CONGRESO DE LA REPÚBLICA

CONGRESO DE LA REPÚBLICA
ÁREA DE TRAMITE DOCUMENTARIO
16 JUN 2017
RECIBIDO
Firma:..... Hora: 2:20

Dictamen

COMISIÓN DE INTELIGENCIA
Período Anual de Sesiones 2016-2017

Señor Presidente:

Han ingresado para dictamen a la Comisión de Inteligencia el **Proyecto de Ley 772-2016–CR** presentado por el Grupo Parlamentario Fuerza Popular, a iniciativa del congresista Marco Miyashiro Arashiro, el cual propone la Ley que modifica los artículos 2, 10, 17, 38 y La incorporación de la Octava Disposición Complementaria Final del Decreto Legislativo 1141, Decreto legislativo de fortalecimiento y modernización del Sistema de Inteligencia Nacional – SINA y de la Dirección Nacional de Inteligencia – DINI.

Luego del análisis y debate correspondiente, en su vigésima sesión ordinaria del 14 de junio de 2017, la Comisión de Inteligencia, por unanimidad acuerda aprobar el proyecto de ley materia de dictamen, con un texto sustitutorio.

I. SITUACIÓN PROCESAL DE LA PROPUESTA

a. Antecedentes

El Proyecto de Ley N° 772-2016–CR, ingresó a la oficina de trámite documentario el 14 de diciembre de 2017 y fue remitido a la Comisión de Inteligencia el 15 de diciembre de 2017 como única comisión dictaminadora.

De conformidad a lo dispuesto en el artículo 72 del Reglamento del Congreso de la República la iniciativa legislativa propone una ley ordinaria.

b. Opiniones recibidas

1. **De la Presidencia del Consejo de Ministros**, mediante oficio 2120-2016-PCM/SG/ de fecha 13 de junio de 2017, recibido por la Comisión de Inteligencia el 14 de junio de 2017, adjunta el Informe 748-2017-PCM-OAGJ, emitido por la Oficina General de Asesoría Jurídica memorando 606 2017-PCM/SGP el cual adjunta el Informe 018-2017-PCM-SGP/SSA-JFRP elaborado por la Sub Secretaría de Administración Pública, los cuales señalan la viabilidad del proyecto de ley y proponen recomendaciones.

   Señalan lo siguiente:

   Respecto a incorporar la "Seguridad Digital" en el desarrollo de las actividades del SINA:

   Respecto al Sistema de Defensa Nacional, la Constitución Política del Perú señala que:
   "Artículo 163.- El Estado garantiza la seguridad de la Nación mediante el Sistema de Defensa Nacional.

La Defensa Nacional ***es integral*** *y permanente. Se desarrolla en los ámbitos interno y externo. Toda persona, natural o jurídica, está obligada a participar en la Defensa Nacional, de conformidad con la ley".* (Énfasis agregado)

Sobre el particular, tal como lo afirma Marcial Rubio Correa cuando comenta el artículo 163 del texto constitucional: por "integral" debe entenderse el concepto *"que abarca a todas las personas, instituciones* ***y actividades de la sociedad****"*; mientras que por "permanente" *"debe entenderse que* ***siempre se hace defensa nacional*** *porque es la única garantía de seguridad que tiene propiamente eficiencia para los fines que persigue"*[1]. (Énfasis agregados)

En tal sentido, se puede afirmar que la Defensa Nacional, al ser integral, también debe incluir acciones relativas a la Seguridad Digital; máxime si tal *"los gobiernos, las empresas, otras organizaciones y los usuarios individuales dependen cada vez más de las tecnologías de la información para el suministro de bienes y servicios esenciales, la gestión de sus asuntos y el intercambio de información"*[2].

Observando dicha situación, mediante la Resolución RES/57/239 denominada *"Creación de una cultura mundial de seguridad cibernética"*, adoptada en su Quincuagésimo séptimo período de sesiones; la Organización de Estados Americanos (OEA), tomó nota de nueve elementos considerados por la Organización como necesarios, con miras a crear una cultura mundial de seguridad cibernética[3].

Uno de los elementos propuestos por la OEA es la evaluación de riesgos, señalando que:

"Evaluación de riesgos: Todos los participantes deben realizar evaluaciones periódicas de los riesgos a fin de determinar las amenazas y vulnerabilidades; esas evaluaciones deben tener una base suficientemente amplia para abarcar los principales factores internos y externos, tales como la tecnología, los factores físicos y humanos, las políticas y los servicios de terceros que tengan consecuencias para la seguridad; permitir la determinación del nivel de riesgo aceptable; y ayudar a la selección de controles apropiados para gestionar el riesgo de posibles daños a los sistemas y redes de información, teniendo en cuenta la naturaleza y la importancia de la información que se debe proteger" [4].

Asimismo, otro de los elementos propuestos por la OEA para la creación de una cultura mundial de seguridad cibernética es la Gestión de la Seguridad, que se configura de la siguiente manera:

"Gestión de la seguridad. Los participantes deben adoptar un enfoque amplio de la gestión de la seguridad basado en una evaluación de los riesgos que sea dinámica e incluya todos los niveles de las actividades de los participantes y todos los aspectos de sus operaciones" [5].

---

[1] RUBIO CORREA, Marcial. Estudio de la Constitución Política de 1993. Fondo Editorial de la Pontificia Universidad Católica del Perú, 1999, Lima, p. 315.

[2] ORGANIZACIÓN DE ESTADOS AMERICANOS. Resolución RES/57/239 *"Creación de una cultura mundial de seguridad cibernética"*, p. 1. En: https://www.itu.int/newsroom/wtd/2006/pdf/UNGA_57-239-es.pdf

[3] Ibíd.

[4] Idem, p. 3.

[5] Ibíd.

Adicionalmente, en la Resolución RES/57/239 *"Creación de una cultura mundial de seguridad cibernética"*, la OEA invitó a todas las organizaciones internacionales pertinentes a que *"en toda labor futura en materia de seguridad cibernética tengan presentes, entre otras cosas, esos elementos para la creación de una cultura mundial de seguridad cibernética"*.

Siendo ello así, y tal como ya se ha señalado, la situación advertida a nivel internacional por la Organización de Estados Americanos, tiene relación con la característica del concepto de Defensa Nacional que contempla la Constitución Política del Perú, pues aquella debe ser integral y permanente; entendiendo por integral, lo que abarca inclusive la Seguridad Digital:

"La defensa se desarrolla tanto en el ámbito interno como en el externo. El ámbito interno está referida a las amenazas que provienen desde dentro mismo del Estado: en un sentido ámbito interno es el terrorismo que mina la fuerza interna del país; pero también pueden ser las graves distancias sociales que dividan al país y puedan facilitar una agresión in terna o externa. También será problema de la defensa nacional en el orden interno, la existencia de grandes discrepancias sobre los grandes objetivos nacionales, que deben ser comunes, Y así sucesivamente". [6]

Por lo expuesto señalan que es posible afirmar que este extremo de la propuesta del Proyecto de Ley N° 772/2016-CR no contraviene la norma constitucional y es legalmente viable; razón por la cual no se formula observación.

Respecto a establecer funciones de la DINI, referidas a los programas académicos a través de la Escuela Nacional de Inteligencia:

El Proyecto de Ley también propone establecer como funciones de la Dirección Nacional de Inteligencia, aprobar y supervisar los programas académicos de formación, capacitación y perfeccionamiento en materia de inteligencia a través de la Escuela Nacional de Inteligencia.

Sobre este particular, conviene resaltar que en el Proyecto de Ley se señala que incorporar dichas funciones tiene como finalidad *"asegurar una* ***formación integral y de calidad*** *del personal del Sistema de Inteligencia Nacional – SINIA, sustentada en principios y valores democráticos"*.

Ahora bien, conforme al numeral 7.1 del artículo 7 del Decreto Legislativo N° 1141, el Sistema de Inteligencia Nacional - SINA es el conjunto de principios, normas, procedimientos, técnicas, instrumentos, organismos y órganos del Estado funcionalmente vinculados, que bajo la dirección y coordinación de la Dirección Nacional de Inteligencia - DINI como ente rector, provee de Inteligencia Estratégica, Inteligencia Militar e Inteligencia Policial, y realizan actividades de contrainteligencia en las áreas de su responsabilidad.

Siendo ello así, se tiene que la rectoría del Sistema de Inteligencia Nacional – SINA, recae en la Dirección Nacional de Inteligencia – DINI; con lo cual, resulta conveniente que tenga como funciones la aprobación y supervisión de los

[6] RUBIO CORREA, Marcial. Ob. Cit. p. 315.

programas académicos de formación, capacitación y perfeccionamiento en materia de inteligencia.

De otro lado, es necesario señalar que en este extremo del Proyecto de Ley se alude a la "Escuela Nacional de Inteligencia". Al respecto, conviene hacer referencia al artículo 51 de la Ley N° 28044 - Ley General de Educación, que dispone que:

"Artículo 51.- Instituciones de Educación Superior
Las instituciones universitarias, así como los institutos, ***escuelas*** *y otros centros* ***que imparten Educación Superior*** *pueden ser públicos o privados y* ***se rigen por ley específica****".*

Por tal sentido, por mandato de la Ley General de Educación, corresponde remitirnos a las disposiciones de la Ley N° 29394 - Ley de Institutos y Escuelas de Educación Superior; que es específica respecto a las Escuelas de Educación Superior, como en el presente caso, pues de acuerdo a lo dispuesto en su artículo 1, la Ley N° 29394:

"regula ***la creación*** *y el funcionamiento de institutos* ***y escuelas de educación superior****, públicos o privados, conducidos por personas naturales o jurídicas, que forman parte de la etapa de educación superior del sistema educativo nacional, de acuerdo con lo establecido en la Ley General de Educación".*

En tal sentido, en tanto el Proyecto de Ley alude de manera general a la "Escuela Nacional de Inteligencia"; resultaría conveniente que se señale de manera expresa en la propuesta de ley que la creación y funcionamiento de dicha Escuela *"se rigen por lo dispuesto en la Ley N° 28044 - Ley General de Educación y en las leyes específicas sobre la materia".*

Dicho lo anterior, es posible afirmar que este extremo de la propuesta del Proyecto de Ley N° 772/2016-CR no contraviene la norma constitucional y es legalmente viable; razón por la cual no se formula observación.

