



COMISIÓN DE DEFENSA NACIONAL,
ORDEN INTERNO, DESARROLLO ALTERNATIVO
Y LUCHA CONTRA LAS DROGAS



DICTAMEN CON RECOMENDACIÓN DE APROBACIÓN CON TEXTO SUSTITUTORIO RECAIDO EN EL PROYECTO N° 4228/2018-CR "LEY DE CIBERDEFENSA"

COMISIÓN DE DEFENSA NACIONAL, ORDEN INTERNO, DESARROLLO ALTERNATIVO Y LUCHA CONTRA LAS DROGAS

DICTAMEN 2018-2019



Señor Presidente:

Se ha remitido para estudio y dictamen de la Comisión de Defensa Nacional, Orden Interno, Desarrollo Alternativo y Lucha Contra las Drogas el **Proyecto de Ley N° 4228/2018-CR** "Ley de Ciberdefensa", presentado por el Congresista Jorge Del Castillo Gálvez.

En la Séptima Sesión Extraordinaria de la Comisión Defensa Nacional, Orden Interno, Desarrollo Alternativo y Lucha contra las Drogas celebrada el 22 de julio del 2019, expuesto y debatido el dictamen fue aprobado por **MAYORÍA** con el voto a favor los señores congresistas: Carlos Tubino Arias Schreiber, César Antonio Segura Izquierdo, Lourdes Alcorta Suero, Joaquín Dipas Huamán, Úrsula Letona Pereyra, Paloma Noceda Chiang, Luis Alberto Yika, Alberto Quintanilla Chacón, Gilmer Trujillo Zegarra, Marco Miyashiro Arashiro, Luis Iberico Nuñez, Jorge Del Castillo Gálvez, con la **ABSTENCIÓN** de la Congresista Luz Salgado Rubianes.

Con la **LICENCIA** de los señores congresistas: Richard Arce Cáceres, Francisco Villavencio Cárdenas y Elard Melgar Valdez.

I. SITUACIÓN PROCESAL DE LA PROPUESTA LEGISLATIVA:

- **Proyecto de Ley 4228/2018-CR**, "Ley de Ciberdefensa!", ingresó a trámite documentario el 16 de abril del 2019, siendo decretado a la Comisión de Defensa Nacional, Orden Interno, Desarrollo Alternativo y Lucha Contra las Drogas, como única comisión dictaminadora el 25 de abril del mismo año.

II. CONTENIDO DE LA PROPUESTA LEGISLATIVA:

El Proyecto de Ley 4228/2018-CR, "Ley de Ciberdefensa" señala lo siguiente:

- La iniciativa legislativa 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.
- Además de 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.
- 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

388413 19

que atenten contra la seguridad nacional.

- La iniciativa legislativa establece la definición de Ciberdefensa, entendiéndose como 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.
- Respecto a los Órganos Ejecutores, establece que sean 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.
- En lo que compete a las capacidades de Ciberdefensa, nos detalla que el uso de conocimiento, habilidades y medios para realizar operaciones en y mediante el ciberespacio se darán a fin de asegurar su empleo por las fuerzas propias.
- La iniciativa legislativa, busca un 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.
- Respecto a 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.
- Respecto a lo que compete al uso de la Fuerza por las Fuerzas Armadas en ciberespacio, ésta 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.
- En cuanto a la Legítima Defensa, menciona que todo ataque en o mediante el 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.
- La Iniciativa legislativa también establece requisitos para el ejercicio del uso de la Fuerza, en el contexto de las operaciones de ciberdefensa está sujeto a los principios de legalidad, necesidad y oportunidad.
- Con respecto al control y protección 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.

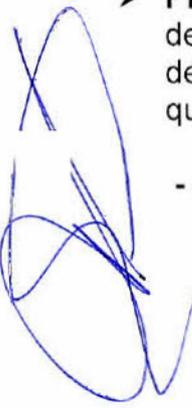
III. MARCO NORMATIVO:

- Constitución Política del Perú
- Reglamento del Congreso de la República
- Decreto Legislativo 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital
- Decreto Legislativo 1136, Decreto Legislativo del CCFFAA

IV. OPINIONES SOLICITADAS:

- **Presidencia del Consejo de Ministros:** Mediante Oficio N° 823-2018-2019/CDNOIDALCLD-CR de fecha 29 de abril del 2019, por el que se solicita opinión del Proyecto de Ley 4228/2018-CR, al Señor Salvador Del Soler Labarthe, en su condición de Presidente del Consejo de Minsitros, no habiéndose recibido respuesta hasta la fecha.
- **Ministerio del Interior:** Mediante Oficio N° 825-2018-2019/CDNOIDALCLD-CR de fecha 29 de abril del 2019, por el que se solicita opinión del Proyecto de Ley 4228/2018-CR, al General José Modesto Huerta Torres, no habiéndose recibido respuesta hasta la fecha.

V. OPINIONES RECIBIDAS:

- 
- **Presidencia del Consejo de Ministros:** Mediante Oficio N° D002765-2019-PCM-SG, de fecha 8 de Julio del 2019, la Sra. Úrsula Desilú León Chempén en su condición de Secretaria General de la PCM, remite el Informe N° D0001066-2019-PCM/OGAJ, que concluye lo siguiente:

- Luego del estudio de la Iniciativa legislativa, observamos que en la exposición de motivos no se advierte cuál es el problema público que pretendería dar solución el PL, asimismo la sola mención de diversos dispositivos legales no puede ser considerado como un sustento idóneo del PL, debiendo en la exposición de motivos haberse desarrollado los mismos estableciendo una coherencia lógica argumentativa entre la necesidad de la regulación y las normas señaladas.
- Asimismo, precisa que "la Segunda Disposición Complementaria Final del PL establece un mandato para que el Ministerio de Defensa formule, en un plazo máximo de noventa (90) días, la Política Nacional de Ciberdefensa. Sobre el particular, conforme a lo dispuesto en el artículo 4 de la Ley N° 29158, Ley Orgánica del Poder Ejecutivo, el diseño y la definición del contenido de las políticas constituye una competencia exclusiva del Poder Ejecutivo. lo cual se aprueba por Decreto Supremo con el voto aprobatorio del Consejo de Ministros; por tanto se debe observar este extremo del PL, toda que el Congreso de la República no tiene competencia para aprobar ni establecer los contenidos de una política. "

