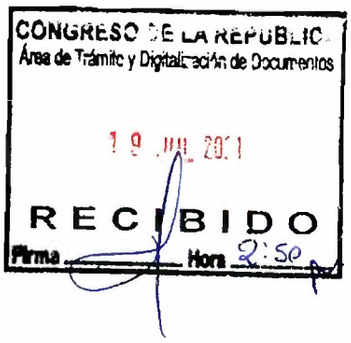
PL 6544

– DEFENSA NACIONAL



"Año del Bicentenario del Perú: 200 años de Independencia"
"Decenio de la Igualdad de oportunidades para mujeres y hombres"

OFICIO Nº 462 -2021 –PR

Lima, 19 de julio de 2021

Señora
MIRTHA ESTHER VÁSQUEZ CHUQUILIN
Presidenta a.i. del Congreso de la República
Presente.-

Tenemos el agrado de dirigirnos a usted, con relación a la Autógrafa de 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. Al respecto, estimamos conveniente observar la misma por lo siguiente:

Beneficios de la Autógrafa

1. Como cuestión previa, cabe señalar que estimamos que **la Autógrafa es, en términos generales, positiva** y **beneficiosa**, pues tiene como finalidad salvaguardar los derechos fundamentales de los ciudadanos en el entorno digital, especialmente en materia de intimidad personal y familiar y seguridad, así como atender el deber constitucional del Estado de proteger a la población de las amenazas contra su seguridad (ámbito digital). En ese sentido, la Autógrafa es importante para el actual contexto de hiperconectividad y pandemia de la COVID-19, que obliga a las entidades públicas y privadas, así como a las personas en general, a depender más de la infraestructura digital, y, por ello, los vuelve más vulnerables frente a brechas de seguridad, ciberdelincuencia y cibercriminalidad. En ese contexto, con el fortalecimiento del Centro Nacional de Seguridad Digital (CNSD) se facilitará la articulación entre entidades públicas y privadas, permitiendo así un rápido intercambio de información sobre seguridad digital, lo que contribuirá a los fines de la Autógrafa.

   No obstante, **es pertinente observarla exclusivamente para proponer textos alternativos o ajustes puntuales (resaltados en negrita) a determinados artículos**, con la finalidad de que sean coherentes con las competencias, responsabilidades y fines del Sistema de Seguridad y Defensa Nacional del Estado, al amparo del artículo 163 de la Constitución, el Decreto Legislativo N° 1129, que regula el Sistema de Defensa Nacional, y la Ley N° 30999, Ley de Ciberdefensa.

Sobre el artículo 1 de la Autógrafa

2. Se sugiere el siguiente texto alternativo, con el fin de precisar que las disposiciones sobre el fortalecimiento del CNSD no afectan las competencias del Ministerio de Defensa (MINDEF) y de sus órganos ejecutores en materia de seguridad y defensa nacional:

   > "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 Trasformación 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 enforno digital, **sin afectar las competencias del Ministerio de Defensa y sus órganos ejecutores en materia de seguridad y defensa nacional**".

Sobre el artículo 6 de la Autógrafa

3. Se propone la modificación del numeral 6.1 del artículo 6, referido a la conformación de equipos técnicos especializados en seguridad y confianza digital, con el fin de suprimir la referencia al Consejo de Seguridad y Defensa Nacional (COSEDENA), en tanto que, por su naturaleza política y estratégica, no corresponde se le asignen responsabilidades técnicas en estas materias. En su lugar, es necesario incluir a la Policía Nacional del Perú (PNP), puesto que dicha institución, a través de la División de Investigación de Delitos de Alta Tecnología (DIVINDAT), conforme lo establece la Ley de la PNP (Decreto Legislativo N° 1267) y su Reglamento (aprobado por Decreto Supremo N° 026-2017-IN), es la única unidad especializada encargada de investigar delitos informáticos en todas sus modalidades. En ese sentido, el texto propuesto es el siguiente:

   "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, el Poder Judicial, el Ministerio Público, **la Policía Nacional del Perú**, 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".

Sobre el artículo 7, numeral 6, de la Autógrafa

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

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

   Siendo así, se advierte la responsabilidad con la que cuenta cada sector con relación a la identificación de los ACN vinculados a la naturaleza y función del activo seleccionado y los servicios que brinda, así como la competencia de la DINI para validar tales propuestas, previo a ser remitidas a la COSEDENA para efectos de su aprobación; por ello, proponemos la siguiente precisión en el texto a efecto de evitar una eventual superposición de funciones:

   "Artículo 7. Responsabilidades del Centro Nacional de Seguridad Digital
   El Centro Nacional de Seguridad Digital tiene las siguientes responsabilidades:
   [...]
   6. Identificar y **participar en la validación de** las propuestas de activos críticos nacionales que impliquen un componente de seguridad y confianza digital".

