente ocupados y complejos para afectar las defensas, las comunicaciones y las administraciones gubernamentales. Los casos más destacados y claros han sido los efectuados por la cibercriminalidad de China, Rusia y Corea del Norte, usando el ciberespacio como un nuevo terreno para la confrontación y disputa geopolítica.

En el caso de la cibercriminalidad en los ataques en Perú, el “detrás” también ha sido bastante complejo, y por lo tanto la magnitud de los ataques ha sido también en el caso de Perú ha aumentado.

En el primer semestre de 2025, Perú registró 748.2 millones de ciberataques, lo que lo ubica como uno de los países más ciberatacados en toda América Latina. Esta cifra es particularmente preocupante porque muestra el alto grado de vulnerabilidad que tanto el sector privado como público en la nación posee, por lo que el ataque podría afectar la seguridad del país y de aspectos como la infraestructura, la seguridad nacional y los datos de los ciudadanos.

2.4. El Papel de las Fuerzas Armadas en la Ciberdefensa

La existente Ley de Ciberdefensa Militar (Ley N° 30999) no debe ser subestimada, pero aun no responde a las necesidades y las demandas contemporáneas. Dentro de las Fuerzas Armadas del Perú, la especialización en la defensa cibernética debe constituirse como un componente de un sistema integrado y alineado con la nueva doctrina en seguridad digital. Y brindar garantías para un acceso seguro para los ciudadanos.

El sistema que se construya en este contexto debe contar con especialización en la ciberdefensa, pero también la ciberofensiva. La constitución de comandos en ciberinteligencia, guerra electrónica, y ciberoperaciones pasivas, bajo la tutela de las Fuerzas Armadas, permitirá a Perú conseguir un avance en la detección, prevención y respuesta a ciberataques. Aparte, que permitirá proteger a los activos críticos como la información digital del estado.



2.5. La Necesidad de una Infraestructura Cibernética Nacional

La creación y el fortalecimiento de una cibernética nacional también la impulso de una ciberseguridad nacional y de la creación de unidades militares especializadas. Es deseable que la ciberseguridad nacional en el Perú cobre vida con el fortalecimiento de la investigación en el país, en el desarrollo de tecnologías de automatización, ciberseguridad, inteligencia artificial y criptografía. Es deseable que la innovación en el ciberespacio en el país se base en la colaboración del sector público, el sector privado y la academia.

El fortalecimiento de las capacidades tecnológicas nacionales desarrollará soluciones propias que contribuyan a la resiliencia de las infraestructuras críticas que no dependan de actores externos ante ciber amenazas.

2.6. La Soberanía Digital como Pilar de la Defensa Nacional

Soberanía digital debe entenderse como la autonomía del Estado en la toma de decisiones y la protección de la información y sus recursos digitales. Esto incluye proteger a sus ciudadanos de ataques cibernéticos, sin depender de potencias extranjeras.

Este tipo de soberanía digital se enmarca dentro de la ciberseguridad a nivel mundial y de las mejores prácticas. Así, diversos Estados han desarrollado, en la creación de capacidades nacionales, una respuesta frente a los desafíos del ciberespacio.

2.7. La Oportunidad para el Perú

La elaboración de un sistema nacional de defensa cibernética no solo se contempla como una necesidad, sino que contribuye a una oportunidad estratégica. Con condiciones globales que permiten un mayor nivel de intercambios y que, a la vez, permiten una mayor cantidad de ciberataques, el Perú tiene la oportunidad de posicionarse como un líder en la defensa digital y cibernética en la región.

El desarrollo tecnológico en conjunto con la expansión de la industria de las tecnologías de la información y la comunicación (TIC) en el Perú y el fortalecimiento de la ciberseguridad crean las condiciones propicias para el crecimiento de la Unidad Orgánica de Operaciones Digitales. Esta será fundamental para la construcción de un sistema de ciber defensa que permita al Estado actuar frente a las ciber amenazas con celeridad, efectividad y autonomía.

III. MARCO JURIDICO

- Constitución Política del Perú
- Decreto Legislativo N° 1412 y Ley N° 29904: Gobierno Digital y Seguridad Digital del Estado.
- Ley N° 30999: regula ciberdefensa militar y el Decreto Supremo N° 017-2024-PCM
- Decreto Legislativo N° 604, que regula la gestión de la información estatal;
- Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital.

VI. ANÁLISIS SOBRE LA NECESIDAD, VIABILIDAD Y OPORTUNIDAD DE LA PROPUESTA LEGISLATIVA

4.1. NECESIDAD

La negligencia en ciberseguridad puede costarle a las MIPYMES cerca de 157,000 dólares estadounidenses, según lo informado por idb invest, entre otras causas, robo de activos financieros (cuentas bancarias, información de pago), pérdida de ingresos por la interrupción de operaciones, costos exorbitantes de recuperación, demandas de rescate en ataques de ransomware, y los costos crecientes del seguro cibernético.

4.2. VIABILIDAD

El caso de la Marina Peruana, que desplegó una plataforma de desarrollo para capacidades de defensa cibernética, atesta la viabilidad técnica para la consolidación de recursos, herramientas y procesos bajo una unidad militar especializada. La existencia de una fuerza laboral nacional capacitada en ciberespacio, así como la industria TIC en crecimiento, hace posible establecer la Unidad Orgánica con el personal e infraestructura necesarios para el cumplimiento de objetivos estratégicos.



4.3. OPORTUNIDAD

Según el Capítulo 3 del Informe Global de Amenazas 2025 publicado por Fortinet, en la primera mitad de 2025, Perú sufrió 748.2 millones de intentos de ataque cibernético junto con 423 millones de escaneos activos, convirtiéndolo en una de las naciones más atacadas de América Latina. El volumen y la sofisticación de los ataques, promediando 8,818 intentos por organización por semana, desencadenan la necesidad de acción legislativa inmediata para frenar las amenazas a la seguridad pública y nacional.⁸

V. ANÁLISIS COSTO - BENEFICIO

La creación de la Unidad Orgánica de Operaciones Digitales implica una inversión inicial en infraestructura, recursos humanos y desarrollo normativo, pero ofrece beneficios cuantificables y estratégicos para el Estado y el sector privado. Estos costos a pesar de parecer cuantiosos, ya no son considerados dada que la inversión ya se realizó, en un grupo especial dentro de la marina de Guerra del Perú y serán trasladados a esta nueva unidad.

Estos retornos, además de la obligación constitucional del estado de salvaguardar el territorio nacional, promueven un valor socioeconómico que se traduce en una soberanía digital fortalecida y una resiliencia nacional ante amenazas emergentes.

VI. EFECTOS DE LA VIGENCIA DE LA NORMA SOBRE LA LEGISLACIÓN NACIONAL

Esto requerirá la modificación de ciertas regulaciones y procedimientos en las agencias gubernamentales, ya que alineará las funciones de la DINI, el Ministerio de Defensa, la PNP y otras instituciones privadas. Además, la Orden asegurará la interoperabilidad funcional y estándares mínimos de protección uniformes.

⁸ <https://www.infobae.com/peru/2025/08/27/ciberataques-en-peru-superan-los-748-millones-de-intentos-en-lo-que-va-del-2025/>



VII.

VINCULACIÓN CON EL ACUERDO NACIONAL

La iniciativa respalda las políticas de desarrollo tecnológico y fortalecimiento de capacidades estatales, contribuyendo a la estabilidad y competitividad del Perú en el escenario geopolítico y