CONGRESO de la REPÚBLICA

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

CONGRESO DE LA REPÚBLICA
ÁREA DE TRÁMITE DOCUMENTARIO
22 JUL 2019
RECIBIDO
Firma _____ Hora 17:04

DICTAMEN CON RECOMENDACIÓN DE APROBACIÓN, CON TEXTO SUSTITORIO RECAIDO EN LOS PROYECTOS DE LEY N° 4237/2018-CR Y 4352/2018-CR "LEY DE CIBERSEGURIDAD".

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 los siguientes Proyectos de Ley:

- **Proyecto de Ley 4237/2018-CR**, presentado por el congresista Carlos Domínguez Herrera, por el que propone la "Ley que promueve la seguridad e informática en el Perú y la conformación de un Consejo Nacional de Ciberseguridad".

- **Proyecto de Ley 4352/2018-CR**, presentado por el congresista Jorge Del Castillo Gálvez, por el que propone la "Ley de Ciberseguridad".

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 N° 4237/2018-CR,** "Ley que promueve la seguridad e informática en el Perú y la conformación de un Consejo Nacional de Ciberseguridad", ingresó a trámite documentario el 17 de abril del 2019, siendo decretado a la Comisión de Defensa Nacional, Orden Interno, Desarrollo Alternativo y Lucha Contra las Drogas y a la Comisión de Ciencia, Innovación y Tecnología el 25 de abril del mismo año.

- **Proyecto de Ley N° 4352/2018-CR,** "Ley de Ciberseguridad", ingresó a trámite documentario el 17 de mayo del 2019, siendo decretado a la Comisión de Defensa Nacional, Orden Interno, Desarrollo Alternativo y Lucha Contra las Drogas y a la Comisión de Ciencia, Innovación y Tecnología el 24 de mayo del mismo año.

II. CONTENIDO DE LAS PROPUESTAS LEGISLATIVAS.

- **Proyecto de Ley N° 4237/2018-CR: "**Ley que promueve la seguridad e informática en el Perú y la conformación de un Consejo Nacional de Ciberseguridad", que detalla lo siguiente:

388397

- La iniciativa legislativa tiene como objetivo promover la seguridad informática en todo el territorio nacional y la conformación de un Consejo Nacional de Ciberseguridad en el marco de las competencias de la Presidencia del Consejo de Ministros y la Secretaría de Gobierno Digital, como ente rector de la materia en el País.

- La iniciativa legislativa se rige por los principios de colaboración multidisciplinaria, multisectorial e inter institucional, respeto a los derechos humanos y enfoque basado en gestión de riesgos.

- Respecto a las Políticas de Seguridad Informática, establece que la Presidencia del Consejo de Ministros (PCM) a través de la Secretaría de Gobierno Digital, sea la que establezca el fortalecimiento de las políticas de seguridad informática en todos los organismos de la administración pública.

- La propuesta legislativa establece una serie de condiciones mínimas para la implementación de la Ciberseguridad, para sistematizar las normas en materia de ciberseguridad con rango ley, clasificar información métricas de ciberseguridad, capacitación en continuidad y realización de pruebas de vulnerabilidades, establecer criterios, normas y metodologías para la generación, uso y adopción de hardware y software con la finalidad de fortalecer el ecosistema de ciberseguridad y disminuir riesgos y vulnerabilidades inherentes a la tecnología y desarrollar un marco jurídico nacional vinculado a la ciberseguridad y de autorregulación; por parte de los concesionarios y distribuidores de servicios de Tecnologías de la Información y Comunicación (TIC).

- La propuesta legislativa también propone la creación de un Comité de respuesta ante la Ciberdelincuencia (CORECY). Como una dependencia del Consejo Nacional de Ciberseguridad, al cual se encargará ser la primera fuente de respuesta y ayuda ante las dificultades de seguridad informática y los ciberataques que se realicen a cualquier entidad de la administración pública y en la actividad privada.

- Propone la creación del Consejo Nacional de Ciberseguridad (CONACY), cuyas entidades que la conformarían sería el Poder Judicial, Presidencia del Consejo de Ministros a través de la Secretaría de Gobierno Digital (SEGDI) quien la preside, Poder Judicial, Dirección Nacional de Inteligencia (DINI). Ministerio de Defensa (MINDEF), Ministerio del Interior (MININTER). Ministerio de Transportes y Comunicaciones (MTC), Policía Nacional del Perú (PNP), Asociación de Gobiernos Regionales, Sociedad Nacional de Industrias (SNI), Asociación de Bancos del Perú (ASBANC), Asociación para el Fomento de la Infraestructura Nacional (AFIN), Red Científica Peruana (RCP), Cámara de Comercio de Lima (CCL) (OBS), Cámara Nacional de Comercio, Producción, Turismo y Servicios – PERUCÁMARAS, Colegio de Abogados de Lima (CAL), Colegio de Ingenieros del

Perú (CIP), NAP (Network Access Point) Perú, y la Confederación Nacional de Institucionales Empresariales Privadas (CONFIEP).

- **Proyecto de Ley N° 4352/2018-CR:** "Ley de Ciberseguridad", que detalla lo siguiente:

  - La iniciativa legislativa tiene por objeto establecer el marco normativo en materia de Seguridad Digital del Estado Peruano, teniendo alcance a todas las entidades del sector público de los niveles de gobierno y a las entidades del sector privado, academia y sociedad civil.

  - La Iniciativa Legislativa establece las siguientes definiciones:

    - **CSIRT:** Se define como un equipo de respuesta frente a incidentes de seguridad informática, como un colectivo o una entidad dentro de un organismo que ofrece servicios y soporte a un grupo en particular, con la finalidad de revenir, gestionar y responder a incidentes de seguridad digital.

    - **Seguridad Digital:** Lo define como el Estado de confianza en el entorno digital que resulta de la gestión y aplicación de un conjunto de medidas proactivas y reactivas frente a los riesgos que afectan la seguridad de las personas, la prosperidad económica y social, la seguridad ciudadana y los objetivos nacionales.

  - Respecto a los principios que rigen la propuesta legislativa, resaltan el respeto de los Derechos Humanos en el ejercicio de la Ciberseguridad (Se debe tomar en cuenta en consideración en todo desarrollo normativo y de políticas en materia de Ciberseguridad el respeto irrestricto a los Derechos Humanos, en concordancia con la Constitución Política del Perú y los Acuerdos Internacionales), y la comunicación de incidentes (Se deberá crear mecanismos de comunicación de incidentes entre la sociedad civil, el sector privado, la academia, la comunidad técnica y el sector gubernamental).

  - También propone la creación del Comité de Ciberseguridad del Estado Peruano, el cual estaría adscrito a la PCM y a la Secretaria de Gobierno Digital, el mismo que deberá contar en su conformación con participación del sector privado, sociedad civil, academia, comunidad técnica de internet y sector gubernamental, éste comité tendrá como función formular la Política de Ciberseguridad del Estado Peruano, generar lineamientos en materia de CSIRT en el sector privado, gestionar el Fondo de Seguridad Digital, fomentar la cultura de Ciberseguridad, coadyuvar al fomento de currículos de educación superior en materia de Ciberseguridad y otras que les pudiera establecer la COSEDENA.

  - La iniciativa legislativa busca crear mecanismos de comunicación de incidentes entre la sociedad civil, el sector privado, la academia, la comunidad técnica y el sector gubernamental. Dichos mecanismos de comunicación de incidentes deberán mantener la reserva de los casos indicados, en los casos que pudiera su revelación afectar a las instituciones o a la sociedad, pero también deberá

evaluarse los casos para divulgar dicha información a otros actores y a la sociedad.

- La iniciativa legislativa establece también los principios, modelos, políticas, normas, procesos, roles, tecnología y estándares mínimos que permitan preservar la confidencialidad, integridad, disponibilidad de la información en el entorno digital administrado por las entidades de la administración pública, serán establecidos por la Secretaría de Gobierno Digital.

- Establece que la Presidencia del Consejo de Ministros formula la Política Nacional de Ciberseguridad 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.

- Busca el establecimiento de un Fondo de Seguridad Digital con los aportes provenientes de cooperación técnica, aportes de entidades públicas y privadas, así como de recursos del Programa Nacional de Telecomunicaciones (PRONATEL), para fomentar la investigación, innovación desarrollo de capacidades, la industria nacional y sensibilización social en materia de Seguridad Digital.

- Establece que sea el Ministerio de Educación quien fomente el desarrollo de currículos especializadas en ciberseguridad 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.