<u>Opinión de la Subsecretaria de Administración Pública</u>:

- Respecto a la propuesta del artículo 2, dada la complejidad del tema que conlleva la definición y delimitación de la materia relativa a "seguridad digital", a fin de no afectar la viabilidad de la propuesta normativa, recomiendan una nueva redacción del inciso 8 y complementariamente se incluya una disposición complementaria facultando al Poder Ejecutivo a que mediante decreto supremo desarrolle la definición de Seguridad Digital en el ámbito nacional. La definición es la siguiente:

  > *"Seguridad Digital: Es la situación de confianza en el entorno digital frente a las amenazas que afectan las capacidades nacionales, a través de la gestión de riesgos y la aplicación de medida de ciberseguridad y las capacidades de ciberdefensa, alineada al logro de los objetivos del Estado."*

- En relación al numeral 10.1 del artículo 10, relativo a Plan de Inteligencia Nacional, considerando que el componente de seguridad digital constituye uno

de los componentes para hacer frente a las amenazas dentro de las materias de inteligencia y contrainteligencia, plantean excluir del texto normativo la referencia a "seguridad digital". En este mismo sentido se pronuncian por el numeral 17.8 del artículo 17.

- Señalan que, no obstante, si lo que se quiere es atribuir a la DINI el marco de competencia para establecer los procedimientos destinados a alcanzar la seguridad digital en el ámbito de su competencia, proponen agregar a la función contenida en el numeral 17.7 un texto complementario que permita que las entidades públicas y privadas se sujeten a tales procedimientos ante amenazas que afectan o que potencialmente puedan afectar las capacidades nacionales y proponen el siguiente texto:

  > *"Realizar actividades y establecer los procedimientos destinados a alcanzar la seguridad digital en el ámbito de su competencia, en concordancia con los principios y objetivos de la actividad de inteligencia establecidos en el presente Decreto Legislativo. Para amenazas que afectan o que potencialmente puedan afectar las capacidades nacionales, las entidades públicas y privadas se sujetan a dichos procedimientos."*

- En el numeral 17.18 del artículo 17 sugieren precisar que la función se refiere a los procedimientos especiales.

- Sobre el numeral 17.16 del artículo 17, recomiendan solicitar opinión a SERVIR en su condición de ente rector del Sistema Administrativo de Gestión de Recursos Humanos.

- Respecto al numeral 3.18 del artículo 38 recomiendan una mejor redacción para una mejor comprensión.

- En relación a la incorporación de la Octava Disposición Complementaria Final, señalan que el Poder Ejecutivo tiene como criterio evitar la aprobación de planes innecesarios, cuando se puede utilizar instrumentos de gestión existentes. Sostienen que por un tema de eficiencia y eficacia carece de objeto aprobar un Plan paralelo al Plan de Inteligencia Nacional (PIN), que afectaría la unidad y articulación en las intervenciones de la DINI. Proponen la siguiente redacción:

  > ***"DISPOSICIONES COMPLEMENTARIAS Y FINALES***
  > ***(...)***
  >
  > ***OCTAVA.- La Dirección Nacional de Inteligencia (DINI) en coordinación con las entidades nacionales correspondientes elabora el componente de Seguridad Digital del Plan de Inteligencia Nacional (PIN)."***

Finalmente concluyen en que la propuesta legislativa materia de dictamen resulta viable, con las observaciones y recomendaciones señaladas.

El informe señala que el pasado 6 de junio del presente, se reunieron representantes de la DINI y de la SEGDI, con la finalidad de formular una propuesta conjunta respecto a la viabilidad de la propuesta normativa y de esta

manera evitar duplicidad o superposición de funciones, y ante la necesidad de precisar y delimitar los alcances de la competencia de la DINI en materia digital, con respecto a las competencias que actualmente ostenta la Secretaría de Gobierno Digital en materia de informática y seguridad de la información. Fruto de esta reunión son las recomendaciones formuladas en el presente informe.

2. **De la Dirección Nacional de Inteligencia – DINI**, mediante oficio 068-2017-DINI-01, de fecha 17 de marzo de 2017, recibido por la Comisión de Inteligencia el 20 de marzo de 2017, remite adjunto el Informe 002-2017-DINI-01, el cual contiene opinión institucional favorable con las siguientes precisiones:

   Respecto a:

   1. **La definición de Seguridad Digital** (artículo 2, numeral 8), **c**onsideran que la propuesta de modificación es pertinente, pues se encuentra ajustada a los lineamientos establecidos por la Organización para la Cooperación y Desarrollo Económico – OCDE, la cual describe a la Seguridad Digital como aquella situación de normalidad y de tranquilidad del entorno digital (ciberespacio), derivada de la realización de los fines esenciales del Estado mediante la gestión del riesgo de seguridad digital.

      Esta definición permite incluir en la normativa nacional la definición adecuada para terminología "Seguridad Digital".

   2. **Plan de Inteligencia Nacional.** (artículo 10, numeral 10.1) Están conforme con la presente modificación referida al Plan de Inteligencia Nacional – PIN, a efecto que dicho documento de gestión considere además del desarrollo de los objetivos, políticas, estrategias y responsabilidades de los componentes del SINA, el aspecto de *"gestión de riesgos"* relacionados con las amenazas a la seguridad nacional, esto con la finalidad que la misma sea considerada al momento de la realización de actividades de inteligencia, contrainteligencia y seguridad digital, inclusive.

   3. **Función técnica normativa en materia de Seguridad Digital. (**numeral 17.8 en el Art. 17) sostienen que la presente modificación referida a las funciones de la Dirección de Inteligencia Nacional – DINI, es pertinente. Se amplía la función técnica normativa en materia de inteligencia y contrainteligencia, propia de la Dirección Nacional de Inteligencia – DINI, al desempeño de la función normativa en materia de seguridad digital. De esta manera, se le reconoce a esta entidad su rol preponderante y significativo para el diseño los lineamientos y orientaciones destinados a la obtención de la seguridad digital del país, en su calidad de ente rector del Sistema de Inteligencia Nacional – SINA, fortaleciendo su rol de autoridad técnica normativa especializada.

   4. **Cooperación y asistencia** (numeral 17.13 del artículo 17), consideran que la propuesta de modificación es pertinente. En el aspecto de la seguridad digital, señalan que el reconocimiento de la función de la DINI de establecer y fortalecer las relaciones de cooperación y asistencia con organismos de inteligencia de otros países, permitirá compartir experiencias y buenas prácticas y promover un enfoque de gestión del riesgo de seguridad digital que no incremente el riesgo de otros países, además de fomentar el apoyo recíproco entre las fuerzas de seguridad de la región en la identificación de

actividades delictivas en internet para el posterior enjuiciamiento de sus autores.

5. **Programas Académicos** (numeral 17.13 del artículo 17), Coinciden con la propuesta la cual se orienta a fortalecer la actual función asignada a la DINI, proponiendo que su capacidad este avocada no solo al desarrollo de actividades de capacitación y perfeccionamiento, sino que sea quien lidere, en su calidad de ente rector, el aspecto de capacitación, otorgándosele la competencia de autorizar y controlar que los programas académicos que formen parte de la política de capacitación para el personal del Sistema de Inteligencia Nacional - SINA, garanticen el desarrollo de competencias genéricas aplicables y necesarias para todo el personal que integra dicho sistema,

   También consideran importante la mención a la "Escuela Nacional de Inteligencia - ENI", siendo el caso que dicho órgano es la encargada de la capacitación y perfeccionamiento en inteligencia y contrainteligencia del personal de la Dirección Nacional de Inteligencia (DINI) y del Sistema de Inteligencia Nacional (SINA).

   Sin perjuicio de lo expuesto consideran necesario que la redacción del articulado a modificar debe precisar que los programas de capacitación y perfeccionamiento a supervisar por parte de la ENI, además de versar en materia de inteligencia, debe de contemplar el aspecto de "Seguridad digital"; dicha precisión permitiría que el contenido del artículo se encuentre concordado con las modificaciones propuestas anteriormente, por lo cual se propone la siguiente redacción:

   > *"**Artículo 17.- Funciones***
   > *Son funciones de la Dirección Nacional de Inteligencia - DINI:*
   > ***(...)***
   > ***17.16** Aprobar y supervisar los programas académicos de formación, capacitación y perfeccionamiento en materia de inteligencia **y seguridad digital** a través de la Escuela Nacional de Inteligencia, con la finalidad de asegurar una formación integral y de calidad del personal del Sistema de Inteligencia Nacional – SINA, sustentada en principios y valores democráticos."*

6. **Actividades destinadas a alcanzar la seguridad digital.** consideran que la propuesta de modificación del artículo 7, numeral 17.7, es pertinente dado que la propuesta faculta a la Dirección Nacional de Inteligencia – DINI, realizar actividades destinadas a alcanzar la seguridad digital en el ámbito de su competencia, en concordancia con los principios y objetivos de la actividad de inteligencia establecidos en el Decreto Legislativo1141, esto con la finalidad de precisar claramente las responsabilidades orgánicas y funcionales de la entidad en materia de seguridad digital.

7. **Procedimientos para la gestión de la información en entornos digitales.** Señalan que la incorporación del numeral 17.18 en el artículo 17 del Decreto Legislativo 1141 es pertinente, pues tiene la finalidad de asignar una nueva función a la Dirección de Inteligencia Nacional – DINI, considerando su calidad de ente rector y autoridad técnica normativa a nivel nacional en materia de inteligencia y contrainteligencia, a efecto que sea el encargado de instituir los

procedimientos para la gestión de la información en entornos digitales, otorgándose énfasis a los procedimientos especiales de obtención de información a que se refiere el artículo 32 del Decreto Legislativo Nº 1141, esto con la finalidad de permitir que el acceso y tratamiento de los recursos de información obtenidos en entornos digitales y los peritajes informáticos se realicen en condiciones de seguridad y con observancia del respeto de los derechos humanos de la ciudadanía.

Sin perjuicio de lo expuesto, consideran necesario simplificar la redacción del articulado, evitando la descripción del detalle de las etapas propias de la gestión de la información a obtener, a efecto de no confundir la terminología utilizada con las normas técnicas relacionadas a seguridad de la información, con la correspondiente a seguridad digital, por lo que proponen el siguiente texto:

> ***Artículo 17.- Funciones***
> *Son funciones de la Dirección Nacional de Inteligencia - DINI:*
> *(...)*
>
> ***17.18 Establecer los procedimientos para la gestión de la información en entornos digitales, a que se refiere el artículo 32 del presente Decreto Legislativo y para peritajes informáticos. El Poder Judicial, a través de convenios interinstitucionales brinda asesoramiento técnico para la elaboración de estos procedimientos.***
>
> ***17.19 Las demás establecidas por Ley.***

8. **Entorno digital** señalan que la propuesta de modificación del numeral 38.1 del artículo 38 del Decreto Legislativo1141, es pertinente. Precisan que el establecimiento extensivo de protección de la identidad del personal y de la actividad de inteligencia en los entornos digitales se justifica en razón del alto riesgo que implican la realización de actividades de inteligencia para los funcionarios que la ejecutan, y de aprobarse la modificación legislativa propuesta, sería la Dirección de Inteligencia Nacional – DINI, quien en su calidad de ente rector, deba de determinar las herramientas y mecanismos de protección necesarios a aplicar para los agentes que prestan servicios en los diversos órganos y organismos componentes del SINA, a efecto de disminuir su vulnerabilidad y promover la realización de sus actividades en mejores condiciones de seguridad.

