CONGRESO DE LA REPÚBLICA
ÁREA DE TRÁMITE Y DIGITALIZACIÓN DE DOCUMENTOS
15 ENE 2021
RECIBIDO
Firma.....Hora.12:29

DICTAMEN RECAÍDO EN EL PROYECTO DE LEY 6544/2020-CR, QUE PROPONE 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.

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

PERÍODO ANUAL DE SESIONES 2020-2021

Dictamen 37-2020-2021-CDNOIDALD-CR

Señora Presidenta:

Ha ingresado para estudio y dictamen de la Comisión de Defensa Nacional, Orden Interno, Desarrollo Alternativo y Lucha Contra las Drogas, el siguiente proyecto de ley:

N°	Proyecto de Ley	Autor(a)	Grupo Parlamentario	Sumilla
1	6544/2020-CR	Daniel Urresti Elera	Podemos Perú	Proyecto de Ley que garantiza la ejecución de operaciones de Ciberseguridad y Seguridad Digital a través de un Centro Nacional de Ciberseguridad.

El presente dictamen fue aprobado con el voto UNÁNIMEde los presentes en la Décimo Octava Sesión Ordinaria de la Comisión, celebrada el 7 de diciembre de 2020. Votaron a favor los señores congresistas Benites Agurto, Guibovich Arteaga, Núñez Marreros, Pantoja Calvo, Pérez Mimbela, Puño Lecarnaqué, Rivas Ocejo, Saavedra Ocharán, Valer Collado, Vivanco Reyes, Yupanqui Miñano y Urresti Elera.

Se deja constancia de que en la citada sesión se encontraban con licencia los congresistas Bazán Villanueva, Benavides Gavidia y Vega Antonio, y que se acordó, con el voto unánime de los presentes, dispensar del trámite de aprobación del acta para ejecutar los acuerdos adoptados. Votaron a favor los señores congresistas Benites Agurto, Guibovich Arteaga, Núñez Marreros, Pantoja Calvo, Pérez Mimbela, Puño Lecarnaqué, Rivas Ocejo, Saavedra Ocharán, Valer Collado, Vivanco Reyes, Yupanqui Miñano y UrrestiElera.

I. SITUACIÓN PROCESAL

A. Ingreso de proyecto a la Comisión

El proyecto de ley6544/2020-CR,ingresó al Área de Trámite Documentario el 23/10/2020, y fue derivado el 02/11/2020 para su estudio y dictamen a la Comisión de Defensa Nacional, Orden Interno, Desarrollo Alternativo y Lucha Contra las Drogas, en calidad de únicacomisión dictaminadora.

B. Cumplimiento de los requisitos reglamentarios

La iniciativa legislativa materia de dictamen cumple con los requisitos generales y específicos señalados en los artículos 75, 76 y 77 del Reglamento del Congreso de la República, por lo cual se realizó el estudio correspondiente.

C. Vinculación con las Políticas de Estado del Acuerdo Nacional

El proyecto de ley se enmarcaconla séptima políticade Estado expresada en el Acuerdo Nacional,denominada:"Erradicación de la violencia y fortalecimiento del civismo y de la seguridad ciudadana"; que promueve normar y fomentar las acciones destinadas a fortalecer el orden público y el respeto al libre ejercicio de los derechos y al cumplimiento de los deberes individuales; así como alanovena política de Estado denominada Política de "Seguridad Nacional"; y en la vigésima política de Estado "Desarrollo de la Ciencia y la Tecnología".

II. CONTENIDO DE LA PROPUESTA

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 establecer medidas de carácter excepcional que garanticen la seguridad en el ciberespacio, frente a las amenazas o los 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 artículo 2,referido alámbito de aplicación, señala que la ley es aplicable a todas las entidades de la Administración Pública comprendidas en el Artículo I del Título Preliminar del Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo N° 006-2017-JUS, a las organizaciones de la sociedad civil, sectores económicos y de servicios, ciudadanos y academia.

En el artículo 3se establece que la ley persigue los siguientes objetivos: (1) Asegurar el máximo nivel de seguridad de la información que se genera en el ciberespacio y 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 o ataques en el ciberespacio.

El artículo 4desarrolla lasdefiniciones en torno a la ciberseguridad, activos en la infraestructura del Estado, seguridad digital, y gobierno digital, concordantes con las normas vigentes en dichas materias.

En cuanto a lasdisposiciones complementarias finales, las tres primeras disponen lo siguiente: Primera: Declaración de interés nacional para la creación del Centro Nacional de Ciberseguridad del Perú-CENACI. Segunda: La Gestión y Coordinación Interinstitucional yTercera: Aspectos del Reglamento.

Para la ejecución de la presente propuesta, en las tres disposiciones complementarias modificatorias, se contempla la modificación del Decreto Legislativo Nº 1412, Ley de Gobierno Digital,modificación del Decreto de Urgencia Nº 006-2020, que crea el Sistema Nacional de Transformación Digital, así como lamodificación del Decreto de Urgencia Nº 007-2020, 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; y en la única disposición complementaria derogatoria se deroga el artículo 7 del Decreto de Urgencia Nº 007-2020, que aprueba el marco de Confianza Digital y dispone medidas para su Fortalecimiento.

En la exposición de motivos se contempla un análisis técnico y legal que parte por lo expresado en la Constitución Política del Perú queinstituye 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 Nº 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 Digital, es el ente rector de la seguridad digital. Cabe mencionar también que la Política de Seguridad y Defensa Nacional, aprobada por Decreto Supremo N° 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.

Respecto a las definiciones de ciberseguridad y seguridad digital, la exposición de motivos señala que el término"ciberseguridad" es más conocido que el de

seguridad digital; la ciberseguridad por lo general está relacionada a las capacidades para hacer frente a los denominados ciberataques; y que si bien, la seguridad digital versa sobre lo mismo, este último sevincula másala interoperabilidad y de poner a los ciudadanos los "servicios" del Estado de manera digitalizada.

Sedestaca 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 -como señala el Reporte de Ciberseguridad-2020 de la OEA[1]. Así también resalta lo señalado por Nayia Barmpaliou, Jefa de Políticas e Iniciativas Públicas del Centro para la Ciberseguridad del Foro Económico Mundial, quien señala que la ciberseguridad en la era de la hiperconectividad y de las pandemias, *marcará un punto de inflexión fundamental en la senda mundial y ha acentuado como nunca antes nuestra dependencia de la infraestructura digital*; la transformación digital por efectos de la pandemia experimentará una aceleración en la puesta en operación la transformación digital; y por ende, va a reconfigurar las vidas de las personas a nivel mundial, siendo así que *en el contexto de un ecosistema digital de vulnerabilidades...;los cibercriminales 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.*

Se menciona también en la exposición de motivos, que el Reporte de Ciberseguridad-2020 de la OEA, cuando se refiere al Perú, indica que: "*si bien Perú aún no cuenta con una Estrategia Nacional de Seguridad Cibernética, sí ha puesto en marcha una Política Nacional de Ciberseguridad que, entre otras cosas, destaca la necesidad de crear una Estrategia Nacional de Ciberseguridad y un Comité Nacional de Ciberseguridad*". En tal sentido, se requiere dar un giro y un enfoque de 360 grados para cambiar el paradigma y armonizar con el real nivel de capacidades de ciberseguridad que tenemos como país. El Reporte de Ciberseguridad-2020 del BID-OEA, mencionaque para medir las capacidades de ciberseguridad de un País se debe tomar en cuenta el "Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones" (CMM), que es un modelo desarrollado por el Centro Global de Capacidad en Seguridad Cibernética (GCSCC) de la Universidad de Oxford, que busca como propósito contar con un medio de evaluación que sigue cinco etapas: inicial (política y estrategia de ciberseguridad); formativa (cultura cibernética y sociedad); consolidada (educación, capacitación y habilidades en ciberseguridad); estratégica (marcos legales y regulatorios); y dinámica (estándares, organizaciones y tecnologías); para medir de manera confiable la capacidad de seguridad cibernética.Para el caso del Perú, el Informe de Ciberseguridad señala –*como se recoge de la*

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

exposición de motivos-, se ha podido notaravances respecto al año 2016 frente al año 2020. Según el citado Reporte de Ciberseguridad, *únicamente 7 países de los 32 analizados en este reporte cuentan con un plan de protección de su infraestructura crítica, y 20 han establecido algún tipo de grupo de respuesta a incidentes, llamado CERT o CSIRT. Esto limita la capacidad de identificar ataques y responder oportunamente a los mismos.*

En el Perú, la Secretaria de Gobierno Digital, -de acuerdo con el Decreto Legislativo Nº 1412,es el órgano de línea, con autoridad técnico normativa a nivel nacional, responsable de formular y proponer políticas nacionales y sectoriales, planes nacionales, normas, lineamientos y estrategias en materia de informática y de Gobierno Electrónico. La Secretaría de Gobierno Digital es el órgano rector de la Seguridad Digital del país; como del Sistema Nacional de Transformación Digital; y es la que administra las Plataformas Digitales del Estado Peruano, liderando los procesos de innovación tecnológica y de transformación digital del Estado, y, por consiguiente,siguelas recomendaciones de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) en materia de gestión de riesgos de seguridad digital. Es un órgano de línea de la Presidencia del Consejo de Ministros.

Por lo señalado, es preciso mencionar que el Perú tiene un arreglo institucional que permite regular, dirigir, orientar y supervisar la seguridad digital en el país, el cual es gestionado por la Presidencia del Consejo de Ministros a través de la Secretaría de Gobierno Digital, tal como se señala en el Decreto Supremo Nº 022-2017-PCM, Decreto Legislativo Nº 1412 y la Ley Nº 30999. Así también, el Perú cuenta con un CSIRT nacional, denominado PeCERT, que a través de un informe y análisis técnico indica los distintos ataques a la seguridad de la información de entidades públicas y empresas privadas en el ciberespacio. El documento es preparado por la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros (PCM), el Comando Conjunto de las Fuerzas Armadas, el Ejército del Perú, la Marina de Guerra del Perú, la Fuerza Aérea del Perú, la Dirección Nacional de Inteligencia, la Policía Nacional del Perú, entre otras instituciones[2].

Por último, según se presenta en la exposición de motivos, se plantea declarar de preferente interés nacional y necesidad pública la creación de un Centro Nacional de Ciberseguridad del Perú-CENACI, puesto que será un hito valioso para replantear las estrategias de Seguridad Digital como país, paraque sirva como el principal soporte con que debe contar el Estado peruano para hacer frente a las diversas amenazas que afecten la seguridad en el ciberespacio.

[2]https://cdn.www.gob.pe/uploads/document/file/1373500/Alerta%20integrada.