III. MARCO NORMATIVO:

- Constitución Política del Perú
- Reglamento del Congreso
- Ley N° 27269, Ley de Firmas y Certificados Digitales
- Ley N° 27291, Ley que modifica el Código Civil permitiendo la utilización de los medios electrónicos para la comunicación de la manifestacipon de la voluntad y la utilización de la fiirma electrónica.
- Ley 27309, Ley que Incorpora los Delitos Informáticos al Código Penal.
- Ley N° 28493, Ley que regula el uso del correo electrónico comercial no solicitado (spam).
- Ley N° 28530, Ley de promoción de acceso a internet para personas con discapacidad y adecuación del espacio físico en cabinas públicas de internet.
- Ley N° 29733, Ley de Protección de Datos Personales
- Ley N° 29904, Ley de Promoción de la Banda Ancha y Construcción de la Red Dorsal Nacional de Fibra Óptima.
- Ley N° 30096, Ley de Delitos Informáticos.
- Ley N° 30618, Ley que modifica el Decreto Legislativo 1141, Decreto Legislativo, de Fortalecimiento y Modernización del Sistema de Inteligencia Nacional – SINA y de la Dirección Nacional de Inteligencia DINI.

- Decreto Legislativo 1141, Decreto Legislativo de Fortalecimiento y Modernización del Sistema de Inteligencia Nacional – SINA y los que señala la Ley.
- Decreto Legislativo N° 1353, Decreto Legislativo que crea la autoridad de transparencia y acceso a la información pública, fortalece el régimen de protección datos personales y la regulación de la Gestión de Intereses.
- Decreto Legislativo N° 1412, Ley de Gobierno Digital.
- Decreto Supremo N° 012-2017-DE:
- Decreto Supremo N° 050-2018-PCM
- Decreto Supremo N° 081-2013-PCM, Decreto Supremo mediante el cual se aprueba la Política Nacional de Gobierno Electrónico.
- Decreto Supremo N°065-2015-PCM, que crea la Comisión Multisectorial Permanente encargada del Seguimiento y evaluación del "Plan de Desarrollo, Sociedad de la Información en el Perú – La agenda digital peruana.
- Resolución Ministerial N° 246-2007-PCM
- Resolución Ministerial N° 004-2016-PCM.
- Resolución Ministerial N° 166-2016-PCM

IV. OPINIONES SOLICITADAS:

4.1. Proyecto de Ley N° 4237/2018-CR "Ley que promueve la seguridad e informática en el Perú y la conformación de un Consejo Nacional de Ciberseguridad"

- **Ministerio de defensa:** Mediante Oficio N° 826-2018-2019/CDNOIDALCLD-CR de fecha 30 de abril del 2019, por el que se solicita opinión del Proyecto de Ley 4237/2018-CR, al General José Modesto Huerta Torres en su condición de ministro, habiéndose recibido la respuesta correspondiente.

- **Presidencia Del Consejo De Ministros – PCM:** Mediante Oficio N° 827-2018-2019/CDNOIDALCLD-CR de fecha 30 de abril del 2019, por el que se solicita opinión del Proyecto de Ley 4237/2018-CR,al Señor Salvador Del Solar Labarthe, no habiéndose recibido respuesta hasta la fecha.

4.2. Proyecto de Ley N° 4352/2018-CR: "Ley de Ciberseguridad"

- **Ministerio de Justicia y Derechos Humanos:** Mediante Oficio N° 911-2018-2019/CDNOIDALCLD-CR de fecha 29 de mayo del 2019, por el que se solicita opinión del Proyecto de Ley 43522018-CR, al señor Vicente Antonio Zeballoss en su condición de ministro, habiéndose recibido la respuesta correspondiente.

- **Ministerio del Interior:** Mediante Oficio N° 912-2018-2019/CDNOIDALCLD-CR de fecha 29 de mayo del 2019, por el que se solicita opinión del Proyecto de Ley 4352/2018-CR, al Señor Carlos Morán Soto, no habiéndose recibido respuesta hasta la fecha.

V. OPINIONES RECIBIDAS

5.1. Proyecto de Ley N° 4352/2018-CR: "Ley de Ciberseguridad".

- **Ministerio de Justicia y Derechos Humanos:** Mediante Oficio N° 22 /2019-MINJUS-SG de fecha 2 de Julio del 2019, el Sr. Carlos Alberto Cavagnaro Pizarro, en su condición de Secretario General, quien remite el Informe N° 262/2019-MINJUS-DGDNCR que concluye lo siguiente:

  - La Ciberseguridad al que hace referencia la Iniciativa Legislativa se refiere a métodos de uso, procesos y tecnologías para prevenir, detectar y recuperarse de daños a la confidencialidad, integridad y disponibilidad de la información en el ciberespacio, todas las partes involucradas en la ciberseguridad, ya sea un usuario individual de internet, un pequeño negocio, una institución, organismos públicos o empresas privadas, deben decidir su propia política para mantener la seguridad en el ciberespacio y estas deben estar directamente correlacionadas entre si y responder a una Estrategia Nacional de Ciberseguridad a nivel superior con una misión y un propósito como nación.

  - En la iniciativa legislativa mediante la Quinta y Sexta Disposición complementaria final, se observa que su finalidad no es establecer el marco normativo, sino dirigir la política nacional en materia de ciberseguridad, motivo por que la propuesta no resulta viable, al contravenir los artículos 43 y 118 de la Constitución.

  - El Proyecto de Ley indica que en el análisis costo – beneficio, la propuesta no demandará recursos adicionales al Tesoro Público, sin embargo propone la creación del Comité de Ciberseguridad del Estado Peruano, éste comité según el artículo 5 del Proyecto, deberá contar en su conformación con participación del sector privado, sociedad civil, academia, comunidad técnica de internet y sector gubernamental, estando adscrito a la Presidencia del Consejo de Ministros a través de la Secretaría de Gobierno Digital quien hará funciones de secretaría técnica, quien coordinará con el secretario técnico del Consejo de Seguridad y Defensa Nacional (COSEDENA), además de que el Comité tendrá como función formular la Política de Ciberseguridad del Estado Peruano, generar lineamientos en materia de CSIRT en el sector privado, gestionar el Fondo de Seguridad al fomento de currículos de educación superior en materia de Ciberseguridad, y otras que les pudiera establecer la COSEDENA.

  - Como se observa, las funciones del Comité de Ciberseguridad del Estado Peruano sí requieren que se destine presupuesto estatal como, por ejemplo, generar lineamientos en materia de CSIRT (Equipo de Respuesta frente a Incidentes de Seguridad Informática, o gestionar el Fondo de Seguridad al fomento de currículos de educación superior en materia de Ciberseguridad y Ciberdefensa.

  - Asimismo, en concordancia con el Reglamento del Congreso de la República señala en su artículo 76 que las proposiciones legislativas de los congresistas "no pueden contener propuestas de creación, ni aumento de gasto público. Esta regla no afecta el derecho de los Congresistas de hacer proposiciones en ese sentido, durante el debate del Presupuesto (...)"

- Así, tenemos que al Poder Ejecutivo es a quien le corresponde dirigir y manejar la economía del Estado, y en exclusividad, la iniciativa de elaborar el presupuesto (fase: programación y formulación), así como administrar los "fondos públicos" (fase: ejecución presupuestaria) , dirigir la política general de gobierno, dictar medidas extraordinarias, en materia económica y financiera, cuando así lo requiera el interés nacional dando cuenta al Congreso; por ende es quien dirige la política económica del País.

- De otro lado, el control de esa política corresponde al Congreso, así como la facultad exclusiva de aprobar presupuesto, sus modificaciones y de emitir pronunciamiento sobre la rendición de cuentas de dicho presupuesto, por lo que pretender modificar dichos roles o invertirnos, atenta contra la Constitución.

  En ese sentido, El Ministerio de Justicia y Derechos Humanos concluye que el Proyecto de Ley **NO RESULTA VIABLE** por contravenir lo dispuesto en el artículo 79 de la Constitución.

– **Ministerio del Interior:** Mediante Oficio N°908-2019/IN-DM de fecha 17 de Julio del 2019, se emite opinión del Proyecto de Ley N° 4352/2018-CR, el Sr. Carlos Morán Soto, en su condición de Minsitro del Interior, donde detallan lo siguiente:

El área legal del MININTER, recomendia que se evalue en la reglamentación los siguientes aspectos:

– Que se establezca la participación de la División de Investigación de Delitos de Alta Tecnología de la Dirección de Investigación Criminal de la Policía Nacional del Perú, teniendo en cuenta que es la unidad especializada en la investigación del cibercrimen, debiendo estar enmarcado su accionar de acuerdo a la Ley Nro. 30096 y su modificatoria Ley Nro. 30171; así como incorporaciones legales que se puedan dar, considerando la conceptualización de Seguridad Digital que involucra la seguridad de las personas, la prosperidad económica y social, la seguridad nacional y los objetivos nacionales.