9. **Plan Nacional de Seguridad Nacional.** Son de la opinión que la propuesta de incorporación de una Octava Disposición Complementaria Final en el texto del Decreto Legislativo Nº 1141, es pertinente.

   Sostienen que es importante que se haya considerado que la DINI la función de elaborar el Plan Nacional de Seguridad Digital y que éste se realice de forma coordinada con autoridades nacionales que provengan de entidades involucradas en el tema, dado que esto permitiría evitar la duplicidad de funciones, considerando que a la fecha existen entidades especializadas en la gestión de algunos aspectos de la Seguridad Digital, como es el caso, por ejemplo, de la Oficina Nacional de Gobierno Electrónico e Informática – ONGEI consideramos importante que el legislador haya considerado que la elaboración

del Plan Nacional de Seguridad Digital se realice de forma coordinada con autoridades nacionales que provengan de entidades involucradas en el tema, dado que esto permitiría evitar la duplicidad de funciones, considerando que a la fecha existen entidades especializadas en la gestión de algunos aspectos de la Seguridad Digital, como es el caso, por ejemplo, de la Oficina Nacional de Gobierno Electrónico e Informática – ONGEI

3. **Del Ministerio del Interior**, mediante oficio 515-2016-IN-DM de fecha 11 de mayo de 2017, recibido por la Comisión de Inteligencia en la misma fecha, remite el informe 000655-2017/IN/OGAJ, elaborado por la Oficina General de Asesoría Jurídica, el cual contiene opinión favorable, con las siguientes observaciones, en base a lo manifestado por la DIRIN PNP:

   Respecto a la incorporación del término "seguridad Digital", manifiesta que dicho término es muy amplio y que en la práctica demandaría la interacción con diversas entidades públicas y privadas, pues engloba muchos aspectos funcionales y6 de diversas entidades del Estado, más aun teniendo en cuenta que la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) actualmente denominada Secretaría de Gobierno Digital de la PCM, es el órgano técnico especializado que en su calidad de ente rector del Sistema Nacional de Informática, lidera los proyectos de normatividad y las diversas actividades que en materia de gobierno electrónico realiza el Estado, por lo cual sostienen que la definición debe ser establecida en consenso con dicha oficina. A su vez consideran incluir los siguientes términos y sus definiciones: "ciberespacio, ciberinteligencia, ciberseguridad y gestión de riesgos".

   Respecto a la modificación del artículo 10 recomiendan cambiar el término seguridad digital por "ciberinteligencia".

   Sobre las modificaciones del artículo 17:

   - En lo que se refiere al numeral 17.8, señalan que la ONGEI ha desarrollado un documento normativo denominado "Política Nacional de Gobierno Electrónico 2013-2017, la que tiene entre sus objetivos "Garantizar la integridad, confidencialidad y disponibilidad de la información en la administración pública mediante mecanismos de seguridad de la información gestionada, así como articular los temas de ciberseguridad en el Estado", por lo cual consideran que resultaría contradictorio indicar que la DINI sea la autoridad técnica normativa a nivel nacional en seguridad digital. Recomiendan la conformación de un "Equipo de Respuesta ante Emergencias Informáticas (CERT)

   - En relación a la modificación del numeral 17.13 comentan que no hay que restringir las relaciones de cooperación y asistencia solo a organismos de inteligencia sino también considerar que existen organizaciones gubernamentales y privadas especializadas en ciberseguridad, ciberinteligencia, análisis de riesgos, etc que no necesariamente están ligados a inteligencia.

   - En cuanto a la modificación del numeral 17.8 plantean la siguiente redacción: "Realizar actividades **en el ámbito de su competencia** en concordancia con los principios y objetivos de la actividad de inteligencia **destinados a mitigar los riesgos a partir de una gestión adecuada de la información basados en análisis de amenazas y vulnerabilidades".**

- Acerca de la modificación del numeral 17.18 recomiendan plantear dos funciones: La primera "establecer los procedimientos para la gestión de información **por los componentes del SINA en entornos digitales** que permitan asegurar su integridad, confidencialidad y disponibilidad" y la segunda "Establecer convenios interinstitucionales con el Poder Judicial, quien brindará asesoramiento técnico en los procedimientos **especiales de obtención de información** a que se refiere el artículo 32 del presente Decreto Legislativo y para peritajes informáticos".

Referente a la modificación de la Octava Disposición Complementaria señalan que no correspondería la formulación de un Plan Nacional de Seguridad Nacional de Seguridad Digital, recomendando considerar "ciberinteligencia" y "ciberseguridad".

4. **Del Ministerio de Defensa**, mediante oficio 1205-2017-MINDEF/SG de fecha 3 de mayo de 2017, recibido por la Comisión de Inteligencia con fecha 4 de mayo de 2017 remiten el Informe legal 087-2016-2017- MINDEF/OGAJ, elaborado por la Oficina General de Asesoría Jurídica, el cual contienen la opinión favorable y sugiere considerar los siguientes comentarios[7]:

Del Comando Conjunto de las Fuerzas Armadas del Perú:

Señalan que las modificaciones que propone el proyecto de ley, no guarda relación con la dación de la ley.

- Que el concepto de seguridad digital resulta necesario que forme parte de las responsabilidades funcionales y orgánicas del SINA y la DINI en materia de seguridad digital, por guardar relación con el desarrollo de las comunicaciones y las tecnologías, los cuales representan riesgos e incertidumbres que justifica una gestión ´permanente por parte del Estado.
- Que de la revisión de la definición de "ciberdefensa", esta involucra acciones reactivas, esto es tener capacidad de reaccionar ante un ciberataque, lo cual desvirtúa la misión que tiene la inteligencia.
- Propone como definición de seguridad Digital lo siguiente: "Es la situación de confianza en el entorno digital, alineada al logro de los objetivos del Estado, a través de riesgos y la aplicación de medidas de ciberseguridad".

De la Fuerza Aérea

- Considera pertinente la inclusión del término Seguridad Digital en el Decreto Legislativo 1141.
- En relación a la modificación del numeral 10.1 del artículo 10, incorporando los conceptos de seguridad digital y gestión de riesgos, sugiere se encuadre la seguridad digital dentro de las actividades de contrainteligencia normando sus procedimientos en la doctrina específica de contrainteligencia.
- Respecto al numeral 17.6 considera no pertinente la modificación puesto que cada Escuela de Inteligencia Institucional, brinda capacitación en ámbitos de inteligencia específica en base a su doctrina, funciones y capacidades, a la cual

[7] Señalan que solicitaron opinión técnica al Comando Conjunto de las Fuerzas Armadas del Perú, Ejército del Perú, Marina de Guerra del Perú, Fuerza Aérea del Perú, Dirección General de Política y Estrategia y a la Dirección General de Educación y Doctrina. (Inf.676-2017-MINDEF/OGAJ) Todos opinaron favorablemente con recomendaciones.

permite tecnificar al personal en las áreas de su competencia, para las diversas funciones operativas.

- En relación a las modificaciones propuestas en los numerales 17.17 y 17.18 sugiere modificar la redacción enmarcando la seguridad digital dentro de las actividades de contrainteligencia.
- En cuanto a los numerales 17.8, 17.13 y numeral 38.1 del artículo 38, los consideran pertinentes.

Ejército del Perú

- Considera pertinente la incorporación del término "Seguridad Digital" en el Decreto Legislativo 114 y por consiguiente viable el proyecto de ley materia de análisis.

Marina de Guerra

En el artículo 2 recomienda definir a su vez los conceptos de "ciberseguridad" y "ciberdefensa" pues están ausentes en la legislación nacional. Recomiendan adoptar los conceptos establecidos por el Consejo Nacional de Política Económica y Social de la República de Colombia, mediante el documento CONPESS 3701.

Propone incorporar en el artículo 17, como función de la DINI:

"Obtener y mantener las capacidades necesarias para el logro de los objetivos de la seguridad digital, explotando la fortalezas adquiridas por los órganos que conforman el Sistema de Inteligencia Nacional – SINA, así como de otras instituciones y organizaciones del Estado, articulando esfuerzos, con el fin de utilizar capacidades existentes a efecto de lograr mayor eficiencia en la utilización de recursos para el logro de los objetivos en el menor tiempo posible".

5. **Del Ministerio de Relaciones Exteriores**, mediante Of RE (DGM-DSD) N°3-0-A/42 de fecha 9 de febrero de 2017, recibido por la Comisión de Inteligencia con fecha 9 de febrero de 2017, remite opinión institucional con las siguientes observaciones:

   Respecto al Plan de Inteligencia Nacional - PIN, manifiestan que no tienen observaciones a la modificación propuesta, la consideran necesaria sustentando que la incorporación de "seguridad digital" fortalecerá la rectoría del Sistema de Inteligencia Nacional; asimismo concuerdan con la definición que el proyecto de ley propone.

   Sobre la incorporación de funciones de la DINI y de la Octava Disposición Complementaria y Final del Decreto Legislativo 1141 señalan no tener observaciones. Finalmente manifiestan que es innecesaria la incorporación del artículo 3 del proyecto de ley por estar en el artículo 109 de la Constitución Política del Perú.

6. **Opinión del ciudadano: Señor Fernando Elías Zegarra López, registrado el 09/03/2017. Remitido a través del Foro Legislativo Virtual**

   Plantea las siguientes observaciones al proyecto de ley 772/2016-CR

Señala que proteger las capacidades nacionales, es un ámbito que sobrepasa al sistema de inteligencia nacional y que corresponde al Sistema de Defensa Nacional.

Sostiene que la función de inteligencia tiene solamente dos ámbitos: inteligencia y contrainteligencia, traducidos a en obtener conocimiento útil para enfrentar a las amenazas a la seguridad nacional, y en negar el acceso a la inteligencia adversaria, lo cual permitirá proteger a los activos críticos nacionales. Estas tareas incluyen el empleo de operaciones encubiertas, de ser necesario; en consecuencia, considerar a la Dirección Nacional de Inteligencia como la Autoridad Técnica Normativa en materia de seguridad digital, no es correcto, pues esa categoría de la seguridad es de competencia del Sistema de Defensa Nacional, que dispone de una entidad responsable en temas de ciberseguridad, a pesar que aún no ha emitido la política nacional de la información que permita hacer frente a las amenazas a la Seguridad Nacional en el ciberespacio, lo que si consideramos adecuado son las otras funciones agregadas sobre la materia , numerales 17.17;17.18, que si se encuentran enmarcadas en el ámbito de la función de inteligencia.