III. OPINIONES E INFORMACIÓN

A. Opiniones solicitadas

La Comisión solicitó opinión a las siguientes instituciones, conforme se detalla a continuación:

Proyecto de Ley 6544/2020-CR		
Institución	**N° de Oficio**	**Fecha de envío**
Presidencia del Consejo de Ministros	Oficio 649- 2020-2021–CDNOIDALCD/CR	03/11/2020
Ministerio del Interior	Oficio 638- 2020-2021–CDNOIDALCD/CR	03/11/2020
Ministerio de Defensa	Oficio 645- 2020-2021–CDNOIDALCD/CR	03/11/2020
Ministerio de Transportes y Comunicaciones	Oficio 646- 2020-2021–CDNOIDALCD/CR	03/11/2020
Ministerio de Justicia y Derechos Humanos	Oficio 647- 2020-2021–CDNOIDALCD/CR	03/11/2020
Superintendencia de Banca, Seguros y AFP´s	Oficio 648- 2020-2021–CDNOIDALCD/CR	03/11/2020
Asociación de Bancos del Perú	Oficio 650- 2020-2021–CDNOIDALCD/CR	03/11/2020

B. Opiniones recibidas

Mediante oficio 469-2020-DINI-01, recibido el 27 de noviembre de 2020, la Dirección Nacional de Inteligencia señala que siendo el propósito de la norma garantizar la seguridad en el ciberespacio frente a amenazas o ataquesque afecten a la Seguridad Nacional, se estima conveniente revisar la necesidad de 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.

Agrega que, sería recomendable 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. En ese sentido, se debe modificar y ampliar el encargo a la Comisión Especial Multisectorial por designar, en el sentido dereconocer y orientar la creación del Centro Nacional de Ciberseguridad del Perú– CENACI, sobre la base del Centro Nacional de Seguridad Digital, creado mediante el Decreto de Urgencia N° 007-2020.

Señala también que se debe considerar en la fórmula legal del proyecto, mientras se define la necesidad de creación de unsistema, responsabilidades y funciones, la gestión de la Seguridad Digital en el Perúdeberá mantenerse conforme lo establece la Ley de Gobierno Digital, aprobada a través del Decreto Legislativo N° 1412 y la Ley N° 30618, que modifica el Decreto Legislativo N° 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 las tareas y actividades de Seguridad Digital; asícomo las normas que para tal efecto se deriven de las mismas.

Al 26/11/2020, en el portal institucional del Congreso de la República, no se han registrado ni ingresado opiniones ciudadanas.

C. Mesas de Trabajo

Reunión Presencial: el 4 de noviembre de 2020 se llevó a cabo una reunión de trabajo entre funcionarios de la Secretaria de Gobierno Digital y el equipo técnico de la Comisión de Defensa Nacional, Orden Interno, Desarrollo Alternativo y Lucha contra las Drogas. En dicha reunión los funcionarios de la Secretaria de Gobierno Digital sostuvieron que, si bien la propuesta pretende declarar de interés nacional un Centro Nacional de Ciberseguridad, el Decreto de Urgencia Nº 007-2020 que aprueba el Marco de Confianza Digital para proteger las personas en el entorno digital crea como una *plataforma virtual* el Centro Nacional de Seguridad Digital (CNSD). Precisan que el Congreso de la República según el artículo 79 de la Constitución Política del Perú no tiene iniciativa para crear ni aumentar gastos públicos; pero que en líneas generales encuentran viabilidad a la propuesta legislativa, pero con modificaciones que podrían ser contempladas con un nuevo texto sustitutorio.

Reunión Virtual: el 24 de noviembre de 2020 se llevó acabo una reunión virtual en la que participaron funcionarios de la Presidencia del Consejo de Ministros, de la Secretaria de Gobierno Digital, del Ministerio de Defensa, de la Dirección Nacional de Inteligencia, de la Superintendencia de Banca, Seguros y AFP, y de la Asociación de Bancos del Perú – ASBANC.

En opinión de la *Superintendencia de Banca, Seguros y AFP*:El proyecto de ley abre un espacio como una oportunidad decoordinación necesaria a nivel nacionalcomo sectorial. Así también, precisaron que se debe modificar el artículo 11 de la iniciativa legislativa para que exista coordinación con la SBS, que como organismo encargado de la regulación y supervisión del Sistema Financiero de Seguros y del Sistema Privado de Pensiones en el Perú, esde carácter necesario.

En opinión de la *Asociación de Bancos del Perú – ASBANC*: El artículo 3 del proyecto de ley señala *asegurar el máximo nivel de seguridad de la información que se genera en el ciberespacio...*, en opinión de ASBANC este objetivo no podría ser realizable y que lo óptimo sería una modificación señalando que: proponen *alcanzar un nivel de seguridad.* Señalaron también que es importante que se considere al Sistema Financiero Nacional dentro de los activos críticos nacionales. Así también, destacan que, en la primera disposición complementaria final, se considere como principal valor salvaguardar la seguridad de las personas;y en lo referido a la gestión y coordinación interinstitucional se considere la participación de otros sectores y actores que podrían integrarse a futuro. Respecto a la tercera disposición referida al reglamento de la iniciativa legislativa, se considere a la Asociación de Bancos del Perú – ASBANC para que participe en la elaboración del reglamento.
Asimismo, respecto a la tercera disposición complementaria modificatoria, referida al Registro Nacional de Incidentes de Seguridad Digital (artículo 8), interrogaron n ¿quiénesvan a tener esa información?Así también, respecto al artículo 9, referido a las obligaciones del proveedor de servicios digitales, señalaron que es importante considerar que cuándo se hace un reporte de la incidencia se establezca determinada información sobre ¿cómosería?, ¿con qué?, ¿en qué momento?; por lo que consideran necesario e importante participar en la elaboración del reglamento de la iniciativa legislativa. Finalmente, señalaronestar de acuerdo con la definición de seguridad digital; e indican que se debe tomar en cuenta que muchas de las amenazasno necesariamente provienen por unataque cibernético, sino queincluso puede ser mediante cualquier dispositivo electrónicoque no necesariamente esté conectado a una red de internet.Consideran necesario incorporar el término de ciberesilencia.

En opinión de la *Dirección Nacional de Inteligencia*:es necesario efectuar algunas modificaciones al proyecto de ley, por lo que proponen que si el propósito de la norma es garantizar la seguridad en el ciberespacio frente a amenazas o ataques que afecten a la Seguridad Nacional, esconveniente revisar la necesidad de integración del Centro Nacional de Ciberseguridad del Perú al Sistema de Defensa Nacional, considerado un Sistema de Ciberseguridad Nacional o Sistema Nacional de Seguridad Digital. De otro lado, mencionan que la Comisión Especial Multisectorial,a fin de evitar confusiones futuras por malas interpretaciones de conceptos y definiciones (artículo 4),sea la que defina los términos y/o los conceptos.

Por otro lado, precisan que la creación del Centro Nacional de Ciberseguridad del Perú tenga como base el Centro Nacional de Seguridad Digital creado por Decreto de Urgencia N° 007-2020; que la Comisión Multisectorial determine las responsabilidades, funciones y alcances en el ámbito de ciberseguridad nacional o seguridad digital, de tal forma que no exista duda de las acciones que deba tomar cada quién como parte de las respuestas a incidentes de seguridad digital. Por último, consideran que mientras se defina la necesidad de creación de un sistema, responsabilidades y funciones, la gestión de la Seguridad Digital en el

Perú debe mantenerse como está establecido en la Ley de Gobierno Digital aprobadopor Decreto Legislativo N° 1412; así como por la Ley N° 30618 que modifica el Decreto Legislativo N° 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; y la Ley N° 30999, Ley de Ciberdefensa.

En opinión del *Ministerio de Defensa* si bien existen normas como la Ley de Gobierno Digital aprobada por Decreto Legislativo N° 1412, el Decreto de Urgencia N° 006-2020, que crea el Sistema Nacional de Transformación Digital, y el Decreto de Urgencia N° 007-2020, que aprueba el marco de Confianza Digital y dispone medidas para su Fortalecimiento, las normas pueden ser perfectibles para hacerlas más fuertes,tomando en consideración también la participación del sector privado.

En opinión de la *Secretaria de Gobierno Digital* el Perú ha logrado avances significativos en materia de Seguridad Digital, y cuenta con normas como la Ley de Gobierno Digital, aprobada por Decreto Legislativo N° 1412; los Decretos de Urgencia N° 006-2020y 007-2020, entre otras normas, lo que sitúa al Perú como una nación en ventaja frente a los países de la región.Asimismo, expresaron estar de acuerdo con que debe incorporarse la definición de ciberesilencia o denominada también resiliencia digital, asíde cómola determinación de los activos críticos y el reporte de incidentes al Centro Nacional de Seguridad Digital. Por último, la Secretaria de Gobierno Digital destaca que el paísestá avanzando para fortalecer el Centro Nacional de Seguridad Digital, por lo queencuentran viable el proyecto de ley, considerando modificaciones.

IV. MARCO NORMATIVO

- Constitución Política del Perú.
- Ley N° 29158, Ley Orgánica del Poder Ejecutivo.
- Ley Nº 30999, Ley de Ciberdefensa.
- Ley Nº 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 N° 012-2017-DE que aprueba la Política de Seguridad y Defensa Nacional.
- Decreto Supremo N° 022-2017-PCM, que aprueba el Reglamento de Organización y Funciones (ROF) de la Presidencia del Consejo de Ministros (PCM) y su modificatoria
- Decreto Legislativo Nº 1412, que aprueba la Ley de Gobierno Digital.
- Decreto Supremo N° 050-2018-PCM, que establece la definición de Seguridad Digital de ámbito nacional.

- Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado mediante Decreto Supremo N° 004-2019-JUS.
- Decreto de Urgencia Nº 006-2020, que crea el Sistema Nacional de Transformación Digital.
- Decreto de Urgencia Nº 007-2020, Decreto de urgencia que aprueba el marco de Confianza Digital y dispone medidas para su Fortalecimiento
- Decreto de Urgencia N° 025-2020, Medidas urgentes destinadas a reforzar el sistema de vigilancia y respuesta sanitaria.
- Decreto Supremo N° 008-2020-SA, 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 Nº 044-2020-PCM, 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 N° 080-2020-PCM, 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 N°1497, 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. ANALISIS DE LA PROPUESTA

A. Respecto a las definiciones de Ciberseguridad y Seguridad Digital

La Unión Internacional de Telecomunicaciones (UIT), organismo especializado para las tecnologías de la información y la comunicación–TIC de las Naciones Unidas define que la "ciberseguridad" "*Describe 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*".