- En ese mismo sentido, mediante Informe N° 2000025-2019-PCM-SSTRD-YAC la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros, señala que "como órgano rector del Sistema Nacional de Informática y en materia de Gobierno Digital, conforme a lo dispuesto en el Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros, concordante con lo establecido en el Decreto Legislativo N° 604, Decreto Legislativo N° 1412 y la Ley N° 29904, tiene las competencias y atribuciones en materia de Seguridad Digital en el Estado Peruano, así como emitir opinión en el ámbito de su competencia. "
- Por tanto, precisa que "es la Presidencia del Consejo de Ministros la entidad responsable de emitir políticas, planes y estrategias nacionales en materia de Gobierno Digital y Seguridad Digital del Estado Peruano, de conformidad con lo establecido en su Reglamento de Organización y Funciones y el Decreto Legislativo N° 1412. En esa línea, precisar, por un lado, que la política de Ciberdefensa es parte de las Políticas, estrategias V planes nacionales que viene formulando esta Secretaría de Gobierno Digital en coordinación con diversas entidades públicas y privadas en materia de Gobierno Digital y Seguridad Digital, conforme a lo establecido en el Reglamento de Organización y Funciones de la PCM; y, por otro lado, no resulta eficiente contar con diversos instrumentos en materia de seguridad digital, ya que genera dispersión normativa y sobre-regulación".
- El Congreso de la República no tiene competencia para aprobar ni establecer los contenidos de una Política, puesto que de conformidad con lo dispuesto en el artículo 4 de la Ley N° 29158, Ley Orgánica del Poder Ejecutivo, son materias exclusivas del Poder Ejecutivo.
- La Política de ciberdefensa es parte de las políticas, estrategias y planes nacionales que viene formulando esta Secretaria de Gobierno Digital en coordinación con diversas entidades públicas y privadas en materia de Seguridad Digital; siendo relevante en su formulación observar las disposiciones y normatividad emitida por el Centro Nacional de Planeamiento Estratégico (CEPLAN) en materia de políticas nacionales, así como atendiendo el rol y atribuciones de la PCM con respecto a la coordinación de políticas y funciones multisectoriales.
- No resulta eficiente contar con diversos instrumentos (políticas) en materia de seguridad digital, la cual comprende a la ciberdefensa, ya que genera dispersión normativa y sobre regulación.
- Respecto al análisis Costo Beneficio (ACB). "El análisis del impacto social y económico de la propuesta del dictamen, Informa y demuestra que el impacto de la propuesta legislativa en el aumento del bienestar social es mayor que el costo de su vigencia", en un marco conceptual que se utiliza para medir el impacto y los efectos de las propuestas normativas sobre diversas variables que afectan a los actores, la sociedad y el bienestar general.

La Presidencia del Consejo de Ministros, emite opinión **CON OBSERVACIONES** de la iniciativa legislativa.

➤ **REUNIÓN DE TRABAJO CON LA PRESIDENCIA DEL CONSEJO DE MINISTROS, MINISTERIO DE DEFENSA Y DIRECCION NACIONAL DE INTELIGENCIA:**

El jueves 18 de julio del 2019, la PCM convocó a una reunión de trabajo para intercambiar ideas y poder levantar las observaciones que plantearon en el Oficio N° D002765-2019-PCM-SG, en dicha reunión participaron las siguientes entidades: la Secretaría de Gobierno Digital, la Secretaría de Gestión Pública, representantes del Ministerio de Defensa, con las Fuerzas Armadas y el Comando Conjunto de las FFAA, Dirección Nacional de Inteligencia y el gabinete de asesores de la Comisión de Defensa Nacional, en la cual se **LEVANTARON LAS OBSERVACIONES** a la Iniciativa Legislativa.

Las mismas que fueron confirmadas mediante correo electrónico de la cuenta mchocobar@pcm.gob.pe, de fecha 20 de Julio del 2019 a horas 15:34, remitido por la Secretaria de la Secretaria de Gobierno Digital de la PCM, al correo jdelcastillo@congreso.gob.pe, cuenta del Presidente la Comisión, Congresista Jorge Del Castillos Gálvez, en la cual adjunta sus conclusiones y recomendaciones.

Teniendo en cuenta que las observaciones fueron levantadas por la Presidencia del Consejo de Ministros, el **PROYECTO DE LEY ES VIABLE SIN OBSERVACIONES**, con la recomendación de aprobación con texto sustitutorio.

VI. ANÁLISIS DE LA PROPUESTA LEGISLATIVA:

6.1. Normativa Vigente:

- **Constitución Política del Perú:**

Artículo 44°

"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"

Artículo 163°

"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.

- **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, atentan contra la seguridad y defensa nacional".

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 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"

6.2. Importancia de la Ciberdefensa:

Existe una relación compleja de interdependencia entre seguridad, defensa y desarrollo. La intensidad de tal interdependencia ha sido matizada fuertemente por la influencia de diferentes intereses y percepciones, relaciones de poder o por intereses geopolíticos y estratégicos dadas en el tiempo, y desarrollos tecnológicos de la humanidad. Justamente, en la actualidad, cuando el desarrollo de las tecnologías de información y comunicaciones (TIC) empiezan a transformar la vida humana y sus estructuras sociales y políticas, la política nacional e internacional, incluyendo las consideraciones de seguridad y defensa. La Internet, las redes de telecomunicaciones, las computadoras, el software, el uso de las redes sociales, la interacción de las personas y las máquinas y las actuaciones que de estas se derivan, han impulsado a la creación un escenario virtual denominado ciberespacio que modifican las acepciones de seguridad y defensa.

