CONGRESO DE LA REPÚBLICA
ÁREA DE TRÁMITE DOCUMENTARIO
17 MAY 2019
RECIBIDO
Firma ____ Hora 9:20

Proyecto de Ley N° 4352 / 2018-CR

# PROYECTO DE LEY DE CIBERSEGURIDAD

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

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

## PROYECTO DE LEY DE 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 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 y Ciberdefensa, coadyuvar al fomento de currículos de educación superior en materia de Ciberseguridad y Ciberdefensa, 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 – Política Nacional de Ciberseguridad**
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.

**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. - Fondo de Seguridad Digital**
Establézcase 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.

**QUINTA. Desarrollo del currículo de educación superior en materia de ciberseguridad**
El Ministerio de Educación fomentarán 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.

**SEXTA. Fomento de la Cultura de Ciberseguridad**
Alineados con las Políticas 9 y 35 del Acuerdo Nacional, el Comité de Ciberseguridad del Estado Peruano conjuntamente con todos los actores públicos y privados involucrados en temas de ciberseguridad deben fomentar la creación de una cultura de ciberseguridad desde los primeros años de la escuela y a nivel de todo nivel de educación, así como en los espacios profesionales y sociales, entendiendo que el desarrollo de una cultura de ciberseguridad permitirá desarrollar capacidades en esta materia.

## 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**

Lima, 16 de mayo del 2019

JORGE DEL CASTILLO GÁLVEZ
Congresista de la República

C. TUBINO

C. SEGURA

Paloma Noceda

MARCO E MIYASHIRO A

MULDER

VOCERO APA

Elías Rodríguez

LUIS FEDERICO

LLEÓN

F. VILLAVICENCIO

Luis Vigo García

QUIPAS

**CONGRESO DE LA REPÚBLICA**

**Lima, ...24.....de.....MAYO.....del 2019.....**

**Según la consulta realizada, de conformidad con el Artículo 77º del Reglamento del Congreso de la República: pase la Proposición Nº4352 para su estudio y dictamen, a la (s) Comisión (ès) de** DEFENSA NACIONAL, ORDEN INTERNO, DESARROLLO ALTERNATIVO Y LUCHA CONTRA LAS DROGAS; CIENCIA, INNOVACIÓN Y TECNOLOGÍA. -

GIANMARCO PAZ MENDOZA
Oficial Mayor
CONGRESO DE LA REPÚBLICA

## EXPOSICIÓN DE MOTIVOS

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

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."*

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

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

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

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

Asimismo, el Congreso de la República 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.

***¿Quiénes son los conformantes del sistema nacional de informática?,*** las podemos encontrar en el DL 604 y son:

- Las Oficinas Sectoriales de Informática y demás Oficinas de Informática de los Ministerios, de los Organismos Centrales, Instituciones Públicas Descentralizadas y Empresas del Estado
- Las Oficinas Sectoriales de Informática y demás Oficinas de Informática de los Ministerios, de los Organismos Centrales, Instituciones Públicas Descentralizadas y Empresas del Estado
- Los Órganos de Informática de las Municipalidades.
- Los Órganos de Informática de los Poderes Públicos y de los Organismos Autónomos

Pero la norma anterior no abarca al sector privado, la sociedad civil, la academia o la comunidad técnica, siendo que tampoco lo hace el Decreto Legislativo 1412, Ley de Gobierno Digital, que indica en su artículo 2:

"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.

En estos esfuerzos también se ha desarrollado una definición de Seguridad Digital que debe colocarse en rango de ley para tener la dimensión completa de lo expresado en el Decreto Supremo Nº 050-2018-PCM, 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 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."*

De los temas recurrentes en diversos estudios en materia de competitividad los temas de ciberseguridad resultan redundantes, como el Ranking de Competitividad Digital Mundial[1] donde la principal debilidad es la ciiberseguridad. En el mismo sentido es relevante lo expresado en el informe **Ciberseguridad: ¿Estamos preparados en América Latina y el Caribe?** elaborado por la OEA[2] 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 Equipo de Respuesta a Incidentes de Seguridad Informática del Perú, PeCERT, respondió con éxito a estos ataques.

