Dictamen recaído en el Proyecto de Ley 1776/2021-CR, mediante el cual se propone, con texto sustitutorio, la "Ley que modifica el Decreto de Urgencia 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone de medidas para su fortalecimiento, para consolidar el Centro Nacional de Seguridad Digital".

COMISIÓN DE CIENCIA, INNOVACIÓN Y TECNOLOGÍA
Período de Sesiones 2021-2022

DICTAMEN 20

Señora presidenta:

Ha sido remitido para estudio y dictamen de la Comisión de Ciencia, Innovación y Tecnología, en atención al Acuerdo 340-2021-2022/CONSEJO-CR[1] del Consejo Directivo del 11 de abril de 2022 y de conformidad con los artículos 34 y 77 del Reglamento del Congreso de la República, el **Proyecto de Ley 1776/2021-CR[2]**, mediante el cual se propone garantizar la ejecución de operaciones de ciberseguridad y seguridad digital a través de un Centro Nacional de Ciberseguridad; iniciativa legislativa que fuera actualizada[3] a solicitud del **grupo parlamentario Podemos Perú (PP)**, a iniciativa de los **congresistas José Luna Gálvez, Carlos Anderson Ramírez y Digna Calle Lobatón**.

La ingeniera **Marushka Chocobar Reyes**, Secretaria de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros, se presentó ante el Pleno de la Comisión de Ciencia, Innovación y Tecnología, en su Vigésima Segunda Sesión Ordinaria del 8 de junio de 2022, para sustentar la necesidad de emitir la *Ley que declara de interés nacional y necesidad pública el fortalecimiento del Centro Nacional de Seguridad Digital para garantizar la confianza en el entorno digital del país*, propuesta por la Comisión de Defensa Nacional, Orden Interno, Desarrollo Alternativo y Lucha Contra las Drogas, aprobada por el Congreso de la República y observada por el Poder Ejecutivo.

Luego del análisis y debate correspondiente, la Comisión de Ciencia, Innovación y Tecnología, en su Vigésima Cuarta Sesión Ordinaria [**modalidad virtual**], del 6 de julio de 2022, realizada en la sala de reuniones de la plataforma[4] de videoconferencia del Congreso de la República, acordó por **UNANIMIDAD/MAYORÍA** aprobar[5] el dictamen recaído en el Proyecto de Ley 1776/2021-CR, mediante el cual se propone, con texto sustitutorio, la *Ley que modifica el Decreto de Urgencia 007-2020, Decreto de*

---

[1] https://bit.ly/3xGRk7B [Página 86]

[2] https://wb2server.congreso.gob.pe/spley-portal-service/archivo/MjI1NzY=/pdf/PL_1776

[3] De conformidad con lo acordado por el Consejo Directivo en su sesión realizada el 11 de abril de 2022, se procedió a actualizar el Proyecto de Ley 6544/2020-CR, asignándole el número 1776/2021-CR.

[4] Según lo establecido en los artículos 27-A y 51-A del Reglamento del Congreso de la República. Se utilizó la herramienta de *Microsoft Teams*.

[5] **Se solicitó autorización para la ejecución de los acuerdos**, aprobándose por **UNANIMIDAD, considerando la dispensa del trámite de aprobación del acta** y de su lectura.

Urgencia que aprueba el Marco de Confianza Digital y dispone de medidas para su fortalecimiento, para consolidar el Centro Nacional de Seguridad Digital, **con el voto favorable de los señores congresistas:** ----------
---

---.

Presentaron licencia para la presente sesión los señores congresistas: ----------
---

Se aprueba el presente dictamen por las siguientes consideraciones:

1. Para contribuir con el fortalecimiento del Centro Nacional de Seguridad Digital (CNSD) a cargo de la Secretaría de Gobierno y Transformación Digital, de la Presidencia del Consejo de Ministros, teniendo en cuenta que se tiene dos años de crisis sanitaria desde la creación del CNSD, donde el nivel de digitalización de los países en el mundo y sobre todo en el Perú ha avanzado, sin embargo, aún existen brechas en cuanto a conectividad y en mejorar la atención de los servicios públicas a la ciudadanía. Según el último informa del INEI da cuenta que las personas que se encuentran en condiciones de muy pobres, tienen 87% de conectividad a través de celulares; las personas que se encuentran en la condición de pobreza tienen 90% de conectividad a través de sus dispositivos móviles. Esto implica que, a pesar de la existencia de brechas, el Estado debe seguir impulsando la seguridad y confianza digital en las personas, en las empresas y en las organizaciones, para proteger sus derechos y activos digitales.

2. Impulsar la articulación de la unidad funcional de Confianza Digital con el Centro Nacional de Seguridad Digital, ambos a cargo de la Secretaría de Gobierno y Transformación Digital, de una manera más rápida, ágil, eficiente y además focalizada, además, de optimizar la inversión que se viene realizando para implementar la Plataforma Nacional de Gobierno Digital.

3. Finalmente, para consolidar las acciones en seguridad y confianza digital para la protección de los derechos y activos digitales de la ciudadanía frente a los riesgos digitales. Quedando pendiente las siguientes acciones a realizar por el Poder Ejecutivo: aprobar la Política Nacional de Seguridad y Confianza Digital; aprobar la Estrategia de Seguridad y Confianza Digital; fortalecer la Mesa de Confianza Digital; realizar una evaluación nacional de madurez técnica, administrativa, organizativa y legal en Seguridad y Confianza digital de todas las entidades públicas.

I. SITUACIÓN PROCESAL

a. Antecedentes

Período Parlamentario 2016-2021

El **Proyecto de Ley 6544/2020-CR**[6] fue presentado al Área de Trámite Documentario el 26 de octubre de 2020; fue decretado el 2 de noviembre y recibido el 3 del mismo mes por la Comisión de Defensa Nacional, Orden Interno, Desarrollo Alternativo y Lucha Contra las Drogas, como única comisión dictaminadora.

El dictamen[7] recaído en el **Proyecto de Ley 6544/2021-CR** fue aprobado por unanimidad en la Décima Octava Sesión Ordinaria de la Comisión de Defensa Nacional, Orden Interno, Desarrollo Alternativo y Lucha Contra las Drogas, del 7 de diciembre de 2020, mediante el cual se propone, con texto sustitutorio, la *Ley que declara de interés nacional y necesidad pública el fortalecimiento del Centro Nacional de Seguridad Digital para garantizar la confianza en el entorno digital del país.*

El Pleno del Congreso de la República lo debatió el 9 de junio del 2021, presentándose un texto sustitutorio[8] como consecuencia del debate, siendo aprobado en primera votación[9] y por acuerdo dispensado su segunda votación[10]. El Congreso de la República remitió la Autógrafa[11] de la Ley al Poder Ejecutivo el 25 de junio de 2021.

El Poder Ejecutivo, en aplicación del artículo 108 de la Constitución Política del Perú, observó la Autógrafa de Ley, mediante el Oficio N° 462-2021-PR[12], de fecha 19 de julio de 2021, con el objeto de proponer textos alternativos y ajustes para garantizar su concordancia con la Constitución Política y el marco normativo vigente.

Finalmente, al concluir el Período Parlamentario 2016-2021, todos los proyectos de ley, dictámenes y observaciones del Poder Ejecutivo fueron derivados al archivo,

---

[6] https://wb2server.congreso.gob.pe/spley-portal-service/archivo/MjI1NzY=/pdf/PL_1776

[7] https://leyes.congreso.gob.pe/Documentos/2016_2021/Dictamenes/Proyectos_de_Ley/06544DC07MAY20210115.pdf

[8] https://leyes.congreso.gob.pe/Documentos/2016_2021/Texto_Sustitutorio/Proyectos_de_Ley/TS06544-20210609.pdf

[9] https://leyes.congreso.gob.pe/Documentos/2016_2021/Asistencia_y_Votacion/Proyectos_de_Ley/AV0654420210609.pdf

[10] https://bit.ly/3bhyrAo

[11] https://bit.ly/3bgEUf9

[12] https://bit.ly/3Qv4pJX

incluyendo el Oficio N° 462-2021-PR, observación a la Autógrafa de la *Ley que declara de interés nacional y necesidad pública el fortalecimiento del Centro Nacional de Seguridad Digital para garantizar la confianza en el entorno digital del país*.

Período Parlamentario 2021-2026

El Consejo Directivo, a solicitud[13] del grupo parlamentario Podemos Perú (PP), con Acuerdo 340-2021-2022/CONSEJO-CR, del 11 de abril de 2022, actualizó el **Proyecto de Ley 6544/2020-CR** y se le asignó la denominación de **Proyecto de Ley 1776/2021-CR**, mediante el cual se propone garantizar la ejecución de operaciones de ciberseguridad y seguridad digital a través de un Centro Nacional de Ciberseguridad.

El **Proyecto de Ley 1776/2021-CR** [**Actualizado**] ingresó al Área de Trámite Documentario el 21 de abril de 2022 y fue decretado el 27 del mismo mes a la Comisión de Defensa Nacional, Orden Interno, Desarrollo Alternativo y Lucha Contra las Drogas y a la Comisión de Ciencia, Innovación y Tecnología, como primera y segunda comisión dictaminadora, respectivamente; siendo recibido por dichas comisiones al día siguiente.

En consecuencia, el pronunciamiento de la Comisión de Ciencia, Innovación y Tecnología incluirá en su fundamentación todo lo actuado a la fecha por la Comisión de Defensa Nacional, Orden Interno, Desarrollo Alternativo y Lucha Contra las Drogas y las observaciones planteadas por el Poder Ejecutivo a la Autógrafa de la *Ley que declara de interés nacional y necesidad pública el fortalecimiento del Centro Nacional de Seguridad Digital para garantizar la confianza en el entorno digital del país*.

b. Opiniones solicitadas

Se han cursado las siguientes solicitudes de opinión:

FECHA	INSTITUCIÓN	DOCUMENTO	RESPUESTAS
29-ABR-2022	Presidencia del Consejo de Ministros (PCM)	Oficio 707-2021-2022-CCIT/CR	**SI**
29-ABR-2022	Secretaría de Gobierno y Transformación Digital (SGTD)	Oficio 708-2021-2022-CCIT/CR	NO
29-ABR-2022	Ministerio de Defensa	Oficio 709-2021-2022-CCIT/CR	NO

[13] Con Oficio N° 39-2021-2022/GPPP-CR, de fecha 16 de diciembre de 2021.

29-ABR-2022	Ministerio del Interior	Oficio 709-2021-2022-CCIT/CR	NO
24-MAY-2022	Cámara de Comercio Americana del Perú (AMCHAM)	Carta GG-528-22 **Remitido a iniciativa propia**	**SI**
08-JUN-2022	Sociedad de Comercio Exterior del Perú (COMEXPERÚ)	Carta N° 138-2022/GG/COMEXPERU **Remitido a iniciativa propia**	**SI**

c. Opiniones recibidas

Para la evaluación del Proyecto de Ley 1776/2021-CR se recibieron las siguientes opiniones:

OPINIÓN DE LA PRESIDENCIA DEL CONSEJO DE MINISTROS

El Presidencia del Consejo de Ministros (PCM), a través de su Secretario General, señor **Carlos Alberto Cavagnaro Pizarro**, mediante Oficio N° D001123-2022-PCM-SG[14], de fecha 13 de mayo de 2022, adjunta la Nota de Elevación N° D000219-2022-PCM-OGAJ y el Informe N° 1080-2021-PCM-OGAJ de la Oficina General de Asesoría Jurídica de la Presidencia del Consejo de Ministros, **ratificándose en las observaciones formuladas a la Autógrafa** de la *Ley que declara de interés nacional y necesidad pública el Fortalecimiento del Centro Nacional de Seguridad Digital para garantizar la confianza en el entorno digital del país*, norma que se origina con el Proyecto de Ley 1776/2021-CR [Actualizado].