Por otro lado, en el artículo 30 del Decreto Legislativo N° 1412, que aprueba la Ley de Gobierno Digital en el Perú, así como el Decreto Supremo N° 050-2018-PCM, que aprueba la definición de seguridad digital en el ámbito nacional,señala 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 entorno. Se sustenta en la articulación con actores del sector público, sector privado y otros quienes apoyan en la implementación de controles, acciones y medidas. Debe tenerse presente para estos efectos los siguientes aspectos:

1. La confianza en el entorno digital o también denominada confianza digital emerge como resultado de cuánveraz, predecible, seguro y confiable son las interacciones digitales que se generan entre empresas, individuos o cosas.
2. Las medidas proactivas y reactivas comprenden tecnología, políticas, controles, programas de capacitación y sensibilización que tienen por finalidad preservar la confidencialidad, integridad y disponibilidad de la información contenida en el entorno digital.
3. Los riesgos en el entorno digital o riesgo de seguridad digital es resultado de una combinación de amenazas y vulnerabilidades en el entorno digital. La gestión del riesgo de seguridad digital comprende los procesos que garantizan que las acciones o medidas son apropiadas con los riesgos y objetivos económicos y sociales en juego.
4. La prosperidad económica y social comprende la creación de riqueza, la innovación, la competitividad, entre otros, así como aspectos vinculados con las libertades individuales, salud, educación, cultura, participación democrática, ciencia, ocio y otras dimensiones del bienestar en las que el entorno digital está impulsando el progreso.

B. Una mirada al Perú en el contexto mundial de la Seguridad Digital

La prestación de servicios digitales de parte de las entidades públicas y organizaciones privadas en el país y el resto del mundo ha crecido de manera exponencial en los últimos años. Los servicios digitales son utilizados por millones de personas para el desarrollo de sus actividades económicas, sociales, educativas, entre otros; no obstante, ello también ha incrementado de manera alarmante los ataques y amenazas digitales que afectan la seguridad y privacidad, sin que a la fecha se establezcan medidas efectivas para su prevención o atención. Por otro lado, mientras la economía digital sigue evolucionando a una velocidad vertiginosa, impulsada por la capacidad para recopilar, utilizar y analizar un volumen masivo de información que se realiza en diversas plataformas digitales, se espera que para el año 2022 el tráfico IP mundial alcance unos 150.700 GB por segundo,lo que hace que la inmensa infraestructura tecnológica de computadoras, redes LAN, WAN, dispositivos móviles, sistemas de transmisión inalámbrica, por cable, centros de datos,

sistemas de satélites, entre otros dispositivos,en el corto plazo, vulnerables a los ciberataques[3].

En el Reporte de Ciberseguridad-2020[4], *-como se recoge de la exposición de motivos-* según el Ministro de Relaciones Exteriores de la República de Estonia, Sven Mikser, en la última década han surgido diversas amenazas en el ciberespacio *que requieren la atención de los gobiernos de todo el mundo*, las mismas que tienen que ver *con la creciente inestabilidad causada por el delito informático, las intrusiones en redes críticas y las operaciones motivadas políticamente*. Si bien, estos elementos han estado o están en proceso de implementación en las agendas políticas de los Estados de todo el mundo, difiere mucho entre los Estados, por lo que se hace necesario armonizar esfuerzos de los Estados para aumentar su ciberseguridad; y se requiere *incentivar a los Estados para que cooperen en un campo que convencionalmente se consideraría un área relacionada con sus asuntos internos*.

Por otro lado, según el Informe de Cibercrimen ThreatMetrix , América Latina es *un foco para realizar fraude en la creación de cuentas* (alrededor del 20%), en relación al resto del mundo (12,2%), lo cual de cierta manera propicia un ambiente de mayor riesgo y vulnerabilidades en el espacio digital, como lo señalan Miguel Porrúa del BID y Belisario Contreras de la OEA; además, los ciberataques en esta parte de la región han ido en aumento, afectando principalmente a las instituciones financieras. Según Pawel Herczynski, Director Gerente de PCSD y Respuesta a Crisis, Servicio Europeo de Acción Exterior, la ciberseguridad es crítica para nuestra prosperidad y seguridad, ya que no sólo amenaza las economías del mundo, sino también el funcionamiento de las democracias, libertades y valores; por lo que esnecesario protegernos contra las amenazas cibernéticas. Tanto la infraestructura civil como la capacidad militar dependen de sistemas digitales seguros.

La Organización de los Estados Americanos (OEA) ha indicado,en el Estudio de Ciberseguridad en América Latina y el Caribe, que alrededor del 37% de los ciberataques que se concretan están dirigidos hacia los bancos y entidades financieras, mientras que el resto va dirigido a personas, proveedores o clientes (63%). Así también, en el caso del sector financiero se ha identificado alrededor de 18 millones de dólares en pérdidas económicas y aproximadamente 17 millones de dólares de pérdidas económicas en servicios públicos y energía[5]; lo que impacta directamente a la competitividad y productividad tanto de las

[3] Centro de Altos Estudios Nacionales-Escuela de Posgrado-CAEN-EPG. Cuadernos de Trabajo - Número Extraordinario 6: Edición 2020: Conectividad Digital:Factor Estratégicopara la Seguridad y Desarrollo Nacional. Rodrigo Guillen en "Redes 5G Calentando la Nueva Guerra Fría": https://drive.google.com/file/d/1LRX8PnLxJ6mo_Od_kO4vR52cbub2SZ7K/view?fbclid=IwAR3yA20dVHgQNhpa_Xaoi7QAtdjr38ZnWBOwnDn9siOR_C7a_7Xylm2FDNo.

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

[5] https://www.asbanc.com.pe/Paginas/Noticias/DetalleNoticia.aspx?ItemID=828&lang=es

empresas como de lasentidades de gobierno. De otro lado, el Informe del observatorio de la Ciberseguridad en América Latina y el Caribe del año 2016, documento elaborado por el BID y la OEA, señala que la "(...) *mayoría de nuestros países aún están poco preparados para contrarrestar la amenaza del cibercrimen* (...)".Indica que, si bien el Perú ha trabajado arduamente en labores de protección, América Latina y el Caribe tienen que trabajar con mayor énfasis en labores vinculadas a la prevención y mitigación de riesgos en el ciberespacio. Agrega que "*cuatro de cada cinco países no tienen estrategias de ciberseguridad o planes de protección de infraestructura crítica. Dos de cada tres no cuentan con un centro de comando y control de seguridad cibernética, más aún señala que la gran mayoría de las fiscalías carece de capacidad para perseguir los delitos cibernéticos*". Es importante indicar que el referido informe ha identificado algunos desafíos para el Perú, como:

1. Diseñar y establecer un marco de seguridad digital para el país
2. Establecer una estrategia y una cadena de mando clara en seguridad digital del país.
3. Fortalecer las capacidades de Ciberdefensa de las Fuerzas Armadas.
4. Fortalecer las capacidades técnicas de la División de Investigación de Delitos de Alta Tecnología (DIVINDAT) de la Policía Nacional del Perú, para el manejo de evidencia electrónica.
5. Fortalecer la conciencia social de seguridad cibernética.
6. Mejorar las capacidades de los docentes de universidades y empresas de capacitación.

El Perú es el segundo país en América Latina que recibe más ataques cibernéticos, y el origen de ataques para otras economías. Según el Microsoft Security Intelligence Report del 2017[6], el 16.9% de las computadoras en el Perú están infectadas con malware, en comparación con el 7.8% del promedio mundial. Más aun, el mismo reporte indica que la infección a través de troyanos (8.13%), gusanos (5.7%) y virus (0.92%) en nuestro país está por encima del promedio mundial. De las estadísticas reportadas por Kaspersky Lab, el 42% de usuarios peruanos sufrieron un intento de ataque de malware. Esta información presenta un panorama preocupante en torno a la seguridad y confianza digital, ubicando al Perú en el segundo lugar del ranking regional debajo de Brasil. Así mismo, informa que las infecciones se incrementaron en 74% en el último semestre del 2016. Según la Encuesta Global de Software de BSA de junio 2018[7], el Perú tiene una tasa de instalación de software sin licencia de 37%, lo cual agrega una variable adicional a la poca cultura y asequibilidad que implica la seguridad digital.

Así también, se ha identificado que lamayoría de los ciudadanos tiene poco conocimiento en materia de seguridad digital, lo que ocasiona que no tomen

[6]https://info.microsoft.com/ww-landing-Security-Intelligence-Report-Vol-23-Landing-Page-eBook.html
[7]https://www.bsa.org/~/media/Files/StudiesDownload/2018_BSA_GSS_Report_eslatam.pdf

medidas preventivas adecuadas para resguardar su información, y, por tanto, también su integridad personal. Las redes sociales son un claro ejemplo de ello, hoy en día, las personas publican un volumen inmenso de información por sus redes, como ubicación, datos de trabajo, datos financieros, entre otros; que, al ser atacados, pueden ocasionar la pérdida del control sobre ellos. En esa línea, 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:

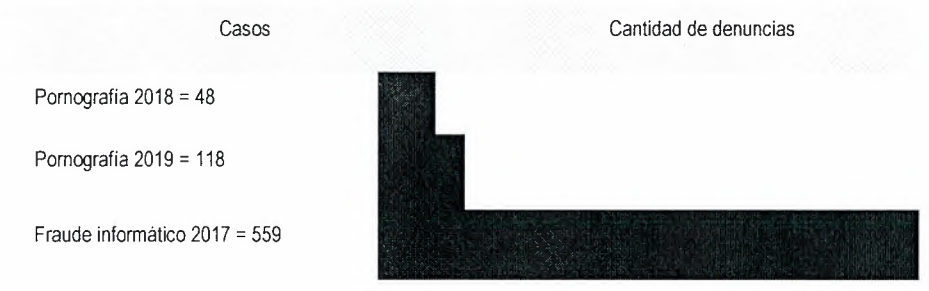
1. Según el reporte de ESET Security Report - Latinoamérica 2019[8]el Perú es el segundo país de América Latina más afectado por incidentes de seguridad (71%), solo después de México (72%). Asimismo, es el segundo país con mayor presencia de variantes de Ransomware (204).
2. Entre los principales ciberataques se encuentra el acceso indebido (61%), el robo de información (58%) y la privacidad de la información (48%).
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 ha 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 afectatanto a los ciudadanos como a organizaciones del sector público yprivado.

En la siguiente figura mostramos el aumento de incidentes,así como las denuncias realizadas por los delitos cibernéticos (Figura 1).