Para el año 2020, se estima que la población mundial con acceso a Internet será de 5 mil millones (60% en línea), habrá aproximadamente 50 mil millones de dispositivos (10

equipos por persona) y una afectación a la economía mundial en más del 10% del producto interno bruto (PIB) mundial. Esto explica el porqué de las economías de los estados, de las compañías y de los propios individuos, dependen del ciberespacio), puntualizaron que "nuestro modo de guerrear, refleja nuestro modo de ganar dinero".

Por lo que podríamos afirmar que si la economía y el bienestar están directamente relacionados con el mercado digital o el manejo de la información en el ciberespacio, nuestra seguridad y defensa deben estar también ligadas, cada vez más, al propio ciberespacio. Es decir, que las acciones para defendernos de riesgos, amenazas, peligros y daños virtuales, deben estar también orientadas a darnos confianza y certeza, tanto en el mundo real como en el virtual.¹

La seguridad del ciberespacio no solo constituye una necesidad individual o propia de las compañías, sino que también es un asunto de seguridad y soberanía nacional que influye en la gobernanza nacional en la política nacional e internacional en diferentes grados en la integridad de la economía y en la protección de la información de sus ciudadanos. El Estado y sus instancias regionales deben afrontar el reto de la seguridad y defensa del ciberespacio, así como proteger y garantizar el acceso, uso y contenidos a la sociedad civil en el ámbito virtual, siendo conscientes de su repercusión local, nacional y global.

6.3. De la realización del Proyecto de Ley:

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 Drogas**, invito a diferentes mesas de trabajo, las mismas que fueron realizadas con el Sector Público, 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.²

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, Ejército del Perú, Marina de Guerra del Perú Fuerza Aérea del Perú.

Las conclusiones a que se llegaron fueron:

• **Importancia de la Ciberdefensa:**

- ¿Cuáles son los organismos Institucionales en cada Instituto Armado que trabaja en el campo de la Ciberdefensa?

¹ <https://www.bancomundial.org/es/news/press-release/2018/01/30/world-bank-report-finds-rise-in-global-wealth-but-inequality-persists>

² Exposición de motivos PL N°4228/2018-CR

➤ **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, Ejército 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 Ejército, Marina, FAP y CC.FF.AA. en referencia a Ciberdefensa .
- 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 residencia 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:

- 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, Ejército 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 .

➤ **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

9

Entidades: UNI, Suma Ciudadana, UTP, ISACA, ESAN, ASUP, RENIEC, Colegio de Ingenieros, Universidad San Marcos, Universidad Villarreal, UPC, RENIEC, UTEC, MINEDU, PCM, Universidad San Martín 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, Ejército del Perú, Marina de Guerra del Perú Fuerza Aérea del Perú, RR.EE.

TC, 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, Villarreal, San Martín, 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 Entidades: Comando Conjunto de las Fuerzas Armadas, MINDEF, MININTER, Ejército 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, Ejército del Perú, Marina de Guerra del Perú Fuerza Aérea del Perú, PCM, ASBANC y Congreso de la República, 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, Ejército 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.

6.4. Definiciones

- 
- **Ciberespacio:** Se refiere al conjunto de medios físico o lógicos que conforman las infraestructuras de los Sistemas de Comunicaciones e informáticos, junto a los usuarios que interactúan con estos sistemas.
 - **Ciberdefensa:** Se orienta a las acciones de un Estado para proteger y controlar las amenazas, peligros o riesgos de naturaleza cibernética, con el fin de permitir el uso del ciberespacio con normalidad, bajo la protección de los derechos, libertades y garantías de los ciudadanos, en apoyo a la defensa de la soberanía y la integridad territorial; sin soslayar que en los nuevos escenarios que plantea el ciberespacio, pueden incidir en el momento de trazar rutas estratégicas plausibles para el cumplimiento de las diversas misiones militares de ciberdefensa. (Virilio 1995). cabe duda que a futuro los Estados serán los encargados de decidir en el ámbito de la ciberdefensa, llegando a definir si un ataque virtual a un individuo u organización pública o privada puede comprometer el desarrollo y la supervivencia de la nación. Por ello, consideramos que la ciberseguridad y ciberdefensa han evolucionado de ser temas netamente técnicos, para convertirse en una capacidad estratégica clave en la conducción de un Estado dentro de los diversos niveles de decisión o niveles internacionales cuando se habla de proyectos de ciberseguridad regional (Samper 2015).

6.5. Legislación comparada sobre Ciberdefensa

- Comisión de Defensa Nacional – Gobierno de Chile:

Debido a la creciente dependencia del ciberespacio, la seguridad de su infraestructura, componentes lógicos y las interacciones humanas que allí tienen lugar se ha constituido en una de las más importantes preocupaciones contemporáneas, y la gestión de dichos riesgos una prioridad a nivel global.

Infraestructuras críticas como los servicios básicos, transportes y diversas industrias como la financiera y del transporte, entre muchas otras, incluidas la administración del Estado y la Defensa Nacional, son susceptibles de ser atacadas en el ciberespacio, pudiendo amenazar la estabilidad, seguridad y soberanía de los países de múltiples formas.

En el ámbito de la Defensa, hoy se considera al ciberespacio como un nuevo ambiente en el que se desenvuelven diversos conflictos de diversa naturaleza, nacionales e internacionales. Esto se traduce en la definición del ciberespacio como una dimensión diferente al espacio terrestre, aéreo y marítimo, que requiere contar con las políticas, planificaciones y capacidades que permitan ejercer los roles propios de la Defensa Nacional en este ámbito.