OPINIÓN DE LA CÁMARA DE COMERCIO AMERICANA DEL PERÚ

El Director Ejecutivo de la Cámara de Comercio Americana del Perú, señor Aldo Defilippi, mediante Carta N° GG-528-22[15], de fecha 24 de mayo de 2022, presenta las siguientes observaciones al Proyecto de Ley 1776/2021-CR:

> *"[...] observamos que en la Disposición Complementaria Transitoria Única del Proyecto se dispone que el Ministerio de Defensa "priorizará y coordinará las medidas necesarias para salvaguardar la seguridad del ciberespacio, con el único objetivo de garantizar la integridad y confidencialidad de los activos en las infraestructuras pertenecientes al estado, organizaciones privadas y ciudadanos en general".*

[14] https://bit.ly/3HELPuJ

[15] https://bit.ly/3y9ykQH

*No obstante, **el texto del Proyecto -ni tampoco su Exposición de Motivos- detallan o dan, al menos, alcances sobre qué tipos de "medidas necesarias" serán las que se pretenden irrogar al Ministerio de Defensa, sobre todo de cara a las infraestructuras de organizaciones privadas y ciudadanos en general; ni qué elementos compondrán las "infraestructuras" de una organización privada y ciudadanos en general**.*

*Dicha redacción no solo es amplia e imprecisa, sino que no se encuentra adecuadamente sustentada y; por el contrario, **podría generar múltiples intromisiones innecesarias por parte de una entidad pública, el Ministerio de Defensa, hacia el sector privado**.*

[…]

Finalmente, **es esencial que se elimine, en la Disposición Complementaria Transitoria Única del Proyecto**, la alusión al sector privado y ciudadanos en general. Con ello, ni futuros gobiernos, ni privados podrán bloquear el contenido de la red, la libertad de empresa ni demás libertades fundamentales; evitándose que se interpreten o emitan regulaciones que atenten contra nuestros principios democráticos, tal como lo padecen regímenes autoritarios. ***[…]***"

[**Subrayado y resaltado es nuestro**]

OPINIÓN DE LA SOCIEDAD DE COMERCIO EXTERIOR DEL PERÚ

La Sociedad de Comercio Exterior del Perú (COMEXPERU), a través de su gerente general, la señora **Jéssica Luna Cárdenas**, mediante Carta N° 138-2022/GG/COMECPERÚ, de fecha 8 de junio de 2022, presenta las siguientes observaciones al Proyecto de Ley 1776/2021-CR:

***"[…]** advertimos que en la Disposición Complementaria Transitoria Única del Proyecto se dispone que el Ministerio de Defensa "priorizará y coordinará las medidas necesarias para salvaguardar la seguridad del ciberespacio, con el único objetivo de garantizar la integridad y confidencialidad de los activos en las infraestructuras pertenecientes al estado, organizaciones privadas y ciudadanos en general". Sin embargo, de la revisión del texto del Proyecto y de su exposición de motivos, no se advierte mayor detalle con relación a (i) qué tipos de "medidas necesarias" serán las que se pretenden irrogar al Ministerio de Defensa, sobre todo de cara a las infraestructuras de organizaciones privadas y ciudadanos en general; ni (ii) qué elementos compondrán las "infraestructuras" de una organización privada y ciudadanos en general.*

La fórmula legal propuesta no solo es amplia e imprecisa, sino que no se encuentra adecuadamente sustentada y; por el contrario, podría generar múltiples intromisiones innecesarias por parte de una entidad pública, el Ministerio de Defensa, para la industria.

[…]

Por ende, ***resulta imperante que se elimine, en la Disposición Complementaria Transitoria Única del Proyecto****, la alusión al sector privado y ciudadanos en general. Con ello, ni futuros gobiernos, ni privados podrán bloquear el contenido de la red, vulnerar la libertad de empresa ni demás libertades fundamentales; evitándose que se interpreten o emitan regulaciones que atenten contra nuestros principios democráticos ".*

[Resaltado y subrayado es nuestro]

III. CONTENIDO DE LA PROPUESTA

El proyecto de ley, materia de estudio, cumple con los requisitos formales señalados en el artículo 75 y en el numeral 2 del artículo 76 del Reglamento del Congreso de la República, y propone un texto legal con el título "Ley que garantiza la ejecución de operaciones de ciberseguridad y seguridad digital a través de un Centro Nacional en Ciberseguridad".

La iniciativa legislativa se compone de cuatro artículos, tres disposiciones complementarias finales; tres disposiciones complementarias modificatorias; una disposición complementaria transitoria; y una disposición complementaria derogatoria.

El proyecto tiene por objeto (artículo 1) establecer medidas de carácter excepcional que garanticen la seguridad en el ciberespacio, frente a las amenazas y ataques que afecten la seguridad nacional, para la ejecución de operaciones de ciberseguridad y seguridad digital a través del Centro Nacional de Ciberseguridad del Perú (CENACI). El ámbito de aplicación (artículo 1) de la ley serían todas las entidades de la Administración Pública comprendidas en el Artículo 1 del Título Preliminar del Texto Único Ordenado de la Ley 27444, Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo 006- 2017-JUS, a las organizaciones de la sociedad civil, sectores económicos y de servicios, ciudadanos y academia.

La iniciativa propone los siguientes objetivos (artículo 3): (1) Asegurar el máximo nivel de seguridad de la información en el ciberespacio y en la infraestructura del Estado. (2) Generar mecanismos de defensa y protección en el ciberespacio, de los

intereses nacionales, los activos críticos nacionales y recursos claves de la nación, frente a las amenazas o los ataques que afecten la seguridad nacional. (3) Promover y garantizar la transparencia y seguridad digital de las entidades de la Administración Pública a los ciudadanos. (4) Promover la creación de un Centro Nacional de Ciberseguridad del Perú (CENACI), con el propósito de hacer frente a amenazas y ataques en el ciberespacio. Asimismo, se propone definiciones (artículo 4) respecto a: ciberseguridad, activos en la infraestructura del Estado, seguridad digital y gobierno digital.

En cuanto a las disposiciones complementarias finales, en la primera se declara de interés nacional para la creación del Centro Nacional de Ciberseguridad del Perú (CENACI); en la segunda se dispone la gestión y coordinación interinstitucional; y en la tercera se dan disposiciones respecto al reglamento. Asimismo, para la ejecución de la norma propuesta, en las tres disposiciones complementarias modificatorias, se contempla la modificación del Decreto Legislativo 1412, Ley de Gobierno Digital; la modificación del Decreto de Urgencia 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digita; así como la modificación del Decreto de Urgencia 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento. En la única disposición complementaria transitoria se propone la adecuación de la ley encargando al Ministerio de Defensa su implementación; y en la única disposición complementaria derogatoria se deroga el artículo 7 del Decreto de Urgencia 007-2020.

El autor de la iniciativa sustenta su propuesta, en la sección "*Exposición de Motivos*", detallando un análisis técnico y legal que parte por lo expresado en la Constitución Política del Perú que instituye que la defensa de la persona humana y el respeto de su dignidad son el fin supremo de la sociedad y del Estado; y que son deberes primordiales del Estado proteger a la población de las amenazas contra su seguridad. De otro lado, también protege que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar; ni que se atente contra el secreto y a la inviolabilidad de sus comunicaciones y de documentos.

Por otro lado, se sustenta con la Ley 30999 Ley de Ciberdefensa, que tiene como finalidad la defensa y protección de la soberanía. Dicha norma señala que la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno y Transformación Digital, es el ente rector de la seguridad digital. Cabe mencionar también que la Política de Seguridad y Defensa Nacional, aprobada por Decreto Supremo 012-2017-DE, identifica como sujetos de la Seguridad y Defensa Nacional al Estado y a la persona humana; y, como objetos de la misma, a la soberanía, la

independencia y la integridad territorial, el Estado de derecho y los intereses nacionales, además la paz social y la protección de los derechos fundamentales.

Se destaca que a pesar de los avances que el Estado Peruano ha venido realizando en los últimos años respecto a la seguridad digital, la pandemia del COVID-19 ha desnudado las falencias que tenemos como Estado; en ese sentido, se requiere también un cambio de paradigma en la cooperación público privada, para afrontar a los cibercriminales que aprovechan rápidamente los nuevos vectores de ataque y se benefician de los vacíos en la cooperación de las fuerzas del orden público en las diferentes jurisdicciones, dada la naturaleza inherentemente transnacional de sus actividades maliciosas, ha traído consigo un aumento de ataque cibernético.

También incluye una sección titulada "*Efectos de la vigencia de la norma en la legislación nacional*", donde se precisa que la presente ley no colisiona con la legislación vigente, sino se ampara en el respeto irrestricto de la Constitución Política del Perú. También se incluye el "*Análisis costo – beneficio*" en donde el autor señala que el Proyecto de Ley 1776/2021-CR *no irrogará gasto al erario nacional,* [solo] *tiene como finalidad poner de manifiesto ante el Poder Ejecutivo la importancia de declarar de interés nacional y necesidad pública la creación del Centro Nacional de Ciberseguridad del Perú, cuyo beneficio está relacionado a la protección de la nación respecto a la ciberseguridad, y de esa manera manejarse a la luz de los tiempos que demanda con urgencia contar con una agencia especializada en ciberseguridad*.

Y, finalmente, señala su "*Vinculación con el Acuerdo Nacional*", precisando que la presente norma se enmarca en las políticas del Acuerdo Nacional números 7, 9 y 20.

IV. MARCO NORMATIVO

El proyecto de ley se sustenta en el siguiente marco normativo, que propone lineamientos relacionados con el Gobierno Digital, Transformación Digital, Marco de Confianza Digital y Ciberseguridad:

- Constitución Política del Perú.
- Ley 29158, Ley Orgánica del Poder Ejecutivo.
- Ley 30999, Ley de Ciberdefensa.
- Ley 30618, Ley que modifica el Decreto Legislativo 1141, Decreto Legislativo de Fortalecimiento y Modernización del Sistema de Inteligencia Nacional (SINA) y de la Dirección Nacional de Inteligencia (DINI), a fin de regular la Seguridad Digital.
- Decreto Supremo 012-2017-DE, Decreto Supremo que aprueba la Política de Seguridad y Defensa Nacional.

- Decreto Supremo 022-2017-PCM, Decreto Supremo que aprueba el Reglamento de Organización y Funciones (ROF) de la Presidencia del Consejo de Ministros (PCM) y su modificatoria.
- Decreto Legislativo 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital.
- Decreto Supremo 050-2018-PCM, Decreto Supremo que establece la definición de Seguridad Digital de ámbito nacional.
- Texto Único Ordenado de la Ley 27444, Ley del Procedimiento Administrativo General, aprobado mediante Decreto Supremo 004- 2019-JUS.
- Decreto de Urgencia 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital.
- Decreto de Urgencia 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.
- Decreto de Urgencia 025-2020, Decreto de Urgencia que dispone medidas urgentes destinadas a reforzar el sistema de vigilancia y respuesta sanitaria.
- Decreto Supremo 008-2020-SA, Decreto Supremo que declara en Emergencia Sanitaria a nivel nacional por el plazo de noventa (90) días calendario y dicta medidas de prevención y control del COVID-19.
- Decreto Supremo 044-2020-PCM, Decreto Supremo que declara Estado de Emergencia Nacional por las graves circunstancias que afectan la vida de la Nación a consecuencia del brote del COVID-19.
- Decreto Supremo 080-2020-PCM, Decreto Supremo que aprueba la reanudación de actividades económicas en forma gradual y progresiva dentro del marco de la declaratoria de Emergencia Sanitaria Nacional por las graves circunstancias que afectan la vida de la Nación a consecuencia del COVID-19.
- Decreto Legislativo 1497, Decreto Legislativo que establece medidas para promover y facilitar condiciones regulatorias que contribuyan a reducir el impacto en la economía peruana por la Emergencia Sanitaria producida por el COVID-19.

V. ANÁLISIS DE LA PROPUESTA LEGISLATIVA

Para el análisis de la iniciativa legislativa, la Comisión utilizará la metodología mayéutica, consistente en realizar preguntas sobre la propuesta legislativa, que nos permitirá identificar y evaluar la existencia, o no, de materia legislable y someterla a la evaluación de su viabilidad y de las alternativas de su implementación a través de una norma.