[8]https://www.welivesecurity.com/wp-content/uploads/2019/07/ESET-security-report-LATAM-2019.pdf

Figura 1. Casos de pornografía infantil y denuncias



Fuente: DIVINDAT

Finalmente, la Unión Internacional de Telecomunicaciones (UIT) elabora anualmente una evaluación del estado de la ciberseguridad en las economías miembros, en base a cinco pilares: (i) Medidas legales, (ii) Medidas técnicas, (iii) Medidas organizativas, (iv) Desarrollo de capacidades, y (v) Cooperación. En el estudio del año 2018 el Perú se ubicó en el puesto 95 de 193 economías evaluadas. Cabe destacar que según el último "Reporte de Ciberseguridad: Riesgos, Avances y el Camino a seguir en América Latina y el Caribe del 2020", publicado por el Banco Interamericano de Desarrollo (BID) y la Organización de los Estados Americanos (OEA)[9]; a pesar del progreso realizado en la región, en parte con el apoyo de la OEA, -señalado líneas arriba- en el año 2016 **cuatro de cada cinco** países ***carecían de estrategias de ciberseguridad o de un plan de protección de infraestructura crítica***.Hoy en día, si bien los gobiernos de la región son más conscientes de la necesidad de proteger el espacio digital del que depende el funcionamiento de una sociedad; sin embargo, enfatizan que la ciberseguridad ***no ha ganado presencia en la agenda política de la región con la urgencia que se esperaría***; indican además que hasta principios del año 2020, solo 12 países de la región como Colombia (2011 y 2016), Panamá (2013), Trinidad y Tobago (2013), Jamaica (2015), Paraguay (2017), Chile (2017), Costa Rica (2017), México (2017), Guatemala (2018), República Dominicana (2018), Argentina (2019) y Brasil (2020), *han aprobado una**estrategia nacional de ciberseguridad, y únicamente (solo) 10 países***

[9]https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf.

han establecido un organismo gubernamental central responsable de la gestión de la ciberseguridad.

C. La crisis sanitaria mundial y sus efectos en la Seguridad Digital

Desde el 30 de enero de 2020, día en que la Organización Mundial de la Salud (OMS) declaró el brote del coronavirus (COVID-2019) como una emergencia de salud pública de relevancia internacional, y el 11 de marzo de 2020 la caracterizó como una pandemia por su rápida expansión a nivel global, el COVID-19 no solo ha afectado (*y viene afectando*) a las naciones en asuntos de salud pública, también viene generando 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 de otro lado por el bajo nivel de articulación de capacidades en materia de seguridad digital.En esa línea, la misma Organización Mundial de la Salud (OMS)ha señalado que el número de ciberataques en el mundo se ha multiplicado por cinco y llama a aumentar su vigilancia[10]; sobre ello, debemos referir 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 virus SARS-CoV-2 (COVID-19), ha 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. Cabe destacar también que desde el comienzo de la pandemia la Organización Mundial de la Salud fuevíctima de ciberataques dirigidos contra su personal, así como de estafas por correo electrónico contra los ciudadanos en el mundo. Recientemente se filtraron en Internet cerca de 450 direcciones y contraseñas de correos electrónicos activos de la OMS, junto con las de otros miles de personas que trabajan en la respuesta al nuevo coronavirus. Si bien, la filtración de esas credenciales no puso en peligro los sistemas de la OMS, el ataque sí ha afectado un sistema de red externa antiguo que es utilizado por personal en actividad, jubilados y asociados. En ese sentido, la OMS viene colaborando con el sector privado para establecer sistemas internos más sólidos y reforzar las medidas de seguridad, y está proporcionando formación al personal sobre los riesgos relacionados con la seguridad cibernética. La OMS pide a los ciudadanos que se mantengan vigilantes frente a los correos electrónicos fraudulentos y recomienda el uso de fuentes fiables para obtener información objetiva sobre la COVID-19 y otras cuestiones de salud.

[10]https://www.who.int/es/news/item/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance

D. Algunas estadísticas respectoa la confianza digital en el Perú

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[11]. Adicionalmente, según datos del Instituto Nacional de Estadística e Informática (INEI) a setiembre 2019[12]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.

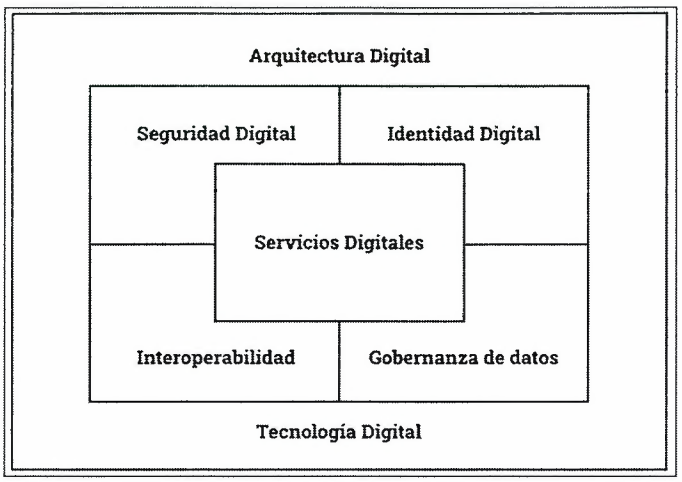
Un aspecto importante a considerar es el porcentaje de población que hace uso de Internet a través del teléfono celular, que es el 82.6%.Con respecto a las actividades que realiza la población en Internet es mayormente para comunicarse (90.2%), obtener información (89.3%) y en actividades de entretenimiento (85.5%), operaciones en banca electrónica (14.5%), transacciones con entidades públicas (12%), comprar productos y/o servicios (13.4%), y vender productos y/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 ofreciendocanales digitales para atender dicha demanda.

E. Normativa nacional respecto a laSeguridad Digital y Gobierno Digital

En los últimos años el Perú ha tenido un avance significativo en materia de normativa sobre la seguridad digital; en tal sentido principalmente, el Decreto Legislativo Nº 1412, Ley de Gobierno Digital (publicado el 13 de setiembre de 2018), establece ***el marco de gobernanza del gobierno digital*** *para la adecuada gestión de la identidad digital, servicios digitales, arquitectura digital, interoperabilidad,* ***seguridad digital*** *y datos digitales; y define también el régimen jurídico aplicable al uso transversal de tecnologías digitales en la digitalización de procesos y prestación de servicios digitales por las entidades de la Administración Pública en los tres niveles de gobierno* (lo subrayado es nuestro). En la siguientefigura (2)señalamos el ámbito del gobierno digital:

[11] Ver: https://www.ecommercenews.pe/ecommerce-insights/2019/crecimiento-del-comercio-electronico-en-peru.html
[12] Ver: https://www.inei.gob.pe/media/MenuRecursivo/boletines/ticdiciembre.pdf

Figura 2. Ámbitos del gobierno digital



Fuente: Decreto Legislativo N° 1412

Asimismo, el precitado Decreto Legislativo señala en su artículo 8 que "*La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, es el ente rector en materia de gobierno digital, comprende tecnologías digitales, identidad digital, interoperabilidad, servicio digital, datos, seguridad digital y arquitectura digital. Dicta las normas y establece los procedimientos en materia de gobierno digital y, es responsable de su operación y correcto funcionamiento*"; y dispone en su artículo 31 que "*el marco de Seguridad Digital del Estado peruano se constituye en el conjunto de principios, modelos, políticas, normas, procesos, roles, tecnología y estándares mínimos que permitan preservar la confidencialidad, integridad, disponibilidad de la información en el entorno digital administrado por las entidades de la Administración Pública*"; adicionalmente, indica en su artículo 32 que "el marco de Seguridad Digital del Estado peruano tiene los siguientes ámbitos:

a. **Defensa:** El Ministerio de Defensa (MINDEF) en el marco de sus funciones y competencias dirige, supervisa y evalúa las normas en materia de Ciberdefensa.
b. **Inteligencia:** La Dirección Nacional de Inteligencia (DINI) como autoridad técnica normativa en el marco de sus funciones emite, supervisa y evalúa las normas en materia de inteligencia, contrainteligencia y seguridad digital en el ámbito de esta competencia.
c. **Justicia:** El Ministerio de Justicia y Derechos Humanos (MINJUS), el Ministerio del Interior (MININTER), la Policía Nacional del Perú (PNP), el

Ministerio Público y el Poder Judicial (PJ) en el marco de sus funciones y competencias dirigen, supervisan y evalúan las normas en materia de ciberdelincuencia.

d. **Institucional:** Las entidades de la Administración Pública deben establecer, mantener y documentar un Sistema de Gestión de la Seguridad de la Información (SGSI).

Cabe destacar *-como señala la exposición de motivos-* que en el 2020 mediantelos Decretos de Urgencia N° 006-2020 se crea el Sistema Nacional de Transformación Digital, estableciendo el marco de gobernanza para la transformación digital en el país para integrar al sector público, privado y la academia en un sistema para promover la seguridad y confianza digital; y el Decreto de UrgenciaN° 007-2020 que aprueba el Marco de Confianza Digital, para proteger a las personas en el entorno digital, integrandoademás a instituciones como el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI), la Autoridad Nacional de Protección de Datos Personales, la Autoridad Nacional de Transparencia y Acceso a la Información Pública, la Presidencia del Consejo de Ministros en su calidad de ente rector de la Seguridad Digital; y crea el Centro Nacional de Seguridad Digital (CNSD) como una "plataforma virtual" (lo subrayado es nuestro).

Con respecto al Decreto de Urgencia No 007-2020, que crea el marco de Confianza Digital, comprende tres (03) ámbitos: a) Protección de datos personales y transparencia, b) Protección del consumidor y c) Seguridad Digital. En el artículo 4 (4.1), el marco de confianza digitalse *constituye en el conjunto de principios, modelos, políticas, normas, procesos, roles, personas, empresas, entidades públicas, tecnologías y estándares mínimos que permiten asegurar y mantener la confianza en el entorno digital*. Así también, respecto a la Seguridad Digital se señala que la Presidencia del Consejo de Ministros (PCM), a través de la Secretaría de Gobierno Digital, en su calidad de ente rector de seguridad digital en el país, norma, dirige, supervisa y evalúa la materia de seguridad digital. En el artículo 7 se señala medidas para el fortalecimiento de la confianza digital, entre las cuales se tiene la creación del Centro Nacional de Seguridad Digital-*como una plataforma virtual-* en el ámbito de la Secretaría de Gobierno Digital; y se creael equipo de Respuestas a Incidentes de Seguridad Digital Nacional (CSIRT-Nacional), en el ámbito del Centro Nacional de Seguridad Digital.Finalmente, la referida norma indica en su numeral 9.3 del artículo 9 que "Las entidades de la administración pública deben implementar un Sistema de Gestión de Seguridad de la Información (SGSI), un Equipo de Respuestas ante Incidentes de Seguridad Digital cuando corresponda y cumplir con la regulación emitida por la Secretaría de Gobierno Digital". Se dispone, entonces, de un marco regulatorio que articula las capacidades para la gestión de incidentes de seguridad digital, gestión de riesgos de seguridad digital, protección de datos y protección de consumidor en el entorno digital.En esa línea, se emite el Decreto de Urgencia N° 006-2020, mediante el cual se crea el Sistema Nacional de

Transformación Digital, estableciendo el marco de articulación adecuado para el uso de tecnologías digitales en el Estado y sociedad, armonizando las necesidades y capacidades del sector público y sector privado, abordando temas como: talento digital, seguridad digital, economía digital, conectividad digital, etc.