Por ello, de conformidad con lo dispuesto en la ley N°20.424, el Sr. Ministro de Defensa ordenó iniciar el proceso de diseño de una política de defensa para temas del ciberespacio, y de la planificación de la defensa nacional en este ámbito, a través de dos instrumentos que complementan el trabajo llevado a cabo para actualizar las políticas de la defensa nacional:

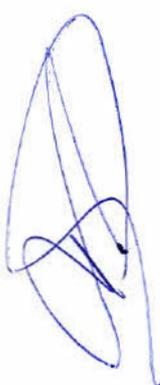
- 
- Una orden ministerial para el diseño de una política de ciberdefensa: el 2014 fue emitida una orden ministerial para la actualización de los planes y políticas de la defensa nacional, con miras a su inclusión en el Libro de la Defensa 2017. En la misma línea, en el año 2015 se emitió la Orden Ministerial N°2, que instruye el diseño de una política de ciberdefensa, cuyo proceso vaya en paralelo al del Libro de la Defensa 2017. Atendida la importancia que ha cobrado la ciberdefensa, se contempla la inclusión de un nuevo capítulo sobre la materia en el Libro referido.

Se afirma que la estructura social y política del Estado-nación actual es una respuesta a la seguridad, que necesariamente implica estar en condiciones de defenderse de amenazas, riesgos y peligros. Por ello, seguridad y defensa son inherentes a la supervivencia y desarrollo del hombre y la sociedad. En suma, el desarrollo de un Estado está íntimamente ligado a su condición de seguridad y a las acciones que se ejecuten para mantener esa condición, es decir, su capacidad de Defensa. Por ende, el conflicto, en sus variadas formas, también es inherente a la historia de la humanidad.

- **Ciberdefensa - Gobierno de Alemania:**

El número de ataques cibernéticos sofisticados contra organismos gubernamentales, industrias e infraestructura en Alemania se ha multiplicado en los últimos años. En el reporte anual sobre actividades extremistas del Ministerio del Interior, publicado el pasado 24 de julio, se sostiene que el ciberespionaje, los actos de sabotaje digital y las campañas de desinformación se han convertido en herramientas estándar tanto de agencias de inteligencia como de hackers extranjeros, sobre todo de Rusia, China e Irán.

Ni siquiera el Ejército alemán ha quedado exento de agresiones digitales: el Bundeswehr dice haber identificado y repelido alrededor de dos millones de incursiones no autorizadas en sus sistemas en 2017; de ellas, 8.000 habrían conseguido acceder a sus redes y causado daños enormes si las medidas defensivas habituales no hubieran funcionado. Fue con ese telón de fondo que la ministra de Defensa de Alemania, Ursula von der Leyen, inauguró el Cyber- und Informationsraum (CIR) en Bonn en abril de 2017.



Sus miembros –260 expertos, civiles y uniformados– se esmeran en proteger la seguridad nacional desde barricadas tan disímiles como la inteligencia militar, las telecomunicaciones, la tecnología de la información y los sistemas de información geográfica. El teniente coronel Marco Kempel y su equipo se ocupan de todo tipo de tareas, desde la conducción de entrenamientos mediante juegos de guerra virtuales hasta la optimización de escudos digitales, como los que impiden la reprogramación no autorizada o el hackeo de los drones.

Con el lanzamiento de su Estrategia de Seguridad Cibernética, la creación de su Centro Nacional de Ciberdefensa y la publicación de su Plan Nacional para la protección de Infraestructuras de información (NPIIP) en el 2011 (Acosta 2009).³

- **Gobierno de Francia:**

Ha creado una Agencia de Seguridad para las Redes e Información (ANSSI) y una Estrategia de Defensa y Seguridad de los Sistemas de información en el 2011 (Acosta 2009). Algunos países en Latinoamérica no han sido la excepción, pues han realizado esfuerzos para aportar a su estrategia en ciberdefensa y ciberseguridad.

Gobierno de España: Ha creado un Centro y un Plan Nacional de Protección de las Infraestructuras Críticas en el 2011 y también un Mando Conjunto de Ciberdefensa en el 2013 (Acosta 2009).

³ <https://www.dw.com/es/ciberdefensa-el-bundeswehr-y-sus-desaf%C3%ADos/a-44989489-0>

Comando Conjunto de Ciber Defensa de España



- Gobierno de Ecuador:

Se evidencia la necesidad de implementar esta capacidad estratégica, lo que evidencia la oportunidad de establecer un modelo local y propio de gobernanza para la seguridad y defensa en el ciberespacio. Se alude al concepto de gobernanza debido a que la inserción de la sociedad de la información en Ecuador ha sido muy rápida en esta última década, integrando las nuevas tecnologías en todas sus actividades e infraestructuras críticas, aumentando la dependencia de sus ciudadanos y del Estado a los sistemas de información y las redes -con alcance global.

Por esta razón, se exige una mirada estratégica para plantear un modelo de intervención, gestión y evaluación que permita controlar la seguridad de la información en los procesos, sistemas e infraestructuras que depende el Estado para su economía y desarrollo.

