Proyecto de Ley N° 4228/2018-CR

PROYECTO DE LEY DE CIBERDEFENSA

Los **CONGRESISTAS DE LA REPÚBLICA** que suscriben, de manera **MULTIPARTIDARIA**, a iniciativa del Congresista **Jorge Del Castillo Gálvez**; miembro del Grupo Parlamentario de la Célula Parlamentaria Aprista, ejerciendo el derecho de iniciativa legislativa que le confieren el artículo 107° de la Constitución Política del Perú, en concordancia con los artículos 75° y numeral 2 del 76° del Reglamento del Congreso de la República, presentan el siguiente Proyecto de Ley:

Fórmula Legal:
El Congreso de la República
Ha dado la Ley siguiente:

PROYECTO DE LEY DE CIBERDEFENSA

TÍTULO I
DISPOSICIONES GENERALES

Artículo 1.- Objeto
La presente ley tiene por objeto establecer el marco normativo en materia de ciberdefensa del Estado Peruano, regulando las operaciones militares en y mediante el ciberespacio a cargo de los órganos ejecutores del Ministerio de Defensa dentro de su ámbito de competencia.

Artículo 2.- Finalidad
Defender y proteger la soberanía, los intereses nacionales, los activos críticos nacionales y recursos claves; así como sistemas de información digital de los activos de los órganos ejecutores del Ministerio de Defensa, de amenazas o ataques en y mediante el ciberespacio.

Artículo 3.- Ámbito de Aplicación
El ámbito de aplicación de la norma se circunscribe a la ejecución de operaciones de ciberdefensa en y mediante el ciberespacio frente a las amenazas o ataques que atenten contra la seguridad nacional.

Artículo 4.- Definición
Entiéndase por Ciberdefensa a la capacidad que permite buscar, detectar, identificar, impedir, contener, neutralizar y responder amenazas y ataques realizados en y mediante el ciberespacio que atenten contra la seguridad de la nación.

Artículo 5.- Órganos Ejecutores
Las Fuerzas Armadas que están constituidas por el Ejército, la Marina y la Fuerza Aérea y el Comando Conjunto de las Fuerzas Armadas; son instituciones con calidad de órganos ejecutores del Ministerio de Defensa.

TÍTULO II
DE LA CIBERDEFENSA

CAPÍTULO I
LAS CAPACIDADES DE CIBERDEFENSA Y LAS OPERACIONES EN Y MEDIANTE EL CIBERESPACIO

328099-ATD

Artículo 6.- De las capacidades de ciberdefensa
Es el uso de conocimiento, habilidades y medios para realizar operaciones en y mediante el ciberespacio a fin de asegurar su empleo por las fuerzas propias.

Artículo 7.- De las operaciones militares en el ciberespacio
Es el eficiente y eficaz empleo de las capacidades de ciberdefensa por parte de los órganos ejecutores del Ministerio de Defensa, de acuerdo a sus funciones y en el ámbito de sus respectivas competencias contra las amenazas o ataques en y mediante el ciberespacio que atenten contra la seguridad nacional.

Artículo 8.- De la planificación y ejecución de las operaciones en el ciberespacio
La planificación y ejecución de las operaciones de ciberdefensa a cargo de los órganos ejecutores del Ministerio de Defensa responde al mandato conferido en la Constitución Política del Perú, así como al cumplimiento de las responsabilidades asignadas en las leyes que regulan su naturaleza jurídica, competencias, funciones y estructura orgánica, las disposiciones contenidas en la presente ley, y los tratados y acuerdos internacionales de los que el Perú es parte y resulten aplicables.

CAPÍTULO II
DEL USO DE LA FUERZA EN Y MEDIANTE EL CIBERESPACIO

Artículo 9.- Del uso de la fuerza por las Fuerzas Armadas
El uso de la fuerza en ciberespacio se sujeta a las disposiciones contenidas en el artículo 51 de la Carta de la Naciones Unidas y el presente dispositivo legal, y está regida por las normas del Derecho Internacional de los Derechos Humanos y el Derecho Internacional Humanitario que sean aplicables.