Cabe señalar también, que el Perú cuenta con la Ley Nº 30999 Ley de Ciberdefensa, promulgada el 26 de agosto de 2019, norma que se circunscribe a la ejecución de operaciones de Ciberdefensa en y mediante el ciberespacio frente a las amenazas o los ataques que afecten la seguridad nacional; entiéndase por "Ciberdefensa" a la capacidad militar que permite actuar frente a amenazas o ataques realizados en y mediante el ciberespacio cuando éstos afecten la seguridad nacional[13].

Por último, es necesario mencionar, *-como se ha indicado en la exposición de motivos de la iniciativa legislativa-*, que en los últimos años en el Congreso de la República[14],se elaboraron tres proyectos de leyentre los años 2018 y 2019,referidos directamente a la Ciberseguridad y Seguridad Digital, y que luegose materializaron en un solo dictamen por acumulación conocido como la*Ley de Ciberseguridad*. Los proyectos en mención fueronel Nº *4237/2018-CR*, el *4344/2018-CR* y el *4352/2018-CR*.Cabe precisar que la Autógrafa derivada de los proyectos de ley fue materia de observación por el Presidente de la República. La observancia a la Autógrafa de Ley[15], entre otros puntos, refiere principalmente a que la autógrafa resulta contraria a los avances en materia de gobernanza digital reconocidos por la Organización para la Cooperación y el Desarrollo Económico (OCDE), por lo que de aprobarse ocasionaría un serio incumplimiento de las recomendaciones en materia digital al fraccionar la rectoría en seguridad digital, desconociendo lo establecido en la regulación vigente y poniendo en riesgo el cumplimiento de las recomendaciones para el ingreso del Perú a la OCDE. Así también, el Poder Ejecutivo, señaló que en materia de seguridad digital (ciberseguridad, según la Autógrafa de Ley), ya se encuentra normado por el Decreto Legislativo Nº 1412 Ley de Gobierno Digital, que establece los principios vinculados con la seguridad digital. El Ejecutivo también ha destacado *–como se recoge de la exposición de motivos-* que el Estudio de Gobernanza Pública de la Organización para la Cooperación y el DesarrolloEconómicos (OCDE) del año 2016, recomienda "*establecer el gobierno digital en el centro de la reforma del sector público*" (lo subrayado es nuestro), y de esa manera, sostiene que es la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros, la entidad que lidera los procesos de innovación tecnológica y de transformación digital del Estado peruano, y por tanto, es el ente rector del Sistema Nacional de Transformación Digital y

[13]https://busquedas.elperuano.pe/normaslegales/ley-de-ciberdefensa-ley-n-30999-1801519-5/.
[14]http://www2.congreso.gob.pe/sicr/tradocestproc/Expvirt_2011.nsf/visbusqptramdoc1621/04352?opendocument.
[15]https://leyes.congreso.gob.pe/Documentos/2016_2021/Observacion_a_la_Autografa/OBAU042372019091 1.pdf.

administra además las Plataformas Digitales del Estado Peruano; así también, el fortalecimiento de la gobernanza digital en el Perú ha sido reconocido en el Estudio de Gobierno Digital en el Perú de la OCDE del año 2019[16] (Digital Government in Perú: Working Closelywith Citizens que incluso recomienda considerar el establecimiento de un Centro Nacional para gestionar los riesgos e incidentes de seguridad digital, conforme las mejores prácticas y las recomendaciones de la OCDE; además de señalar la necesidad de cooperación con el sector privado y otros actores relevantes en este entorno. De esa manera, el Perú daríacumplimiento a los lineamientos estipulados por la OCDE.

VI. SOBRE EL TEXTO SUSTITUTORIO

El dictamen 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. Si revisamos el Foro Económico Mundial (FEM), este señala en su "Informe Global sobre Riesgos 2018"[17](Global Risk Report, su denominación en inglés), que uno de los cinco riesgos con mayor probabilidad es la ocurrencia de un "ciberataque a gran escala o malware", que causaría grandes daños económicos, tensiones geopolíticas o pérdida generalizada de la confianza en Internet. Por otro lado, en el 2018 Microsoft publicó el documento denominado "Global Cyber Risk Perception Survey"[18], un estudio que proporciona una perspectiva sobre el estado de la gestión del riesgo cibernético en organizaciones a nivel mundial, concluyendo que éstas últimas cada vez más, son parte de una cadena de valor digital y por ende la gestión de riesgos de seguridad digital se constituye entre sus más altas prioridades en la gestión de riesgos.

La propuesta incide y reafirma que la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros lidera los procesos de innovación tecnológica y de transformación digital del país, es el ente rector del Sistema Nacional de Transformación Digital y administra las Plataformas Digitales del Estado Peruano, líder nacional de Gobierno Digital. Reviste vital importancia, destacarel esfuerzo que viene desplegando el Perú materializadocon la promulgación de la Ley de Gobierno Digital, el Decreto de Urgencia Nº 006-2020; y el Decreto de Urgencia Nº 007-2020, entre otros instrumentos legales; pero que requieren ser fortalecidos en la medida de desplegar las acciones estratégicas y tecnológicas de gestión y de impulso de la seguridad digital para proteger a los ciudadanos. Ello se sustenta en la necesidad de mejorar los indicadores internacionales dado que aún a finales del 2019 el Perú ocupaba el último lugar de los países de América Latina en implementar prácticas de gestión para la seguridad del país[19].

[16] OECD (2019), Digital Government in Peru: Working Closely with Citizens, OECD Digital Government Studies, OECD Publishing, Paris: https://doi.org/10.1787/0c1eb85b-en
[17] El documento puede ser consultado en:https://www.weforum.org/reports/the-global-risks-report-2018
[18] El documento puede ser consultado enhttps://bit.ly/2EFzKUX
[19] Ver: https://www.welivesecurity.com/wp-content/uploads/2019/07/ESET-security-report-LATAM-2019.pdf

Al respecto, países como Colombia, Estonia, Uruguay, Reino Unido y Estados Unidos han establecido normas con rango de ley para implementar equipos de respuesta ante incidentes de seguridad digital y, sobre todo, mejorar la relación e intercambio de información con las autoridades responsables de proteger los datos personales (privacidad), protección del consumidor en el entorno digital y la seguridad digital en el país. En los países más desarrollados en materia de confianza y seguridad digital, se han desplegado Centros de Seguridad Digital para atender esta problemática tan compleja sobre los riesgos y confianza en el entorno digital. Por ejemplo, Dinamarca tiene un Centro Nacional de Ciberseguridad[20]para la seguridad de la información y ciberseguridad. Australia tiene un Centro Nacional de Ciberseguridad y ha establecido una red de intercambio de información de confianza[21]para atender los incidentes de seguridad digital a actividades e infraestructuras relevantes para las operaciones del país.

En esa línea, el Perú ha avanzado definiendo obligaciones para las entidades públicas y privadas; y, sobre todo estableciendo un marco de confianza en el que se establece quién es responsable y de qué en el entorno digital. Se tiene el reto de viabilizar procedimental y técnicamente la protección del ciudadano en el entorno digital que sirva para atender casos de ciberestafa, ciberespionaje, ciberacoso, cibercrimen, etc., entre otras situaciones; por lo que se hace necesario un abordaje integral e inmediato, no solo basta con castigar el delito o el mal comportamiento en internet o mediante el uso de tecnologías digitales (Ley de Delitos Informáticos); sino se debe prevenir y atender articuladamente -empresa y entidad pública-, un incidente a la seguridad digital, con el fin de evitar pérdidas humanas y financieras, entre otras.

Como se ha podido observar el COVID-19 nos ha obligado a la digitalización apresurada de servicios, procesos y relaciones, no obstante, ha generado las condiciones ideales para que agentes maliciosos nos ataquen o aprovechen nuestras vulnerabilidades en el entorno digital, generando pérdidas económicas, afectaciones a la reputación e imagen, y, sobre todo, pérdida de confianza en el entorno digital. Por ello,resulta de suma importancia aprobar medidas que fortalezcan la seguridad y confianza digital. Así también, a raíz de la última crisis política, se incrementaron los ciberataques tanto en el ámbito público como privado; se identificó un incremento de los ciberataques a entidades públicas, como el Congreso de la Republica, el Poder Ejecutivo y empresas del Estado, por lo cual resulta importante fortalecer nuestras capacidades en monitoreo de redes, identificando patrones que evidencien un ataque, el cual puede darse por actores nacionales como internacionales, proviniendo de cualquier parte del mundo. Los agentes maliciosos que buscan realizar un ataque a los servicios digitales en una nación, siempre están pendientes de sus vulnerabilidades, y más aún en contextos de pandemia y crisis política; por lo que, la adecuada satisfacción de las

[20] Ver: https://digst.dk/media/16943/danish_cyber_and_information_security_strategy_pdfa.pdf
[21] Ver: https://www.tisn.gov.au/Pages/default.aspx

expectativas y la atención de las demandas y necesidades de los ciudadanos cuando realizan transacciones, consultas, compras, descarga de información, etc., configura lo que denominamos confianza digital, la cual tiene una serie de variables que necesitan ser entendidas, valoradas y tratadas con miras a favorecer que las personas, organizaciones y entidades usen y aprovechen las tecnologías digitales de manera sencilla, segura y confiable, atendiendo sus expectativas y necesidades.

Dado lo expuesto, la situación actual plantea la urgencia de promulgar una ley que fortalezca la seguridad y la confianza digital; asimismo, es imperativo acelerar el despliegue de medidas para garantizar la confianza de las personas en su interacción con los servicios digitales prestados en el país, con el fin primario de salvaguardar los derechos fundamentales de las personas y ciudadanos en el entorno digital[22], especialmente en materia de intimidad personal y familiar y seguridad, así como también atender el deber constitucional del Estado peruano de proteger a la población de las amenazas contra su seguridad[23], incluyendo aquellas que provienen del referido entorno digital.

El presente análisis es el fruto de las reuniones con entidades públicas y privadas, el texto sustitutorio contiene medidas para declarar de interés nacional y necesidad pública el fortalecimiento del Centro Nacional de Seguridad Digital,gestionado por la Secretaria de Gobierno Digital de la Presidencia del Consejo de Ministros, entre otras disposiciones.

Este sustento, también se requiere un cambio de paradigma en la cooperación público-privada *-como señala el Reporte de Ciberseguridad 2020-*, porque el entorno digital es de naturaleza intrínsecamente compleja y de partes interesadas.