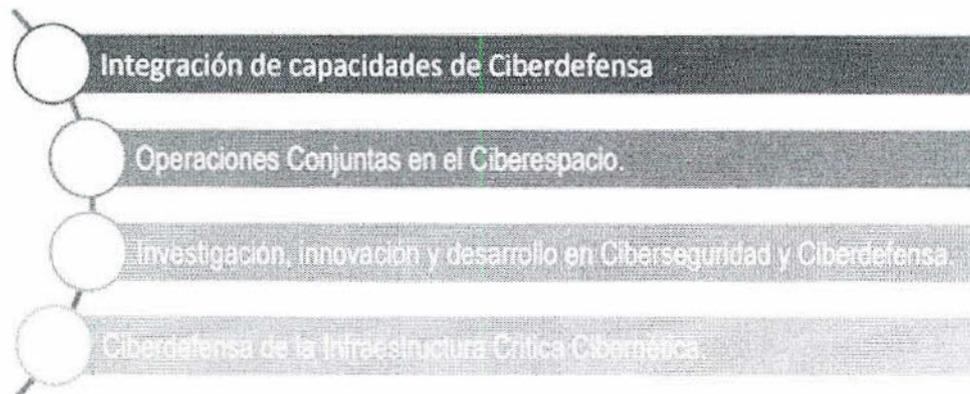
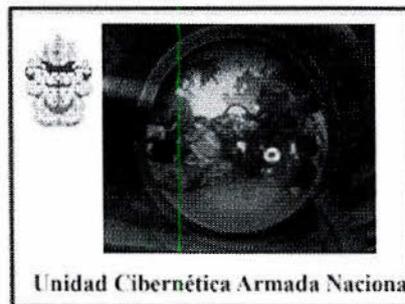
En Ecuador, el acceso al internet ha registrado un elevado incremento durante los últimos 5 años. Por ejemplo, los datos muestran que en el año 2012 la población ecuatoriana alcanzaba el 22,5% y que en el 2015 se alcanzó el 32,8%, según estadísticas del Instituto Nacional de Estadísticas y Censo.⁴

⁴ <https://revistas.flacsoandes.edu.ec/urvio/article/view/2601/2106>

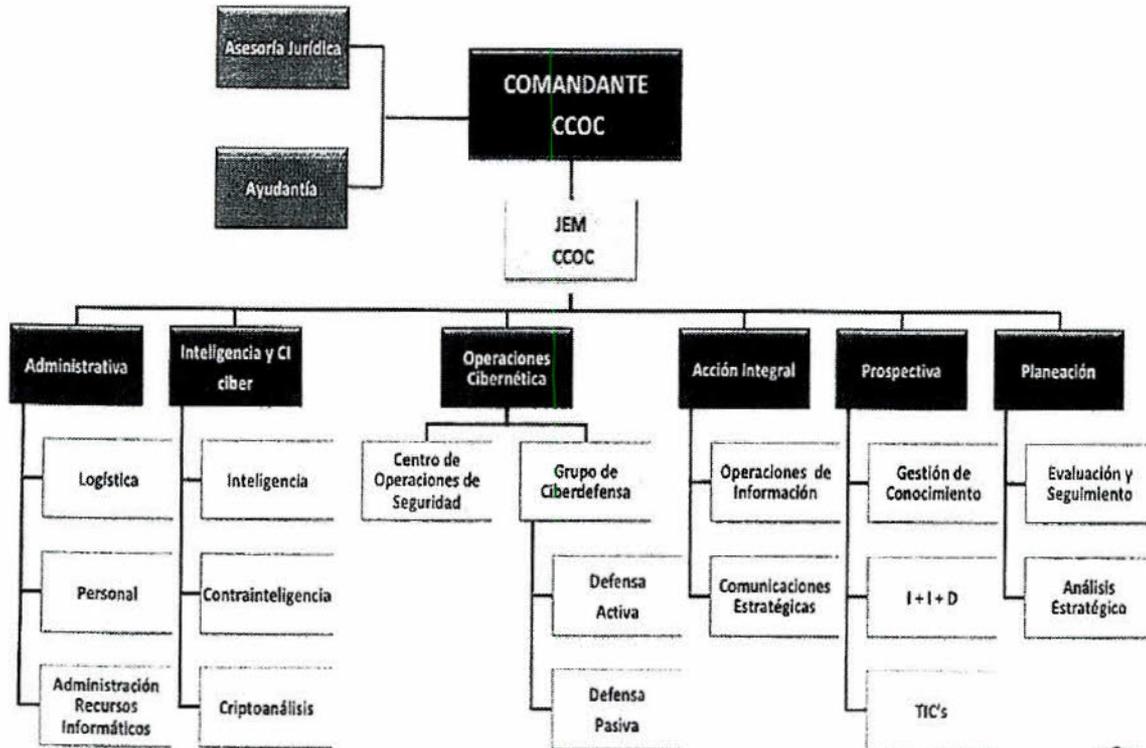
- **Gobierno de Colombia:**

Ha creado el grupo de inteligencia para análisis del ciberespacio en el 2005, reforzado el 2009 y la Estrategia Integral para Ciberseguridad y Ciberdefensa CONPES en el 2011 (Acosta 2009) (Ministerio de Defensa Nacional de Colombia 2009).

- En la actualidad busca ha implementado una Estrategia de Ciberdefensa para el país, basado en personas, tecnologías y procesos. (Operaciones Militares en el Ciberespacio).
- Que está desarrollando capacidades de neutralización y reacción ante incidentes informáticos, que atenten contra la Seguridad y Defensa Nacional.
- Ciberdefensa de la infraestructura crítica del País en el ámbito Cibernético, incluida la del Sector Defensa.



Comando Conjunto Cibernético de Colombia



6.6. Recomendaciones de la Comisión de Defensa Nacional:

Posterior al análisis a la iniciativa legislativa materia de estudio, y de los aportes recogidos en las diferentes mesas de Trabajo impulsados por ésta Comisión y sobre todo de las opiniones de la PCM, MINDEF y DINI, concluimos lo siguiente:

- La Comisión considera que resulta de vital importancia reforzar el trabajo que viene realizando el Estado en materia de ciberdefensa, con el objeto de mitigar el riesgo en la que se expone el Estado Peruano en su conjunto.

VII. ANÁLISIS COSTO BENEFICIO:

El análisis costo beneficio sirve como método de análisis para conocer, en términos cuantitativos, los impactos y efectos que tiene una propuesta normativa sobre diversas variables que afectan a los actores, la sociedad y el bienestar general, de tal forma que permite cuantificar los costos y beneficios de la misma.