Dice que, empleando el mismo argumento, no es adecuado que la DINI elabore el Plan Nacional de Seguridad Digital, pues las acciones de seguridad y Defensa Nacional son de competencia del sistema de Defensa Nacional, debe tenerse en cuenta que la DINI, brinda el conocimiento útil, a sus usuarios y sin ellos quienes adoptan las medidas de seguridad o defensa, conforme lo establezca y apruebe el Presidente de la República, quien es también quien preside y dirige el Sistema de Defensa Nacional.

Por otro lado, estima inadecuado volver a modificar el artículo 10 relativo al Plan de Inteligencia Nacional, incluyendo a la Seguridad Digital y Gestión de Riesgos, manifestando que este plan debe centrarse en dar las responsabilidades para orientar el esfuerzo de búsqueda de información en todas las dimensiones, no solo en el ciberespacio, en atención a las conclusiones obtenidas en la apreciación de inteligencia. Así mismo, es pertinente recordar la doctrina que explica que en "el proceso de planeamiento de inteligencia (PPI), la gestión de riesgos se materializa principalmente en la determinación de escenarios de riesgos se materializa principalmente en la determinación de escenarios de riesgos, esta determinación se realiza tomando en cuenta el inventario de activos críticos nacionales (IACN) que contiene la relación de activos imprescindibles para el logro de los objetivos de estado. La misión u objetivos de Estado y la inteligencia disponible con fines de generar conocimientos (inteligencia), el análisis consiste en evaluar el riesgo de un proceso o política en particular, en función a las capacidades o ventajas que puede presentar un actor determinado con fines de seguridad (contrainteligencia), el análisis consiste en establecer los niveles de riesgo que soporta cada activo critico tomando en cuenta las formas de acción establecidas en la inteligencia disponible.

Finalmente señala que es posible realizar (sobre la planteada en el IACN) una nueva priorización y así orientar de manera eficiente los recursos de inteligencia y contrainteligencia, en la planificación de las actividades de Inteligencia Nacional. En síntesis, la gestión es una actividad que se realiza tanto en el proceso de inteligencia como en el de contrainteligencia, no constituye un proceso independiente, en este sentido, considera que el artículo 10 debe permanecer tal como lo establece la Ley 30535.

7. Mesas de Trabajo

Se realizaron dos mesas de Trabajo, con invitados representantes de las entidades públicas involucradas y especialistas y consultores.

- La primera realizada el 1 de Junio de 2017
- La segunda el 9 de Junio de 2017

Asistieron los siguientes invitados:

1. Sra. Patricia Gamio Franco- Funcionaria de la Subsecretaria de Transformación Digital de la Secretaria de Gobierno Digital-PCM
2. Sr. Miguel Adolfo del Carpio Wong - Representante de la Subsecretaria de Tecnologías Digitales-PCM
3. Sr. Fernando Veliz Fazzio - Subsecretario de Transformación Digital-PCM
4. Sr. Raúl Carrasco Clavijo – Subsecretario de Gestión Publica- PCM
5. Sr. Heber Cusma Saldaña- Abogado de la Subsecretaría de Gestión Pública
6. Sr. César Vilchez Inga - Subsecretario de Tecnología Digital
7. Sr. Luis García Barrionuevo – Jefe del Gabinete Asesores de la DINI
8. Sr. Luis Carranza Micalay - Asesor de la Dirección Inteligencia Nacional
9. Sr. Crl. FAP Daniel Taipe Domínguez - Jefe de Operaciones de Ciberdefensa-Ministerio de Defensa.
10. Sra.Martina Marangunich Rachumi - Consultora
11. Sr. Rafael Zegarra Valdivia - Consultor
12. Sr. Erick Iriarte Ahon - Abogado, Magister en la Ciencia Política de la PUCP-Consultor
13. Sr. Carlos Miguel Guerrero Argote - Director de Investigación ONG Hiperderecho
14. Sra.Ing. Isabel Falla Zevallos - Consultora
15. Sr. Miguel Yamasaki Koizumi - Consultor

A su vez como resultado del debate luego de realizadas las Mesas de Trabajo, se recibieron por escrito, sus aportes y comentarios, siendo los siguientes:

a. Dr. RAFAEL ZEGARRA VALDIVIA, consultor

Presentó las siguientes apreciaciones:

Sostiene que el marco en el cual se desarrolla el proyecto de Ley es el de la seguridad nacional y las amenazas que puedan impactar en las capacidades nacionales, siendo una de ellas las que se desarrollan en el ámbito cibernético.

Incide en que se confunde la seguridad de la información con la seguridad digital. La seguridad de la información en el País se desarrolla en el marco del objetivo 7: promover una administración pública de calidad a la población de la Agenda Digital 2.0, siendo la estrategia 4 la de implementar mecanismos para mejorar la seguridad de la información, a fin de minimizar los riesgos de sufrir algún tipo de incidente en las infraestructuras críticas de la información y las disuasión del crimen cibernético; mientras que la seguridad digital está orientada a la detección y alertas de posibles amenazas que afecten a las capacidades nacionales.

En este sentido sostiene que no existe interferencia ni superposición de funciones entre ambos conceptos, siendo complementarios en todos sus aspectos; en consecuencia, es necesario fortalecer las actividades de la secretaria de Gobierno digital y la dirección de Inteligencia Nacional, cada uno en el ámbito de su competencia.

Propuso la siguiente definición sobre seguridad digital:
"Es la situación de confianza en el entorno digital frente a amenazas que afecten las capacidades nacionales, a través de la gestión de riesgos, la aplicación de medidas de ciberseguridad y las capacidades de ciberdefensa, alineadas al logro de los objetivos del Estado".

b. Dr. ERICK IRIARTE, consultor
Hace alcances respecto a las definiciones que existen en el ámbito internacional.

Resaltó aspectos positivos del proyecto de ley:
- Incluir disposiciones sobre seguridad digital está acorde con las recomendaciones del informe del BID/OEA.
- Es un desarrollo necesario para afrontar los desafíos de Ciberdefensa en las entidades encargadas de la Defensa Nacional en el país.
- Esta acorde a las prerrogativas actuales de dichas autoridades

A su vez formuló las siguientes observaciones:

- En la práctica, asignar a la DINI la elaboración del Plan Nacional de Seguridad Digital desconoce los avances realizados por la SGD (Ex ONGEI).
- Por naturaleza, el trabajo desarrollado por la DINI se va nutrir de la cooperación entre el SINA y otros espacios ligados al Sector Defensa.
- Existe un valor en que un Plan Nacional de Ciberseguridad sea elaborado en un ambiente multistakeholder, es decir, con participación de todas las partes interesadas. Ese espacio difícilmente se puede desarrollar en el Sector Defensa.
- A nivel regional, los Planes de Ciberseguridad han sido desarrollados en espacios multistakeholder y promovidos desde instancias técnicas (CERTs) y (NICs)

Respecto a las definiciones, para los fines del presente Decreto Legislativo y de las actividades reguladas por el mismo, propuso lo siguiente:

8) Ciberseguiridad: El conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, practicas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos del estado y a sus ciudadanos, en el ámbito de sus competencias

"Articulo 10.- Plan de Inteligencia Nacional. PIN. 10.1 Para **"Artículo 10.- Plan de Inteligencia Nacional - PIN**
10.1 Para efectos del desarrollo de actividades de inteligencia, contrainteligencia, incluyendo aspectos de ciberseguridad en el ámbito de su competencia, el Sistema de Inteligencia Nacional - SINA cuenta con el Plan de Inteligencia Nacional - PIN, que contiene los objetivos, políticas, estrategias, gestión de

riesgos y responsabilidades de sus componentes, relacionados con las amenazas a la seguridad nacional y la identificación de oportunidades favorables a ella, siendo su cumplimiento de carácter obligatorio. Es aprobado por el Consejo de Seguridad y Defensa Nacional en abril del año anterior a su ejecución, a propuesta del ente rector del Sistema de Inteligencia Nacional -SINA"

"Articulo.17.-Funciones. Son funciones de la Dirección Nacional de Inteligencia - DINI:
(...)
17.8 Constituir la autoridad técnica normativa a nivel nacional en materia de inteligencia, contrainteligencia. (...)
17.13 Establecer y fortalecer las relaciones de cooperación y asistencia con organismos de inteligencia de otros países.
17.16 Aprobar y supervisar los programas académicos de formación, capacitación y perfeccionamiento en materia de inteligencia a través de la Escuela Nacional de Inteligencia, con la finalidad de asegurar una formación integral y de calidad del personal del Sistema de Inteligencia Nacional - SINA, sustentada en principios y valores democráticos.
17.17 Realizar actividades destinadas de ciberseguridad en el ámbito de su competencia, en concordancia con los principios y objetivos de la actividad de inteligencia establecidos en el presente Decreto Legislativo.

Identidad.-
38.1 Los procedimientos de protección de identidad del personal y de la actividad de inteligencia tiene carácter secreto, incluyendo la identidad en entornos digitales.

c. CRNL. FAP DANIEL TAIPE DOMÍNGUEZ
Propuso excluir el término de "Capacidades de Ciberdefensa", por corresponder a las funciones del sector Defensa y no a las desarrolladas por inteligencias. Asimismo la siguiente definición

Seguridad Digital: Es la situación de confianza en el entorno digital frente a las amenazas que afectan las capacidades nacionales, a través de la gestión de riesgos y la aplicación de medidas de Ciberseguridad, alineada al logro de los objetivos del Estado.

Señaló que estas "Capacidades de Ciberdefensa" no les corresponden a la labor de Inteligencia.

d. Dr. Carlos Guerrero Argote
Hizo manifiesta su preocupación de que el "Plan Nacional de Seguridad Digital" del que habla la octava disposición complementaria y final, que define la estrategia y los lineamientos a emplear en materia de Ciberseguridad, no debería recaer en la DINI por los siguientes motivos:

El Plan compromete no solo a entidades del gobierno sino también al sector privado y a la sociedad civil (para colaboración, prevención, etc.). Por lo tanto, su creación debe contar con la participación de estos stakeholders. En ese sentido, la DINI no posee espacios de este tipo en el que todos los participantes puedan interactuar en pie de igualdad para la redacción del Plan. Una instancia que sí cuenta con ese espacio es la Secretaría del Gobierno Digital - PCM a través del CCONI (Comité Coordinador Nacional de Informática para entidades no estatales).

Señaló que la DINI es un órgano importante al interior del Sector Defensa, por lo que debería enfocar su trabajo a la "Ciberdefensa", entendida como todas aquellas acciones preventivas y tácticas del Estado Peruano contra ataques, lo que es competencia de este sector. Pero la Ciberseguridad ("Seguridad Digital" en este PL) posee un enfoque más amplio que no necesariamente compromete acciones tácticas o del Sector Defensa, por lo que una instancia superior es la que debe elaborar este Plan Nacional, en tanto que la DINI u otro órgano complementario deben emplearlo para definir su estrategia dentro del Sector Defensa.