Artículo 10.- De la legítima defensa
Todo ataque en o mediante del ciberespacio que ponga en riesgo la soberanía, los intereses nacionales, los activos críticos nacionales y recursos claves, así como los sistemas de información digital de los activos de los órganos ejecutores del Ministerio de Defensa, de ataques o amenazas en el ciberespacio, dará lugar al ejercicio del derecho de legítima defensa.

Artículo 11.- Requisitos para el ejercicio del uso de la fuerza
El ejercicio del derecho de legítima defensa en el contexto de las operaciones de ciberdefensa está sujeto a los principios de legalidad, necesidad y oportunidad.
En el caso de conducir una operación de respuesta en y mediante ciberespacio que contenga un ataque deliberado, deberá realizarse de acuerdo a la normativa vigente.

CAPÍTULO III
DE LA SEGURIDAD DE LOS ACTIVOS CRÍTICOS NACIONALES Y RECURSOS CLAVES

Artículo 12.- Del control y protección de los activos críticos nacionales y recursos claves
El Comando Conjunto de las Fuerzas Armadas estará a cargo de la ciberdefensa de los activos críticos nacionales y recursos claves, cuando la capacidad de protección de sus operadores o administradores, del sector responsable de cada uno de ellos y la seguridad pública, sea sobrepasada.

2

Artículo 13. Modificación del artículo 32° del Decreto Legislativo 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital.

Modifícanse el artículo 32° del Decreto Legislativo 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, los cuales quedan redactados de la siguiente manera:

> ***"Artículo 32.- Gestión del Marco de Seguridad Digital del Estado Peruano***
>
> *El Marco de Seguridad Digital del Estado Peruano tiene los siguientes ámbitos:*
>
> ***a. Defensa:*** *El Ministerio de Defensa (MINDEF) en el marco de sus funciones y competencias dirige,* ***norma****, supervisa y evalúa las normas en materia de ciberdefensa."*
> *(...)*

DISPOSICIONES COMPLEMENTARIAS FINALES

PRIMERA. - Reglamentación en materia de Ciberdefensa
La Presidencia del Consejo de Ministros conjuntamente con el Ministerio de Defensa, aprobaran 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.

SEGUNDA. - Política Nacional de Ciberdefensa
El Ministerio de Defensa formula la Política Nacional de Ciberdefensa en un plazo no mayor de noventa (90) días, contados a partir del día siguiente de su publicación en el Diario Oficial El Peruano, el mismo que será aprobado por el Consejo de Seguridad y Defensa Nacional.

TERCERA .- Modificaciones a normas de las Fuerzas Armadas en materia de ciberdefensa.
El Ministerio de Defensa en un plazo de noventa (90) días, contados a partir de la fecha de entrada en vigencia la presente ley, presentará las modificaciones, derogaciones e incorporaciones a las normas correspondientes a las Fuerzas Armadas en materia de la presente Ley.

CUARTA. - Recursos Críticos de Internet
Se reconoce a las entidades que gestionen recursos críticos de internet (nombres de dominio, números IP y protocolos) en su naturaleza de entidades vinculadas a la ciberdefensa debiendo mantener mecanismos de comunicación de incidentes que pudieran afectar la capacidad Ciberdefensa Nacional.

QUINTA. Desarrollo de currículos de educación superior en materia de ciberdefensa
El Ministerio de Educación fomentarán el desarrollo de currículos especializados en ciberdefensa en las instituciones de educación superior universitaria e institutos tecnológicos, a nivel de pre y post-grado. Para ello se establecerán instrumentos de cooperación interinstitucional con entidades del sector privado, la academia, la sociedad civil y la comunidad técnica.

SEXTA. Fomento de la Cultura de Seguridad Digital
Alineados con las Políticas 9 y 35 del Acuerdo Nacional, los actores públicos y privados involucrados en temas de seguridad digital deben fomentar la creación de una cultura de seguridad digital desde los primeros años de la escuela y a nivel de todo nivel de

educación, así como en los espacios profesionales y sociales, entendiendo que el desarrollo de una cultura de seguridad digital permitirá desarrollar capacidades en esta materia.

SEPTIMA. Aplicación de Recursos Especiales
Los procesos para las capacidades de ciberdefensa, deberán considerarse dentro del alcance de la aplicación de los artículos 30° y 31° del Decreto Legislativo 1141.