Entonces, siguiendo el método de evaluación elegido por la Comisión, se formulan las siguientes interrogantes:

i) ¿Cuáles fueron las razones de la Comisión de Defensa Nacional, Orden Interno, Desarrollo Alternativo y Lucha Contra las Drogas que motivaron la aprobación del Proyecto de Ley 6544/2020-CR[16]?

ii) ¿Cuáles fueron las razones del Poder Ejecutivo que motivaron observar la Autógrafa de la Ley derivada del Proyecto de Ley 6544/2020-CR[17]?

iii) ¿Por qué es necesario una norma de fortalecimiento del Centro Nacional de Seguridad Digital?

iv) ¿Se requiere perfeccionar la iniciativa legislativa?

A continuación, se da respuesta a cada una de ellas.

i. ¿Cuáles fueron las razones de la Comisión de Defensa Nacional, Orden Interno, Desarrollo Alternativo y Lucha Contra las Drogas que motivaron la aprobación del Proyecto de Ley 6544/2020-CR?

El **Proyecto de Ley 6544/2020-CR** fue presentado al Área de Trámite Documentario el 26 de octubre de 2020; fue decretado el 2 de noviembre y recibido el 3 del mismo mes por la Comisión de Defensa Nacional, Orden Interno, Desarrollo Alternativo y Lucha Contra las Drogas [en adelante Comisión de Defensa Nacional], como única comisión dictaminadora.

El dictamen[18] recaído en el **Proyecto de Ley 6544/2020-CR** fue aprobado por unanimidad en la Décima Octava Sesión Ordinaria de la Comisión de Defensa Nacional, del 7 de diciembre de 2020, mediante el cual se propone, con texto sustitutorio, la *Ley que declara de interés nacional y necesidad pública el fortalecimiento del Centro Nacional de Seguridad Digital para garantizar la confianza en el entorno digital del país.*

La Comisión de Defensa Nacional si bien solicitó opiniones a la Presidencia del Consejo de Ministros, al Ministerio del Interior, al Ministerio de Defensa, al Ministerio de Transportes y Comunicaciones, al Ministerio de Justicia y Derechos Humanos, a la Superintendencia de Banca Seguros y AFPs y a la Asociación de

---

[16] Iniciativa actualizada y denominada como Proyecto de Ley 1776/2021-CR.

[17] Iniciativa actualizada y denominada como Proyecto de Ley 1776/2021-CR.

[18] https://leyes.congreso.gob.pe/Documentos/2016_2021/Dictamenes/Proyectos_de_Ley/06544DC07MAY20210115.pdf

Bancos del Perú, solo consigna en su dictamen la opinión de la Dirección de Inteligencia Nacional (DINI), quien recomienda *la integración del Centro Nacional de Ciberseguridad del Perú - CENACI al Sistema de Defensa Nacional, lo que podría materializarse a través de la creación de un Sistema de Ciberseguridad Nacional o Sistema Nacional de Seguridad Digital*, además, de encargar a la Comisión Especial Multisectorial por designar la revisión integral de los dispositivos vigentes, a fin de evitar confusiones futuras por una interpretación errónea a lo ya conocido e implementado en el Estado sobre la materia; y, que la creación CENACI debería realizarse sobre la base del Centro Nacional de Seguridad Digital, creado mediante el Decreto de Urgencia 007-2020.

Asimismo, la Comisión de Defensa Nacional desarrolló dos reuniones para evaluar el Proyecto de Ley 6544/2020-CR:

- En la primera reunión [04.NOV.2020] participaron funcionarios de la Secretaría de Gobierno y Transformación Digital conjuntamente con los asesores de la Comisión, **precisando que ya existe un Centro Nacional de Seguridad Digital (CNSD), creado con el Decreto de Urgencia 007-2020**.
- En la segunda reunión [24.NOV.2020] participaron funcionarios de la Presidencia del Consejo de Ministros, de la Secretaria de Gobierno y Transformación Digital, del Ministerio de Defensa, de la Dirección Nacional de Inteligencia, de la Superintendencia de Banca, Seguros y AFPs, y de la Asociación de Bancos del Perú - ASBANC.
  En esta reunión se **presentaron observaciones** a las siguientes disposiciones: artículos 3, 4, primera y tercera disposición complementaria final del proyecto de ley; además, respecto al DU 007-2020, propusieron modificar los artículos 8, 9 y 11, **concluyendo que es viable la iniciativa legislativa con las respectivas modificaciones**.

Así también, la Comisión de Defensa Nacional analizó la propuesta considerando los siguientes aspectos:

a. Respecto a las definiciones de Ciberseguridad y Seguridad Digital

Precisan que la Unión Internacional de Telecomunicaciones (UIT), organismo especializado para las tecnologías de la información y la comunicación, define a la *ciberseguridad* como *la colección de herramientas, políticas, directrices, enfoques de gestión de riesgos, acciones, capacitaciones, mejores prácticas, garantía y tecnologías que se pueden utilizar para proteger la disponibilidad, integridad y confidencialidad de los activos en los infraestructuras pertenecientes al gobierno, organizaciones privadas y ciudadanos. Estos activos incluyen dispositivos informáticos conectados, personal,*

infraestructura, aplicaciones, servicios, sistemas de telecomunicaciones y datos en el entorno cibernético.

Precisan también que, el Decreto Legislativo 1412, Ley de Gobierno Digital, así como el Decreto Supremo 050-2018- PCM, que aprueba la definición de seguridad digital en el ámbito nacional, señalando en su artículo 30 que, la *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 entamo. Se sustenta en la articulación con actores del sector público, sector privado y otros quienes apoyan en la implementación de controles, acciones y medidas*.

b. Una mirada al Perú en el contexto mundial de la seguridad digital

En esta sección, la Comisión de Defensa Nacional hace un análisis del avance vertiginoso del uso de las nuevas tecnologías para digitalizar los servicios públicos y privados, incrementándose paralelamente los ataques y amenazas digitales que afectan la seguridad y privacidad, vulnerando derechos fundamentales de los ciudadanos.

Sustentan su análisis en los siguientes documentos: Reporte de Ciberseguridad-2020[19]; Informe de Cibercrimen Threat Metrix; Informe del Observatorio de la Ciberseguridad en América Latina y el Caribe del año 2016; Microsoft Security lntelligence Report del 2017; Estadísticas reportadas por Kaspersky Lab; Encuesta Global de Software de BSA de junio 2018; y el Reporte de Ciberseguridad: Riesgos, Avances y el Camino a seguir en América Latina y el Caribe del 2020. En esa línea, refiere la Comisión que, en los últimos años nuestro país viene sufriendo las consecuencias de los ciberataques producto del incremento en las interacciones por parte de las personas, entidades públicas y empresas en el entorno digital; así tenemos, por ejemplo:

1. Según el reporte de ESET Security Report - Latinoamérica 2019, el Perú es el segundo país de América Latina más afectado por incidentes de seguridad (71 %), solo después de México (72%). Asimismo, es el segundo país con mayor presencia de variantes de Ransomware (204).
2. Entre los principales ciberataques se encuentra el acceso indebido (61%), el robo de información (58%) y la privacidad de la información (48%).

[19] BID-OEA: Reporte de Ciberseguridad-2020-BID-OEA.

3. Dos de cada tres empresas sufrieron un incidente de seguridad durante el año 2018, y el 40% sufrió una infección con códigos maliciosos, siendo el incidente más recurrente.
4. Ataque cibernético al Banco de Crédito del Perú en el año 2018, en el cual accedieron a datos de identificación personal de clientes de dicho banco (números de tarjeta, cuentas, saldos).
5. Ataque cibernético al sector financiero de alcance mundial, que afectó la banca peruana en agosto de 2018, debiendo suspender o limitar algunos servicios financieros como parte de los procedimientos de respuesta a incidentes de seguridad, según lo informado por la Superintendencia de Banca, Seguros y AFP (SBS).
6. Incremento en un 600% de los ciberataques según la Asociación de Bancos del Perú (ASBANC).

Por otro lado, según la División de Investigación de Delitos de Alta Tecnología (DIVINDAT) de la Policía Nacional del Perú, conforme a los casos atendidos, se había evidenciado un incremento de delitos en el entorno digital. Por lo general, consisten en la clonación de tarjetas, acoso cibernético, espionaje cibernético, robo de información por medio de páginas web falsas o fraudulentas, chantaje, extorsión, difamación, estafas, comercio electrónico de pornografía infantil, entre otras modalidades; lo que afecta tanto a los ciudadanos como a organizaciones del sector público y privado.

c. La crisis sanitaria mundial y sus efectos en la seguridad digital

La Comisión de Defensa Nacional refiere que, la Organización para la Cooperación y Desarrollo Económico (OCDE) en el documento *Manejo del riesgo de seguridad digital en tiempos de COVID-19* ha sido clara en señalar que la propagación del COVID-19, había creado condiciones favorables para que agentes maliciosos ataquen a organizaciones, empresas, hospitales y personas; aprovechando por un lado, la carencia de buenas prácticas de seguridad digital, y, por otro, las condiciones propias de estrés ante la crisis económica y social que conlleva el avance del virus.

d. Algunas estadísticas respecto a la confianza digital en el Perú

La Comisión de Defensa Nacional refiere que, según estadísticas de la Cámara Peruana de Comercio Electrónico (CAPECE), se sabe que el comercio electrónico en el Perú creció un 30% en el año 2018, ascendiendo a un monto de $3,100 millones, estimando para el 2019 un crecimiento entre el 40% y 45% y un monto aproximado de $4,000 millones. Adicionalmente, según datos del Instituto Nacional de Estadística e Informática (INEI) a setiembre 2019 en el

Perú la población de 6 años a más de edad que hace uso de internet es de 59.8%, el 76.8% de adolescentes de 12 a 18 años de edad, el 88.5% de los jóvenes de 19 a 24 años, y el 72.5% de adultos entre los 25 y 40 años, siendo estos grupos la población que más accede a internet.

Un aspecto importante a considerar es el porcentaje de población que hace uso de Internet a través del teléfono celular, que es el 82.6%.Con respecto a las actividades que realiza la población en internet es mayormente para comunicarse (90.2%), obtener información (89.3%) y en actividades de entretenimiento (85.5%), operaciones en banca electrónica (14.5%), transacciones con entidades públicas (12%), comprar productos o servicios (13.4%), y vender productos o servicios (4.1%), descargar antivirus y aplicativos o software (23.3%). Lo anterior, evidencia que, para el caso peruano, la población viene incrementado su presencia e interacción en el entorno digital, aumentaron las transacciones, las ventas y compras, lo cual es producto de una mayor conectividad, que tanto entidades públicas como empresas privadas vienen ofreciendo canales digitales para atender dicha demanda.

e. Normativa nacional respecto a la seguridad digital y gobierno digital

La Comisión de Defensa Nacional refiere que, el Perú tiene vigente las siguientes normas:

- El Decreto Legislativo 1412, Ley de Gobierno Digital.
- El Decreto de Urgencia 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital.
- El Decreto de Urgencia 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.
- Ley 30999, Ley de Ciberdefensa.

Luego del análisis realizado la Comisión de Defensa Nacional propone un texto sustitutorio con las siguientes consideraciones:

- Ratificar el deber constitucional del Estado peruano de proteger a la población ante las amenazas contra su seguridad[20], en este caso a aquellas que provienen del entorno digital.
- La propuesta normativa responde a la necesidad constituir al Perú en uno de los primeros países de la región que cuenta con un Centro Nacional de Seguridad Digital, poniendo como valor principal a los ciudadanos.

[20] Artículo 44 de la Constitución Política del Perú.

- La propuesta reafirma que la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros lidera los procesos de innovación tecnológica y de transformación digital del país, además, es el ente rector del Sistema Nacional de Transformación Digital y administra las Plataformas Digitales del Estado Peruano, líder nacional de Gobierno Digital.
- Se requiere fortalecer las acciones estratégicas y tecnológicas de gestión y de impulso de la confianza y seguridad digital para proteger a los derechos fundamentales y activos de las personas y ciudadanos, iniciada con el Decreto de Urgencia 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone de medidas para su fortalecimiento.
- Se propone declarar de interés nacional y necesidad pública el fortalecimiento del Centro Nacional de Seguridad Digital, que si bien fue *creado* mediante Decreto de Urgencia 007 -2020, esto solo fue instituido como una *plataforma virtual*, mas no como un órgano de la Secretaria de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros, entre otras disposiciones; a fin de salvaguardar la seguridad de las personas y los intereses nacionales; constituyéndolo como el Centro Nacional de Operaciones en Seguridad Digital y componente del Sistema Nacional de Transformación Digital, que impulsará la articulación entre entidades públicas y privadas, para permitir un intercambio de información rápida estableciendo obligaciones mínimas a los proveedores de servicios digitales conforme a las buenas prácticas y experiencia internacional.