– Que se disponga en forma obligatoria y sujeto a sanciones que todos los organismos conformantes del Sector Gubernamental, Sector Privado, Sociedad Civil, y demás sectores involucrados en este Proyecto de Ley, comuniquen los incidentes relacionados a ciberataques o similares a la Dirección de Investigación Criminal de la Policía Nacional del Perú, a fin se efectúen las acciones pertinentes y de ser el caso asuma las investigaciones.

– Que los organismos del Estado responsables efectúen acuerdos con los proveedores de servicios internacionales (Facebook, Google entre otros) así como con las operadoras de comunicaciones locales (Claro, Movistar, Bitel, Entel entre otros), a fin de establecer plazos en la entrega de información que se requiere para las investigaciones en todos sus niveles.

Se advierte la existencia de dispositivos normativos vigentes que contienen:

- El marco de gobernanza del gobierno digital para la adecuada gestión de la Seguridad Digital y datos, así como el régimen jurídico aplicable al uso transversal de tecnologías digitales en la digitalización de procesos y prestación de servicios digitales por parte de las entidades de la Administración Pública en los tres niveles de Gobierno; i) Las responsabilidades de distintas entidades

respecto a los ámbitos de gestión del Marco de Seguridad Digital de Estado peruano; ii) Los instrumentos legales para la prevención, sanción y persecución de ilícitos administrativos o penales vinculados a la Seguridad Cibernética, además de otros aspectos propuestos en el Proyecto de Ley.

- La propuesta legislativa debe señalar que contiene aspectos que complementan el marco legal vigente, al incluir al sector privado en los alcances de ta normativa sobre Seguridad Digital (Cibeseguridad); sin embargo, dada la rectoría ejercida por la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, se RECOMIENDA contar con la opinión técnica de dicha entidad, a efectos afinar los aspectos pertinentes, con el fin de que el Proyecto de Ley se traduzca, de ser el caso, en una Ley bien estructurada cuidando que no se regule más de una vez una hipótesis, evitando redundancias innecesarias para facilitar su interpretación y cumplimient0[23] y en su caso proponiendo las modificaciones o ampliaciones que puedan mejorar las normas legales a fin de alcanzar los fines por los cuales fueron emitidas.

  En este sentido, el Ministerio del Interior se emite opinión legal sobre el presente Proyecto del Ley, resultando legalmente **VIABLE CON COMENTARIOS**, conforme a lo señalado en et párrafo anterior y en el presente informe.

VI. ANÁLISIS DE LA PROPUESTA LEGISLATIVA:

6.1. Sobre Ciberseguridad:

Existen varias definiciones sobre lo que significa Ciberseguridad, en la cual la Comisiñon ha considerado la siguiente:

> "La Ciberseguridad se refiere a métodos de uso, proceso y tecnologias para prevenir, detectar y recperarse de daños a la confidencialidad, ya sea un usuario individual de internet, un pequeño negocio, una institución, oganismos públicos o empresas privadas, deben de decidir su propia politica para manetener la seguridad en el ciberespacio u estas deben estar directamente correlacionadas entre si y responden a una estrategia nacional de Ciberseguridad de nivel superior con una misión y un propósito como nación".[1]

En uso de las teconologías de la información y las comunicaciones trae consigo cambios y retos permanentes y se constitue como uno de los pilares del mundo globalizado. De manera simultánea el avance de estas tecnologías ha incrementado el uso de medios tecnológicos con fines delictivivos alrrededor del mundo.

La continua evolución, crecimiento y sofisticación de los ataques cibernéticos, al igual que la convergencia tecnológica, ponen de manifiesto la necesidad de adoptar las medidas y controles que permitan proteger al Estado ante estas nuevas amenazas[2].

---

[1] LEIVA, Alfredo (2015) "Estrategias Nacionales de Ciberseguridad: Estudio Comparativo basado en Enfoque To´-Down, desde una visión local", Revista Latinoamericana de Ingeniería de Software 3(4), p. 161-176

[2] Jenkins, Henrry (2006) Convergence Culture, Nwe York University Press, New York).

El aumento de la capacidad delincuencial en el ciberespaci, así como la utilización de nuevas teconlogías para generar amenazas informáticas, constituyen una precupación común a todos los

Países, dado que impactan de manera significativa la seguridad de la información, en los ámbitos tanto públicos como privados e incluyendo a la sociedad civil.

Trabajar en temas de ciberseguridad implica un compromiso del Gobierno Nacional por garantizar la seguridad de la información, en atención a éste tema, varios paises ya viene implementando estrategias de Ciberseguridad Nacional, considerando a éste como un documento estratégico que le sirve como fundamento al Gobierno para desarrollar las previsiones de la Estrategia de Seguridad Nacional en materia de protección del ciberespacio con el fin de implantar de forma coherente y estructurada acciones de prevención, defensa, detencción y respuesta de Ciberseguridad.

Diferentes países alrededor del mundo han establecido como una de sus estrategias fundamentales el planteamiento de alternativas metodológicas desarrolladas en términos de políticas, normas, procedimientos, estándares y de la definición de niveles específicos de referencia en términos de Ciberseguridad que se encuentren alineados con las diferentes estrategias nacionales, con los desarrollos normativos particulares y con las directrices planteadas a través de Ministerios, Unidades Administrativas y Programas nacionales, así como también con legislación internacional, con directrices dadas por los organismos de normalización y estandarización y con políticas establecidas por las diferentes asociaciones internacionales, todo con el fin de fortalecer la posición estratégica del Estado en el ciberespacio y enfrentar de manera adecuada los riesgos de naturaleza cibernética a los que se ve expuesto.[3]

6.2. Legislación comparada sobre Ciberseguridad en otros Países:

- **Colombia**.- Fue el primero en adoptar una Estrategia Integral de Ciberseguridad[4], cuyos vectores de desarrollo sobre materia de Ciberseguridad para Colombia, están orientadas a fortalecer la posición del País, alineados con las diferentes estrategias nacionales provenientes desde las entidades del Estado y del sector privado, y que con su fortalecimiento conlleven a mejorar la posición estratégica del país en estos temas.

  Colombia ha empezado a plantear una visión rectora consolidada en el documento CONPES 3701, el cual busca generar los lineamientos nacionales de política en Ciberseguridad orientados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país. En este marco de referencia se define la Ciberseguridad como la capacidad del Estado

---

[3] Sistema de investigación, desarrollo e innovación subsistema de innovación para el uso y apropiación de tic en el gobierno de la República de Colombia, 2014.

[4] LEIVA, Alfredo (2015). "Estrategias Nacionales de Ciberseguridad: Estudio Comparativo Basado en Enfoque Top-Down desde una Visión Global a una Visión Local", Revista Latinoamericana de Ingeniería de Software, 3(4), p. 161-176. 4 Para mayor información, ver: https://www.alianzaciberseguridad.cl/

para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética.[5]

Dentro de sus antecedentes normativos en Colombia, se encuentra la Ley N° 527 de 1999, por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y de dictan otras disposiciones.

El más reciente trabajo sobre Ciberseguridad, se realizó en Bogotá en el 2014, y es la Agenda estratégica de Innovación-Ciberseguridad, preparado por el Ministerio de la Tecnología y de la Información de la República de Colombia la cual trata de los vectores de Desarrollo, los cuales son los siguientes:

- Principios rectores de Ciberseguridad
- Educación, Formación y Divulgación de Ciberseguridad.
- Gestión Integrada de riesgos e incidentes de naturaleza cibernética
- Identificación, autentificación y autorización
- Aseguramiento de aplicaciones y ambientes móviles en el Gobierno
- Tecnologías de la Información y las Comunicaciones para el Sector Defensa.

- **Chile**.- Existe la "Alianza Chile de Ciberseguridad", la cual fue fundada por nueve instituciones que representan importantes sectores del país, a través de organismos estatales, privados y de la academia. Esta tiene por objetivo cooperar con las autoridades en esta materia, generar nuevas redes de contacto y alianzas internacionales.