La digitalización ha transformado nuestra sociedad en un "sistema de sistemas" en donde las funciones críticas se distribuyen entre los actores públicos y privados; por lo que la cooperación público-privada en materia de ciberseguridad, requiere ser pensada fuera de los formatos tradicionales y rígidos para superar las barreras y ser verdaderamente efectivos, tal como lo señala Nayia Barmpaliou, Jefa de Políticas e Iniciativas Públicas, Centro para la Ciberseguridad, Foro Económico Mundial[24].

En esa línea, resulta urgente declarar de interés nacional y necesidad pública el fortalecimiento del Centro Nacional de Seguridad Digital, que si bien fue "creado" mediante Decreto de Urgencia N° 007-2020, esto solo fue instituido como una "plataforma virtual", mas no como un órgano de la Secretaria de Gobierno Digital; a fin de salvaguardar la seguridad de las personas y los intereses nacionales;

---

[22]Es el dominio o ámbito habilitado por las tecnologías y dispositivos digitales, generalmente interconectados a través de redes de datos o comunicación, incluyendo el Internet, que soportan los procesos, servicios, infraestructuras y la interacción entre personas. Fuente: Decreto Legislativo N° 1412

[23] Artículo 44 de la Constitución Política del Perú de 1993.

[24]BID-OEA: Reporte de Ciberseguridad-2020, pág. 32.

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.

VII. IMPACTO DE LA NORMA EN LA LEGISLACION VIGENTE

El presente dictamen materia del proyecto de leyarticula con la normatividad emitida en materia de gobierno digital, confianza digital y transformación digital. En ese sentido, la norma es complementaria a las disposiciones normativas que regulan las funciones y competencias de los entes rectores.

VIII. ANALISIS COSTO-BENEFICIO

En atención a lo previsto en el artículo 76 del Reglamento del Congreso de la Republica, el presente dictamen no contiene propuesta de creación ni aumento del gasto público; puesto que no irrogará gasto al erario nacional, ya que 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 Seguridad Digital, cuyo beneficio 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.

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.

IX. CONCLUSIÓN

Por las consideraciones expuestas, la Comisión de Defensa Nacional, Orden Interno, Desarrollo Alternativo y Lucha Contra las Drogas, de conformidad con el literal b) del artículo 70 del Reglamento del Congreso de la Republica, recomienda

la **APROBACIÓN** del presente dictamen, recaído en el proyecto de ley 6544/2020-CR; con el siguiente texto sustitutorio:

TEXTO SUSTITUTORIO

El Congreso de la República;

Ha dado la siguiente Ley:

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 PAIS

En debate 9/6/2021
F:
C:
A:

Artículo 1. Objeto de la Ley
La presente ley tiene por objeto fortalecer el Centro Nacional de Seguridad Digital, gestionado por la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros, en su calidad de Autoridad Nacional para la Transformación y la Innovación Digital y ente rector en materia de seguridad y confianza digital, como componente del Sistema Nacional de Transformación Digital, responsable de planificar, dirigir y evaluar de manera integral las operaciones de seguridad digital a nivel nacional, a fin de garantizar la confianza en el entorno digital como pilar de la seguridad nacional.

Artículo 2. Declaración
Declárase de interés nacional y necesidad pública el fortalecimiento del Centro Nacional de Seguridad Digital, a fin de garantizar la confianza en el entorno digital de las entidades de la Administración Pública, los ciudadanos, las organizaciones del sector privado, la sociedad civil, la academia y otros actores del ecosistema digital, para impulsar la inclusión social, reactivación económica, competitividad y productividad, economía digital y la transformación digital del país.

Artículo 3. Ámbito de aplicación
La presente ley es aplicable a las entidades establecidas en el Artículo I del Título Preliminar del Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado mediante Decreto Supremo N° 004-2019-JUS, y, a las organizaciones de la sociedad civil, del sector privado, la academia y los ciudadanos.

Artículo 4. Finalidad
La finalidad de la presente ley es:

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.

Artículo 5. Definiciones

La presente ley recoge las definiciones contenidas en el Decreto de Urgencia N° 006-2020 que crea el Sistema Nacional de Transformación Digital, Decreto de Urgencia N° 007-2020 que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento y el Decreto Legislativo N° 1412 que aprueba la Ley de Gobierno digital y dispositivos afines. En adición a ello se adoptan las siguientes definiciones:

a. **Actividad crítica.-** Es la actividad económica y/o social cuya interrupción tiene graves consecuencias en la salud y seguridad de los ciudadanos, en el funcionamiento efectivo de los servicios esenciales que mantienen la economía, sociedad y el gobierno, y en la prosperidad económica y social en general.

b. **Activo digital.-** 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

c. **Ciberseguridad.-** Capacidad tecnológica de preservar el adecuado funcionamiento de las redes, activos y sistemas informáticos y protegerlos ante amenazas y vulnerabilidades en el entorno digital. Comprende la perspectiva técnica de la Seguridad Digital y es un ámbito del Marco de Seguridad Digital del país.

d. **Confianza Digital.-** Es el estado que emerge como resultado de cuán veraces, predecibles, éticas, proactivas, transparentes, seguras, inclusivas y confiables son las interacciones digitales que se generan entre personas, empresas, entidades públicas o cosas en el entorno digital, con el propósito

de impulsar el desarrollo de la economía digital y la transformación digital. Es un componente de la transformación digital y tiene como ámbitos la protección de datos personales, la ética, la transparencia, la seguridad digital y la protección del consumidor en el entorno digital.

e. **Entorno Digital.-** Es el dominio o ámbito habilitado por las tecnologías y dispositivos digitales, generalmente interconectados a través de redes e infraestructuras de datos o comunicación, incluyendo el Internet, que soportan los procesos, servicios, plataformas que sirven como base para la interacción entre personas, empresas, entidades públicas o dispositivos.

f. **Experto en seguridad y confianza digital.-** Es la persona con experiencia comprobada en materia de seguridad y confianza digital y que se encuentra capacitado técnicamente para desarrollar y desplegar estrategias para prevenir, mitigar, afrontar y proteger los principales activos digitales del sector público, privado, academia, entre otros actores del ecosistema digital ante inminentes riesgos que afecten el bienestar de las personas y la seguridad nacional.

g. **Gobierno Digital.-** Es el uso estratégico de las tecnologías digitales y datos en la Administración Pública para la creación de valor público. Se sustenta en un ecosistema compuesto por actores del sector público, ciudadanos y otros interesados, quienes apoyan en la implementación de iniciativas y acciones de diseño, creación de servicios digitales y contenidos, asegurando el pleno respeto de los derechos de los ciudadanos y personas en general en el entorno digital. Comprende el conjunto de principios, políticas, normas, procedimientos, técnicas e instrumentos utilizados por las entidades de la Administración Pública en la gobernanza, gestión e implementación de tecnologías digitales para la digitalización de procesos, datos, contenidos y servicios digitales de valor para los ciudadanos.

h. **Oficial de Seguridad Digital.-** Es el rol 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 punto de contacto con el Centro Nacional de Seguridad Digital.

i. **Resiliencia Digital.-** Capacidad de las organizaciones y personas en general para adaptarse y recuperarse frente a la ausencia de servicios esenciales digitales que permitan afrontar situaciones de crisis nacionales como incidentes de seguridad digital, no disponibilidad de infraestructuras o sistemas, entre otros.

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

Artículo 6. Conformación de Equipos Técnicos Especializados en Seguridad y confianza digital

6.1 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, Poder Judicial, Ministerio Público Fiscalía de la Nación, el Consejo Nacional de la Seguridad y Defensa, el Comando Conjunto de las Fuerzas Armadas, la Dirección Nacional de Inteligencia, el sector privado de telecomunicaciones, del sector financiero, de tecnología, la academia, la sociedad civil y ciudadanos.

6.2 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.

6.3 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.

6.4 La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital convoca a expertos nacionales e internacionales, del sector público y privado, de la academia, 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.

Artículo 7. Responsabilidades del Centro Nacional de Seguridad Digital

El Centro Nacional de Seguridad Digital tiene las siguientes responsabilidades:

7.1 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 Decreto de Urgencia N° 007-2020, Decreto de Urgencia que

aprueba el marco de Confianza Digital y dispone medidas para su fortalecimiento, y su Reglamento.

7.2 Articular acciones para la gestión de incidentes y riesgos de seguridad digital que afecten a la sociedad con los responsables de los ámbitos del Marco de Seguridad Digital del Estado Peruano y del Marco de Confianza Digital, de conformidad con lo establecido en el Decreto Legislativo N° 1412 y el Decreto de Urgencia N° 007-2020.

7.3 Promover una cultura de seguridad y confianza digital en los ciudadanos y personas 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 Nº 30254, a través de programas de difusión y concientización u otras acciones estratégicas.

7.4 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.

7.5 Identificar y evaluar el riesgo de las actividades críticas que incluyen 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.

7.6 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.

7.7 Promover la colaboración y cooperación 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, sociedad civil del ámbito nacional y, con países extranjeros, organizaciones y actores internacionales de similar naturaleza.

7.8 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 y personas en general.

7.9 Impulsar, participar y colaborar en la creación de comunidades y/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.

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

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

7.12 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.

7.13 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 y confianza digital.

7.14 Otras que determine la la Presidencia del Consejo de Ministros.

Artículo 8. Líneas de acción del Centro Nacional de Seguridad Digital

8.1 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 y/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 y personas en general, a los servidores públicos, 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.

8.2 La Presidencia del Consejo de Ministros establece las nuevas líneas de acción.

Artículo 9. Procesos Operativos del Centro Nacional de Seguridad Digital

9.1 El Centro Nacional de Seguridad Digital, conforme a sus líneas de acción dirige los siguientes procesos operativos: i) Gestión de Alertas Digitales, ii)

Gestión de Incidentes, iii) Gestión de Seguridad de la Información, iv) Gestión de Riesgos Digitales, v) Gestión del Observatorio Nacional de Seguridad y confianza digital, vi) Gestión del Equipo de Respuestas ante Incidentes de Seguridad Digital, vii) Análisis Forense Digital, viii) Monitoreo de Operaciones de Seguridad, ix) Gestión de Seguridad de las Comunicaciones, x) Generación y Transferencia de Conocimiento.

9.2 La Presidencia del Consejo de Ministros, establece nuevos procesos operativos.

Artículo 10. 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 Digital en su calidad de ente rector en Seguridad y Confianza Digital en el país, puede convocar y contratar excepcionalmente a proveedores especialistas expertos nacionales e internacionales en materia de Seguridad y Confianza Digital, conforme a lo dispuesto en la Ley de Contrataciones del Estado y su Reglamento.

DISPOSICIONES COMPLEMENTARIAS FINALES

PRIMERA. Reglamentación
La Presidencia del Consejo de Ministros, a propuesta de la Secretaría de Gobierno Digital, mediante Decreto Supremo, aprueba el reglamento de la presente Ley, en un plazo máximo de noventa (90) días contados a partir del día siguiente de su publicación en el Diario Oficial El Peruano. La Secretaria de Gobierno Digital puede convocar a diversos actores del sector público como privado, para que participen en la elaboración del reglamento.