Sobre la Segunda Disposición Complementaria Modificatoria de la Autógrafa

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

   En todo caso, en el supuesto que la agenda del órgano tuviese un punto vinculado a dicha materia, el penúltimo párrafo del mismo artículo 6 ya habilita la participación del SGD, en tanto señala que el Presidente de la República, en su calidad de Presidente del COSEDENA, **de acuerdo a la naturaleza de los asuntos a tratar o a petición de cualquiera de sus miembros**, dispone la participación de **cualquier otro funcionario del Poder Ejecutivo y de otros poderes del Estado**, así como de autoridades de Gobiernos Regionales y Locales, con derecho a voz, pero sin voto.

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

   > "DISPOSICIONES COMPLEMENTARIAS FINALES
   > [...]
   > **CUARTA. De la participación en el Consejo de Seguridad y Defensa Nacional**
   >
   > **En los casos en los que la agenda del Consejo de Seguridad y Defensa Nacional incluya algún tema de seguridad digital, será de aplicación lo establecido en el penúltimo párrafo del artículo 6 del Decreto Legislativo N° 1129, Decreto Legislativo que regula el Sistema de Defensa Nacional, que habilita la participación de cualquier otro funcionario del Poder Ejecutivo y de otros poderes del Estado**".

Por las razones expuestas, en aplicación del artículo 108 de la Constitución Política del Perú, se observa la Autógrafa de Ley con el objeto de proponer textos alternativos o ajustes que garanticen su concordancia con la Constitución y el marco normativo vigente.

Atentamente,

FRANCISCO RAFAEL SAGASTI HOCHHAUSLER
Presidente de la República

VIOLETA BERMÚDEZ VALDIVIA
Presidenta del Consejo de Ministros

Proyecto de Ley: 6544/2020-CR

CONGRESO DE LA REPÚBLICA

Lima, 20 de julio de 2021

Pase a la Comisión de Defensa Nacional, Orden interno, Desarrollo alternativo y Lucha contra las Drogas, con cargo de dar cuenta de este procedimiento al Consejo Directivo.

.....
YON JAVIER PÉREZ PAREDES
Oficial Mayor
CONGRESO DE LA REPÚBLICA

EL CONGRESO DE LA REPÚBLICA;

Ha dado la Ley siguiente:

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

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 de interés nacional

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 27444, Ley del Procedimiento Administrativo General, aprobado mediante Decreto Supremo 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 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital; Decreto de Urgencia 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y Dispone Medidas para su Fortalecimiento, y el Decreto Legislativo 1412, Decreto Legislativo 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, el Poder Judicial, el Ministerio Público, 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:

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 007-2020, Decreto de Urgencia que Aprueba el Marco de Confianza Digital y Dispone Medidas para su Fortalecimiento, y su reglamento.*
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 1412 y el Decreto de Urgencia 007-2020.*
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 30254, a través de programas de difusión y concientización u otras acciones estratégicas.*
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.*
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.*
6. *Identificar y validar las propuestas de activos críticos nacionales que impliquen un componente de seguridad y confianza digital.*
7. *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.*

8. *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.*

9. *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.*

10. *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.*

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

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

13. *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.*

14. *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.*

15. *Otras que determine la Presidencia del Consejo de Ministros.*

<u>Artículo 8</u>. 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.

<u>Artículo 9</u>. 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.

<u>Artículo 10</u>. 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 30225, 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 Secretaría 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.

TERCERA. Declaración de interés nacional del uso ético y el aprovechamiento de las tecnologías emergentes

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

DISPOSICIONES COMPLEMENTARIAS MODIFICATORIAS

PRIMERA. Modificación de los artículos 7 y 13 del Decreto de Urgencia 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y Dispone Medidas para su Fortalecimiento

Modifícanse los artículos 7 y 13 del Decreto de Urgencia 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y Dispone Medidas para su Fortalecimiento, en los siguientes términos:

*"**Artículo 7. Centro Nacional de Seguridad Digital***

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

información sobre incidentes de seguridad digital en el ámbito nacional para gestionarlos.

7.2. El Centro Nacional de Seguridad Digital se encuentra adscrito a la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno 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 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 infraestructura oficial que gestiona, dirige, articula y supervisa la operación, educación, promoción, colaboración y cooperación de datos a nivel nacional, a fin de fortalecer la confianza y bienestar de las personas en el entorno digital en el marco de la presente norma.

13.2. El Centro Nacional de Datos se encuentra a cargo de la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno 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 1129, Decreto Legislativo que regula el Sistema de Defensa Nacional

Modifícase el artículo 6 del Decreto Legislativo 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;

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.

Comuníquese al señor Presidente de la República para su promulgación.

En Lima, a los veinticinco días del mes de junio de dos mil veintiuno.

MIRTHA ESTHER VÁSQUEZ CHUQUILIN
Presidenta a. i. del Congreso de la República

LUIS ANDRÉS ROEL ALVA
Segundo Vicepresidente del Congreso de la República

AL SEÑOR PRESIDENTE DE LA REPÚBLICA