  Para Michelle Bachelet Jería, ex Presidente de la República de Chile, una Política de Ciberseguridad está acompañada de las tecnologías de la información y la Comunicación (TIC), como una herramienta sin parangón en la historia de las personas, para las interacciones institucionales, los trámites, las operaciones económicas y las comunicaciones privadas y públicas.

  Las TIC en chile han tenido un impacto social si precedentes, permitiendo, entre otros usos, que las ciudadanos y ciudadanas se informen, organicen y participen a través de internet y particularmente en niños, y adolescentes permitiendo que realicen el uso intensivo de las denominadas redes sociales.

  Chile, con miras al año 2022 trabajó la Política de Ciberseguridad, con lineamientos que le permitan alcanzar el objetivo de contar con un ciberespacio libre, abierto, seguro y resiliente, sobre todo por la necesidad de contar con políticas de gestión y minimización de riesgos y amenazas, especialmente en los relativos en la infraestructuras críticas de la información, considerando reglas especiales para la adquisición y operación de soluciones tecnológicas que toman en cuenta el contexto internacional existente en materia de ciberseguridad.

  Decreto Supremo N° 533/2015 – Chile, cuyo objetivo principal es definir una Política Nacional de Ciberseguridad y órgano asesor de Gobierno.

[5] https://www.mintic.gov.co/portal/604/w3-article-6120.html

- **México**.- Tiene una Estrategia Nacional de Ciberseguridad, el cual es un documento que establece la visión del Estado Mexicano en la materia, a partir del reconocimiento de:

  - La importancia de las Tecnologías de la información y comunicación (TIC) como un factor de desarrollo político, social y económico de México; en el entendido de que cada vez más individuos están conectados a Internet y que tanto organizaciones privadas como públicas desarrollan sus actividades en el ciberespacio.

  - Los Riesgos asociados al uso de las tecnologías y el creciente número de ciberdelitos.

  - La necesidad de una cultura general de Ciberdefensa.

Diversos Países han desarrollado estrategias de ciberseguridad con sus propias circunstancias y particularidades, en razón de su capacidad económica, social y Política. Algunas de las estrategias ya están en una etapa de madurez y se encuentran en su segunda o tercera versión, con varios años de implementación y experiencia, con instituciones consolidadas y recursos dedicados al tema. Otros Países llevan pocos años, o incluso meses, de haber publicado su estrategia de Ciberseguridad. Los diferentes grados de avance de los Países y sus estrategias de Ciberseguridad dejan en claro la necesidad e importancia de impactar positivamente a los individuos, organizaciones privadas, academia e instituciones de gobierno con acciones concretas en ciberseguridad. De todo esto se aprecia la existencia de una creciente voluntad de los Estados por adoptar medidas que garanticen la seguridad del ciberespacio.

En ocasiones, tal como las señaladas, es el Gobierno, a través de estrategias nacionales, el encargado de centralizar los esfuerzos y adoptar acciones para alcanzar dicho objetivo.

6.3. Normativa Nacional:

- **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 la amenazas contra su seguridad y promover el bienestar general que se fundamenta en la justicia contra su seguridad, y promover el bienestar general que se fundamenta en la Justicia y en el Desarrollo Integral y equilibrado de la Nación.

- **Ley N° 27269,** Ley de Firmas y Certificados Digitales (26/05/2000)

  Regula la utilización de la firma electrónica otorgándole la misma validez y eficacia jurídica que el uso de la una firma manuscrita u otra análoga que conlleve la manifestación de voluntad.

- **Ley N° 27291,** Ley que modifica el código civil permitiendo la utilización de los medios electrónicos para la comunicación de la manifestación de voluntad y la utilización de la firma electrónica (23/06/2000).

- **Ley N°27309,** Ley que Incorpora los Delitos Informáticos al Código Penal

- **Ley N° 28493,** Ley que regula el uso del correo electrónico comercial no solicitado (spam) (18/03/2005).

  Regula el envío de comunicaciones comerciales publicitarias o promocionales no solicitadas, realizadas por correo electrónico, sin perjuicio de la aplicación de las disposiciones vigentes en materia comercial sobre publicidad y protección al consumidor.

- **Ley N° 28530,** Ley de promoción de acceso a internet para personas con discapacidad y de adecuación del espacio físico en cabinas públicas de internet (29/04/2005).

  Declaración de interés social de la promoción de acceso al uso de internet y de las tecnologías de la información a las personas con discapacidad y la progresiva eliminación de las barreras físicas y tecnologías que les impida su integración a la Sociedad de la información y su reinserción al mercado laboral.

- **Ley N° 29733,** Ley de Protección de Datos Personales (2/07/2011)
  Garantiza el derecho fundamental a la protección de los datos personales, previsto en el artículo 2 numeral 6 de la Constitución Política del Perú, a través de su adecuado tratamiento, en un marco de respeto de los derechos fundamentales que en ella se reconocen.

- **Ley N° 29904,** "Ley de Promoción de la Banda Ancha y Construcción de la Red Dorsal Nacional de Fibra Óptima (28/07/2012)

  Impulsa el desarrollo, utilización y masificación de la Banda Ancha en todo el territorio nacional, tanto en la oferta como en la demanda por este servicio, promoviendo el despliegue de infraestructura, servicios, contenidos, aplicaciones y habilidades digitales, como medio que favorece y facilita la inclusión social, el desarrollo socioeconómico, la competitividad, la seguridad del País y la transformación organizacional hacia una sociedad de la información y el conocimiento.

- **Ley 30096,** Ley de Delitos Informáticos (21/10/2013)

  Cuyo objeto es prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utiliación de tecnologías de la infromación o de la comunicación, con la fianlidad de garantizar la lucha eficaz contra la Ciberdelincuencia.

- **Ley N° 30618,** Ley que modifica el Decreo Legislativo 1141, Decreto Legislativo de Fortalecimiento y Modernización del Sistema de Inteligencia Nacional – SINA y de la Direccón Nacional de Inteligencia – DINI, a fin de regular la Seguridad Digital.

- **Decreto Legislativo 1141,** Decreto Legislativo de Fortalecimiento y Moderización del Sistema de Inteligencia Nacional-SINA y de la Dirección Nacional de Inteligencia – DINI (10/12/2012).

  El cual establece el marco jurídico que regula la finalidad, principios, organización, atribuciones, funciones, coordinación, control y fiscalización, que deben observar los compnentes del Sistema de Inteligencia Nacional – SINA y los que señala la norma.

- **Decreto Legislativo N° 1353,** Decreto Legislativo que crea la autoridad nacional de transparencia y acceso a la información pública, fortalece el régimen de protección de datos personales y la regulación de la Gestión de Intereses (06/01/2017).

  Crea la Autoidad Nacional de Transparencia y Acceso a la Información Pública, fortalecer el Régimen de Protección de Datos Personales y la regulación de la Gestión de intereses.

- **Decreto Legislativo 1412 "Ley de Gobierno Digital"**

  Artículo 2.- Ámbito de aplicación.
  2.1. La presente Ley es de aplicación a toda entidad que forma parte de la Administración Pública a que se refiere el artículo I del Título Preliminar del Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General. Sus regulaciones también alcanzan a las personas jurídicas o naturales que, por mandato legal, encargo o relación contractual ejercen potestades administrativas, y por tanto su accionar se encuentra sujeto a normas de derecho público, en los términos dispuestos por la Presidencia del Consejo de Ministros."

  Si bien es cierto que seguridad de la información no abarca seguridad digital (o ciberseguridad) debemos entender que los esfuerzos regulatorios han ido en la construcción de instrumentos para lo antes indicado, como ha sido Resolución Ministerial N° 360-2009-PCM que crea el Grupo de Trabajo denominado Coordinadora de Respuestas a Emergencias en Redes Teleinformáticas de la Administración Pública del Perú (Pe-CERT), pero que requiere de una institucionalización ante las diversas amenazas que enfrentan los entornos digitales.

- **Decreto Supremo N° 012-2017-DE**:

  Se aprobó la Política de Seguridad y Defensa Nacional, reseñándose como parte dei Diagnóstico del Problema, en relación a la Infraestructura para enfrentar ataques a los sistemas de información: Ciberseguridad que los esfuerzos aislados y la falta de reconocimiento del problema público debilitan la defensa sincronizada a nivel público-privado. Además. la carencia de tecnologías de última generación y la ausencia de un ente rector especializado agravan esta situación; a pesar de los esfuerzos realizados por la Secretaría de Gobierno Digital y el Sistema de

Coordinación de Emergencias en Redes Teleinformáticas de la Presidencia del Consejo de Ministros - PECERT. Por otro lado, se precisa que, habiéndose alcanzado un elevado nivel de informatización a nivel nacional, concordante con la tendencia global, se impulsará la creación de un Sistema Nacional de Cibersequridad, con la participación del sector privado y la sociedad en su conjunto, que promuevan la formación de especialistas para la defensa del ciberespacio.