DISPOSICIÓN COMPLEMENTARIA DEROGATORIA

ÚNICA. - Derogatoria
Derogase o déjese en suspenso, según el caso, las disposiciones legales y reglamentarias que se opongan a lo establecido por la presente ley o limiten su aplicación, con la entrada en vigencia de la presente ley.

Lima, 11 de abril del 2019

EXPOSICIÓN DE MOTIVOS

La Constitución Política del Perú dispone en su artículo 44°, que son deberes primordiales del Estado: defender la soberanía nacional, garantizar la plena vigencia de los derechos humanos, proteger a la población de las amenazas contra su seguridad, y promover el bienestar general que se fundamenta en la justicia y en el desarrollo integral y equilibrado de la Nación.

Asimismo, el artículo 163° de la Carta Magna refiere que el Estado garantiza la Seguridad de la Nación mediante el Sistema de Defensa Nacional, el cual precisa es integral y permanente y se desarrolla en los ámbitos interno y externo; acotando que toda persona, natural o jurídica, está obligada a participar en la Defensa Nacional conforme a Ley.

En ese contexto, el Acuerdo Nacional señala que la "Política de Seguridad Nacional" es un compromiso del Estado para mantener una política que garantice la independencia, soberanía, integridad territorial y salvaguarda de los intereses nacionales.

Es así que por Decreto Supremo N° 012-2017-DE de fecha 20 de diciembre del 2017, se promulgó la Política de Seguridad y Defensa Nacional, la misma que establece como Objetivo N°1: "Garantizar la soberanía, independencia e integridad territorial y la protección de los intereses nacionales", Lineamiento N°7: "Proteger a los activos críticos nacionales contra todo tipo de amenaza, así como los sistemas de información de las amenazas que, desde el ciberespacio, atenten contra la seguridad y defensa nacional". (...) Se impulsará la creación de un Sistema Nacional de Ciberseguridad, con la participación del sector privado y la sociedad en su conjunto (...), se fortalecerá las misiones constitucionales de las Fuerzas Armadas y la Policía Nacional para incrementar sus capacidades militares/ policiales y sus recursos humanos, con la finalidad de garantizar la paz internacional y el orden interno (...)".

Bajo este contexto, el Plan Estratégico Sectorial Multianual PESEM 2017-2021 del Ministerio de Defensa, prevé como Acción Estratégica N° 1.7: "Desarrollar la ciberdefensa, protegiendo la infraestructura crítica del Estado de ciberataques".

Los avances tecnológicos producidos a lo largo de los últimos 30 años, así como la aparición de la internet, ha devenido en la sistematización de muchos de los servicios públicos que se encuentran a cargo del Estado o bajo la administración de un tercero.

Es en esta línea que en la Política 35, Política de Sociedad de la información y sociedad del conocimiento, o también denominada #PeruDigital, incorporada al Acuerdo Nacional el 24 de agosto del 2017 señala que el eje no es la tecnología en sí misma, sino la utilización de la misma para el bienestar de todos. Indica la Política 35 "Nos comprometemos a impulsar una sociedad de la información hacia una sociedad del conocimiento orientada al desarrollo humano integral y sostenible, en base al ejercicio pleno de las libertades y derechos de las personas, y capaz de identificar, producir, transformar, utilizar y difundir información en todas las dimensiones humanadas incluyendo la dimensión ambiental."

De igual manera indica la Política 35 del Acuerdo Nacional que se " (...) (i) diseñará las políticas y la regulación en materia de sociedad de la información y del conocimiento teniendo como base los principios de internet libre, abierto, neutro y para todos, así como el adecuado resguardo de la seguridad de la información"

5

Es en el marco de un diseño multisectorial, el trabajo para el desarrollo del presente proyecto de Ley de Ciberdefensa, la Comisión de Defensa Nacional, Orden Interno, Desarrollo Alternativo y Lucha Contra las Drogras, invito a diferentes mesas de trabajo, las mismas que fueron realizadas con el Sector Publico, Sector Privado, Academia y las Fuerzas Armadas; con el fin de consensuar conceptos y recoger experiencias y aportes de los diferentes participantes sobre la implementación de la Ciberdefensa en el Perú.