Sugiere la octava disposición complementaria y final o, con el fin de armonizar los otros cambios, modifíquese de la siguiente forma:

"La dirección Nacional de Inteligencia (DINI) participará de la elaboración del Plan Nacional de Seguridad Digital y la empleará como instrumento de gestión complementario al Plan de Inteligencia Nacional (PIN)"

Prefiérase la eliminación en los siguientes casos:

El artículo 8 del PL no se modifique sustantivamente, restringiendo el ámbito de aplicación.

No existan modificaciones sustantivas en las definiciones de los artículos 17; incisos incisos 8, 17, 18 y artículo 38; inciso 1.

e. Lic. Martina Marangunich Rachumi- Consultora

Luego de sus intervenciones en las Mesas de Trabajo formuló los siguientes aportes:

Aporte I

Respecto a la modificación del artículo 2 referido a definiciones:

8) Seguridad Digital: Es la situación de confianza ***en el uso de la TIC, mediante capacidades de inteligencia para la protección de la información que constituya un activo nacional estratégico, relevante para los intereses nacionales, permitiendo ejercer respuestas oportunas, legítimas y proporcionadas en el ciberespacio, ante amenazas, riesgos o agresiones que afecten a la Seguridad y Defensa Nacional.***

Aporte II

Respecto a la modificación del Artículo 17referido a funciones:

17.8 Construir .....de inteligencia y contrainteligencia ***que incorpore adicionalmente al ámbito del ciberespacio.***

17.16. Aprobar ... Escuela Nacional de Inteligencia ***que incluya además la formación en temas del ciberseguridad ,*** con la finalidad ...

17.17 ***Fortalecimiento de capacidades destinados*** a alcanzar.....

Aporte III

Propuso: conformar el Comité Especializado en Ciberseguridad, que será un capítulo del Consejo de Seguridad y Defensa Nacional, cuya función principal será articular con todos los organismos responsables de la ciberseguridad a nivel de organismos Públicos, Privados, Internacionales y de la Sociedad Civil.

II. CONTENIDO DE LA PROPUESTA DE LEY

El Proyecto de Ley 772-2016–CR, propone la Ley que modifica diversos artículos del Decreto Legislativo 1141, Decreto legislativo de fortalecimiento y modernización del

Sistema de Inteligencia Nacional – SINA y de la Dirección Nacional de Inteligencia – DINI.

Tiene como objeto promover la eficiencia de la DINI en el aspecto estratégico nacional como componente del Sistema de Inteligencia Nacional y propiciar el desarrollo de la seguridad digital

En este contexto propone modificar cuatro artículos del Decreto Legislativo 1141, Decreto legislativo de fortalecimiento y modernización del Sistema de Inteligencia Nacional – SINA y de la Dirección Nacional de Inteligencia – DINI e incorpora una Disposición Complementaria Final, y plantea:

1. Incorporar la definición de "Seguridad Digital" en la legislación especial de la actividad de inteligencia.

2. Incorporar la gestión de riesgos como parte del Plan de Inteligencia Nacional – PIN, para el desarrollo de actividades de inteligencia, contrainteligencia y seguridad digital.

3. Establecer como funciones de la DINI:

   - Función técnica normativa en materia de Seguridad Digital.
   - Establecer y fortalecer relaciones de cooperación y asistencia con organismos de inteligencia de otros países.
   - Aprobar y supervisar programas académicos de formación, capacitación y perfeccionamiento especializado del personal del SINA.
   - Realizar actividades destinadas a alcanzar la seguridad digital en el ámbito de su competencia.
   - Establecer procedimientos para la gestión de la información en entornos digitales.

4. Incorporar la protección de la identidad del personal y de la actividad de inteligencia en entornos digitales.

5. Establecer el deber de la DINI de elaborar el Plan Nacional de Seguridad Digital, como instrumento de gestión complementario al Plan de Inteligencia Nacional – PIN.

Decreto Legislativo N° 1141	Proyecto de Ley N° 772/2016-CR
Artículo 2.- Definiciones Para los fines del presente Decreto Legislativo y de las actividades reguladas por el mismo se entenderá por: (...)	**Artículo 2.- Definiciones** Para los fines del presente Decreto Legislativo y de las actividades reguladas por el mismo se entenderá por: (...) **8. Seguridad Digital: Es la situación de confianza en el entorno digital, alineada al logro de los objetivos del Estado, a través de la gestión de riesgos, la aplicación de medidas de ciberseguridad y las capacidades de ciberdefensa.**
Artículo 10.- Plan de Inteligencia Nacional - PIN	**Artículo 10.- Plan de Inteligencia Nacional - PIN**

10.1 Para efectos del desarrollo de actividades de inteligencia y contrainteligencia, el Sistema de Inteligencia Nacional - SINA cuenta con el Plan de Inteligencia Nacional - PIN, que contiene los objetivos, políticas, estrategias y responsabilidades de sus componentes, relacionados con las amenazas a la seguridad nacional y la identificación de oportunidades favorables a ella, siendo su cumplimiento de carácter obligatorio. Es aprobado por el Consejo de Seguridad y Defensa Nacional en abril del año anterior a su ejecución, a propuesta del ente rector del Sistema de Inteligencia Nacional – SINA, previa conformidad del Consejo de Inteligencia Nacional – COIN.	**10.1** Para efectos del desarrollo de actividades de inteligencia, contrainteligencia **y seguridad digital**, el Sistema de Inteligencia Nacional - SINA cuenta con el Plan de Inteligencia Nacional - PIN, que contiene los objetivos, políticas, estrategias, **gestión de riesgos** y responsabilidades de sus componentes, relacionados con las amenazas a la seguridad nacional y la identificación de oportunidades favorables a ella, siendo su cumplimiento de carácter obligatorio. Es aprobado por el Consejo de Seguridad y Defensa Nacional en abril del año anterior a su ejecución, a propuesta del ente rector del Sistema de Inteligencia Nacional – SINA, previa conformidad del Consejo de Inteligencia Nacional – COIN.
Artículo 17.- Funciones Son funciones de la Dirección Nacional de Inteligencia - DINI: **(...)** **17.8** Constituir la autoridad técnica normativa a nivel nacional en materia de inteligencia y contrainteligencia.	**Artículo 17.- Funciones** Son funciones de la Dirección Nacional de Inteligencia - DINI: **(...)** **17.8** Constituir la autoridad técnica normativa a nivel nacional en materia de inteligencia y contrainteligencia **y seguridad digital.**
Artículo 17.- Funciones Son funciones de la Dirección Nacional de Inteligencia - DINI: (...) **17.13** Establecer y fortalecer las relaciones de cooperación con organismos de inteligencia de otros países.	**Artículo 17.- Funciones** Son funciones de la Dirección Nacional de Inteligencia - DINI: (...) **17.13** Establecer y fortalecer las relaciones de cooperación **y asistencia** con organismos de inteligencia de otros países.
Artículo 17.- Funciones Son funciones de la Dirección Nacional de Inteligencia - DINI: **(...)** **17.16** Capacitar y perfeccionar académicamente al personal del Sistema de Inteligencia Nacional - SINA.	**Artículo 17.- Funciones** Son funciones de la Dirección Nacional de Inteligencia - DINI: **(...)** **17.16 Aprobar y supervisar los programas académicos de formación, capacitación y perfeccionamiento en materia de inteligencia a través de la Escuela Nacional de Inteligencia, con la finalidad de asegurar una formación integral y de calidad del personal del Sistema de Inteligencia Nacional – SINA, sustentada en principios y valores democráticos.**
Artículo 17.- Funciones Son funciones de la Dirección Nacional de Inteligencia - DINI: (...) **17.17** Las demás establecidas por ley.	**Artículo 17.- Funciones** Son funciones de la Dirección Nacional de Inteligencia - DINI: (...) **17.17 Realizar actividades destinadas a alcanzar la seguridad digital en el ámbito de su competencia, en concordancia con los principios y objetivos de la actividad de**

	inteligencia establecidos en el presente Decreto Legislativo.
Artículo 17.- Funciones Son funciones de la Dirección Nacional de Inteligencia - DINI: (...)	**Artículo 17.- Funciones** Son funciones de la Dirección Nacional de Inteligencia - DINI: (...) **17.18 Establecer los procedimientos para la gestión de la información en entornos digitales que permitan asegurar su integridad, confidencialidad y disponibilidad, especialmente para los procedimientos especiales de obtención de información a que se refiere el artículo 32 del presente Decreto Legislativo y para peritajes informáticos. El Poder Judicial, a través de convenios interinstitucionales brinda asesoramiento técnico para la elaboración de estos procedimientos.** **17.19 Las demás establecidas por Ley.**
Artículo 38.- Protección de la identidad **38.1** Los procedimientos de protección de identidad del personal y de la actividad de inteligencia, tienen carácter secreto.	**Artículo 38.- Protección de la identidad** **38.1** Los procedimientos de protección de identidad del personal y de la actividad de inteligencia, tienen carácter secreto, **incluyendo la identidad en entornos digitales.** **(...)**
DISPOSICIONES COMPLEMENTARIAS FINALES (...)	**DISPOSICIONES COMPLEMENTARIAS FINALES** (...) **OCTAVA.-** La Dirección Nacional de Inteligencia (DINI) en coordinación con las autoridades nacionales correspondientes elaborará el Plan Nacional de Seguridad Digital como instrumento de gestión complementario al Plan de Inteligencia Nacional (PIN).

III. MARCO NORMATIVO

Marco normativo nacional

- Constitución Política del Perú.
- Reglamento del congreso de la República del Perú
- Decreto Legislativo 1141 – Decreto Legislativo de Fortalecimiento y Modernización del Sistema de Inteligencia Nacional – SINA y de la Dirección Nacional de Inteligencia.
- Ley 30535que modifica el Decreto Legislativo 1141
- Decreto Supremo 016-2014-PCM Reglamento del Decreto Legislativo 411
- Decreto Supremo 035-2015-PCM que aprueba el Reglamento de Organización y Funciones de la DINI.

IV. ANÁLISIS DE LA PROPUESTA

Antecedentes del Proyecto de Ley 772/2016-CR

La presente iniciativa legislativa, según consta en la exposición de motivos, recoge aquellas propuestas formuladas por la Dirección Nacional de Inteligencia DINI en la oportunidad en que emitieron opinión del proyecto de ley 71/2016-CR el cual fue dictaminado por la Comisión de Inteligencia en la legislatura anterior y actualmente es ley.