Finalmente, el Pleno del Congreso de la República debatió el dictamen recaído en el Proyecto de Ley 6544/2020-CR el 9 de junio del 2021, presentándose un texto sustitutorio[21] como consecuencia del debate, siendo aprobado en primera votación[22] y por acuerdo dispensado su segunda votación[23]. El Congreso de la República remitió la Autógrafa[24] de la Ley al Poder Ejecutivo el 25 de junio de 2021. Ver Anexo 01.

ii. ¿Cuáles fueron las razones del Poder Ejecutivo que motivaron observar la Autógrafa de la Ley derivada del Proyecto de Ley 6544/2020-CR?

[21] https://leyes.congreso.gob.pe/Documentos/2016_2021/Texto_Sustitutorio/Proyectos_de_Ley/TS06544-20210609.pdf

[22] https://leyes.congreso.gob.pe/Documentos/2016_2021/Asistencia_y_Votacion/Proyectos_de_Ley/AV0654420210609.pdf

[23] https://bit.ly/3bhyrAo

[24] https://bit.ly/3bgEUf9

El Poder Ejecutivo, en aplicación del artículo 108 de la Constitución Política del Perú, observó la Autógrafa de Ley, mediante el Oficio N° 462-2021-PR[25], de fecha 19 de julio de 2021, con el objeto de proponer textos alternativos y ajustes para garantizar su concordancia con la Constitución Política y el marco normativo vigente, resaltando que la *Autógrafa es, en términos generales, positiva y beneficiosa, pues tiene como finalidad salvaguardar los derechos fundamentales de los ciudadanos en el entorno digital, especialmente en materia de intimidad personal y familiar y seguridad, así como atender el deber constitucional del Estado de proteger a la población de las amenazas contra su seguridad (ámbito digital).*

En ese sentido, [el Poder Ejecutivo considera que,] *la Autógrafa es importante para el actual contexto de hiperconectividad y pandemia de la COVID-19, que obliga a las entidades públicas y privadas, así como a las personas en general, a depender más de la infraestructura digital, y, por ello, los vuelve más vulnerables frente a brechas de seguridad, ciberdelincuencia y cibercriminalidad. En ese contexto, con el fortalecimiento del Centro Nacional de Seguridad Digital (CNSD) se facilitará la articulación entre entidades públicas y privadas, permitiendo así un rápido intercambio de información sobre seguridad digital, lo que contribuirá a los fines de la Autógrafa.*

No obstante, se observar los siguientes artículos, con la finalidad de que sean coherentes con las competencias, responsabilidades y fines del Sistema de Seguridad y Defensa Nacional del Estado, al amparo del artículo 163 de la Constitución, el Decreto Legislativo 1129, Decreto Legislativo que regula el Sistema de Defensa Nacional, y la Ley 30999, Ley de Ciberdefensa.

Observaciones al artículo 1:

Se propone incorporar al final la siguiente frase *sin afectar las competencias del Ministerio de Defensa y sus órganos ejecutores en materia de seguridad y defensa nacional*; con el fin de precisar que las disposiciones sobre el fortalecimiento del CNSD no afectan las competencias del Ministerio de Defensa (MINDEF) y de sus órganos ejecutores en materia de seguridad y defensa nacional.

Observaciones al artículo 6:

Se propone la modificación del numeral 6.1 del artículo 6, referido a la conformación de equipos técnicos especializados en seguridad y confianza digital, con el fin de suprimir la referencia al **Consejo de Seguridad y Defensa Nacional (COSEDENA)**, en tanto que, por su naturaleza política y estratégica, no corresponde se le asignen

[25] https://bit.ly/3Qv4pJX

responsabilidades técnicas en estas materias. En su lugar, es necesario incluir a la **Policía Nacional del Perú (PNP)**, puesto que dicha institución, a través de la División de Investigación de Delitos de Alta Tecnología (DIVINDAT), conforme lo establece la Ley de la PNP (Decreto Legislativo Nº 1267) y su Reglamento (aprobado por Decreto Supremo Nº 026-2017-IN), es la única unidad especializada encargada de investigar delitos informáticos en todas sus modalidades.

Observaciones al artículo 7, numeral 6:

Se establece como una responsabilidad del CNSD la de identificar y validar las propuestas de activos críticos nacionales (ACN) que impliquen un componente de seguridad y confianza digital.

Sobre el particular, el Reglamento para la Identificación, Evaluación y Gestión de Riesgos de los Activos Críticos Nacionales, aprobado por Decreto Supremo 106-2017-PCM, establece en su artículo 8 que cada sector, una vez identificados los ACN, presenta su propuesta de inventarío sectorial a la Dirección Nacional de Inteligencia (DINI), que valida las propuestas de inventario sectorial de los ACN y formula el Inventario Nacional de los ACN, con base a las propuestas de inventario sectorial validadas, el cual es presentado al COSEDENA para su aprobación o actualización.

Siendo así, se advierte la responsabilidad con la que cuenta cada sector con relación a la identificación de los ACN vinculados a la naturaleza y función del activo seleccionado y los servicios que brinda, así como la competencia de la DINI para validar tales propuestas, previo a ser remitidas a la COSEDENA para efectos de su aprobación; por ello, proponemos la siguiente precisión en el texto a efecto de evitar una eventual superposición de funciones: *6. Identificar y **participar en la validación de** las propuestas de activos críticos nacionales que impliquen un componente de seguridad y confianza digital*.

Sobre la Segunda Disposición Complementaria Modificatoria:

La modificación propuesta al artículo 6 del Decreto Legislativo 1129, por el que se pretende incorporar dentro de la conformación del COSEDENA al Secretario de Gobierno y Transformación Digital (SGTD), **resulta innecesario**, pues la norma ya prevé expresamente la participación del Presidente del Consejo de Ministros como integrante. Asimismo, en las sesiones del COSEDENA no siempre se tocarán temas de seguridad digital, por lo que la participación permanente del SGTD carece de sentido.

En todo caso, en el supuesto que la agenda del órgano tuviese un punto vinculado a dicha materia, el penúltimo párrafo del mismo artículo 6 ya habilita la

participación del SGTD, en tanto señala que el Presidente de la República, en su calidad de Presidente del COSEDENA, de acuerdo a la naturaleza de los asuntos a tratar o a petición de cualquiera de sus miembros, dispone la participación de cualquier otro funcionario del Poder Ejecutivo y de otros poderes del Estado, así como de autoridades de Gobiernos Regionales y Locales, con derecho a voz, pero sin voto.

Por lo expuesto, **no corresponde al SGTD integrar el COSEDENA**, por lo que se recomienda excluir la Segunda Disposición Complementaria Modificatoria de la Autógrafa de Ley. En su lugar, **se recomienda incorporar una Cuarta Disposición Complementaria Final** que precise que la participación en el COSEDENA, de cualquier otro funcionario del Poder Ejecutivo y de otros poderes del Estado, cuando se aborden temas de seguridad digital, se efectuará conforme a lo dispuesto en el penúltimo párrafo del artículo 6 del Decreto Legislativo 1129; ello, en los siguientes términos:

> ***DISPOSICIONES COMPLEMENTARIAS FINALES***
> *[…l*
> ***CUARTA. De la participación en el Consejo de Seguridad y Defensa Nacional***
> *En los casos en los que la agenda del Consejo de Seguridad y Defensa Nacional incluya algún tema de seguridad digital, será de aplicación lo establecido en el penúltimo párrafo del artículo 6 del Decreto Legislativo Nº 1129, Decreto Legislativo que regula el Sistema de Defensa Nacional, que habilita la participación de cualquier otro funcionario del Poder Ejecutivo y de otros poderes del Estado.*

iii) ¿Por qué es necesario una norma de fortalecimiento del Centro Nacional de Seguridad Digital?

La Comisión de Ciencia, Innovación y Tecnología convocó a la ingeniera **Marushka Chocobar Reyes**, en su condición de Secretaria de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros, quien se presentó ante el Pleno de la Comisión en su Vigésima Segunda Sesión Ordinaria, del 8 de junio de 2022, para sustentar la necesidad de emitir la *Ley que declara de interés nacional y necesidad pública el fortalecimiento del Centro Nacional de Seguridad Digital para garantizar la confianza en el entorno digital del país*, propuesta por la Comisión de Defensa Nacional, Orden Interno, Desarrollo Alternativo y Lucha Contra las Drogas, aprobada por el Congreso de la República y observada por el Poder Ejecutivo.

La Secretaria de Gobierno y Transformación Digital respondió las siguientes preguntas formuladas por la Comisión de Ciencia, Innovación y Tecnología:

1. ¿Cuál es la situación del reglamento del Decreto de Urgencia 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento?
2. ¿Cuál es el estado de implementación del Centro Nacional de Seguridad Digital, creado con el Decreto de Urgencia 007-2020?
3. ¿Qué equipos técnicos especializados en seguridad y confianza digital integran el Centro Nacional de Seguridad Digital?
4. ¿Cuáles son las funciones y responsabilidades del Centro Nacional de Seguridad Digital?
5. ¿Se requiere de una ley para fortalecer el Centro Nacional de Seguridad Digital?
6. ¿Qué incidentes de seguridad digital ha gestionado la Secretaría de Gobierno y Transformación Digital en el presente año y cuáles fueron sus consecuencias?

La ingeniera **Chocobar**, manifestó ante el Pleno de la Comisión de Ciencia, Innovación y Tecnología lo siguiente:

Manifestó que, es importante iniciar esta presentación dando el marco de la Gobernanza Digital en el país, a raíz de 3 normas con rango de ley: el Decreto Legislativo 1412, que aprueba la Ley de Gobierno Digital; el Decreto de Urgencia 006-2020, que crea el Sistema Nacional de Transformación Digital, donde se involucra al sector público, al sector privado, la sociedad civil a la academia con un enfoque de múltiples partes interesadas para llevar adelante el proceso nacional de transformación digital; y el Decreto de Urgencia 007-2020, que crea el marco de Confianza Digital en el Perú y dispone medidas para su fortalecimiento; estas tres normas con rango de ley son los pilares de la Gobernanza Digital en el Perú, dijo que esto se recoge de alguna manera en el eje 8 de la política general de gobierno que es el Decreto Supremo 164-2022-PCM y se tiene estas tres normas con rango de ley establecidas en el lineamiento 8.1.5 que habla del despliegue de acciones para garantizar la seguridad de la confianza digital para la ciudadanía, teniendo este panorama, presentó un resumen sobre de cómo se ha avanzado sobre la regulación institucionalidad digital en el Perú.

Se informó como avances en la regulación e institucionalidad digital en el Perú, lo siguiente:

1. El 2016, la OCDE entrega el Estudio de Gobernanza Pública para el Perú recomendando evolucionar del gobierno electrónico al gobierno digital, fortalecer la institucionalidad digital en el país y establecer el gobierno y la transformación digital en el Centro de Gobierno siendo éste la Presidencia del Consejo de Ministros.
2. Inicios de 2017, se crea la Secretaría de Gobierno y Transformación Digital en PCM la cual absorbe la Oficina Nacional de Gobierno Electrónico e Informática y se constituye en el ente rector en materia digital con mayor empoderamiento y nivel público.
3. El 2018, el Perú adopta la definición de Seguridad Digital mediante Decreto Supremo 051-2018- PCM definiéndola como el estado que emerge de cuán confiables, éticas, veraces, transparentes y proactivas son las interacciones digitales con los ciudadanos y su impulso en la prosperidad económica y social de las personas. El Perú se convierte en el segundo país en América Latina en adoptar esa definición en favor de los ciudadanos.
4. El 2018, se promulga el Decreto Legislativo 1412 que aprueba la Ley de Gobierno Digital fortaleciendo la rectoría de la Secretaría en materia de interoperabilidad, servicios digitales, gobierno de datos, arquitectura digital, seguridad digital e identidad digital.
5. La Ley de Gobierno Digital establece el Marco de Seguridad Digital para el Estado Peruano contemplando 4 ámbitos: Ciberdefensa, Ciberinteligencia, Ciberdelincuencia y Ciberseguridad.
6. En octubre 2018, se promulgó el Decreto Supremo 118-2018-PCM que declara de interés nacional el gobierno digital, la innovación y la economía digital con enfoque territorial.