- **Decreto Supremo N° 050-2018-PCM**

  En éste Decreto Supremo se desarrolla una definición de Seguridad Digital que debe colocarse en rango de ley para tener la dimensión completa, que aprueba la definición de Seguridad Digital en el Ámbito Nacional, pero que tiene alcance solo para el sector gubernamental, tal como lo indica el artículo 3 de dicho Decreto Supremo:

  Artículo 2.- Definición de Seguridad Digital en el ámbito nacional
  La Seguridad Digital en el ámbito nacional es el estado de confianza en el entorno digital que resulta de la gestión y aplicación de un conjunto de medidas proactivas y reactivas frente a los riesgos que afectan la seguridad de las personas, la prosperidad económica y social, la seguridad nacional y los objetivos nacionales en dicho entorno. Se sustenta en la articulación con actores del sector público, sector privado y otros quienes apoyan en la implementación de controles, acciones y medidas; debiéndose tener presente para estos efectos los aspectos siguientes:

  [...]

  Artículo 3.- Alcance
  "El presente Decreto Supremo es de alcance obligatorio a todas las entidades de la Administración Pública comprendidas en el Artículo I del Título Preliminar del Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo N° 006-2017-JUS."

- **Decreto Supremo N° 081-2013-PCM,** Decreto Supremo mediante el cual se aprueba la Política Nacional de Gobierno Electrónico 2013-2017.

  Prevé determinados lineamientos estratégicos para el Gobierno Electrónico en el Perú, entre otros, el relacionado con la Seguridad de la Información, el mismo que enfatiza la necesidad de velar por la integridad, seguridad y disponibilidad de los datos, así como definir lineamientos en seguridad de la información para mitigar el riesgo de exposición de información sensible del ciudadano,

- **Decreto Supremo N° 065-2015-PCM**, Que crea la Comisión Multisectorial Permanente encargada del Seguimiento y evaluación del "Plan de Desarrollo de la Sociedad de la Información en el Perú-La Agenda Digital Peruana 2.0-CODESI.

  Crea ésta comisión para el seguimiento y la evaluación del "Plan de Desarrollo de la Sociedad de la Información en el Perú - La Agenda Digital Peruana.

- **Resolución Ministerial N°246-2007-PCM,** que aprueba la Norma Técnica Peruana

  "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información: Código de buenas prácticas para la gestión de la seguridad de la información, en todas las entidades integrantes del Sistema Nacional de Informática, o la que haga sus veces.

- **Resolución Ministerial 004-2016-PCM**, que aprueba el uso obligatorio de la Norma Técnica Peruano "ISO NTP/IEC 27001:2014, Tecnología de la Información, Técnicas de Seguridad, Sistemas de Gestión de Seguridad de la Información, requisitos 2 edición "En todas las entidades integrantes del Sistema Nacional de Informática, o la que haga sus veces).

- **Resolución Ministerial N° 166-2016-PCM,** que modifica el artículo 5 de la R.M N° 004-2016-PCM referente al Comité de Gestión de Seguridad de la Información.

- **Resolución Ministerio N° 033-2018-PCM,** el artículo 8 del Decreto Supremo N° 033-2018-PCM, Decreto Supremo que crea la Plataforma Digital Única del Estado Peruano y establecen disposiciones adicionales para el desarrollo det Gobierno Digital, precisa que la Presidencia del Consejo de Ministros, a través de la SEGDI, es el Líder Nacional de Gobierno Digital encargado de dirigir, evaluar y supervisar el proceso de transformación digital y dirección estratégica del Gobierno Digital, para lo cual dirige, evalúa y supervisa el proceso de transformación digital y dirección estratégica del Gobierno Digital, para to cual en el ejercicio de sus funciones articula acciones con los diferentes entes y niveles de la administración pública integrantes del Sistema Nacional de Informática y otros interesados.

- **Convenio Sobre la Ciberdelincuencia de Budapest:**

  Éste convenio es un mecanismo de cooperación entre los Estados miembros del Consejo de Europa y las demás economías firmantes o suscriptoras, que tiene como finalidad proteger a la sociedad frente a la "ciberdelincuencia", particularmente mediante la adopción de una legislación adecuada y la mejora de la cooperación internacional.

  Asimismo, constituye una respuesta ante los riesgos que emergen con el uso de las tecnologías digitales, poniendo énfasis en la prevención de actos que afecten la confidencialidad, la integridad y la disponibilidad de los sistemas, redes y datos informáticos; así como la piratería, la pornografía infantil, la violación de la propiedad intelectual, entre otros.

  En esa línea, la Presidencia del Consejo de Ministros (PCM), a través de la Secretaría de Gobierno Digital, en el marco de la rectoría en materia digital en el país, viene desplegando una serie de acciones estratégicas a fin de fortalecer la seguridad digital en nuestro país.

  La incorporación del Perú al Convenio de Budapest constituye un notable avance hacia el desarrollo de una economía digital donde se promueva el bienestar social, la productividad territorial, la competitividad y el desarrollo económico en un ambiente de confianza digital para las empresas y todos nuestros ciudadanos.

La suscripción del referido Convenio permitirá fortalecer los esfuerzos que ha venido desplegando el Estado en materia de seguridad digital habilitando la posibilidad de establecer consecuencias penales para los ciberdelincuentes, permitiendo el despliegue de acciones contra la pornografía infantil, la piratería y la violación de la propiedad intelectual. De igual manera, permitirá recibir capacitación técnica internacional en materia de seguridad digital para fortalecer las competencias de los profesionales peruanos en todos los niveles.

Cabe recordar, que a la fecha el Convenido de Budapest ha sido ratificado por 61 estados, destacándose que la mayoría son europeos y de américa del Norte. Por otro lado, en la región son miembros del Tratado: Argentina, Chile, Costa Rica, Paraguay, República Dominicana, Colombia, Panamá y Perú.

El Congreso de la República del Perú ha aprobado la adhesión del Perú al **Convenio de Cibercrimen, también conocido como Convenio de Budapest**, pero requiere de un instrumento de coordinación y enlace para el despliegue de dicho convenio, siendo necesario contar con una normativa para el tema de Ciberseguridad que abarque los temas de Cibercrimen y ayude a desarrollar los instrumentos para combatir el cibercrimen, así como sirva de enlace al despliegue de normativa sobre Ciberdefensa.

Esta adhesión al Convenio de Cibercrimen requiere asimismo el desarrollo de capacidades en los diversos actores involucrados en el cumplimiento normativo, así como el desarrollo de instrumentos para la persecución del delito, y la protección de los activos críticos que puedan verse afectados por dichas acciones.

El Sector Gubernamental ha desarrollado diversas normativas para implementar de instrumentos para la seguridad de la información, de esta manera la Resolución Ministerial 004-2016-PCM, aprueba el uso obligatorio de la NTP ISO/IEC 27001:2014 en todas las entidades integrantes del Sistema Nacional de Informática.

6.4. Importancia de Ciberseguridad:

De los temas recurrentes en diversos estudios en materia de competitividad los temas de ciberseguridad resultan redundantes, como el Ranking de Competitividad Digital Mundial[6] donde la principal debilidad es la ciiberseguridad.

Informe Ciberseguridad: ¿Estamos preparados en América Latina y el Caribe? elaborado por la OEA[7] que indica con respecto al Perú:

"Con más de 12 millones de usuarios de Internet (el 40% de la población del país), Perú es un eje regional de actividad y comercio digital y en consecuencia, con riesgos a la seguridad cibernética27. Los datos muestran que los incidentes cibernéticos aumentaron un 30% en 2013 y el país experimentó también un incremento de los ataques de malware durante la Copa Mundial de 2014, que se celebró en Brasil. Afortunadamente el

[6] https://andina.pe/agencia/noticia-real-madrid-pierde-31-pero-se-clasifica-para-semifinales-de-champions-706238.aspx/portal.andina.com.pe/edpespeciales/2017/ciberseguridad/www.digesa.sld.pe/noticia-peru-sube-dos-posiciones-ranking-competitividad-digital-mundial-2018-713847.aspx

[7] https://publications.iadb.org/es/publicacion/17071/ciberseguridad-estamos-preparados-en-america-latina-y-el-caribe

Equipo de Respuesta a Incidentes de Seguridad Informática del Perú, PeceRT, respondió con éxito a estos ataques¨.