Asimismo, se ha tomado como antecedente el Proyecto de Ley 71/2016-CR presentado por la Congresista Luz Filomena Salgado Rubianes, dictaminado por nuestra Comisión.

Antecedentes

En el ámbito internacional se tiene como antecedente de Seguridad Digital el Convenio sobre la Ciberdelincuencia del Consejo de Europa, el cual entró en vigencia desde el 01 de julio de 2004, plasmándose como un objetivo la necesidad de aplicar, con carácter prioritario una política penal común encaminada a proteger a la sociedad frente a la ciberdelincuencia; entre otras formas, mediante la adopción de la legislación adecuada y el fomento de la cooperación internacional.

Asimismo, mediante Resolución de la Asamblea General de la Organización de los Estados Americanos – OEA, se respalda las recomendaciones y se apoya el proceso de elaboración de la Estrategia Interamericana para Combatir las Amenazas a la Seguridad Cibernética.

Colombia a través de su Consejo Nacional de Política Económica y Social – CONPES, aprobó la nueva Política Nacional se Seguridad Digital el 11 de abril de 2016, convirtiéndose en el primer país de Latinoamérica y uno de los primeros en el mundo en incorporar las recomendaciones en gestión de riesgos de seguridad digital expedida por la Organización para la Cooperación y el Desarrollo Económico (OCDE).

La Organización para la Cooperación y el Desarrollo Económico (OCDE) con fecha 17 de septiembre de 2015, emitió las Recomendaciones sobre gestión de riesgos de seguridad digital para la prosperidad económica y social. Este documento guía la formulación de las nuevas estrategias respecto a la gestión de la seguridad digital, con el objetivo de optimizar los beneficios económicos y sociales que se esperan por el desarrollo de actividades en un entorno digital abierto; asimismo contiene, entre otros, las definiciones básicas que debe contener las políticas nacionales de seguridad digital de los países.

El Consejo Nacional de Política Económica y Social –CONPES describe la importancia del entorno digital como herramienta para el crecimiento económico, resaltando la importancia de que se tenga un enfoque de gestión de riesgos en seguridad digital que involucre a las partes interesadas. A su vez define a la seguridad digital como la situación de normalidad y de tranquilidad en el entorno digital (ciberespacio), derivada de la realización de los fines esenciales del Estado mediante (i) la gestión del riesgo de seguridad digital; (ii) la implementación efectiva de medidas de ciberseguridad; y (iii) el uso efectivo de las capacidades de

ciberdefensa; que demanda la voluntad social y política de las múltiples partes interesadas y de los ciudadanos del país.

Es por todo lo antes dicho que se hace necesaria la incorporación de la definición de "Seguridad Digital", más aun teniendo en cuenta que en el Decreto Legislativo N°1141 no se observa indicio alguno de este concepto, siendo importante su desarrollo e implementación por parte del Estado.

Análisis Técnico

Definiciones[8]

Ciberseguridad. De acuerdo a ITU: (Perú es miembro de UIT): Ciberseguridad es el conjunto de herramientas políticas, conceptos de seguridad, salvaguardas de seguridad, directrices métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. Las propiedades de seguridad incluyen una o más de las siguientes:

a. Disponibilidad
b. Integridad: que puede incluir la autenticidad y el no repudio
c. Confidencialidad

Ciberdefensa:
"(Una) medida proactiva para detectar u obtener información sobre una instrucción cibernética, ataque cibernético u operación cibernética inminente o para determinar el origen de una operación que implica el lanzamiento de una contra-acción preventiva, preventiva o cibernética contra la fuente." (Definición del Centro Cooperativo para la Ciberdefensa de la OTAN)

Entorno digital:
"Incluye a los usuarios, redes, dispositivos, todo tipo de software, procesos, información almacenada o en tránsito, aplicaciones, servicios y sistemas que pueden ser conectados directamente o indirectamente a otras redes." (Definición ITU)

Actores Nacionales en materia de Ciberseguridad

- **Secretaria Gobierno Digital** (ex ONGEI)

  "La Oficina Nacional de Gobierno Eléctrico e Informática (ONGEI), es el Órgano Técnico Especializado que depende directamente del Despacho de la Presidencia del Consejo de Ministros (PCM). ONGEI, en su calidad de Ente Rector del Sistema Nacional de Informática, se encarga de liderar los proyectos, la normatividad, y las diversas actividades que en materia de Gobierno Electrónico realiza el Estado. Entre sus actividades permanentes se encuentran las vinculadas a la normatividad informática, la seguridad de la

[8] Información proporcionada por el señor Erik Iriarte

información, el desarrollo de proyectos emblemáticos en Tecnologías de la Información y la Comunicación (TIC), brindar asesoría técnica e informática a las entidades públicas, así como, ofrecer capacitación y difusión en temas de Gobierno Electrónico y la modernización y descentralización del Estado."

- **PECERT:**
  Es el Sistema de Coordinación de la Administración Pública, creado por RM 360-2009-PCM y es el encargado de liderar los esfuerzos para resolver, anticipar y enfrentar los ciber-desafios y coordinar la defensa ante los ciber ataques, con el fin de proveer a la Nación de una postura Segura en el Ámbito de la Seguridad Informática."

- **Sistema Nacional de Informática (SIN):**
  El Sistema Nacional de Informática fue creado mediante Decreto Legislativo N° 604, y tiene por finalidad planificar, dirigir, normar y organizar las actividades y proyectos que en materia de Informática realiza las entidades de la Administración Pública, todo ello de manera articulada con otros sistemas y áreas de la Administración Pública.
  La oficina Nacional de Gobierno Electrónico e Informática (ONGEI) de la Presidencia del Consejo de Ministros (PCM) es el ente rector del Sistema Nacional de Informática, de acuerdo a lo establecido por el Decreto Legislativo, y concordante con lo dispuesto en el Reglamento de Organización y Funciones de la PCM, aprobado mediante Decreto Supremo N° 063-2007-PCM y sus modificatorias.
  Está conformado por: El Consejo Consultivo Nacional de Informática (CCONI), El Comité de Coordinación Interinstitucional de informática (CCOI); El Comité de Coordinación Interinstitucional de Informática (CCOII); 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 los Gobiernos Regionales; Los Órganos de Informática de las Municipalidades; Los órganos de Informática de los Poderes Públicos; y de los Organismos Autónomos."
  (Consejo Consultivo Nacional de Informática (CCONI):
  "El Consejo Consultivo Nacional de Informática es el órgano de participación del sector no público, en el Sistema Nacional de Informática, encargado de asesor a los órganos y organismos integrantes del Sistema."

Objeto de la propuesta

La iniciativa pretende fortalecer la rectoría del sistema de inteligencia nacional para lograr eficiencia en la producción de inteligencia en materia de seguridad digital, por lo que se precisa las responsabilidades funcionales y orgánicas del SINA y de la DINI en esta materia.

Fundamentación

El desarrollo de las comunicaciones y tecnologías, han generado nuevos problemas en cuanto a su uso y vulnerabilidad; situación que podría afectar desde la seguridad nacional hasta las actividades cotidianas de la población en general, escenario que fuerza la creación y fortalecimiento de políticas públicas destinadas a cautelar la seguridad digital del país, más aun teniendo en cuenta el mundo globalizado en que vivimos donde se genera mucha información para el desarrollo de diversas actividades tales como económicas, sociales, ocasionando

riesgo e incertidumbre en la seguridad digital que amerita una gestión continua y permanente por parte del Estado.

El Decreto Legislativo 1141 - Decreto Legislativo de Fortalecimiento y Modernización del Sistema de Inteligencia Nacional - SINA y de la Dirección Nacional de Inteligencia – DINI; establece el marco jurídico que regula la finalidad, principios, organización, atribuciones, funciones, coordinación, control y fiscalización, que deben observar los componentes del Sistema de Inteligencia Nacional - SINA.

En este sentido, el proyecto de Ley 772/2016-CR, propone modificar el Decreto Legislativo 1141, incorporando la "seguridad digital" en el desarrollo de las actividades del Sistema de Inteligencia Nacional – SINA. A su vez se incorpora en las funciones de la Dirección Nacional de Inteligencia – DINI el tema de seguridad digital y se le permite aprobar y supervisar los programas académicos de formación, capacitación y perfeccionamiento en materia de inteligencia a través de la Escuela Nacional de Inteligencia.

En la Mesa de trabajo se resaltó la importancia que el proyecto de ley, materia de dictamen aborde el tema de seguridad digital (ciberseguridad), como una política pública que en los últimos tiempos ha tomado realce tanto en el ámbito nacional como en otros países. Es que la propuesta aborda aspectos importantes respecto al tema, empezando por definirlo, desarrollando las funciones de la DINI en este ámbito y los lineamientos para su tratamiento, en el marco de sus competencias.

No obstante las observaciones han recaído en la definición que propone el proyecto de ley en la cual no se distinguía claramente las competencias de los organismos nacionales tanto de la Secretaria Gobierno Digital como de la Dirección Nacional de Inteligencia – DINI; se consideró que la definición de seguridad digital era muy amplia y que estaría invadiendo competencias de otros organismos especializados.

El espíritu de la propuesta legislativa radica en incorporar la seguridad digital, en el marco de las competencias de la DINI. Este aspecto quedó perfectamente esclarecido en la segunda mesa de trabajo, en donde los señores representantes de la Presidencia del Consejo de Ministros, expusieron sus recomendaciones, las cuales fueron trabajadas en una reunión sostenida con representantes de la DINI.

No sólo hubo consenso en la definición sino en el contenido del proyecto con las sugerencias que formuló la PCM, considerándose necesario, para mayor claridad, incorporar un artículo en la presente ley encargando a la Presidencia del Consejo de Ministros, como institución competente para que desarrolle la definición de seguridad digital en el ámbito nacional.

La definición, las funciones dadas a la DINI y las demás propuestas que plantea el texto sustitutorio del presente dictamen sobre seguridad digital, conlleva el acuerdo de los organismos involucrados del Poder Ejecutivo y especialistas que participaron en las Mesas de trabajo realizadas por la Comisión de Inteligencia, con sus aportes e información que sustentan la fórmula legal..

Por lo antes señalado se considera pertinente la incorporación del término de Seguridad Digital en el Decreto Legislativo 1141.

Contenido del Texto que propone la Comisión

La Comisión de Inteligencia, recogiendo las recomendaciones de la Presidencia del Consejo de Ministros, de los ministerios e instituciones involucradas, de los expertos y especialistas plantea el siguiente texto sustitutorio:

- Incorpora el numeral 8) del artículo 2 del Decreto Legislativo 1141 definiendo a la seguridad digital como "la situación de confianza en el entorno digital, frente a las amenazas que afectan las capacidades nacionales, a través de la gestión de riesgos y la aplicación de medidas de ciberseguridad y las capacidades de ciberdefensa, alineada al logro de los objetivos del Estado."