7. Dicho Decreto Supremo crea el Comité de Alto Nivel por un Perú Digital, Innovador y Competitivo conformado por PCM, titulares de entidades públicas relacionadas a la economía digital, conectividad, educación digital y gobierno digital y el Despacho Presidencial.
8. La Secretaría de Gobierno Digital ejerce la Secretaría Técnica del Comité de Alto Nivel y lleva la responsabilidad de dirigir la Agenda Digital Peruana.
9. El 2019, el Perú se adhiere al Convenio de Budapest o Convenio contra la Ciberdelincuencia mediante Resolución Legislativa 30913 y con ello se abre una agenda legislativa pendiente en materia de ciberdelincuencia.
10. El 2019 se promulga la Ley 30999, Ley de Ciberdefensa, que establece claramente el rol de las Fuerzas Armadas cuando un incidente de seguridad digital atenta contra la seguridad y defensa nacional.
11. La Ley de Ciberdefensa fortalece la rectoría de la Secretaría de Gobierno Digital en materia de Seguridad Digital en el país.
12. La Ley de Ciberdefensa estable que la Presidencia del Consejo de Ministros, como miembro del Consejo Seguridad y Defensa Nacional (COSEDENA), establece los protocolos de actuación en caso se atente contra la seguridad nacional mediante ataques digitales disponiendo que este rol se cumpla a través de la Secretaría de Gobierno Digital en su calidad de ente rector en el país.
13. A inicios del 2020, se promulgó el Decreto de Urgencia 006-2020 que crea el Sistema Nacional de Transformación Digital, incluyendo en el ecosistema digital al sector privado, la sociedad civil, la academia, el sector público y los ciudadanos estableciendo la rectoría en materia de Transformación Digital del país en la Secretaría de Gobierno y Transformación Digital.
14. De igual manera, se promulgó el Decreto de Urgencia 007-2020, que aprueba el Marco de Confianza Digital y dicta medidas para su fortalecimiento.
15. El Marco de Confianza Digital establece tres ámbitos fundamentales: seguridad digital (cuyo marco recae en el DL 1412), privacidad (MINJUS) y protección del consumidor (Indecopi).
16. El Decreto de Urgencia 007-2020 recoge la normatividad en materia de ciberseguridad y eleva la regulación digital peruana al nivel de países OCDE:
    - Crea el Centro Nacional de Seguridad Digital a fin de gestionar los incidentes de seguridad digital en el país y promover la articulación público - privada para gestionar los riesgos digitales.
    - Crea el Centro Nacional de Datos a fin de gestionar el gobierno de datos público - privado impulsando el uso ético de las tecnologías digitales y la adopción de los datos como objetivo estratégico.
    - Crea el Registro Nacional de Incidentes de Seguridad Digital y establece la obligatoriedad del reporte del sector privado sobre ataques digitales.

- Se establece la rectoría en materia de confianza digital en el país en la Secretaría de Gobierno Digital fortaleciendo la institucionalidad

17. A inicios del 2020, se promulgó el Decreto de Urgencia 006-2020, que crea el Sistema Nacional de Transformación Digital, incluyendo en el ecosistema digital al sector privado, la sociedad civil, la academia, el sector público y los ciudadanos estableciendo la rectoría en materia de Transformación Digital del país en la Secretaría de Gobierno Digital.

Instrumentos para fortalecer la Confianza digital: El Centro Nacional de Seguridad Digital; el Centro Nacional de Datos; el Centro Nacional de Innovación e Inteligencia Artificial; la Infraestructura Oficial de Firma Electrónica y el Registro Nacional de Protección de Datos Personales y de Incidentes de Seguridad Digital.

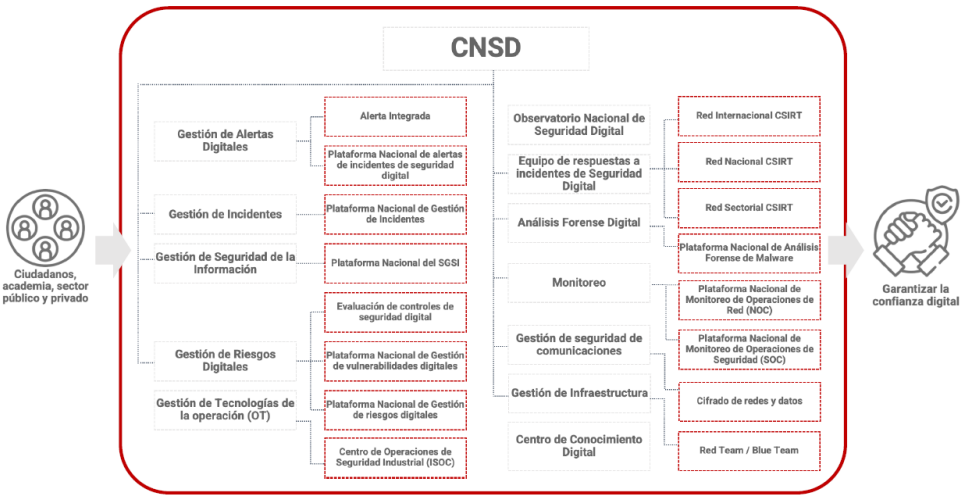
Respecto a la pregunta **¿Cuál es la situación del reglamento del Decreto de Urgencia 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento?** refirió que se realizaron las siguientes acciones:

1. Se publicó el Documento de Trabajo de la Estrategia Nacional de Seguridad y Confianza Digital.
2. Se publicó la Guía para el Perfil y Responsabilidades del Oficial de Seguridad y Confianza Digital.
3. Se publicó la Guía para la Conformación e Implementación de Equipos de Respuestas ante Incidentes de Seguridad Digital.
4. Se emitieron las Alertas Integradas de Seguridad Digital.
5. Se publicó Políticas orientadas a implementar el Sistema de Gestión de Seguridad de la Información.
6. Se ha implementado el Centro de Conocimiento Digital para capacitación en Seguridad Digital.

7. Se publicó la Directiva que establece el Perfil y Responsabilidades del Oficial de Gobierno de Datos.
8. Conformación del Grupo de Trabajo Multisectorial de naturaleza temporal denominado "Mesa Técnica para proponer acciones y medidas que fortalezcan la Confianza Digital en el país".
9. Se encuentra en proceso de aprobación la Unidad Funcional de Confianza Digital para fortalecer estrategia de prevención y mitigación de riesgos digitales.
10. El reglamento ya se ha concluido, sin embargo, se encuentra en la etapa de opiniones MINJUS e INDECOPI para su posterior aprobación.

Respecto a la pregunta **¿cuál es el estado de implementación del Centro Nacional de Seguridad Digital, creado con el Decreto de Urgencia 007-2020?** refirió que, la conformación de los equipos en el Centro Nacional de Seguridad Digital es: Gestión de Alerta; Gestión de Incidentes; Gestión de Seguridad de la Información; el Observatorio Nacional de Seguridad Digital; Análisis Forense y el Monitoreo permanente. Se precisó que la seguridad digital y la confianza digital en los servicios digitales que despliegan las entidades públicas es responsabilidad de cada titular, esto quiere decir desde el titular del pliego hasta las autoridades administrativas, los jefes de tecnología, el Oficial de Seguridad y Confianza Digital.

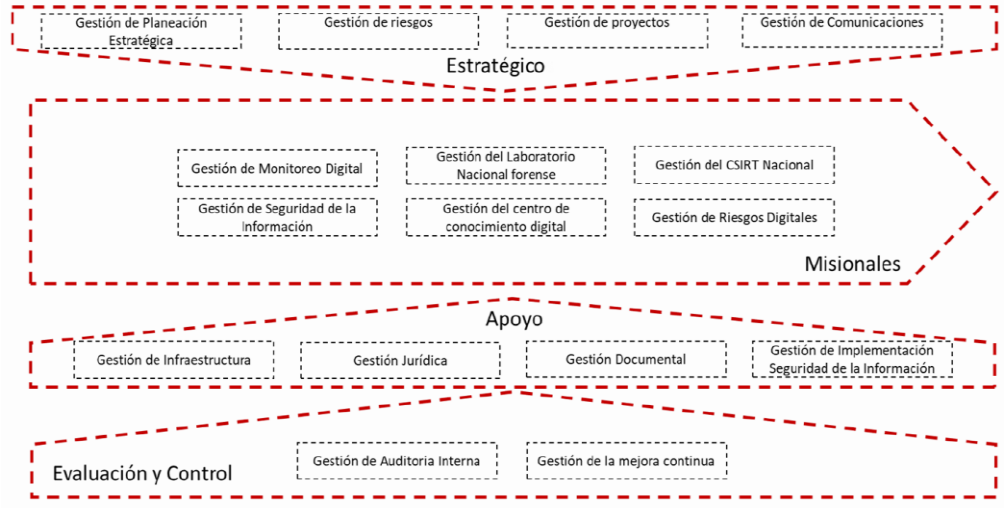
El rol de Centro Nacional de Seguridad Digital cuando recibe una alerta es ayudar y prevenir al resto de las entidades públicas cuando una de ellas ha sido afectada, para brindar asistencia técnica. Se presentó una gráfica mostrando la configuración del Centro Nacional de Seguridad Digital.



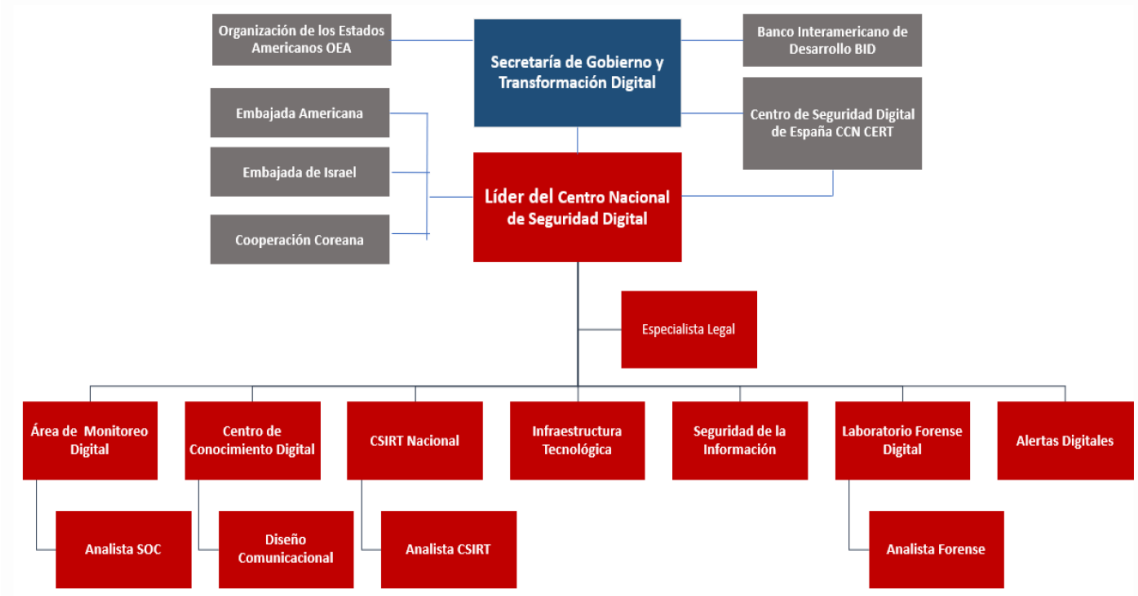
Además, se informó que los ministerios habían avanzado, tanto en sus Equipos de Respuestas a Incidentes de Seguridad Digital como asignar a su Oficial de Confianza y Seguridad Digital. El Sistema de Gestión de Seguridad de la Información todavía está al 53%. En cuanto a los gobiernos regionales todos han definido a su Oficial de Confianza y Seguridad Digital, pero aún se está en un 36% de avance de implementación de los CSIRT y 48% en el Sistema de Gestión de la Seguridad de la Información (SGSI). En los Organismos Autónomos el 60% han determinado el Oficial de Seguridad y Confianza Digital. El 90% tiene un CSIRT y en el SGSI todavía se está al 50%.