Además de la respuesta a incidentes, el PeCERT también analiza los asuntos de seguridad con la policía, las fuerzas militares y el sector privado, y está actualizando y ampliando sus capacidades. El Gobierno de Perú ha solicitado la asistencia técnica de la OEA para desarrollar un marco de seguridad cibernética para el país, para lo cual la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) ha asumido la responsabilidad. Mientras que la conciencia de las partes interesadas ha aumentado con gestiones recientes, la ausencia de una estrategia y una cadena de mando clara continúan impidiendo el fortalecimiento de la seguridad cibernética del país. Las fuerzas armadas también tienen un nivel básico de capacidad de defensa cibernética, pero no existe una política de defensa cibernética.

Tres piezas clave de legislación guían el marco legal para la seguridad cibernética del Perú: la Ley 27309, que incluyó la delincuencia cibernética en el código penal; la Ley

29733 de Protección de Datos; y la Ley 30096, que estableció normas jurídicas relacionadas con la delincuencia cibernética. La División de Investigación de Delitos de Alta Tecnología (DIVINDAT) de la Policía Nacional del Perú (PNP) es la unidad máxima para el manejo de la delincuencia cibernética de esta nación. Equipada con capacidad de laboratorio forense, la DIVINDAT descubrió una serie de recientes ataques cibernéticos dirigidos contra instituciones gubernamentales de alto nivel. Entre los constantes desafíos que se enfrentan, cabe citar su limitada capacidad técnica para el manejo de evidencia electrónica en los tribunales y la falta de una política de divulgación para el sector privado.

El sector privado y los operadores de infraestructura crítica nacional han adoptado algunas normas de seguridad, incluyendo procesos de desarrollo de software. proporcionando directrices sobre la gestión de crisis; sin embargo, el alcance de denuncia responsable sigue siendo bajo, ya que las tecnologías de seguridad y la Infraestructura Crítica Nacional son gestionadas de manera informal.
Las entidades peruanas están discutiendo la posibilidad de contar con un seguro de delincuencia cibernética y otros mecanismos para protegerse mejor.

Mientras que los servicios de gobierno electrónico y comercio electrónico continúan expandiéndose en el Perú, la conciencia social de la seguridad cibernética es generalmente baja.

6.5. ¿Cómo estamos en Ciberseguridad?

En el 2016 el BID hizo un informe sobre Ciberseguridad en Latinoamérica, basado en el modelo de madurez desarrollado por Centro de Global de Capacidad sobre Seguridad Cibernética (Oxford) que utiliza 49 indicadores. Este estudio concluye que muchos países de la región son vulnerables a ataques cibernéticos potencialmente devastadores.

- Según el BID, en general, el promedio de los Países Sudamericanos es relativamente bajo.

- En Perú llego a 1.8, superado por Uruguar, Argentina, Brasil, Chile y Colombia.
- En el año 2017 la UIT ha publicado el índice de ciberseguridad Global
- El índice tiene un mínimo de cero y un máximo de 1
- Según este indicador, Perú está en la posición 78 de 193 Países, inclusiva debajo de Ecuador.

6.6. Avances Tecnológicos:

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 de 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".

6.7. Acciones de la Secretaría de Gobierno Digital:

La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, plantea el objetivo de proteger la infraestructura, los datos e información del Estado y la tecnología utilizada para procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

Asegurar la implementación de las propuestas legislativas, y en general la normatividad relacionada con la seguridad de la información o ciberseguridad comprendida en esta Política, identificando los recursos involucrados y las partidas presupuestales correspondientes.

Para ello consideran importante mantener la Política Nacional de Ciberseguridad actualizada, a efectos de asegurar su vigencia y por ende su eficacia, promoviendo la participación de las entidades del sector público y privado, así como representantes de la sociedad civil y la academia.

- Fortalecer las capacidades para enfrentar las amenazas que atentan contra su seguridad y defensa en el de la ciberseguridad, creando un entorno y las condiciones necesarias que permitan brindar protección en el ciberespacio.

- Brindar Capacitación especializada en seguridad de la información y ampliar las líneas de investigación en materia de ciberseguridad dentro de la Administración Pública.

– Desarrollar un Plan de sensibilización y capacitación a todos los ciudadanos respecto a la Ciberseguridad.

– Fortalecer la legislación en materia de ciberseguridad, la cooperación internacional y propiciar la adhesión del Perú a los diferentes organismos internacionales en esta temática.

– Afianzar la integración y coordinación eficaz, entre los diversas coordinadoras de Respuestas a Emergencias en redes Teleinformáticas de la Administración Pública y el Sector Privado.

– Elaborar un Plan de Acción Nacional en Ciberseguridad.

– Crear un comité nacional de Ciberseguridad.

6.8. Agenda de Competitividad 2014-2018 – Ministerio de Economía y Finanzas:

– **65 metas en 8 líneas estratégicas:**

- Desarrollo Productivo y Empresarial
- Ciencia, Tecnología e Innovación
- Internacionalización
- Infraestructura logística y de transportes
- Tecnologías de la Información y Comunicaciones
- Capital Human
- Facilitación de Negocios
- Recursos Naturales y Energía

6.9. Acciones del Viceministerio de Comunicaciones hacia un Perú Digital – MTC.

Cuyos objetivos son:

– Presentar la problemática de la Ciberseguridad en el Perú
– Estrategias y propuestas que buscan resolver esa problemática.

Riesgo de la Transformación Digital:

– La Transformación digital involucra una mayor penetración de la Internet y mejor interconexión de las personas.
– Se incrementará el uso de nuevas tecnologías que usarán información vital para servicios críticos y sensibles.
– Habrá un incremento del delito y abuso informático
– La Ciberseguridad se convierte en un asunto clave y la transversal a la sociedad de la información.

Planificación ¿Qué se puede hacer?

- Elaborar y documentar política y un plan de ciberseguridad alineados a los objetivos nacionales.
- Desarrollar una gestión de la Defensa Cibernética con una estructura de mando clara.
- Preparar instructores nacionales en ciberseguridad, dotar de un presupuesto para la educación e investigación en este rubro.
- Promover la divulgación responsable de la información de vulnerabilidades
- Aplicación de normas relacionadas a ciberseguridad en los reglamentos de adquisiciones de equipos y software.
- Implantar un centro de mando y control de ciberseguridad para los estamentos públicos y privados.
- Planificar coordinadamente las respuestas y ataques a los activos críticos
- Desarrollar diálogos formales entre el sector público y privado para la protección de la infraestructura crítica nacional.
- Desarrollar conciencia de los operadores respecto a las amenazas a la ICN.
- Promover la aplicación de la gestión de riesgos en las prácticas empresariales para la protección de datos en todos los niveles.
- Planificar medidas de redundancia digital de la ICN.
- Evaluar Protocolos y procedimientos para la gestión de crisis respecto a la ICN.
- Desarrollar un mercado de seguros contra la delincuencia cibernética.

6.10. Mesas de Trabajo y Conversatorios sobre Ciberseguridad:

La Comisión de Defensa Nacional, Orden Interno, Desarrollo Alternativo y lucha contra las Drogas, presidida por el Congresista Jorge Del Castillo Gálvez en la Legislatura 2018-2019, realizó 9 mesas de trabajo "Sobre la necesidad de legislar respecto a Ciberdefensa, Ciberseguridad, Ciberdelincuencia y Ciberespacio, en concordancia con el Convenio sobre la Ciberdelincuencia Budapest y la normativa vigente".