La iniciativa legislativa debe ser analizada no desde el tradicional costobeneficio, sino se debe utilizar un análisis costo-eficiencia, considerando que la propuesta legislativa es de

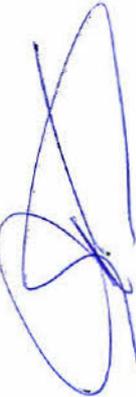
puro derecho, pues lo que se busca es establecer el marco normativo en materia de ciberdefensa del Estado Peruano, por lo que la presente iniciativa no irrogará gasto alguno al Estado.

VIII. CONCLUSIÓN:

Por lo expuesto, la Comisión de Defensa Nacional, Orden Interno, Desarrollo Alternativo y Lucha contra las Drogas, de conformidad con lo establecido en el inciso b) del artículo 70 del Reglamento del Congreso de la República, recomienda la **APROBACIÓN con TEXTO SUSTITORIO** del Proyecto de Ley N° 4228/2018-CR "Ley de Ciberdefensa".

FÓRMULA LEGAL CON TEXTO SUSTITUTORIO

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, conforme a Ley.

Artículo 2.- Finalidad

Defender y proteger la soberanía, los intereses nacionales, los activos críticos nacionales y recursos claves para mantener las capacidades nacionales frente a amenazas o ataques en y mediante el ciberespacio, cuando estos afecten la seguridad nacional.

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 afecten la seguridad nacional.

Artículo 4.- Definición

Entiéndase por Ciberdefensa a la capacidad militar que permite actuar frente amenazas o ataques realizados en y mediante el ciberespacio cuando estos afecten la seguridad nacional.

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.

S/M
En debate
24/7/19
F: 16
C: 1
A: 2
APROB.
7000
Votación
C.P.

**TÍTULO II
DE LA CIBERDEFENSA
CAPÍTULO 1**

**LAS CAPACIDADES DE CIBERDEFENSA Y LAS OPERACIONES EN Y MEDIANTE
EL CIBERESPACIO**

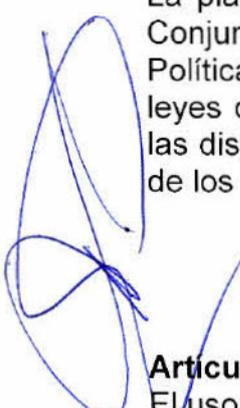
Artículo 6.- De las capacidades de ciberdefensa

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 cuando estos afecten 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 del Comando Conjunto de las Fuerzas Armadas 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

Toda amenaza o ataque en o mediante del ciberespacio que ponga en riesgo la soberanía, los intereses nacionales, los activos críticos nacionales y recursos claves, para mantener las capacidades nacionales, 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 el ciberespacio que contenga un ataque deliberado, deberá realizarse de acuerdo a Ley.

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 y/o del sector responsable de cada uno de ellos y/o de la Dirección Nacional de Inteligencia, sean sobrepasadas, a fin de mantener las capacidades nacionales, en el ámbito de la seguridad nacional.

Artículo 13.- De los Protocolos de Escalamiento, Coordinación, Intercambio y Activación

La Presidencia del Consejo de Ministros, en su calidad de miembro del Consejo de Seguridad y Defensa Nacional, establece los protocolos de escalamiento, coordinación, intercambio y activación para lo indicado en la presente Ley.

Esta función se ejerce a través de la Secretaría de Gobierno Digital en su calidad de ente rector del Sistema Nacional de Informática y de la Seguridad Digital en el país, quien emite los lineamientos y directivas correspondientes.

Artículo 14. 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 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 en coordinación con el Ministerio de Defensa, aprueba 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. - 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.

TERCERA. - 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.

CUARTA. Desarrollo de currículos de educación superior en materia de ciberdefensa

La Presidencia del Consejo de Ministros, en su calidad de ente rector en materia de Seguridad Digital, coordina con el Ministerio de Defensa y el Ministerio de Educación, la pertinencia del desarrollo de contenidos especializados en materia de Seguridad Digital, que incluye la Ciberdefensa, en las instituciones de educación superior universitaria y tecnológica, a nivel de pre y postgrado. Para ello, establece instrumentos de cooperación interinstitucional con entidades del sector privado, la academia, la sociedad civil y la comunidad técnica.

QUINTA. 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

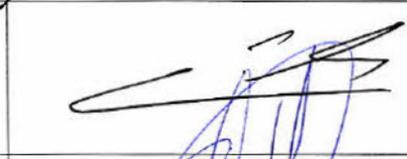
Derogase o déjese en suspenso, según el caso, las disposiciones legales y reglamentarias que se opongan a lo establecido por la presente ley o limiten su aplicación, con la entrada en vigencia de la presente Ley.

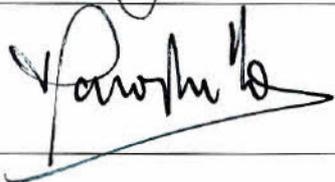
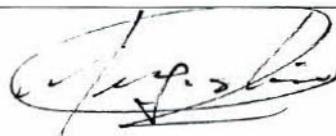
Salvo distinto parecer

Dése cuenta

Sala de Comisión

Lima, julio del 2019

	Del Castillo Gálvez Jorge Alfonso Alejandro Célula Parlamentaria Aprista	Presidente	
	Tubino Arias Schreiber Carlos Mario Del Carmen Fuerza Popular	VicePresidente	
	Segura Izquierdo César Antonio Fuerza Popular	Secretario	

	Alcorta Suero María Lourdes Pía Luisa Fuerza Popular	Titular	
	Arce Cáceres Richard Nuevo Perú	Titular	
	Dipas Huamán Joaquín Fuerza Popular	Titular	
	Dávila Vizcarra Sergio Francisco Félix Peruanos por el Kambio	Titular	
	Iberico Núñez Luis Alianza para el Progreso	Titular	
	Letona Pereyra María Urula Ingrid Fuerza Popular	Titular	
	Melgar Valdez Elard Galo Fuerza Popular	Titular	
	Miyashiro Arashiro Marco Enrique Fuerza Popular	Titular	
	Noceda Chiang Paloma Rosa No Agrupados	Titular	
	Salazar Miranda Octavio Edilberto Fuerza Popular	Titular	
	Salgado Rubianes Luz Filomena Fuerza Popular	Titular	
	Villavicencio Cárdenas Francisco Javier Fuerza Popular	Titular	