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

DISPOSICIONES COMPLEMENTARIAS MODIFICATORIAS

PRIMERA. Modificación de los artículos 7 y 13 del Decreto de Urgencia N° 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.
Modifícanse los artículos 7 y 13 del Decreto de Urgencia N° 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento, en los siguientes términos:

*"**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 deSeguridad Digital se encuentra **adscrito** a la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno 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 el Marco de Confianza Digital, de conformidad con el artículo 32 del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital y el artículo 4 del presente Decreto de Urgencia.

7.4 El Centro Nacional de Seguridad Digital incorpora al Equipo de Respuesta a Incidentes de Seguridad Digital Nacional responsable de: i) Gestionar la respuesta y/o recuperación ante incidentes de seguridad digital en el ámbito nacional y, ii) Coordinar y articular acciones con otros equipos de similar naturaleza nacionales e internacionales para atender los incidentes de seguridad digital.

*7.5 La Secretaría de Gobierno 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 ***infraestructuraoficial*** *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 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 intercambiar información y acciones con entidades tanto a nivel nacional como extranjeras de ser requeridas.

13.4 La Secretaría de Gobierno 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."

SEGUNDA. Modificación del artículo 6 del Decreto Legislativo N° 1129, Decreto Legislativo que regula el Sistema de Defensa Nacional

Modifícase el artículo 6 del Decreto Legislativo N° 1129, Decreto Legislativo que regula el Sistema de Defensa Nacional, en los siguientes términos:

*"**Artículo 6°.- Estructura***

El Consejo de Seguridad y Defensa Nacional está conformado por:

a) El Presidente de la República, quien ejerce la Presidencia del Consejo;
b) El Presidente del Consejo de Ministros;
c) El Ministro de Relaciones Exteriores;
d) El Ministro de Defensa;
e) El Ministro de Economía y Finanzas;
f) El Ministro del Interior
g) El Ministro de Justicia y Derechos Humanos;
h) El Jefe del Comando Conjunto de las Fuerzas Armadas;
i) El Director General de la Policía Nacional del Perú;
j) El Director Ejecutivo de la Dirección Nacional de Inteligencia;

Firmado digitalmente por: VIVANCO REYES Miguel Angel FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 21/12/2020 11:[illegible]

k) El Secretario de Gobierno Digital, en su calidad de ente rector de la seguridad digital y confianza digital en el país."

DISPOSICIÓN COMPLEMENTARIA TRANSITORIA

ÚNICA. Articulación del Sistema Nacional de Transformación Digital y el Sistema de Defensa Nacional

La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, priorizará y coordinará las medidas necesarias a fin de que se constituya el Sistema Nacional de Seguridad Digital. El Centro Nacional de Seguridad Digital es un componente articulador entre el Sistema Nacional de Transformación Digital y el Sistema de Defensa Nacional.

Firmado digitalmente por: RIVAS OCEJO Perci FAU 20161749126 soft
Motivo: En señal de conformidad
Fecha: 15/12/2020 [illegible]

Firmado digitalmente por: PEREZ MIMBELA Jhosept Amado FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 11/12/2020 12:51:47-0500

Firmado digitalmente por: PUÑO LECARNAQUE Napoleon FAU 20161749126 soft
Motivo: En señal de conformidad
Fecha: 17/12/2020 22:59:10-0500

Dese cuenta.

Lima, 7 de diciembre de 2020.

Firmado digitalmente por: BENITES AGURTO ALFREDO FIR 42930319 hard
Motivo: Soy el autor del documento
Fecha: 11/12/2020 15:19:07-0500

Firmado digitalmente por: URRESTI ELERA Daniel Belizario FIR 43863835 hard
Motivo: Soy el autor del documento
Fecha: 11/12/2020 12:39:27-0500

Firmado digitalmente por: VALER COLLADO Valeria Carolina FAU 20161749126 soft
Motivo: En señal de conformidad
Fecha: 11/12/2020 16:36:16-0500

Firmado digitalmente por: PEREZ MIMBELA Jhosept Amado FAU 20161749126 soft
Motivo: En señal de conformidad
Fecha: 11/12/2020 12:52:14-0500

Firmado digitalmente por: SAAVEDRA OCHARAN Monica Elizabeth FAU 20161749126 soft
Motivo: En señal de conformidad
Fecha: 11/12/2020 13:29:23-0500

Firmado digitalmente por: PANTOJA CALVO RUBEN FIR 44171668 hard
Motivo: En señal de conformidad
Fecha: 12/12/2020 10:14:53-0500

CONSEJO DIRECTIVO DEL
CONGRESO DE LA REPÚBLICA

Lima, 6 de abril de 2021

Al orden del día

HUGO F. ROVIRA ZAGAL
Director General Parlamentario
CONGRESO DE LA REPÚBLICA

DICTAMEN RECAÍDO EN EL PROYECTO DE LEY 6544/2020-CR, QUE PROPONE 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.

FIRMA DIGITAL
Firmado digitalmente por: NUÑEZ MARREROS JESUS DEL CARMEN FIR 16694109 hard
Motivo: Doy V° B°
Fecha: 21/12/2020 12:17:52-0500

FIRMA DIGITAL
Firmado digitalmente por: GUIBOVICH ARTEAGA Otto Napoleon FAU 20161749126 soft
Motivo: En señal de conformidad
Fecha: 22/12/2020 12:43:07-0500

FIRMA DIGITAL
Firmado digitalmente por: YUPANQUI MIÑANO MARIANO ANDRES FIR 41551757 hard
Motivo: En señal de conformidad
Fecha: 22/12/2020 21:43:52-0500

PERIODO ANUAL DE SESIONES 2020-2021

ACTA DE LA DÉCIMO OCTAVA SESIÓN ORDINARIA
(SESIÓN VIRTUAL)

LUNES, 7 DE DICIEMBRE DE 2020

En Lima, a través de la plataforma Microsoft Teams y siendo las quince horas y treinta minutos del día lunes 7 de diciembre de 2020, se reunieron los miembros de la Comisión de Defensa Nacional, Orden Interno, Desarrollo Alternativo y Lucha contra las Drogas bajo la presidencia del señor congresista **Daniel Urresti Elera,** los señores congresistas **Miguel Vivanco Reyes (Vicepresidente), Jhosept Pérez Mimbela (Secretario), Alfredo Benites Agurto, Cecilia García Rodríguez, Otto Guibovich Arteaga, Jesús Núñez Marreros, Rubén Pantoja Calvo**, **Perci Rivas Ocejo, Mónica Saavedra Ocharán**, **Valeria Valer Collado y Mariano Yupanqui Miñano** como miembros titulares. **Napoleón Puño Lecarnaqué y Robertina Santillana Paredes,** miembros accesitarios.

Con licencia, los señores congresistas **Lenin Bazán Villanueva, Walter Benavides Gavidia y José Vega Antonio**.

Con el quórum reglamentario, el **PRESIDENTE,** dio inicio a la Décimo Octava sesión ordinaria de la Comisión de Defensa Nacional, Orden Interno, Desarrollo Alternativo y Lucha contra las Drogas.

I. ACTA

El PRESIDENTE consultó la aprobación del Acta de la Décimo Séptima sesión ordinaria de la Comisión, realizada el 30 de noviembre de 2020.

No existiendo observaciones se dio por aprobada.

II. DESPACHO

El PRESIDENTE dio cuenta de la distribución electrónica de la relación de los documentos recibidos y emitidos por la Comisión, al 3 de diciembre de 2020. Asimismo, informó el ingreso a la Comisión del proyecto de ley 6687/2020-CR, del grupo parlamentario Acción Popular, que propone la ley que incorpora a los bomberos voluntarios a EsSalud.

III. INFORMES

El PRESIDENTE ofreció el uso de la palabra.
El señor congresista Vivanco Reyes manifestó que junto con las congresistas

Santillana y Fabián habían recibido a los representantes de la Asociación Nacional de Defensores de la Democracia "Roberto Delgado" quienes buscan ser apoyados y escuchados por ser excombatientes en la lucha contra el terrorismo, y cuya materia se relaciona con el proyecto de ley 4271/2020-CR que estaba agendado para la presente sesión.

Seguidamente, el PRESIDENTE informó que porponía invitar para la próxima sesión a la señora ministra de Defensa, Nuria Esparch, por lo que lo sometía la propuesta a votación. No habiendo oposiciones fue aprobado por unanimidad.

IV. PEDIDOS

El PRESIDENTE ofreció el uso de la palabra a los integrantes de la comisión.

La señora congresista Saavedra Ocharán solicitó se priorice el dictamen del proyecto de ley 6387/2020-CR, de su autoría, sobre la Ley de Servoicio de Serenazgo, el mismo que cuenta con opiniones favorables. El PRESIDENTE manifestó que tomaba en cuenta el pedido y se atendería.

La señora congresista García Rodríguez solicitó priorizar el dictamen del proyecto de ley 6525/2020-CR que proponía soluciones al marco legal de la legítima defensa.

El señor congresista Rivas Ocejo señaló que ante el debate del proyecto de ley 4271/2018-CR había recibido una carta de la confederación de licenciados de las FFAA que solicitaban ser escuchados antes del debate de dicho proyecto de ley. El PRESIDENTE solicitó que el congresista solicitante sea el portavoz de los pedidos ciudadanos y haga llegar las inquietudes.

El cogresistas Vivanco Reyes señaló la importancia de continuar con el trabajo avanzado sobre el dictamen de legítima defensa. El PRESIDENTE señaló que se está trabajando una nueva versión del dictamen.

La congresista Valer Collado informó que apoyaría a la mesa de trabajo que analiza los proyectos sobre legítima defensa a fin de tener un dictamen pronto.

V. ORDEN DEL DÍA

1. Informe parcial de los grupos de trabajo de la Comisión

El PRESIDENTE dio cuenta que en la sesión pasada se inició la exposición de los coordinadores de los grupos de trabajo, quedando pendiente la presentación del coordinador del grupo de trabajo N° 2, congresista Miguel Vivanco, que se suspendió por no contar con el quorum reglamentario.

El PRESIDENTE recordó que en la Décimo Primera Sesión Ordinaria, celebrada el 17 de agosto de 2020, se aprobó la conformación del grupo de trabajo que se encargue de la evaluación de la problemática que se refleja en los proyectos de ley que plantean ascensos, cambio de grupo ocupacional, reconocimientos de tiempo de servicios y otras medidas. Asimismo, que en dicha sesión se señaló que el grupo "reciba los informes de los especialistas de todos los ámbitos involucrados, invite a los potenciales beneficiarios, a las instituciones públicas, etc., con la mayor amplitud posible, y que proponga a esta comisión las medidas que, desde nuestro ámbito de competencias y funciones se pueden implementar o recomendar, a fin de atender la problemática y arribar a las soluciones posibles".