Las mesas de trabajo convocadas por la Comisión son las siguientes:

PRIMERA MESA DE TRABAJO:

La primera mesa de trabajo se llevó a cabo el 07 de enero de 2019, siendo promovido por la Presidencia de la Comisión de Defensa Nacional, al cual asistieron las siguientes Entidades: Presidencia del Consejo de Ministros, Ministerio de Defensa, Ministerio del Interior, Dirección Nacional de Inteligencia, Comando Conjunto de las Fuerzas Armadas, Ejercito del Perú, Marina de Guerra del Perú Fuerza Aérea del Perú.

Las conclusiones a que se llegaron fueron:

- Importancia de la Ciberdefensa y Ciberseguridad en las Fuerzas Armadas.
- ¿Cuáles son los organismos Institucionales en cada Instituto Armado que trabaja en el campo de la Ciberdefensa?
- ¿Qué Instituciones trabajan en la Ciberseguridad?

SEGUNDA MESA DE TRABAJO:

La segunda mesa de trabajo se llevó a cabo el 14 de enero de 2019, siendo promovido por la Presidencia de la Comisión de Defensa Nacional, al cual asistieron las siguientes Entidades: Presidencia del Consejo de Ministros, Comando Conjunto de las Fuerzas Armadas, Ministerio de Defensa, Ministerio del Interior, Ministerio de Relaciones Exteriores, Ministerio de Transporte y Comunicaciones, Dirección Nacional de Inteligencia, Comando Conjunto de las Fuerzas Armadas, Ejercito del Perú, Marina de Guerra del Perú Fuerza Aérea del Perú.

Las conclusiones a que se llegaron fueron:

- Exposición de la SEGDI.
- Exposiciones Institucionales de la situación actual del Ejercito, Marina, FAP y CC.FF.AA. en referencia a Ciberdefensa y Ciberseguridad.
- Necesidad de articular entre cada Fuerza Armada.

TERCERA MESA DE TRABAJO:

La tercera mesa de trabajo se llevó a cabo el 18 de enero de 2019, siendo promovido por la Presidencia de la Comisión de Defensa Nacional, al cual asistieron las siguientes Entidades: Red Científica Peruana, Telefónica del Perú, Claro, CISCO, Bolsa de Valores de Lima, Microsoft, AFIN, Network Acces Point, ASBANC, SIN y representantes de Empresas Privadas.

Las conclusiones a que se llegaron fueron:

- Las entidades privadas que usan la ciberseguridad no están normadas y necesitan un marco regulatorio.

6

- Cada Entidad privada tiene su propio protocolo y no lo comparte con las demás instituciones.
- Es necesaria la coordinación con la SEGDI.

CUARTA MESA DE TRABAJO:

La cuarta mesa de trabajo se llevó a cabo el 23 de enero de 2019, siendo promovido por la Presidencia de la Comisión de Defensa Nacional, al cual asistieron las siguientes Entidades: Presidencia del Consejo de Ministros, Ministerio de Defensa, Ministerio del Interior, Dirección Nacional de Inteligencia, Comando Conjunto de las Fuerzas Armadas, Ejercito del Perú, Marina de Guerra del Perú, Fuerza Aérea del Perú y ASBANC.

Las conclusiones a que se llegaron fueron:

- La participación del Sector Privado y de las Fuerzas Armadas han permitido consensuar algunos conceptos de Ciberdefensa y Ciberseguridad.

QUINTA MESA DE TRABAJO:

La quinta mesa de trabajo se llevó a cabo el 05 de febrero de 2019, siendo promovido por la Presidencia de la Comisión de Defensa Nacional, al cual asistieron las siguientes Entidades: UNI, Suma Ciudadana, UTP, ISACA, ESAN, ASUP, RENIEC, Colegio de Ingenieros, Universidad San Marcos, Universidad Villarreal, UPC, RENIEC, UTEC, MINEDU, PCM, Universidad San Martin de Porres, SERVIR y representantes de Universidades y Entidades Privadas.

Las conclusiones a que se llegaron fueron:

- La participación de la Comunidad Universitaria ha sido importante por la instrucción que da en las aulas universitarias, en el tema de Ciberdefensa y Ciberseguridad.
- Las Universidades tienen la necesidad de coordinar con la SEGDI para coordinar con el Sector Público.