El tema más difícil de avanzar es en los Gobiernos Locales, donde desde el Centro Nacional de Seguridad Digital se ha comenzado a entregar todos los apoyos de asistencias digitales, que ahora son muchos más agiles de realizarse con un CSIRT, es decir, con un equipo de respuesta de antecedentes de seguridad digital de manera digital. Si bien la responsabilidad e cumplir las directivas es del Gobierno Regional y del Gobierno Local y de las entidades públicas en general, es importante este apoyo que se despliega desde el Centro Nacional de Seguridad Digital. En ese sentido, un avance en números del Centro Nacional de Seguridad Digital son los siguientes datos: se ha capacitado a más de 43 mil personas en seguridad digital, 2 mil efectivos policiales capacitados en ciberseguridad digital, 800 entidades públicas monitoreadas a través del Centro Nacional de Seguridad Digita, se han emitido 700 alertas, 70 políticas y se han dictado 35 cursos.

Respecto a la pregunta **¿qué equipos técnicos especializados en seguridad y confianza digital integran el Centro Nacional de Seguridad Digital?** Se presentó un mapa de procesos de los Equipo Técnicos Especializados en Seguridad u Confianza Digital que integran el Centro Nacional de Seguridad.



Sin embargo, estos procesos no están incorporados en del Decreto de Urgencia 007-2020, sino que, estos procesos forman parte del reglamento, la misma que se incorporarían a la unidad funcional que se está proponiendo. En la actualidad se encuentran laborando 12 personas en el Centro Nacional de Seguridad Digital, en otros países se tienen 100 o 200 personas dedicadas a seguridad digital. En Brasil tienen 30 personas dedicadas y tienen una serie de oficiales de seguridad de la información.



Se tiene el apoyo del Banco Interamericano de Desarrollo y esto a raíz de toda la amenaza de ciberataque mundial que ha venido ocurriendo en Costa Rica, nos pusimos en contacto con las embajadas de Estados Unidos, Israel, la Cooperación Coreana, la OEA, el BID y el Centro de Seguridad de España. También manifestó su voluntad de apoyo las Embajada de Brasil que es con la que se tuvo una reunión recientemente.

Presentó el organigrama con los respectivos equipos, organigrama que responde al mapa de procesos y dispone de los siguientes componentes:

1. Equipo de Respuestas ante Incidentes de Seguridad Digital
2. Laboratorio Nacional Forense Digital
3. Gestión de Incidentes de Seguridad Digital
4. Alertas de Seguridad Digital
5. Análisis de Vulnerabilidades
6. Centro de Operaciones de Seguridad Digital SOC
7. Centro de Operaciones de Seguridad Digital Industrial iSOC

8. Gestión de la seguridad de la información
9. Gestión de conocimiento digital
10. Gestión del Centro de Conocimiento Digital

Respecto a la pregunta **¿Cuáles son las funciones y responsabilidades del Centro Nacional de Seguridad Digital?** refirió que, las funciones y responsabilidades del Centro Nacional de Seguridad Digital que señalará se desprenden del Decreto de Urgencia 007-2020, sin embargo, precisó que se puede fortalecer estas funciones y responsabilidades el Centro porque entre la emisión del decreto de urgencia, en enero del 2020, han pasado dos años de pandemia, si hubieran pasado dos años normales, probablemente no sería necesario fortalecer el Centro, porque se había avanzado bastante en cuanto a la constitución, inversión de tecnología, también se ha avanzado en cuanto a la conformación de los equipos, el intercambio de información con embajadas. Ahora se tiene un equipo, antes de la emisión del Decreto de Urgencia 007-2020 solo se tenía dos a tres personas encargadas de estos temas, siendo un hito para poder comenzar a invertir en seguridad, pero estos dos años de crisis sanitaria han acelerado la necesidad de mejorar en cuanto a laboratorio forense, además de mejorar y fortalecer las competencias de las personas en el Perú y que estén involucradas en los temas de seguridad y confianza digital.

Respecto a las funciones que tiene el Centro Nacional de Seguridad Digital son las siguientes:

1. Es el encargado de gestionar, dirigir, articular y supervisar la operación, educación, promoción, colaboración y cooperación de la Seguridad Digital a nivel nacional como componente integrante de la seguridad nacional, a fin de fortalecer la confianza digital.
2. Es responsable de identificar, proteger, detectar, responder, recuperar y recopilar información sobre incidentes de seguridad digital en el ámbito nacional para gestionarlos, no obstante, esta función no se puede llevar adelante sin la colaboración de las entidades públicas y privadas.
3. Constituye el mecanismo de intercambio de información y articulación de acciones con los responsables de los ámbitos del Marco de Seguridad Digital del Estado Peruano.
4. Se encuentra a cargo de la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno y Transformación Digital.
5. Entre otros.

Respecto a la pregunta **¿Se requiere de una ley para fortalecer el Centro Nacional de Seguridad Digital?** manifestó que, la respuesta técnica sería, sí es necesario fortalecer el Centro Nacional de Seguridad Digital, teniendo en cuenta que se tiene

dos años de crisis sanitaria, donde el nivel de digitalización de los países en el mundo y sobre todo en el Perú ha avanzado, si bien todavía hay fuertes brechas en cuanto a conectividad y en cuanto a poder llegar a la ciudadanía, el último informa del INEI da cuenta que las personas, las familias, que se encuentran en condiciones de muy pobres tienen 87% de conectividad a través de celulares y las familias que se encuentra en condiciones de pobreza tienen 90% de conectividad a través de sus dispositivos móviles, esto significa que se debe llegar de manera masiva y con una decisión enfocada de poder abarcar los ámbitos de la seguridad y confianza digital en las personas, en las empresas y en las organizaciones.

Se ha creado la Unidad Funcional de Confianza Digital para poder establecer esta articulación con el Centro Nacional de Seguridad Digital de manera más rápida, ágil, eficiente y además focalizada, entonces ya se tiene una unidad especializada dentro de la Secretaría de Gobierno y Transformación Digital, además, manifestó que se está invirtiendo en la formación de la Plataforma Nacional de Gobierno Digital que tiene un componente que fortalece técnicamente el Centro Nacional de Seguridad Digital, que se vincula con una conformación de micro servicios, aplicaciones digitales, etc., esta Plataforma Nacional de Gobierno Digital será entregada oficialmente pronto, infraestructura que funcionará en el Banco de la Nación y se está proyectando para el 2023 tener nudos descentralizados en las regiones.

Entonces, se ha dado un paso para consolidar las acciones en seguridad y confianza digital para la protección de la ciudadanía frente a los riesgos digitales con el Decreto Supremo 164-2022-PCM. Ahora, los siguientes pasos son: aprobar la Política Nacional; aprobar la Estrategia de Seguridad y Confianza Digital; fortalecer la Mesa de Confianza Digital; realizar una evaluación nacional de madurez técnica, administrativa, organizativa y legal en Seguridad y Confianza digital de todas las entidades públicas. Para esto se está trabajando para conseguir fondos no reembolsables y poder apalancar esa reevaluación y dotar de mayor presupuesto al Centro Nacional de Seguridad Digital y a las entidades públicas en general.

Finalmente, respecto a la pregunta **¿Qué incidentes de seguridad digital ha gestionado la Secretaría de Gobierno y Transformación Digital en el presente año y cuáles fueron sus consecuencias?** Manifestó que, esta declaratoria de emergencia nacional del país [Costa Rica] a causa del ciberataque en la categoría de extorsión, porque roban datos, documentos, este grupo que ha realizado estas acciones han exigido dinero a ese país. La SGTD ha venido buscando mitigar el impacto con una serie de comunicados emitidos a las entidades públicas y reuniones permanentes de capacitación a los Oficiales de Seguridad Digital, que es el más reciente de los eventos que han venido ocurriendo.

Se han emitido más de 700 alertas de seguridad digital y a la fecha se tiene una vigente campaña nacional de confianza digital, las consecuencias en cuanto a la falta de seguridad de la ciudadanía se evidencian en un estudio que ha publicado UNICEF con respecto a la protección de niños, niñas y adolescentes en internet, esto no se ve cuando se analiza la ciberseguridad o la seguridad digital más pensado en las infraestructuras críticas, lo que en realidad esto afecta también a las personas, se ha lanzado esta campaña nacional de alerta por un internet seguro para los niño, niñas y adolescentes y esto dedicado directamente a las personas y están permanentemente avanzando en ese sentido.

Sobre los retos de regulación indicó que el Perú se adhirió en el 2019 al Convenio de Budapest y en el corto plazo se está trabajando en las redes de confianza, en la priorización en la Agenda Pública, y dijo que esta presentación en la Comisión es muy importante para la Secretaría de Gobierno y Transformación Digital y en ese sentido, están buscando que la Transformación Digital se incorpore como objetivo estratégico de los planes institucionales, porque es la única manera de garantizar de que exista una inversión en temas de tecnología para la protección de los servicios digitales; el fortalecimiento de instituciones de justicia, por ejemplo, no se tiene juzgados especializados en ciberdelincuencia, se debe fortalecer a la DIVINDAT, si bien se tiene una unidad fiscal especializada en ciberdelitos, que seguramente al momento de ser creada han recibido todo un reto importante en cuanto a la gestión de lo hoy se viene manejando a nivel de retos de ciberespacio; el fortalecimiento del marco normativo el Decreto de Urgencia 007-2020, la Ley de Ciberdefensa, la Ley de fortalecimiento del Centro Nacional de Seguridad Digital; y en el largo con el apoyo de esta Comisión se debe fortalecer las leyes y los protocolos, leyes que son transversales hacia los derechos para poder prevenir y poder adecuarnos al convenio de Budapest.

iv) ¿Se requiere perfeccionar la iniciativa legislativa?

Luego del análisis realizado en las secciones anteriores, la Comisión de Ciencia, Innovación y Tecnología concluye que **el Proyecto de Ley 1775/2021-CR debe ser perfeccionado, priorizando el fortalecimiento del Centro Nacional de Seguridad Digital** (CNSD) que está a cargo de la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros, **desestimando declarar de interés nacional la creación del Centro Nacional de Ciberseguridad del Perú (CENACI)**. En esa línea, se prioriza el fortalecimiento del CNSD con la siguiente finalidad:

a. Fortalecer el Centro Nacional de Seguridad Digital con el propósito de garantizar la seguridad digital a nivel nacional para hacer frente a los riesgos,

amenazas o ataques en el entorno digital.

b. Fortalecer el nivel de seguridad digital en el entorno digital del territorio nacional a fin de garantizar la confianza digital de los ciudadanos y personas en general.
c. Fortalecer los mecanismos de defensa y protección de los activos críticos nacionales y recursos claves de la nación frente a riesgos en el entorno digital que afecten la seguridad digital a nivel nacional.
d. Promover y garantizar la confianza y seguridad digital en los servicios digitales que brindan las entidades de la administración pública y las organizaciones del sector privado a los ciudadanos y personas en general.
e. Articular y desplegar acciones con actores expertos del sector público, privado, la academia y la sociedad civil para fortalecer la confianza digital en el país.
f. Impulsar y fortalecer el talento digital en el ámbito de seguridad y confianza digital para que el país cuente con expertos en esta materia.

Por otro lado, la Comisión hace suyo la propuesta de la Comisión de Defensa Nacional Orden Interno, Desarrollo Alternativo y Lucha Contra las Drogas, expresado en su dictamen del 7 de diciembre de 2020, **ratificando la necesidad de aprobar una norma para fortalecer el Centro Nacional de Seguridad Digital**, habiéndose evaluado en su momento su necesidad, viabilidad y eficacia presunta; en razón de ello sería infructuoso volver a realizar dicha evaluación en el presente pronunciamiento. Con esta decisión se da por atendido las preocupaciones expresadas por la Cámara de Comercio Americana del Perú (AMCHAM) y la Sociedad de Comercio Exterior del Perú (COMEXPERÚ), plasmadas en sus respectivos documentos de opinión.