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 trabajándose el Proyecto de Ley sobre Ciberseguridad, contando con los siguientes expertos:

- **Universidades:**

  - Representante Universidad ESAN – Dirección del Diplomado de Ciberseguridad.
  - Jefe de la Oficina de Proyectos Master Business Administration MBA –ESAN
  - Director de la Carrera de Ingeniería Electrónica – UPC
  - Director de Programas de Gestión Pública – UTEC
  - Director de Capacitación y Transferencia Tecnológica – UNI
  - Director de Investigación y Desarrollo Tecnológico – UNI
  - Decano de la Facultad de Ingeniera y Sistemas – SAN MARCOS

- Decano de la Facultad de Ingeniería Industrial y Sistemas – FEDERICO VILLAREAL
- Representante de la Universidad La Salle

➢ **Ministerios y otras Instituciones Públicas:**

- Ministerio de Defensa (FOVIMFAP, FOVIMAR, FOVIME)
- Ministerio de Economía y Finanzas
- Ministerio de Relaciones Exteriores
- Ministerio de la Producción
- Ministerio de Trabajo y Promoción del Empleo

➢ **Sociedad Civil:**

- Asociación de Usuarios Elegir
- Secretaría Ejecutiva Adjunta de la Coordinadora Nacional de Derechos Humanos
- Instituto para la Sociedad de la Información – IPSI
- Representante de Democracia Digital
- Suma Ciudadana
- Red Científica Peruana
- Abogada del Equipo Legal de Microsoft
- Director Comercial de Optical Network
- Gerente Comercial IBM
- Superintendente Adjunto de Riesgos SBS
- Intendente de Supervisión de Sistemas de Información Tecnológica SBS
- Gerente Central de Navegación – CORPAC
- Gerente de Tecnología de la Información – CORPAC
- Representante de Terminales Portuarios Euroandinos S.A
- Representante de la Autoridad Portuaria Nacional
- Representante de la Red Científica Peruana
- Representante de ENTEL

➢ **La Comisión realizó una conferencia sobre Ciberseguridad para estudiantes universitarios.**
24/04/2019
Auditorio CCORIWASI de la Universidad Ricardo Palma

- Universidad de Lima
- Universidad Ricardo Palma
- Pontificia Universidad Católica del Perú – PUCP
- Universidad San Martín de Porres

➢ **La Comisión también la conferencia "Ciberdefensa, Ciberseguridad y Ciberespacio en el marco de la Implementación del Convenio de Budapest", que contó con la presencia de Representantes de :**

- Ministerio de Defensa
- Ministerio de la Producción
- Ministerio de Transportes y Comunicaciones
- Ministerio de Trabajo y Promoción del Empleo
- Ministerio de Relaciones Exteriores
- OSITRAN
- Oficina Nacional de Procesos Electorales - ONNPE
- Bolsa de Valores de Lima
- BBVA Continental
- Entel

Posterior a la realización de las conferencias con universitarios, Instituciones Públicas, Privadas y Sociedad civil, además de todas las mesas de Trabajo con el con el apoyo
de expertos, se vino realizando sesión por sesión un borrador de Proyecto de Ley con las ideas y aportes de todos los participantes en las que se concluyó lo siguiente:

- Existe la necesidad de legislar en materia de Seguridad Digital del Estado Peruano.
- La iniciativa legislativa deberá involucrar a todas las entidades del Sector Público, debiendo tener alcances al privado, academia y sociedad civil.
- Deberá establecer en el marco normativo la Ciberseguridad en el ámbito privado, con lineamientos para el establecimiento de CSIRTS, y deberá existir una cooperación para el mantenimiento de la Ciberseguridad en el Estado Peruano.
- Deberá fomentarse el Desarrollo del Currículo de Educación en materia de Ciberseguridad.
- Deberá existir un Fondo de Seguridad Digital que recoja los aportes provenientes de las entidades públicas y privadas, para que exista una buena cooperación interinstitucional que fomente la investigación, cooperación e innovación en materia de Seguridad Digital.
- Se deberá fomentar la Cultura de Ciberseguridad
- Deberá haber modificaciones complementarias al Decreto Legislativo 1141, de fortalecimiento y modernización del Sistema de Inteligencia Nacional SINA y de la Dirección Nacional de Inteligencia DINI.

6.11. Recomendaciones de la Comisión:

Posterior al análisis de las dos iniciativas legislativas materia de estudio, y de los aportes recogidos en las diferentes mesas de Trabajo impulsados por ésta Comisión, concluimos lo siguiente:

- La Comisión considera que resulta de vital importancia reforzar el trabajo que viene realizando el Estado en materia de seguridad digital y seguridad de la información, con el objeto de mitigar el riesgo de exposición de información sensible del ciudadano que pueda ser objeto de atentados contra su propia seguridad personal y de la comunidad

- Consideramos que resulta positiva y viable el incluir al sector privado, a la sociedad civil, a la academia y otros, lo cual refuerza y contribuye a la Seguridad Cibernética y recomienda la adición de un artículo vinculado al régimen sancionador en caso de incumplimiento de las disposiciones contenidas en el proyecto normativo y en la reglamentación a emitir.

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 presentes iniciativas legislativas deben ser analizadas no desde el tradicional costo-beneficio, sino se debe utilizar un análisis costo-eficiencia, considerando que la propuesta legislativa ordena nuestro ordenamiento administrativo, haciéndolo más idóneo, necesario y ponderado respecto a la Ciberseguridad o seguridad informática, además de ordenar la situación que puedan presentarse dentro de las acciones y/o contingencias que tengan que ver con la materia y de esa manera coberturar en su mayoría las situaciones a presentarse.

BENEFICIOS /ACTOR	POSITIVO	NINGUNO
ESTADO PERUANO	Contará con una estrategia de Ciberseguridad y un Plan Multianual que abrirá nuestra visión de un Gobierno digital moderno y seguro	-
ADMINISTRADOS	Verán resguardados sus derechos fundamentales y estar seguros durante su estadía en internet, generando confianza en usuarios cibernéticos	-
DEMÁS ESTADOS	Podrán contar con la cooperación internacional para colaboración en la implementación de la Ciberseguridad y la lucha contra el Ciberdelito.	-

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** de los **Proyectos de Ley N° 4237/2018-CR Y 4352/2018-CR "LEY DE CIBERSEGURIDAD"**

FÓRMULA LEGAL CON TEXTO SUSTITUTORIO "LEY DE CIBERSEGURIDAD"

TÍTULO I
DISPOSICIONES GENERALES

Artículo 1.- Objeto
La presente ley tiene por objeto establecer el marco normativo en materia de Seguridad Digital del Estado Peruano.

Artículo 2.- Ámbito de Aplicación
La presente ley tiene alcance a todas las entidades del sector público de los niveles de gobierno. De igual manera tiene alcance sobre entidades del sector privado, academia y sociedad civil en lo que le aplique la presente ley.

Artículo 3.- Definición

3.1 CSIRT. - Se define un CSIRT (Equipo de Respuesta frente a Incidentes de Seguridad Informática) como un colectivo o una entidad dentro de un organismo que ofrece servicios y soporte a un grupo en particular (comunidad objetivo) con la finalidad de prevenir, gestionar y responder a incidentes de seguridad digital. Estos equipos deben estar conformados por especialistas multidisciplinarios que actúan según procedimientos y políticas predefinidas, de manera que respondan, en forma rápida y efectiva, a incidentes de seguridad, además de coadyuvar a mitigar el riesgo de los ataques cibernéticos.

3.2 Seguridad Digital. - Es el estado de confianza en el entorno digital que resulta de la gestión y aplicación de un conjunto de medidas proactivas y reactivas frente a los riesgos que afectan la seguridad de las personas, la prosperidad económica y social, la seguridad nacional y los objetivos nacionales en dicho entorno. Se sustenta en la articulación con actores del sector público, sector privado y otros quienes apoyan en la implementación de controles, acciones y medidas.

Artículo 4. Principios de la Ciberseguridad

4.1 Respeto de los Derechos Humanos en el ejercicio de la Ciberseguridad Se deberán tomar en consideración en todo desarrollo normativo y de políticas en materia de Ciberseguridad el respeto irrestricto a los Derechos Humanos, en concordancia con la Constitución Política del Perú y los Acuerdos Internacionales en la materia.

4.2 Comunicación de Incidentes

Se deberá crear mecanismos de comunicación de incidentes entre la sociedad civil, el sector privado, la academia, la comunidad técnica y el sector gubernamental. Dichos mecanismos de comunicación de incidentes deberán mantener la reserva de los casos indicados, en los casos que pudiera su revelación afectar a las instituciones o a la sociedad, pero también deberá evaluarse los casos para divulgar dicha información a otros actores y a la sociedad. Tanto el compartimentaje como la diseminación de la información a los organismos pertinentes no debe afectar la Defensa o la Seguridad Nacional.

En el caso que los incidentes impliquen violación a datos personales deberá informarse al funcionario público responsable de transparencia y acceso a la información pública y a la protección de datos personales, de dicha afectación.

De igual manera los incidentes deberán ser reportados antes las autoridades competentes de acuerdo a la naturaleza de la entidad vulnerada y de los individuos y entidades afectadas, para que respondan a dicha afectación en la medida de sus funciones.