SEXTA MESA DE TRABAJO: FORO SOBRE CIBERDEFENSA Y CIBERSEGURIDAD

La sexta mesa de trabajo fue un Foro sobre Ciberdefensa y Ciberseguridad y se llevó a cabo el 13 de febrero de 2019, siendo promovido por la Presidencia de la Comisión de Defensa Nacional, al cual asistieron las siguientes Entidades: Comando Conjunto de las Fuerzas Armadas, MINDEF, MININTER, DINI, Ejercito del Perú, Marina de Guerra del Perú Fuerza Aérea del Perú, RR.EE., MTC, PCM, Red Científica Peruana, Telefónica del Perú, Claro, CISCO, Bolsa de Valores de Lima, Microsoft, AFIN, Network Acces Point, ASBANC, SNI, las Universidades San Marcos, Villareal, San Martin, UNI, UTP, UPC, La Salle y RR.EE . A este Foro asistieron aproximadamente 900 participantes, como Funcionarios Públicos, representantes de Universidades, Entidades Privadas y Fuerzas Armadas.

Las conclusiones a que se llegaron fueron:

- Se difundió la propuesta de Ley sobre Ciberdefensa y Ciberseguridad.

SÉPTIMA MESA DE TRABAJO:
La séptima mesa de trabajo se llevó a cabo el 06 de marzo de 2019, siendo promovido por la Presidencia de la Comisión de Defensa Nacional, al cual asistieron las siguientes

7

Entidades: Comando Conjunto de las Fuerzas Armadas, MINDEF, MININTER, Ejercito del Perú, Marina de Guerra del Perú Fuerza Aérea del Perú, PCM, ASBANC y representantes de FF.AA y CC.FF.AA.

Las conclusiones a que se llegaron fueron:

- Definición de conceptos de la Ciberdefensa y Ciberseguridad y los alcances de la propuesta de Ley.
- Trabajo de grupo de las FF.AA y CC.FF.AA a fin de definir conceptos y responsabilidades Institucionales.

OCTAVA MESA DE TRABAJO:

La octava mesa de trabajo se llevó a cabo el 18 de marzo de 2019, siendo promovido por la Presidencia de la Comisión de Defensa Nacional, al cual asistieron las siguientes Entidades: Comando Conjunto de las Fuerzas Armadas, MINDEF, MININTER, Ejercito del Perú, Marina de Guerra del Perú Fuerza Aérea del Perú, PCM, ASBANC y Congreso de la Republica, asistieron 18 Funcionarios Públicos y representantes de FF.AA y CC.FF.AA.

Las conclusiones a que se llegaron fueron:

- Discusión y análisis del proyecto de Ley.

NOVENA MESA DE TRABAJO:
La novena mesa de trabajo se llevó a cabo el 20/02/2019, siendo promovido por la RENIEC, al cual asistieron las siguientes Entidades: Comando Conjunto de las Fuerzas Armadas, MINDEF, MININTER, Ejercito del Perú, Marina de Guerra del Perú Fuerza Aérea del Perú, PCM.

Las conclusiones a que se llegaron fueron:

- Niveles de articulación de la SEGDI y la Entidades del Sector Público y Privado.

De las 09 mesas de trabajo, 08 han sido convocadas por la Comisión de Defensa Nacional, Orden Interno, Desarrollo Alternativo y Lucha Contra las Drogas y 01 ha sido convocado por la RENIEC, y se ha tomado en consideración la posición de todos los actores relevantes.

EFECTO DE LA NORMA EN LA LEGISLACIÓN NACIONAL

La presente iniciativa legislativa no altera la normatividad vigente, sino que establece el marco normativo en materia de ciberdefensa del Estado Peruano, regulando las operaciones militares en y mediante el ciberespacio a cargo de los órganos ejecutores del Ministerio de Defensa dentro de su ámbito de competencia.

ANÁLISIS COSTO BENEFICIO

La presente iniciativa legislativa debe ser analizada no desde el tradicional costo-beneficio, sino se debe utilizar un análisis costo-eficiencia, considerando que la propuesta legislativa es de puro derecho, pues lo que se busca es establecer el marco normativo en materia de ciberdefensa del Estado Peruano, por lo que la presente iniciativa no irrogará gasto alguno al Estado.

8