Así también, la Comisión hace suyo las observaciones planteadas por el Poder Ejecutivo a la Autógrafa de la *Ley que declara de interés nacional y necesidad pública el fortalecimiento del Centro Nacional de Seguridad Digital para garantizar la confianza en el entorno digital del país*, procediendo a incorporar las recomendaciones planteadas en el nuevo texto sustitutorio a considerarse en el presente dictamen.

Con estas premisas, la Comisión de Ciencia, Innovación y Tecnología procederá a perfeccionar la propuesta de norma de la iniciativa legislativa, planteando un texto sustitutorio, con las siguientes consideraciones:

1. Habiéndose optado por fortalecer el Centro Nacional de Seguridad Digital (CNSD) y contando con su norma de creación, el Decreto de Urgencia 007-2020, Decreto de Urgencia que aprueba que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento, **la Comisión colige que no es necesario generar una nueva ley, sino circunscribir la propuesta**

normativa en una ley modificatoria, es decir, modificar el Decreto de Urgencia 007-2020, incorporando nuevas definiciones, precisando el rol del CNSD y el del Centro Nacional de Datos, además, de establecer las responsabilidades, las líneas de acción y los procesos operativos del CNSD, Incorporándose la conformación de equipos especiales en seguridad y confianza digital y las acciones en situaciones de emergencia nacional.

2. Al proponerse una ley modificatoria, el título de la norma que se considerará en el texto sustitutorio será: *Ley que modifica el Decreto de Urgencia 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone de medidas para su fortalecimiento, para consolidar el Centro Nacional de Seguridad Digital*.
3. Respecto a las definiciones propuestas, solo se considerarán las nuevas definiciones, y las modificaciones propuestas, que no se encuentran establecidas en el Decreto Legislativo 1412, Ley de Gobierno Digital; en el Decreto de Urgencia 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital; y en el Decreto de Urgencia 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento. En esa línea, la Comisión colige que sería infructuoso repetir las siguientes definiciones que ya se encuentran establecidas: ciberseguridad, confianza digital, entorno digital, gobierno digital y seguridad digital.
4. Se desestima disponer que la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno y Transformación Digital, constituya el sistema funcional de Seguridad Nacional de Seguridad Digital. Si bien, *los sistemas* [funcionales y administrativos] *son los conjuntos de principios, normas, procedimientos, técnicas e instrumentos mediante los cuales se organizan las actividades de la Administración Pública que requieren ser realizadas por todas o varias entidades de los Poderes del Estado, los Organismos Constitucionales y los niveles de Gobierno*[26], la Comisión considera que estos *principios, normas, procedimientos, técnicas e instrumentos* deberían implementarse mediante el Decreto de Urgencia 007-2020, para ello el Poder Ejecutivo debería plantear las modificaciones que considere necesarias.

VI. ANÁLISIS DEL IMPACTO NORMATIVO

Como parte del análisis del marco normativo se ha identificado que en el año 2020 se promulga el Decreto de Urgencia 007-2020, Decreto de Urgencia que aprueba el

[26] Artículo 432 de la Ley 29158, Ley Orgánica del Poder Ejecutivo.

Marco de Confianza Digital y dispone medidas para su fortalecimiento, a través de esta norma se crea el Centro Nacional de Seguridad Digital bajo la administración de la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros.

Por otro lado, habiéndose optado por fortalecer el Centro Nacional de Seguridad Digital (CNSD) corresponderá entonces modificar el Decreto de Urgencia 007-2020, incorporando nuevas definiciones, precisando el rol del CNSD y el del Centro Nacional de Datos, además, de establecer las responsabilidades, las líneas de acción y los procesos operativos del CNSD. Incorporándose también la conformación de equipos especiales en seguridad y confianza digital y las acciones en situaciones de emergencia nacional. Al no estar, a la fecha, aprobado el reglamento del Decreto de Urgencia 007-2020, cuando se apruebe esta norma corresponderá incluir las modificaciones propuestas en el presente dictamen.

Así también, al establecerse nuevas definiciones, y en otros casos modificaciones, que no se encuentran establecidas en el Decreto Legislativo 1412, Ley de Gobierno Digital; y en el Decreto de Urgencia 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital; una vez promulgada la norma, corresponderá actualizar los respectivos reglamentos de dichas normas para incorporar las respectivas definiciones.

VII. ANÁLISIS COSTO BENEFICIO

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

Entonces, en atención a lo previsto en el artículo 76 del Reglamento del Congreso de la Republica, si bien la presente propuesta implica la generación de un gasto adicional al erario nacional, esto porque se establece que deberán conformarse equipos especializados en seguridad y confianza digital, integrada por expertos nacionales e internacional, como parte del Centro Nacional de Seguridad Digital, estas posibles contrataciones deberán circunscribirse en el artículo 14 del Decreto de Urgencia 007-2020, del financiamiento, que establece que la implementación de lo establecido en el presente Decreto de Urgencia [y de sus modificaciones] se financia con cargo al presupuesto institucional de las entidades involucradas, sin demandar recursos adicionales al Tesoro Público. Es decir, todo gasto deberá realizarse con cargo al presupuesto aprobado.

Respecto a los beneficios de la presente norma, está relacionado a la protección de la nación respecto a la ciberseguridad, y en su aspiración más alta a garantizar la confianza en el entorno digital del país; y de esa manera manejarse a la luz de estos tiempos, lo que la nación y la ciudadanía demanda con urgencia.

Por otro lado, de aprobarse la propuesta con el presente texto sustitutorio se contribuirá a garantizar la seguridad digital a nivel nacional para hacer frente a los riesgos, amenazas o ataques en el entorno digital; fortaleciendo el Centro Nacional de Seguridad Digital para garantizar la confianza digital de los ciudadanos y de las personas en general; promover la confianza y seguridad digital en los servicios digitales que brindan las entidades de la Administración Pública y las organizaciones del sector privado; lo que permitirá que el país esté a la vanguardia en la protección de los intereses ciudadanos, de las entidades públicas, privadas y de la sociedad, beneficiando por tanto a la población en general, y por ende al país, lo cual conlleva de manera directa a incrementar la competitividad y transformación digital del Estado y de la sociedad en su conjunto.

VIII. CONCLUSIÓN

En ese sentido, la Comisión de Ciencia, Innovación y Tecnología, de conformidad con lo establecido por el literal b) de artículo 70 del Reglamento del Congreso de la República, recomienda la **APROBACIÓN** del presente dictamen recaído en el **Proyecto de Ley 1776/2021-CR**, mediante el cual se propone la **LEY QUE MODIFICA EL DECRETO DE URGENCIA 007-2020, DECRETO DE URGENCIA QUE APRUEBA EL MARCO DE CONFIANZA DIGITAL Y DISPONE MEDIDAS PARA SU FORTALECIMIENTO, A FIN DE CONSOLIDAR EL CENTRO NACIONAL DE SEGURIDAD DIGITAL**, con el siguiente **TEXTO SUSTITUTORIO**:

EL CONGRESO DE LA REPÚBLICA:

Ha dado la Ley siguiente:

LEY QUE MODIFICA EL DECRETO DE URGENCIA 007-2020, DECRETO DE URGENCIA QUE APRUEBA EL MARCO DE CONFIANZA DIGITAL Y DISPONE MEDIDAS PARA SU FORTALECIMIENTO, A FIN DE CONSOLIDAR EL CENTRO NACIONAL DE SEGURIDAD DIGITAL

Artículo 1. Objeto de la Ley
La presente ley tiene por objeto modificar el Decreto de Urgencia 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su

fortalecimiento, a fin de consolidar el Centro Nacional de Seguridad Digital para garantizar la confianza en el entorno digital. Esta modificación no afecta las competencias del Ministerio de Defensa y sus órganos ejecutores en materia de seguridad y defensa nacional.

Artículo 2. Modificación de los artículos 3, 7 y 13 del Decreto de Urgencia 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento

Se modifican los artículos 3, 7 y 13 del Decreto de Urgencia 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento, en los siguientes términos:

> **"Artículo 3. Definiciones**
>
> Para la aplicación del presente Decreto de Urgencia se establece las siguientes definiciones:
>
> […]
>
> d) Actividad crítica. Es la actividad económica y/o social cuya interrupción tiene graves consecuencias en la salud y seguridad de los ciudadanos, **y** en el funcionamiento efectivo de los servicios esenciales que mantienen la economía, sociedad y el gobierno, **o afecta** la prosperidad económica y social en general.
>
> […]
>
> **k) Activo digital. Es el elemento, objeto o recurso que se puede utilizar para adquirir, procesar, almacenar y distribuir información digital y que tiene un valor potencial o real para una organización. Incluye activos de software, activos de contenidos de información digital, entre otros.**
>
> **l) Experto en seguridad y confianza digital. Es la persona con experiencia comprobada en materia de seguridad y confianza digital y que se encuentra capacitada técnicamente para desarrollar y desplegar estrategias a fin de prevenir, mitigar, afrontar y proteger los principales activos digitales de los sectores público, privado, academia, entre otros actores del ecosistema digital, de los inminentes riesgos que afecten el bienestar de las personas y la seguridad nacional.**
>
> **m) Oficial de seguridad digital. Es la persona responsable de planificar, gestionar y evaluar las medidas y controles de ciberseguridad y seguridad de la información en la organización con el fin de proteger los activos y plataformas digitales. Asimismo, gestiona y supervisa el funcionamiento integral del proceso de seguridad digital. Es el contacto con el Centro Nacional de Seguridad Digital.**

n) Resiliencia digital. Capacidad de las organizaciones y personas en general para adaptarse y recuperarse frente a la ausencia de servicios esenciales digitales que permite afrontar situaciones de crisis nacional como incidentes de seguridad digital, no disponibilidad de infraestructuras o sistemas, entre otros.

Artículo 7. Centro Nacional de Seguridad Digital

7.1. Créase el Centro Nacional de Seguridad Digital como **infraestructura oficial** que gestiona, dirige, articula y supervisa la operación, educación, promoción, colaboración y cooperación de la Seguridad Digital a nivel nacional como componente integrante de la seguridad nacional, a fin de fortalecer **y garantizar** la confianza **en el entorno** digital. Asimismo, es responsable de identificar, **prevenir, mitigar, afrontar**, proteger, detectar, responder, recuperar y recopilar información sobre incidentes de seguridad digital en el ámbito nacional para gestionarlos.

7.2. El Centro Nacional de Seguridad Digital se encuentra **adscrito** a la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno **y Transformación** Digital, **y se constituye en el centro nacional de operaciones en seguridad digital que comprende la generación de instrumentos legales y técnicos para garantizar la confianza en el entorno digital, la gestión de plataformas digitales, los equipos de especialistas expertos en la materia de seguridad y confianza digital, y el observatorio de seguridad digital, siendo** único punto de contacto nacional en las comunicaciones y coordinaciones con otros organismos, centros o equipos nacionales e internacionales de similar naturaleza.

7.3. El Centro Nacional de Seguridad Digital constituye el mecanismo de intercambio de información y articulación de acciones con los responsables de los ámbitos del Marco de Seguridad Digital del Estado Peruano **y del Marco de Confianza Digital**, de conformidad con el artículo 32 del Decreto Legislativo 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, **y el artículo 4 del presente decreto de urgencia**.

7.4. […]

7.5. La Secretaría de Gobierno **y Transformación** Digital, **en su calidad de ente rector en materia de seguridad y confianza digital,** establece los

protocolos de escalamiento, coordinación, intercambio y activación **de capacidades** ante incidentes de seguridad **y confianza** digital en el país y emite los lineamientos y las directivas correspondientes.

Artículo 13. Centro Nacional de Datos

13.1. Créase el Centro Nacional de Datos como una **infraestructura oficial** que gestiona, dirige, articula y supervisa la operación, educación, promoción, colaboración y cooperación de datos a nivel nacional, a fin de fortalecer la confianza y bienestar de las personas en el entorno digital en el marco de la presente norma.