	Yika García Luis Alberto	Titular	
	Becerril Rodríguez Héctor Virgilio Fuerza Popular	Accesitario	
	Del Águila Cárdenas Juan Carlos Fuerza Popular	Accesitario	
	Domínguez Herrera Carlos Alberto Fuerza Popular	Accesitario	
	García Belaúnde Víctor Andrés Acción Popular	Accesitario	
	Lapa Inga Zacarías Reymundo Frente Amplio por Justicia, Vida y Libertad	Accesitario	
	Martorell Sobero Guillermo Hernán Fuerza Popular	Accesitario	
	Pariona Galindo Federico Fuerza Popular	Accesitario	
	Quintanilla Chacón Alberto Eugenio Nuevo Perú	Accesitario	
	Trujillo Zegarra Gilmer Fuerza Popular	Accesitario	
	Velásquez Quesquén Angel Javier Célula Parlamentaria Aprista	Accesitario	
	Beteta Rubín Karina Juliza Fuerza Popular	Accesitaria	

	Cuadros Candia Nelly Lady Fuerza Popular	Accesitaria	
	Schaefer Cuculiza Karla Melissa Fuerza Popular	Accesitaria	
	Galarreta Velarde Luis Fernando Fuerza Popular	Accesitario	

JUNTA DE PORTAVOCES DEL CONGRESO DE LA REPÚBLICA

Lima, 23 de julio de 2019

Se acordó la exoneración de plazo de publicación del dictamen de la Comisión de Defensa Nacional, Orden Interno, Desarrollo Alternativo y Lucha contra las Drogas de respecto del Proyecto de Ley 4228/2018-CR, y la ampliación de Agenda.-----



GUILLERMO LLANOS CISNEROS
Director General Parlamentario
CONGRESO DE LA REPÚBLICA

COMISIÓN PERMANENTE DEL CONGRESO DE LA REPÚBLICA

Lima, 24 de julio de 2019

Efectuada la votación nominal, se aprobó, en primera votación, el texto sustitutorio contenido en el dictamen de la Comisión de Defensa Nacional, Orden Interno, Desarrollo Alternativo y Lucha contra las Drogas respecto del Proyecto de Ley 4228/2018-CR, por 16 votos a favor, 1 voto en contra y 2 abstenciones.-----

De conformidad con el artículo 78 del Reglamento del Congreso el proyecto aprobado será materia de segunda votación transcurrido siete días calendarios, salvo que la Junta de Portavoces acuerde la exoneración de este trámite reglamentario.-----

Se solicita la dispensa del trámite de sanción del Acta para ejecutar lo acordado en la presente sesión.-----



GUILLERMO LLANOS CISNEROS
Director General Parlamentario
CONGRESO DE LA REPÚBLICA

JUNTA DE PORTAVOCES DEL CONGRESO DE LA REPÚBLICA

Lima, 24 de julio de 2019

Se acordó la exoneración de segunda votación del texto sustitutorio contenido en el dictamen de la Comisión de Defensa Nacional, Orden Interno, Desarrollo Alternativo y Lucha contra las Drogas respecto del Proyecto de Ley 4228/2018-CR.-----



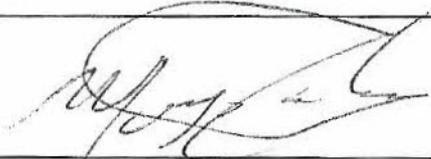
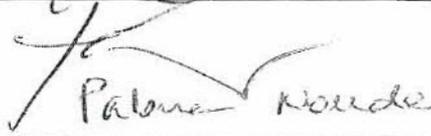
GUILLERMO LLANOS CISNEROS
Director General Parlamentario
CONGRESO DE LA REPÚBLICA

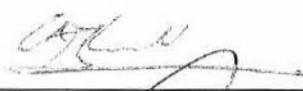
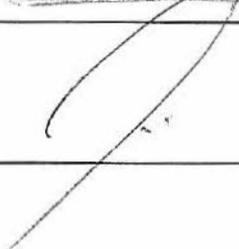


Defensa Nacional, Orden Interno, Desarrollo Alternativo y Lucha Contra Las Drogas

VII Sesión Extraordinaria
Fecha: 22 de julio de 2019
Hora: 09:00 horas
Sala: Miguel Grau Seminario

	Del Castillo Gálvez Jorge Alfonso Alejandro Célula Parlamentaria Aprista	Presidente	
	Tubino Arias Schreiber Carlos Mario Del Carmen Fuerza Popular	VicePresidente	
	Segura Izquierdo César Antonio Fuerza Popular	Secretario	
	Alcorta Suero María Lourdes Pía Luisa Fuerza Popular	Titular	
	Arce Cáceres Richard Nuevo Perú	Titular	
	Dipas Huamán Joaquín Fuerza Popular	Titular	
	Iberico Núñez, Luis Alianza para el Progreso	Titular	
	Dávila Vizcarra Sergio Francisco Félix Peruanos por el Cambio	Titular	
	Letona Pereyra María Úrsula Ingrid Fuerza Popular	Titular	
	Melgar Valdez Elard Galo Fuerza Popular	Titular	