TÍTULO II
DE LA CIBERSEGURIDAD

CAPÍTULO I
CIBERSEGURIDAD EN EL ÁMBITO DEL SECTOR PÚBLICO

Artículo 5. Comité de Ciberseguridad del Estado Peruano
Dispóngase la creación del Comité de Ciberseguridad del Estado Peruano, el mismo que deberá contar en su conformación con participación del sector privado, sociedad civil, academia, comunidad técnica de internet y sector gubernamental. Este Comité estará adscrito a la Presidencia del Consejo de Ministros y la Secretaría de Gobierno Digital será la secretaría técnica, quien coordinará con el secretario técnico del Consejo de Seguridad y Defensa Nacional (COSEDENA).
El Comité tendrá como función formular la Política de Ciberseguridad del Estado Peruano, generar lineamientos en materia de CSIRT en el sector privado, gestionar el Fondo de Seguridad Digital, fomentar la cultura de Ciberseguridad, coadyuvar al fomento de currículos de educación superior en materia de Ciberseguridad y otras que les pudiera establecer la COSEDENA.

La conformación del Comité de Ciberseguridad del Estado Peruano, será establecida en el reglamento de la presente ley.

Artículo 6.- Marco de Seguridad Digital del Sector Gubernamental
Los principios, modelos, políticas, normas, procesos, roles, tecnología y estándares mínimos que permitan preservar la confidencialidad, integridad, disponibilidad de la información en el entorno digital administrado por las entidades de la administración pública, serán establecidos por la Secretaría de Gobierno Digital.

Artículo 7. Establecimiento del Pe-CSIRT
Crease en el ámbito de la Secretaria de Gobierno Digital de la Presidencia del Consejo de Ministros, el CSIRT del Perú.
La Secretaría de Gobierno Digital establecerá los estándares mínimos que se deberá cumplir para participar en el CSIRT del Perú, por parte de cualquier entidad pública, privada, de la sociedad civil, la academia o de la comunidad técnica.

CAPÍTULO II
CIBERSEGURIDAD EN EL ÁMBITO DEL SECTOR PRIVADO

Artículo 8. Lineamientos para el establecimiento de CSIRTs en sector privado
El Comité de Ciberseguridad del Estado Peruano establecerá los lineamientos para el establecimiento de CSIRTs en el sector privado, la academia, la sociedad civil y la comunidad técnica. De igual manera fomentará el desarrollo de instrumentos de cooperación público-privado en materia de Ciberseguridad.

Artículo 9. Cooperación Público-Privada en materia de ciberseguridad
Las entidades públicas y privadas, así como de la academia, la sociedad civil y la comunidad técnica deberán tener como principio a la cooperación para el mantenimiento de la Ciberseguridad a nivel del Estado Peruano.

DISPOSICIONES COMPLEMENTARIAS MODIFICATORIAS

PRIMERA. - Modificación del numeral 8) del artículo 2 del Decreto Legislativo 1141, Decreto Legislativo de fortalecimiento y modernización del Sistema de Inteligencia Nacional - SINA y de la Dirección Nacional de Inteligencia – DINI.

Modifíquese el numeral 8) del artículo 2 del Decreto Legislativo 1141, Decreto Legislativo de fortalecimiento y modernización del Sistema de Inteligencia Nacional - SINA y de la Dirección Nacional de Inteligencia - DINI en los siguientes términos:

"Artículo 2.- Definiciones

Para los fines del presente Decreto Legislativo y de las actividades reguladas por el mismo, se entenderá por:
(...)
Seguridad Digital: **Es el estado de confianza en el entorno digital que resulta de la gestión y aplicación de un conjunto de medidas proactivas y reactivas frente a los riesgos que afectan la seguridad de las personas,**
la prosperidad económica y social, la seguridad nacional y los objetivos

nacionales en dicho entorno. Se sustenta en la articulación con actores del sector público, sector privado y otros quienes apoyan en la implementación de controles, acciones y medidas."

DISPOSICIONES COMPLEMENTARIAS FINALES

PRIMERA. - Reglamentación en materia de Ciberseguridad
La Presidencia del Consejo de Ministros mediante Decreto Supremo aprueba el reglamento de la presente ley, en lo referido a ciberseguridad, 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 la Policía Nacional del Perú en materia de ciberseguridad.
El Ministerio del Interior 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 Policía Nacional del Perú 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 seguridad digital debiendo mantener mecanismos de comunicación de incidentes que pudieran afectar la capacidad Seguridad Digital Nacional.

CUARTA. Desarrollo del currículo de educación superior en materia de ciberseguridad

El Ministerior del Interior, en su calidad de ente rector en materia de Seguridad Digital, coordina con el Ministerio de Educación, la pertinencia del desarrollo de contenidos especializados en materia de Seguridad Digital, que incluye la Ciberseguridad, 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. De la participación de los Organismos reguladores del Estado.

Para la conformación del Comité de Ciberseguridad del Estado peruano, propuesto en el artículo 5 de la presente ley, se deberá considerar la participación de los organismos reguladores de la Inversión Privada en los Servicios Públicos.

DISPOSICIÓN COMPLEMENTARIA DEROGATORIA

ÚNICA. - Derogatoria

Deróguese la **Segunda Disposición Complementaria Final de la Ley 30618, Ley que modifica el DL 1141, Decreto Legislativo de Fortalecimiento y Modernización del Sistema de Inteligencia Nacional - SINA y de la Dirección Nacional de Inteligencia – DINI.**

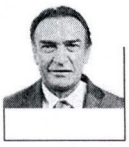
Salvo distinto parecer
Dése cuenta
Sala de Comisión
Lima, julio del 2019

	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**	

CONGRESO DE LA REPÚBLICA

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

DICTAMEN CON RECOMENDACIÓN DE APROBACIÓN, CON TEXTO SUSTITORIO RECAIDO EN LOS PROYECTOS DE LEY N° 4237/2018-CR Y 4352/2018-CR "LEY DE CIBERSEGURIDAD".

 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**	

CONGRESO DE LA REPÚBLICA

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

DICTAMEN CON RECOMENDACIÓN DE APROBACIÓN, CON TEXTO SUSTITORIO RECAIDO EN LOS PROYECTOS DE LEY N° 4237/2018-CR Y 4352/2018-CR "LEY DE CIBERSEGURIDAD".

	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**	

CONGRESO de la REPÚBLICA

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

DICTAMEN CON RECOMENDACIÓN DE APROBACIÓN, CON TEXTO SUSTITORIO RECAIDO EN LOS PROYECTOS DE LEY N° 4237/2018-CR Y 4352/2018-CR "LEY DE CIBERSEGURIDAD".

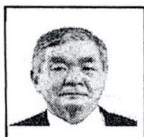
	Galarreta Velarde Luis Fernando Fuerza Popular	**Accesitario**	

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 Kambio	**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**	

CONGRESO
REPÚBLICA

RICHARD ARCE CÁCERES
Congresista de la República

"Año del Diálogo y la Reconciliación Nacional"

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,

CONGRESO DE LA REPÚBLICA
RICHARD ARCE CÁCERES

HERNÁN VIDALÓN SEVILLA
ASESOR I
DESPACHO DEL CONGRESISTA RICHARD ARCE

22/09/19
9:45.

Palacio Legislativo Plaza Bolívar s/n Of. 307 Lima
Teléfono 3117334
Correo rarce@congreso.gob.pe

35

CONGRESO
REPÚBLICA

Despacho Cong. Francisco Villavicencio C.

"Decenio de Igualdad de Oportunidades para mujeres y Hombres"
"Año de la Lucha contra la Corrupción y la Impunidad"

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 Republica **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/YAO

35

CONGRESO DE LA REPÚBLICA

ELARD MELGAR VALDÉZ
CONGRESISTA DE LA REPÚBLICA
"Decenio de la igualdad de oportunidades para mujeres y hombres"

Lima, 22 de julio 2019

Oficio Nº 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 22º literal i) del Reglamento del Congreso de la República.

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

Atentamente,

CONGRESO DE LA REPÚBLICA
ELARD MELGAR VALDEZ

Lic. LUIS HUMBERTO VILLA
Primer Asesor
del Congresista Elard Melgar Valdéz

CONGRESO DE LA REPÚBLICA
COMISIÓN DE DEFENSA NACIONAL, ORDEN INTERNO, DESARROLLO ALTERNATIVO Y LUCHA CONTRA LAS DROGAS
22 JUL 2019
RECIBIDO
Firma ____ Hora 9:37 am

Azángaro 468, Oficina 711
Teléfono: 311- 7355