13.2. El Centro Nacional de Datos se encuentra a cargo de la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno **y Transformación** Digital y es el único punto de contacto nacional **e internacional** en las comunicaciones y coordinaciones con otros organismos, centros o equipos nacionales e internacionales de similar naturaleza.

13.3. El Centro Nacional de Datos intercambia información y articula acciones con las entidades públicas, academia, sociedad civil y sector privado y con las entidades responsables de los ámbitos del Marco de Confianza Digital para la gobernanza de datos, **pudiendo también intercambiar información y acciones con entidades tanto a nivel nacional como extranjeras de ser requeridas**.

13.4. La Secretaría de Gobierno **y Transformación** Digital, en su calidad de ente rector en gobernanza de datos, establece los protocolos y mecanismos en materia de gobierno de datos y emite los lineamientos y las directivas correspondientes".

Artículo 3. Incorporación de los capítulos V, VI y VII al Decreto de Urgencia 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento

Se incorporan los capítulos V, VI y VII al Decreto de Urgencia 007- 2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento, en los siguientes términos:

"CAPÍTULO V
CENTRO NACIONAL DE SEGURIDAD DIGITAL

Artículo 16. Responsabilidades del Centro Nacional de Seguridad Digital

El Centro Nacional de Seguridad Digital tiene las siguientes responsabilidades:

a) Gestionar los incidentes de seguridad digital, el Registro Nacional de Incidentes de Seguridad Digital y las redes de confianza, conforme a lo dispuesto en el presente decreto de urgencia.
b) Articular acciones con los responsables de los ámbitos del Marco de Seguridad Digital del Estado Peruano y del Marco de Confianza Digital para la gestión de incidentes y riesgos de seguridad digital que afecten a la sociedad, de conformidad con lo establecido en el presente decreto de urgencia y en el Decreto Legislativo 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital.
c) Promover una cultura de seguridad y confianza digital en los ciudadanos en general, priorizando el uso seguro y responsable de las tecnologías de la información y comunicaciones por niños, niñas y adolescentes conforme a lo establecido por la Ley 30254, Ley de promoción para el uso seguro y responsable de las tecnologías de la información y comunicaciones por niños, niñas y adolescentes, a través de programas de difusión y concientización u otras acciones estratégicas.
d) Realizar evaluaciones sectoriales de exposición al riesgo en las materias de seguridad y confianza digital en el marco de las acciones del Observatorio Nacional de Seguridad y Confianza Digital como componente del Centro Nacional de Seguridad Digital.
e) Identificar y evaluar el riesgo de las actividades críticas que incluya los activos críticos nacionales y recursos claves en las capacidades nacionales de tecnologías de información y comunicaciones y en las materias de gobierno digital, confianza y transformación digital.
f) Identificar y participar en la validación de las propuestas de activos críticos nacionales que impliquen un componente de seguridad y confianza digital.
g) Desarrollar y fortalecer políticas, estrategias, acciones, actividades, instrumentos, lineamientos, planes e iniciativas; así como brindar soporte y asesoría a los actores del ecosistema digital en acciones relacionadas a la gestión de riesgos de seguridad digital para garantizar la confianza en el entorno digital.
h) Promover e implementar acuerdos de colaboración, confianza y cooperación en materia de seguridad digital con otros centros de similar naturaleza del sector privado, academia, centros de investigación, saciedad civil del ámbito nacional y con países extranjeros, organizaciones y actores internacionales de similar naturaleza.
i) Fortalecer el desarrollo de capacidades y competencias en materia de seguridad y confianza digital en el marco del impulso del talento digital;

así como el desarrollo de contenidos y generación y transferencia de conocimiento en materia de seguridad y confianza digital dirigidos a los ciudadanos en general.

j) Impulsar y participar en la creación de comunidades o espacios de colaboración en los cuales se genere, comparta e intercambie información y conocimiento sobre mejores prácticas y experiencias relativas a investigación, innovación y desarrollo en materia de seguridad y confianza digital.

k) Implementar los protocolos de comunicaciones, escalamiento, coordinación, intercambio y activación para la atención de inminentes incidentes de seguridad digital a nivel nacional.

l) Gestionar proyectos de seguridad digital que permitan fortalecer la confianza digital entre los actores del ecosistema digital.

m) Monitorear campañas de propaganda, ciberdelincuencia, suplantación de identidad y estafas en el entorno digital que afecten la confianza y seguridad digital; así como definir y ejecutar estrategias de recolección de datos, informaciones e inteligencia de seguridad digital en distintos ámbitos.

n) Supervisar el cumplimiento de las obligaciones en materia de seguridad digital por parte de las entidades públicas y los responsables de las actividades y servicios esenciales; así como los responsables de los ámbitos de los marcos de seguridad digital y confianza digital.

o) Otras que determine la Presidencia del Consejo de Ministros en el marco de lo que dispone el presente decreto de urgencia.

Artículo 17. Líneas de acción del Centro Nacional de Seguridad Digital

17.1. El Centro Nacional de Seguridad Digital orienta y desarrolla sus actividades en base a las siguientes líneas de acción:

a) Planificación. Comprende los objetivos, estrategias y planes de acción a mediano y largo plazo para dirigir y guiar las actividades del Centro Nacional de Seguridad Digital, de acuerdo a lo establecido por el ente rector.

b) Operación. Comprende los procesos de análisis e intercambio de información, tratamiento de riesgos, prevención y gestión de inminentes incidentes de seguridad digital, la vigilancia y monitorización continuada de los activos digitales que se consideren relevantes o críticos y, en general, todo lo que tiene que ver con las situaciones rutinarias.

c) Transferencia de conocimiento. Comprende la generación de contenidos digitales, así como la generación y transferencia de conocimiento en materia de seguridad y confianza digital dirigidos

a los ciudadanos en general, a los servidores públicos y especialistas en seguridad digital, aliados estratégicos en el marco del impulso del talento digital para fortalecer la confianza digital en el país.

d) Promoción. Comprende la difusión y comunicación de contenidos sobre seguridad digital, así como de las actividades del propio Centro, con la finalidad de desarrollar una consciencia y una cultura de seguridad digital en la sociedad.

e) Colaboración y cooperación. Comprende el establecimiento de relaciones bilaterales de cooperación, la articulación y coordinación con actores del ecosistema digital para el eficiente y oportuno desarrollo de las actividades y líneas de acción del Centro Nacional de Seguridad Digital.

17.2. La Presidencia del Consejo de Ministros, en el marco de lo dispuesto en el presente decreto de urgencia, puede establecer nuevas líneas de acción.

Artículo 18. Procesos operativos del Centro Nacional de Seguridad Digital

18.1. El Centro Nacional de Seguridad Digital, conforme a sus líneas de acción, dirige los siguientes procesos operativos:

a) Gestión de alertas digitales.
b) Gestión de incidentes.
c) Gestión de seguridad de la información.
d) Gestión de riesgos digitales.
e) Gestión del Observatorio Nacional de Seguridad y Confianza Digital.
f) Gestión del equipo de respuestas ante incidentes de seguridad digital.
g) Análisis forense digital.
h) Monitoreo de operaciones de seguridad.
i) Gestión de seguridad de las comunicaciones.
j) Generación y transferencia de conocimiento.

18.2. La Presidencia del Consejo de Ministros, en el marco de lo dispuesto en el presente decreto de urgencia, puede establecer nuevos procesos operativos.

Artículo 19. Articulación entre el Sistema Nacional de Transformación Digital y el Sistema de Defensa Nacional

El Centro Nacional de Seguridad Digital es el componente articulador entre el Sistema Nacional de Transformación Digital y el Sistema de Defensa Nacional.

CAPÍTULO VI
EQUIPOS ESPECIALIZADOS EN SEGURIDAD Y CONFIANZA DIGITAL

Artículo 20. Conformación de equipos técnicos especializados en seguridad y confianza digital

20.1. La Presidencia del Consejo de Ministros conforma los equipos técnicos especializados en seguridad y confianza digital que involucren la participación articulada de expertos en materia de seguridad y confianza digital del Poder Legislativo, del Poder Judicial, del Ministerio Público, de la Policía Nacional del Perú, del Comando Conjunto de las Fuerzas Armadas, de la Dirección Nacional de Inteligencia, del sector privado de telecomunicaciones, del sector financiero, del sector de tecnología, de la academia, de la sociedad civil y ciudadanos.

20.2. La conformación de equipos técnicos especializados responde al contexto regulatorio, cambio tecnológico, evolución de los riesgos en el entorno digital, entre otros factores inherentes a una sociedad digital.

20.3. Los equipos técnicos especializados cooperan con el Centro Nacional de Seguridad Digital en el desarrollo y despliegue de acciones estratégicas para prevenir, mitigar, afrontar y proteger las actividades críticas nacionales ante incidentes de seguridad digital que afecten la seguridad nacional.

20.4. La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno y Transformación Digital, convoca a expertos nacionales e internacionales de los sectores público y privado, de la academia y de la sociedad civil; así como activa las capacidades nacionales del Estado, en recursos humanos y tecnológicos u otros que sean necesarios, en materia de seguridad y confianza digital, a fin de integrarlos al Centro Nacional de Seguridad Digital, en situaciones de crisis sanitaria, política o social que pongan en riesgo la estabilidad de los servicios del Estado y, en consecuencia, afecten a la población.

CAPÍTULO VII
SITUACIONES DE EMERGENCIA NACIONAL EN SEGURIDAD Y CONFIANZA DIGITAL

Artículo 21. Situaciones de emergencia nacional en seguridad y confianza digital

En situaciones de emergencia nacional en seguridad y confianza digital derivadas de acontecimientos catastróficos, de emergencia sanitaria, de crisis social u otras situaciones que afecten el bienestar nacional, la Secretaría de Gobierno y Transformación Digital en su calidad de ente rector en seguridad y confianza digital en el país, convoca y realiza contrataciones de bienes y servicios prioritariamente mediante contrataciones directas, que incluyan especialistas y expertos nacionales o internacionales en materia de seguridad y confianza digital, en concordancia con el artículo 27 del Texto Único Ordenado de la Ley 30225, Ley de Contrataciones del Estado."

DISPOSICIONES COMPLEMENTARIAS FINALES

PRIMERA. Actualización de la reglamentación
El Poder Ejecutivo, a propuesta de la Secretaría de Gobierno y Transformación Digital, en un plazo máximo de noventa (90) días contados a partir del día siguiente de la entrada en vigor de la presente ley, actualiza y aprueba los reglamentos del Decreto Legislativo 1412, Ley de Gobierno Digital; del Decreto de Urgencia 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital; y del Decreto de Urgencia 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.

La Secretaría de Gobierno y Transformación Digital convoca a diversos actores de los sectores público y privado, para que participen en el proceso de actualización de los reglamentos.

SEGUNDA. Oficial de seguridad digital
Toda mención al oficial de seguridad de la información se entenderá referida al oficial de seguridad digital.

TERCERA. Declaración de interés nacional del uso ético y el aprovechamiento de las tecnologías emergentes
Se declara de interés nacional el uso ético y el aprovechamiento de las tecnologías emergentes en favor de la confianza digital y de la reactivación económica en el país, a través del uso intensivo de la inteligencia artificial, la nanotecnología, el internet de las cosas, cadena de bloques, impresión 3D, entre otras que conforman la industria 4.0, de manera que se asegure la transparencia, predictibilidad, veracidad, seguridad, inclusión, accesibilidad, ética y confiabilidad en su interacción con las personas en favor del desarrollo del talento digital, la economía digital y la transformación digital del país.

CUARTA. Participación en el Consejo de Seguridad y Defensa Nacional

En los casos en los que la agenda del Consejo de Seguridad y Defensa Nacional incluya algún tema de seguridad digital, será de aplicación lo establecido en el penúltimo párrafo del artículo 6 del Decreto Legislativo 1129, Decreto Legislativo que regula el Sistema de Defensa Nacional, que habilita la participación de cualquier otro funcionario del Poder Ejecutivo y de otros poderes del Estado.

Dase cuenta.

Sala de Sesiones de la Plataforma de Videoconferencia del Congreso de la República.

Lima, miércoles 6 de julio de 2022.