	Miyashiro Arashiro Marco Enrique Fuerza Popular	Titular	
	Noceda Chiang Paloma Rosa Acción Popular	Titular	
	Salazar Miranda Octavio Edilberto Fuerza Popular	Titular	
	Salgado Rubianes Luz Filomena Fuerza Popular	Titular	
	Villavicencio Cárdenas Francisco Javier Fuerza Popular	Titular	
	Yika García Luis Alberto Fuerza Popular	Titular	
	Becerril Rodríguez Héctor Virgilio Fuerza Popular	Accesitario	
	Del Águila Cárdenas Juan Carlos Fuerza Popular	Accesitario	
	Domínguez Herrera Carlos Alberto Fuerza Popular	Accesitario	
	García Belaúnde Víctor Andrés Acción Popular	Accesitario	
	Lapa Inga Zacarías Reymundo Frente Amplio por Justicia, Vida y Libertad	Accesitario	
	Martorell Sobero Guillermo Hernán Fuerza Popular	Accesitario	
	Pariona Galindo Federico Fuerza Popular	Accesitario	

	Quintanilla Chacón Alberto Eugenio Nuevo Perú	Accesitario	
	Trujillo Zegarra Gilmer Fuerza Popular	Accesitario	
	Velásquez Quesquén Angel Javier Célula Parlamentaria Aprista	Accesitario	
	Beteta Rubín Karina Juliza Fuerza Popular	Accesitaria	
	Cuadros Candia Nelly Lady Fuerza Popular	Accesitaria	
	Schaefer Cuculiza Karla Melissa Fuerza Popular	Accesitaria	
	Galarreta Velarde Luis Fernando Fuerza Popular	Accesitario	
	Castro Grandez, Miguel Alianza para el Progreso	Accesitario	

Lima, 22 de julio de 2019

CARTA N°072-2019-RAC-CR

Señor

JORGE DEL CASTILLO GÁLVEZ

Presidente de la Comisión de Defensa Nacional, Orden Interno,

Desarrollo Alternativo y Lucha Contra Las Drogas

Presente

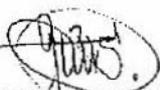
De mi especial consideración.

Es grato dirigirme a usted para saludarlo cordialmente y a la vez, por especial encargo del congresista Richard Arce, solicito considere como licencia su inasistencia a la sesión de la Comisión de Defensa Nacional, Orden Interno, que se desarrollará hoy 22/07/2019, por motivo que se encuentra fuera de Lima.

Sin otro particular, quedo de usted.

Atentamente,




HERNÁN VIDALÓN SEVILLA
ASESOR I
DESPACHO DEL CONGRESISTA RICHARD ARCE



22/09/19

9:45.

Lima, 22 de julio de 2019

CARTA N°072-2019-RAC-CR

Señor

JORGE DEL CASTILLO GÁLVEZ

Presidente de la Comisión de Defensa Nacional, Orden Interno,

Desarrollo Alternativo y Lucha Contra Las Drogas

Presente

De mi especial consideración.

Es grato dirigirme a usted para saludarlo cordialmente y a la vez, por especial encargo del congresista Richard Arce, solicito considere como licencia su inasistencia a la sesión de la Comisión de Defensa Nacional, Orden Interno, que se desarrollará hoy 22/07/2019, por motivo que se encuentra fuera de Lima.

Sin otro particular, quedo de usted.

Atentamente,



[Handwritten signature]
HERNÁN VIDALÓN SEVILLA
ASESOR I
DESPACHO DEL CONGRESISTA RICHARD ARCE

[Handwritten signature]

22/09/19

9:45.

Lima, 22 de julio del 2019

OFICIO N° 274 - 2018-2019-FVC/CR

Señor
Jorge del Castillo Gálvez
Presidente de la Comisión de Defensa Nacional, Orden Interno, Desarrollo Alternativo y Lucha
contra las Drogas.
Congreso de la República del Perú.
Presente. -

De mi mayor consideración:

Tengo el agrado de dirigirme a usted, por encargo del congresista de la República **Francisco Villavicencio Cárdenas**, para que se le conceda la dispensa del caso en la **Séptima Sesión Extraordinaria**, que se llevará a cabo este 22 de julio del presente año, por motivos personales; para los fines que estime pertinente.

Agradeciendo la atención al presente, reciba mi respeto y consideración.

Atentamente,


Miguel Picoaga Vargas
Asesor II



22-07-19

9:22.

FVC/AD

Lima, 22 de julio 2019

Oficio N° 076 -2019/DCEMV-CR

Señor Congresista

Jorge Del Castillo Gálvez

Presidente de la Comisión de Defensa Nacional, Orden Interno, Desarrollo Alternativo
y Lucha Contra las Drogas

Presente. -

**ASUNTO: SOLICITA LICENCIA – SESION
ORDINARIA DIA 22/07/2019**

De mi especial consideración:

Tengo el agrado de dirigirme a usted, para expresarle mi saludo cordial y por especial encargo del **Congresista Elard Melgar Valdez**, hacer de vuestro conocimiento que no podrá asistir a la Sesión de la Comisión de Defensa Nacional, Orden Interno, Desarrollo Alternativo y Lucha Contra las Drogas, convocada para el día de hoy lunes 22 de julio de 2019, en razón que debe atender reuniones oficiales de trabajo a realizarse en provincias, las mismas que fueron concertados con antelación.

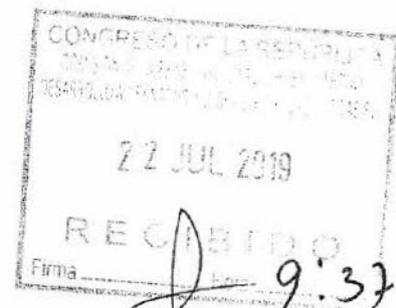
Por la razón expuesta, mucho agradeceré tenga a bien considerar su ausencia justificada y autorizar la licencia respectiva, en concordancia con el Artículo 22° literal i) del Reglamento del Congreso de la República.

Aprovecho la oportunidad para reiterar a usted la expresión de mi distinguida consideración.

Atentamente,



[Firma manuscrita]
Luis Humberto Villa
Primer Asesor
del Congresista Elard Melgar Valdez



29

47