- Incorpora el numeral 8.3 al artículo 8 precisando como objetivo del SINA realizar actividades destinadas a alcanzar la seguridad digital en materia de seguridad nacional

- En el numeral 10.1 del artículo 10, en el plan de Plan de inteligencia Nacional se incorpora la seguridad digital y la gestión de riesgos, resaltando que es en el ámbito de la competencia del SINA.

- Por otro lado, en el artículo 17 se incorpora el numeral 17.8 y se amplia la función técnica normativa en materia de inteligencia y contrainteligencia, propia de la Dirección Nacional de Inteligencia – DINI, al desempeño de la función normativa en materia de seguridad digital.

- En el numeral 17.13 del artículo 17 se amplía la función de la DINI a fin de establecer y fortalecer las relaciones de cooperación y asistencia con organismos de inteligencia de otros países, ya que permitirá compartir experiencias y buenas prácticas y promover un enfoque de gestión del riesgo de otros países, además de fomentar el apoyo recíproco entre las fuerzas de seguridad de la región.

- En el Numeral 17.16 se establece como función adicional de la DINI, aprobar y supervisar los programas académicos de formación laboral y profesional, capacitación y perfeccionamiento en materia de inteligencia que se brinden a través de la Escuela Nacional de Inteligencia- ENI, con la finalidad de asegurar una formación integral y de calidad del personal del Sistema de Inteligencia Nacional - SINA, sustentada en principios y valores democráticos. Asimismo, brindar capacitación y formación laboral y profesional al personal del Sistema de Inteligencia Nacional - SINA, a través de la Escuela Nacional de Inteligencia – ENI o mediante suscripción de convenios de cooperación interinstitucional con universidades, institutos tecnológicos y centros de formación de las Fuerzas Armadas y Policía Nacional del Perú y de otros países. En este numeral se acogió la propuesta realizada por la Secretaría de Gestión Pública de la PCM, precisándose que es en el ámbito de su competencia y de conformidad con la ley de la materia.

- En el Numeral 17.17 se establece como función de la DINI realizar actividades y establecer procedimientos destinados a alcanzar la seguridad digital en el ámbito de su competencia y asimismo se agrega un texto complementario que permita que las entidades públicas o privadas se sujeten a tales procedimientos ante amenazas que afectan o que potencialmente puedan afectar las capacidades nacionales.

- Por otro lado, en el artículo 17 se incorpora el numeral 17.18 y se señala como una de las funciones de la Dirección Nacional de Inteligencia – DINI el establecer los procedimientos especiales para la obtención de información en entornos digitales a que se refiere el artículo 32 del presente Decreto Legislativo y para peritajes informáticos. El Poder Judicial a través de convenios interinstitucionales brinda asesoramiento técnico para la elaboración de estos procedimientos.

- Se agrega el numeral 17.19 al artículo 17 facultando a la DINI para suscribir convenios interinstitucionales, en el ámbito de su competencia, a nivel nacional o internacional, así como disponer su modificación, ampliación o resolución en materia de inteligencia, cotrainteligencia y seguridad digital.

- En el artículo 38 se incorpora la protección de identidad del personal y de la actividad de inteligencia en entornos digitales.

- Finalmente, se incorpora la Octava Disposición Complementaria y Final del Decreto Legislativo 1141, en la que se propone que la Dirección Nacional de Inteligencia (DINI) se constituya como coordinador con las entidades nacionales correspondientes elabore el componente del Plan Nacional de Seguridad Digital del Plan de Inteligencia Nacional (PIN). Dicha propuesta se justifica en la necesidad de lograr una visión estratégica en materia de seguridad digital para nuestro país.

- En la Primera Disposición Complementaria y Final de la presente ley se dispone que el Poder Ejecutivo adecúe el Reglamento del Decreto Legislativo 1141, Decreto Legislativo de fortalecimiento y modernización del Sistema de Inteligencia Nacional – SINA y de la Dirección Nacional de Inteligencia – DINI, aprobado mediante Decreto Supremo 016-2014-PCM, a las modificaciones **y definiciones** establecidas en la presente Ley, en el plazo de noventa días calendario siguientes a su entrada en vigencia.

- En la SEGUNDA. Disposición Complementaria y Final se dispone que la Presidencia del Consejo de Ministros, mediante decreto supremo desarrollará la definición de seguridad digital en el ámbito nacional.

Análisis costo – beneficio

La presente iniciativa responde a una necesidad de dotar de mecanismos eficaces a la DINI, a fin de que ésta pueda realizar su trabajo de inteligencia, previniendo los peligros que hoy en día representan la tecnología. Con ello su actividad sería beneficiosa para la sociedad y los ciudadanos. No representa iniciativa de gasto al Estado.

Por las consideraciones expuestas y de conformidad a lo establecido en el inciso b) del Artículo 70 del Reglamento del Congreso de la República, la Comisión de Inteligencia recomienda aprobar el Proyecto de Ley 772/2016-CR, con el siguiente texto sustitutorio:

TEXTO SUSTITUTORIO

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 A FIN DE REGULAR EL TEMA DE LA SEGURIDAD DIGITAL

Artículo 1. Modificación de artículos 2, 8, 10, 17 Y 38, y de la disposición complementaria final octava del Decreto Legislativo 1141, Decreto Legislativo de fortalecimiento y modernización del Sistema de Inteligencia Nacional – SINA y de la Dirección Nacional de Inteligencia – DINI.

Incorpóranse los numerales 8 al artículo 2 y 8.3 al artículo 8; modifícanse el numeral 10.1 del artículo 10 y los numerales 17.8, 17.13, 17.16, 17.17 del artículo 17; asimismo incorpóranse los numerales 17.18, 17.19 y 17.20 a este mismo artículo 17, modifícase el numeral 38.1 del artículo 38 e incorpórase la disposición complementaria final octava al Decreto Legislativo 1141, Decreto Legislativo de Fortalecimiento y Modernización del Sistema de Inteligencia Nacional – SINA y de la Dirección Nacional de Inteligencia – DINI, modificado por Ley 30535, 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:
[...]

8) **Seguridad Digital: Es la situación de confianza en el entorno digital, frente a las amenazas que afectan las capacidades nacionales, a través de la gestión de riesgos y la aplicación de medidas de ciberseguridad y las capacidades de ciberdefensa, alineada al logro de los objetivos del Estado.**

Artículo 8.- Objetivos
El Sistema de Inteligencia Nacional – SINA tiene los siguientes objetivos:
[...]

8.3. Realizar actividades destinadas a alcanzar la seguridad digital en materia de seguridad nacional.

Artículo 10.- Plan de Inteligencia Nacional – PIN
10.1 Para efectos del desarrollo de actividades de inteligencia, contrainteligencia **y seguridad digital, en el ámbito de su competencia,** el Sistema de Inteligencia Nacional – SINA cuenta con el Plan de Inteligencia Nacional – PIN, que contiene los objetivos, políticas, estrategias, **gestión de riesgos** y responsabilidades de sus componentes, relacionados con las amenazas a la seguridad nacional y la identificación de oportunidades favorables a ella, siendo su cumplimiento de carácter obligatorio. Es aprobado por el Consejo de Seguridad y Defensa Nacional en abril del año anterior a su ejecución, a propuesta del ente rector del Sistema de Inteligencia Nacional – SINA."

Art. 17.- Funciones
Son funciones de la Dirección Nacional de Inteligencia – DINI:
[...]

17.8 Constituir la autoridad técnica normativa a nivel nacional en materia de inteligencia, contrainteligencia **y seguridad digital, en el ámbito de su competencia.**

[...]

17.13 Establecer y fortalecer las relaciones de cooperación y **asistencia** con organismos de inteligencia de otros países.

[...]

17.16 En el ámbito de su competencia y de conformidad con la ley de la materia, aprobar y supervisar los programas académicos de formación laboral y profesional, capacitación y perfeccionamiento en materia de inteligencia que se brinden a través de la Escuela Nacional de Inteligencia- ENI, con la finalidad de asegurar una formación integral y de calidad del personal del Sistema de Inteligencia Nacional - SINA, sustentada en principios y valores democráticos. Asimismo, brindar capacitación y formación laboral y profesional al personal del Sistema de Inteligencia Nacional - SINA, a través de la Escuela Nacional de Inteligencia – ENI o mediante suscripción de convenios de cooperación interinstitucional con universidades, institutos tecnológicos y centros de formación de las Fuerzas Armadas y Policía Nacional del Perú y de otros países.

17.17 Realizar actividades y establecer los procedimientos destinados a alcanzar la seguridad digital en el ámbito de su competencia, en concordancia con los principios y objetivos de la actividad de inteligencia establecidos en el presente decreto legislativo. En el caso de amenazas que afectan o que potencialmente afecten las capacidades nacionales, las entidades públicas y privadas se sujetan a dichos procedimientos.

17.18 Establecer los procedimientos especiales para la obtención de información en entornos digitales a que se refiere el artículo 32 del presente decreto legislativo y para peritajes informáticos. El Poder Judicial, a través de convenios interinstitucionales brinda asesoramiento técnico para la elaboración de estos procedimientos.

17.19 Suscribir convenios interinstitucionales, en el ámbito de su competencia, a nivel nacional o internacional, así como disponer su modificación, ampliación o resolución en materia de inteligencia, cotrainteligencia y seguridad digital.

17.20 Las demás establecidas por Ley."

Artículo 38.- Protección de la identidad

38.1 Los procedimientos de protección de identidad del personal y de la actividad de inteligencia, **incluyendo los que se encuentran en entornos digitales,** tienen carácter secreto.

[...]

"DISPOSICIONES COMPLEMENTARIAS FINALES

[...]

OCTAVA.- Elaboración del componente de Seguridad Digital del Plan de Inteligencia Nacional (PIN)
La Dirección Nacional de Inteligencia (DINI) en coordinación con las entidades nacionales correspondientes elabora el componente de Seguridad Digital del Plan de Inteligencia Nacional (PIN)."

DISPOSICIONES COMPLEMENTARIAS FINALES

PRIMERA. Adecuación del Reglamento del Decreto Legislativo 1141.
El Poder Ejecutivo adecúa el Reglamento del Decreto Legislativo 1141, Decreto Legislativo de fortalecimiento y modernización del Sistema de Inteligencia Nacional – SINA y de la Dirección Nacional de Inteligencia – DINI, aprobado mediante Decreto Supremo 016-2014-PCM, a las modificaciones **y definiciones** establecidas en la presente Ley, en el plazo de noventa días calendario siguientes a su entrada en vigencia.

SEGUNDA. Definición de Seguridad Digital en el ámbito nacional
La Presidencia del Consejo de Ministros, mediante decreto supremo desarrollará la definición de seguridad digital en el ámbito nacional.