---

[1] 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

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

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. La ONGEI también proporciona 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 (ICN) son gestionadas de manera informal. Las entidades peruanas están discutiendo la posibilidad de contar con un seguro de delincuencia cibernética y otros mecanismos para proteger mejor la ICN.

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. La ONGEI ofrece literatura en línea sobre este tema, pero no hay una amplia campaña de sensibilización que esté actualmente vigente. Muchas universidades nacionales y empresas privadas ofrecen educación y capacitación en seguridad cibernética. Sin embargo, suele carecerse de tecnología adecuada y personal educativo con experiencia"[3]

[3] OEA. Informe Ciberseguridad: ¿Estamos preparados en América Latina y el Caribe? https://publications.iadb.org/es/publicacion/17071/ciberseguridad-estamos-preparados-en-america-latina-y-el-caribe . 2016

## Política y estrategia

**Estrategia nacional de seguridad cibernética oficial o documentada**
- Desarrollo de la estrategia
- Organización
- Contenido

**Defensa cibernética**
- Estrategia
- Organización
- Coordinación

## Cultura y sociedad

**Mentalidad de seguridad cibernética**
- En el gobierno
- En el sector privado
- En la sociedad

**Conciencia de seguridad cibernética**
- Sensibilización

**Confianza en el uso de Internet**
- En los servicios en línea
- En el gobierno electrónico
- En el comercio electrónico

**Privacidad en línea**
- Normas de privacidad
- Privacidad del empleado

## Educación

**Disponibilidad nacional de la educación y formación cibernéticas**
- Educación
- Formación

**Desarrollo nacional de la educación de seguridad cibernética**
- Desarrollo nacional de la educación de seguridad cibernética

**Formación e iniciativas educativas públicas y privadas**
- Capacitación de empleados en seguridad cibernética

**Gobernanza corporativa, conocimiento y normas**
- Comprensión de la seguridad cibernética por parte de empresas privadas y estatales

## Marcos legales

**Marcos jurídicos de seguridad cibernética**
- Para la seguridad de las TIC
- Privacidad, protección de datos y otros derechos humanos
- Derecho sustantivo de delincuencia cibernética
- Derecho procesal de delincuencia cibernética

**Investigación jurídica**
- Cumplimiento de la ley
- La fiscalía
- Tribunales

**Divulgación responsable de la información**
- Divulgación responsable de la información

## Tecnologías

**Adhesión a las normas**
- Aplicación de las normas y prácticas mínimas aceptables
- Adquisiciones
- Desarrollo de softwre

**Organizaciones de coordinación de seguridad cibernética**
- Centro de mando y control
- Capacidad de respuesta a incidentes

**Respuesta a incidentes**
- Identificación y designación
- Organización
- Coordinación

**Resiliencia de la infraestructura nacional**
- Infraestructura tecnológica
- Resiliencia nacional

**Protección de la Infraestructura Crítica Nacional (ICN)**
- Identificación
- Organización
- Planeación de respuesta
- Coordinación
- Gestión de riesgos

**Gestión de crisis**
- Planeación
- Evaluación

**Redundancia digital**
- Planeación
- Organización

**Mercado de la ciberseguridad**
- Tecnologías de seguridad cibernética
- Seguros de delincuencia cibernética

OBSERVATORIO DE LA **CIBERSEGURIDAD** EN AMÉRICA LATINA Y EL CARIBE 95

Es en el marco de un diseño multiestamentario, el trabajo para el desarrollo del presente ante proyecto de Ley de Ciberseguridad y Ciberdefensa, la Comisión de Defensa Nacional, Orden Interno, Desarrollo Alternativo y Lucha Contra las Drogas, invito a mesas de trabajo con el Sector Publico, Sector Privado, Academia y las Fuerzas Armadas; con el fin de consensuar concepto y recoger experiencias y aportes de los diferentes participantes sobre Ciberdefensa.

## EFECTO DE LA NORMA EN LA LEGISLACIÓN NACIONAL

La presente iniciativa legislativa no altera la normatividad vigente, sino que establece un marco normativo en materia de Seguridad Digital del Estado Peruano.

## ANÁLISIS COSTO BENEFICIO

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