Explicado el contexto en que se conformó el grupo de trabajo, cedió el uso de la palabra al señor congresista Miguel Vivanco para que presente su informe parcial.

El señor congresista Vivanco Reyes informó sobre la materia del encargo al grupo de trabajo que coordina y pasó a detallar el contenido del proyecto de ley 5935/2020-CR. Asimismo, informó que había recibido las opiniones del Ministerio de Defensa y de la Defensoría del Pueblo, las mismas que consideraba no se oponían al proyecto de ley. Seguidamente, concluyó que el proyecto de ley cumplía con los requisitos dispuestos en la Constitución Política y el Reglamento del Congreso por lo que se encontraba expedito para su dictamen por la comisión.

Al término de la exposición, el PRESIDENTE agradeció la intervención e hizo precisiones sobre los plazos de los grupos de trabajo para el desarrollo de su encargo. Luego de intercambios de opiniones se estableció ampliar a 60 días hábiles adicionales al grupo número uno y en el caso del segundo grupo, no se estableció plazo pero se indicó que, según el Reglamento Interno de la Comisión, el plazo máximo era el 15 de mayo del próximo año. Fue aprobado por unanimidad.

2. **Propuesta de texto sustitutorio del proyecto de ley 6730/2020-CR, que propone modificar el Decreto Legislativo 1267, Ley de la Policía Nacional del Perú**

El PRESIDENTE informó que el proyecto de ley, presentado por Fuerza Popular y de autoría del congresista Miguel Vivanco, planteaba modificar el artículo 8 del Decreto Legislativo 1267, Ley de la Policía Nacional. Asimismo, recordó que fue incluido por acuerdo de la Junta de Portavoces en la agenda del Pleno del Congreso de la sesión del viernes 4 de diciembre, iniciándose el debate correspondiente. Explicó que solicitó un cuarto intermedio, a fin de poder elevar una propuesta de texto sustitutorio para mejorar la iniciativa y adecuar además las normas adicionales que resulten necesarias.

Seguidamente, explicó detalladamente las propuestas de modificación a la fórmula legal, precisando que se busca que la Policía Nacional cumpla con el mandato constitucional señalado en el artículo 166, y responda a la necesaria modernización que garantice la eficiencia, eficacia y transparencia, por lo cual precisa contar con una estructura orgánica dinámica y coherente con la doctrina del Estado Mayor, que se aplica en las Fuerzas Armadas, que le permita ejercer sus competencias y funciones al servicio de la ciudadanía.

Al terminar su explicación, ofreció el uso de la palabra a los congresistas que desearan intervenir. Participaron los señores congresistas Benites Agurto, Saavedra Ocharán y Vivanco Reyes a fin de recalcar la importancia del proyecto dentro del actual contexto, que aclara y precisa los términos para la designación de oficiales del más alto nivel, así como la necesidad de contar con normas claras.

Agotado el debate, el PRESIDENTE pidió consultar la propuesta de texto sustitutorio que se presentaría en el pleno del Congreso. Luego de votación, el resultado fue: Aprobado por unanimidad.

Votaron a favor: Benites Agurto, García Rodríguez, Núñez Marreros, Pantoja Calvo, Puño Lecarnaqué, Rivas Ocejo, Saavedra Elera, Santillana Paredes, Valer Collado, Vivanco Reyes, Yupanqui Miñano y Urresti Elera.

3. **Debate del predictamen recaído en el proyecto de ley 6544/2020-CR, que propone 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 PRESIDENTE, sobre este punto de la agenda, señaló que se trata de un dictamen declarativo y que uno de sus objetivos principales es fortalecer la seguridad y la confianza digital, que se construye como una garantía en la interacción de los ciudadanos con los servicios digitales prestados en el país, con el respeto de sus derechos fundamentales, especialmente en materia de intimidad personal y familiar y seguridad, así como también atender el deber constitucional del Estado peruano de proteger a la población de las amenazas contra su seguridad, incluyendo aquellas que provienen del referido entorno digital.

Explicó, que para la elaboración del dictamen el equipo técnico de la comisión había desarrollado un trabajo de coordinación con entidades públicas y privadas, a fin de alcanzar el texto sustitutorio que contiene medidas para declarar de interés nacional y necesidad pública el fortalecimiento del Centro Nacional de Seguridad Digital, gestionado por la Secretaria de Gobierno Digital de la Presidencia del Consejo de Ministros, entre otras disposiciones.

Finalmente, el PRESIDENTE señaló que la norma propuesta promovía la confianza y seguridad digital en los servicios digitales que brindan las entidades de la Administración Pública y las organizaciones del sector privado, a fin de permitir al país ubicarse 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.

Seguidamente, ofreció el uso de la palabra a los congresistas que deseen intervenir. Participaron los señores congresistas Benites Agurto, Nuñez Marreros y Guibovich Arteaga quienes formularon comentarios favorables y observaciones sobre el proyecto de dictamen.

Al agotarse el debate se procedió a la votación. Fue aprobado por unanimidad. Votaron a favor los señores congresistas Benites Agurto, Guibovich Arteaga, Núñez Marreros, Pantoja Calvo, Pérez Mimbela, Puño Lecarnaqué, Rivas Ocejo, Saavedra Ocharán, Valer Collado, Vivanco Reyes, Yupanqui Miñano y Urresti Elera.

4. **Debate del predictamen recaído en el proyecto de ley 4271/2018-CR, que modifica los artículos 1 y 4 de la Ley 29031, Ley que instituye el Día de los Defensores de la Democracia y crea la condecoración correspondiente.**

El PRESIDENTE puso a consideración el dictamen que propone mejorar el proceso de calificación de los Defensores de la Democracia, a fin de que dicho reconocimiento alcance a militares, policías, licenciados y ciudadanos que en la lucha antiterrorista prestaron eminentes servicios a la Nación, a través del otorgamiento de la condecoración "Medalla al Defensor de la Democracia".

Aclaró que, además de ajustes de técnica legislativa y precisiones derivados del estudio de la iniciativa, se consideraba conveniente suprimir la propuesta modificatoria del artículo 4, a fin de que guarde concordancia con el marco legal vigente. En ese extremo, se acogieron las observaciones realizadas por el Ministerio de Defensa y el Ministerio del Interior. Asimismo, se agregó una segunda disposición complementaria final que menciona expresamente: "Los efectos de la presente Ley no son aplicables a las personas que tengan sentencia firme condenatoria par la comisión de delitos", repitiendo la formula legislativa de la Ley 30758 y de la Ley 30655, a fin de evitar que personas sentenciadas puedan ser condecoradas como héroes.

Seguidamente, ofreció el uso de la palabra a los congresistas que deseen intervenir. Participaron los señores congresistas Benites Agurto, Saavedra Ocharán, Vivanco Reyes, Nuñez Marreros y Rivas Ocejo quienes destacaron la importancia de reconocer los servicios prestados a la nación por los valerosos defensores de la democracia. Asimismo, se formularon aportes para precisar unos términos de la fórmula legal, que fueron aceptados por la presidencia.

Al agotarse el debate se procedió a la votación. Fue aprobado por unanimidad. Votaron a favor: Urresti Elera, Vivanco Reyes, Pérez Mimbela, Saavedra Ocharán, Rivas Ocejo, Nuñez Marreros, Benites Agurto, Valer Collado, Pantoja Calvo, Yupanqui Miñano y Puño Lecarnaqué.

5. **Propuesta de retorno a la Comisión, para mayor estudio, del Dictamen recaído en los proyectos de ley 2871/2017-CR, 3815/2018-CR, 3830/018-CR y 4036/2018-CR, que proponen la Ley del Serenazgo**

EL PRESIDENTE sustentó la propuesta de retorno señalando que el 10 de junio de 2019 esta Comisión aprobó un dictamen que propone la Ley de Serenazgo Municipal, que acumulaba los 4 proyectos de ley que sobre la materia existían a dicha fecha. Con posterioridad, y ya en el marco del ejercicio de sus funciones como congresistas, diversos grupos parlamentarios han presentado iniciativas sobre la misma materia, que requieren de un pronunciamiento por la comisión, proyectos que contienen planteamientos más actuales, integrales y que han sido elaborados consultando a las mismas municipalidades y cuerpos de serenazgo de diversos gobiernos locales, como el proyecto de la congresista Mónica Saavedra.

El PRESIDENTE explicó que a fin de elaborar un nuevo dictamen, que recoja lo mejor del dictamen ya aprobado y los nuevos planteamientos ingresados con posterioridad a su aprobación, se hacía necesario el retorno del dictamen para un mayor estudio. En este punto, la señora congresista Saavedra Ocharán solicitó que se elabore un texto sustitutorio del dictamen que ya se encuentra en orden del día y estando de acuerdo con la explicación brindada por la secretaria técnica, el PRESIDENTE indicó que se trabajará un nuevo texto que recoja una mejor propuesta e incorpore los planteamientos de los últimos proyectos de ley ingresados a la comisión. Dicho texto sustituttorio se presentaría en el marco del debate del dictamen recaído en los proyectos de ley 2871/2017-CR, 3815/2018-CR, 3830/018-CR y 4036/2018-CR, que proponen la Ley del Serenazgo, al cual se acumularían en el pleno los nuevos proyectos de ley. Para ello, solicitó la colaboración de los voceros de los grupos parlamentarios representados en la comisión, a fin de poder priorizar en la agenda del pleno el citado dictamen.

Finalmente, el PRESIDENTE solicitó la dispensa de aprobación del Acta con el quórum reglamentario presente en la sesión virtual. Al no haber oposición se dio por aprobada por unanimidad.

En este estado, el PRESIDENTE levantó la sesión siendo las dieciocho horas con once minutos.

DANIEL BELIZARIO URRESTI ELERA
PRESIDENTE
COMISIÓN DE DEFENSA NACIONAL, ORDEN INTERNO, DESARROLLO ALTERNATIVO Y LUCHA CONTRA LAS DROGAS

JHOSEPT PÉREZ MIMBELA
SECRETARIO
COMISIÓN DE DEFENSA NACIONAL, ORDEN INTERNO, DESARROLLO ALTERNATIVO Y LUCHA CONTRA LAS DROGAS

Forma parte del Acta la transcripción de la versión magnetofónica de la sesión, elaborada por el Área de Transcripciones del Congreso de la República.

FIRMA DIGITAL
Firmado digitalmente por: URRESTI ELERA Daniel Belizario FIR 43863835 hard
Motivo: Soy el autor del documento
Fecha: 14/01/2021 18:03:21-0500

FIRMA DIGITAL
Firmado digitalmente por: PEREZ MIMBELA Jhosept Amado FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 15/01/2021 10:55:31-0500