Salvo mejor parecer
Dese cuenta,
Sala de la Comisión

Lima, 14 de junio de 2017

MESA DIRECTIVA	
	1. **MIYASHIRO ARASHIRO, MARCO ENRIQUE** **Presidente** Fuerza Popular .....
	2. **COSTA SANTOLALLA, GINO FRANCISCO** **Vicepresidente** **Peruanos Por El Kambio** .....
	3. **VILLANUEVA ARÉVALO, CÉSAR** **Secretario** Alianza Para El Progreso Licencia .....

Pleno del Congreso de la República

Lima, 28 de Junio de 2017

En sesión de la fecha, se aprobó en primera votación y se exoneró de la segunda votación. _____

JAVIER ANGELES ILLMANN
Director General Parlamentario (e)
CONGRESO DE LA REPÚBLICA

MIEMBROS TITULARES

4. **APAZA ORDÓÑEZ, JUSTINIANO RÓMULO**
   Frente Amplio Por Justicia, Vida Y Libertad

.....

5. **SALAZAR MIRANDA, OCTAVIO EDILBERTO**
   Fuerza Popular

.....

6. **TUBINO ARIAS SCHREIBER, CARLOS MARIO DEL CARMEN**
   Fuerza Popular

.....

7. **YIKA GARCÍA, LUIS ALBERTO**
   Fuerza Popular

.....

CONGRESO
REPÚBLICA

COMISIÓN DE INTELIGENCIA
Periodo Anual de Sesiones 2016-2017
ASISTENCIA
Vigésima Sesión Ordinaria
Fecha: 14 de junio de 2017
Hora: 14:00 Horas
Sala 4: Martha Hildebrandt Pèrez Treviño-E.V.R.H.T.

MESA DIRECTIVA

1. **MIYASHIRO ARASHIRO, MARCO ENRIQUE**
   Presidente
   Fuerza Popular

2. **COSTA SANTOLALLA, GINO FRANCISCO**
   Vicepresidente
   Peruanos Por El Kambio

3. **VILLANUEVA ARÉVALO, CÉSAR**
   Secretario
   Alianza Para El Progreso — Licencia

MIEMBROS TITULARES

4. **APAZA ORDÓÑEZ, JUSTINIANO RÓMULO**
   Frente Amplio Por Justicia, Vida Y Libertad — Licencia

5. **SALAZAR MIRANDA, OCTAVIO EDILBERTO**
   Fuerza Popular

30

COMISIÓN DE INTELIGENCIA
Periodo Anual de Sesiones 2016-2017
ASISTENCIA
Vigésima Sesión Ordinaria
Fecha: 14 de junio de 2017
Hora: 14:00 Horas
Sala 4: Martha Hildebrandt Pèrez Treviño-E.V.R.H.T.

	**6. TUBINO ARIAS SCHREIBER, CARLOS MARIO DEL CARMEN** Fuerza Popular Licencia
	**7. YIKA GARCÍA, LUIS ALBERTO** Fuerza Popular

31

CONGRESO
REPÚBLICA

JUSTINIANO APAZA ORDOÑEZ
Congresista de la República

"Año de la consolidación del Mar de GRAU"

R/286
CONGRESO DE LA REPÚBLICA
COMISIÓN DE INTELIGENCIA
14:55 p.m.
14/6/2017

Lima, 14 de junio de 2017

OFICIO N° 857-2016-2017-JAO-CR

Señor
MARCO ENRIQUE MIYASHIRO ARASHIRO
Presidente de la Comisión de Inteligencia
Presente

Asunto : Licencia por salud

Referencia : Oficio N° 856-2016-2017-JAO-CR

De mi mayor consideración:

Tengo el agrado de dirigirme a usted, para saludarlo cordialmente y al mismo tiempo solicitarle por especial encargo del señor Congresista **JUSTINIANO ROMULO APAZA ORDOÑEZ**, se sirva otorgar la licencia correspondiente, a la Vigésima Sesión Ordinaria de la Comisión de Inteligencia, del día de hoy miércoles 14 de junio de los corrientes; y tal como informé en el documento de la referencia, señalar que durante mi reunión por motivos de representación congresal tuve una descompensación de salud, motivo por el cual tuve que retirarme y acudir a la clínica correspondiente, hechos que informo para su conocimiento y se otorgue la licencia respectiva.

Sin otro particular, reitero los sentimientos de mi especial consideración y estima personal.

Atentamente,

Manuel Rodolfo Yarlequé Miller
Asesor Congresista Justiniano Apaza Ordóñez

32

CONGRESO DE LA REPÚBLICA
COMISIÓN DE INTELIGENCIA

CONGRESO
REPÚBLICA

JUSTINIANO APAZA ORDOÑEZ
Congresista de la República

"Año de la consolidación del Mar de GRAU"

Lima, 14 de junio de 2017

OFICIO N° 856-2016-2017-JAO-CR

Señor
MARCO ENRIQUE MIYASHIRO ARASHIRO
Presidente de la Comisión de Inteligencia
Presente

Asunto : Licencia

De mi mayor consideración:

Tengo el agrado de dirigirme a usted, para saludarlo cordialmente y al mismo tiempo solicitarle por especial encargo del señor Congresista **JUSTINIANO ROMULO APAZA ORDOÑEZ**, se sirva otorgar la licencia correspondiente, a la Vigésima Sesión Ordinaria de la Comisión de Inteligencia, del día de hoy miércoles 14 de junio de los corrientes; por motivos de representación congresal, toda vez que me encuentro coadyuvando a un grupo de profesores universitarios de la Universidad Nacional San Agustín de Arequipa en sus gestiones para la modificación del artículo 84 de la ley universitaria, límite de edad para jubilarse.

Sin otro particular, reitero los sentimientos de mi especial consideración y estima personal.

Atentamente,

CONGRESO DE LA REPÚBLICA
JUSTINIANO APAZA ORDÓÑEZ

Manuel Rodolfo Yarlequé Miller
Asesor Congresista Justiniano Apaza Ordóñez

33

R/285

CONGRESO DE LA REPÚBLICA
COMISIÓN DE INTELIGENCIA

14/6/17

CONGRESO
REPÚBLICA

JUSTINIANO APAZA ORDOÑEZ
Congresista de la República

"Año de la consolidación del Mar de GRAU"

Lima, 14 de junio de 2017

OFICIO N° 856-2016-2017-JAO-CR

Señor
MARCO ENRIQUE MIYASHIRO ARASHIRO
Presidente de la Comisión de Inteligencia
Presente

Asunto : Licencia

De mi mayor consideración:

Tengo el agrado de dirigirme a usted, para saludarlo cordialmente y al mismo tiempo solicitarle por especial encargo del señor Congresista **JUSTINIANO ROMULO APAZA ORDOÑEZ**, se sirva otorgar la licencia correspondiente, a la Vigésima Sesión Ordinaria de la Comisión de Inteligencia, del día de hoy miércoles 14 de junio de los corrientes; por motivos de representación congresal, toda vez que me encuentro coadyuvando a un grupo de profesores universitarios de la Universidad Nacional San Agustín de Arequipa en sus gestiones para la modificación del artículo 84 de la ley universitaria, límite de edad para jubilarse.

Sin otro particular, reitero los sentimientos de mi especial consideración y estima personal.

Atentamente,

CONGRESO DE LA REPÚBLICA
JUSTINIANO APAZA ORDOÑEZ

Manuel Rodolfo Yarlequé Miller
Asesor Congresista Justiniano Apaza Ordóñez

34

Lima, 14 de junio de 2017

R) 283
CONGRESO DE LA REPÚBLICA
COMISIÓN DE INTELIGENCIA
14 JUN 2017
10:26 PM
RECIBIDO
Firma ..... Hora .....

OFICIO Nº 429 -2016-2017/CVA-CR

Señor Congresista
MARCO ENRIQUE MIYASHIRO ARASHIRO
Presidente de la Comisión de Inteligencia
Congreso de la República

Asunto: Licencia por Salud

De mi consideración,

Me dirijo a usted para saludarlo y al mismo tiempo presenta la licencia del caso por la inasistencia a la Vigésima Sesión Ordinaria – Secreta de la Comisión de Inteligencia, a realizarse el día miércoles 14 de junio de 2017, a las 14:00 horas, en la sala 4 "Martha Hildebrant Pérez Treviño" del edificio "Víctor Raúl Haya de la Torre".

Los motivos son de razón a encontrarme con descanso médico, por cual adjunto el documento que acredita lo expuesto.

Por lo expresado y en virtud de lo establecido por el literal i) del Art. 22 del Reglamento del Congreso de la República. le solicito se sirva considerar la licencia correspondiente.

Sin otro particular me despido de usted, no sin antes expresarles las muestras de mi especial consideración y estima personal.

Atentamente,

CONGRESO DE LA REPÚBLICA - CESAR VILLANUEVA AREVALO

César Villanueva Arévalo
CONGRESISTA DE LA REPÚBLICA

35

Mediante la presente se
[illegible] curso
[illegible] de
[illegible] Raul Flores
[illegible] motivo
[illegible] de mis hijos
[illegible] y
[illegible] especialista
[illegible] 1 - Enero
30 - Junio del 2017
[illegible] pendiente
[illegible].

Se expide la
presente a solicitud de
[illegible].

7 - Junio 2017

Av. Gregorio Escobedo 650
Jesús María, Lima, Perú
Call Center: 219-0000
www.clinicasanfelipe.com

Lima, 13 JUN. 2017

CARTA Nº 192 -2016-2017-CTAS/CR

R/281

CONGRESO DE LA REPÚBLICA
COMISIÓN DE INTELIGENCIA
13 JUN 2017
RECIBIDO
Firma ..... Hora .....

Señor
MARCO ENRIQUE MIYASHIRO ARASHIRO
Presidente de la Comisión de Inteligencia
Presente

De mi consideración:

Tengo el agrado de dirigirme a Ud. para saludarlo cordialmente y a la vez solicitarle tenga a bien extenderme la licencia correspondiente, ya que no podré estar presente en la Sesión de la Comisión bajo su presidencia del día **miércoles 14** del presente mes, por encontrarme en esa fecha en Viaje Oficial fuera del país.

Sin otro particular, hago propicia la oportunidad para expresarle las seguridades de mi consideración y estima.

Atentamente,

CONGRESO DE LA REPÚBLICA · CARLOS TUBINO ARIAS SCHREIBER

CARLOS TUBINO ARIAS SCHREIBER
Congresista de la República

CTAS/Ece.

37

Av. Abancay, Cdra. 2; Edificio Juan Santos Atahualpa, Oficina 401 – Cercado de Lima
Teléfono: 311-7210
ctubino@congreso.gob.pe