CONGRESO DE LA REPÚBLICA
ÁREA DE TRAMITE DOCUMENTARIO

10 ENE 2020

RECIBIDO

Firma ..... Hora 13.00 hrs.

"Decenio de la Igualdad de oportunidades para mujeres y hombres"

Lima, 9 de enero de 2020

OFICIO Nº 007 -2020 -PR

Señor
PEDRO CARLOS OLAECHEA ÁLVAREZ-CALDERÓN
Presidente de la Comisión Permanente
Congreso de la República
Presente. -

De acuerdo con lo dispuesto por el artículo 135° de la Constitución Política del Perú, nos dirigimos a usted señor Presidente de la Comisión Permanente, con el objeto de dar cuenta de la promulgación del Decreto de Urgencia N° 007 -2020, que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento, para que lo examine y lo eleve al Congreso, una vez que éste se instale.

Sin otro particular, hacemos propicia la oportunidad para renovarle los sentimientos de nuestra consideración.

Atentamente,

MARTIN ALBERTO VIZCARRA CORNEJO
Presidente de la República

VICENTE ANTONIO ZEBALLOS SALINAS
Presidente del Consejo de Ministros

451385 ATD

COMISIÓN PERMANENTE DEL CONGRESO DE LA REPÚBLICA

Lima, 13 de ENERO de 2020

De conformidad con el segundo párrafo del artículo 135° de la Constitución Política del Perú, pase el Decreto de Urgencia N° 004 a la Comisión Permanente.

GIOVANNI FORNO FLÓREZ
Oficial Mayor
CONGRESO DE LA REPÚBLICA

DEPARTAMENTO DE RELATORÍA, AGENDA Y ACTAS		URGENTE ☐		IMPORTANTE ☐	
Área de Despacho Parlamentario	☐	Atender	☐	Agregar a sus Antecedentes	☐
Área de Redacción de Actas	☐	Tramitar	☐	Junta de Portavoces	☐
Área de Relatoría y Agenda	☒	Conocimiento y Fines	☐	Consejo Directivo	☐
Área de Trámite Documentario	☐	Elaborar Informe	☐	Comisión Permanente	☒
		Conformidad V°B°	☐	Licencia	☐
		Otros			

GIULIANA LASTRES BLANCO
Jefa del Departamento de Relatoría, Agenda y Actas
CONGRESO DE LA REPÚBLICA

2

COMISIÓN PERMANENTE DEL CONGRESO DE LA REPÚBLICA

Lima, 15 de enero de 2020

En sesión de la fecha, la Presidencia dio cuenta de los siguientes decretos de urgencia remitidos por el Poder Ejecutivo.----------

Decreto de Urgencia 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital, presentado mediante el Oficio 006-2020-PR, recibido el 10 de enero de 2020.----------

Decreto de Urgencia 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento, presentado mediante el Oficio 007-2020-PR, recibido el 10 de enero de 2020.----------

Seguidamente, la Presidencia propuso como coordinador al congresista Neyra Olaychea para la elaboración del informe sobre los **Decretos de Urgencia 006 y 007-2020** con el congresista Palma Mendoza.----------

Efectuada la votación nominal, se aprobó por 14 votos a favor, ningún voto en contra y ninguna abstención la designación del congresista Neyra Olaychea como coordinador para la elaboración del informe de los **Decretos de Urgencia 006 y 007-2020**, con el congresista Palma Mendoza quienes recibirán la asesoría técnica legal del Departamento de Comisiones.----------

La Presidencia dejó constancia del voto a favor de los congresistas Huilca Flores y Arana Zegarra.---

Se acordó la dispensa del trámite de aprobación del Acta para ejecutar lo acordado en la presente sesión.----------

JAIME ABENSUR PINASCO
Director General Parlamentario
CONGRESO DE LA REPÚBLICA

REPÚBLICA DEL PERÚ

ES COPIA FIEL DEL ORIGINAL
FÉLIX PINO FIGUEROA
SECRETARIO DEL CONSEJO DE MINISTROS

Decreto de Urgencia

N° 007 -2020

DECRETO DE URGENCIA QUE APRUEBA EL MARCO DE CONFIANZA DIGITAL Y DISPONE MEDIDAS PARA SU FORTALECIMIENTO

EL PRESIDENTE DE LA REPÚBLICA

CONSIDERANDO:

Que, de conformidad con el artículo 135 de la Constitución Política del Perú, durante el interregno parlamentario, el Poder Ejecutivo legisla mediante decretos de urgencia de los que da cuenta a la Comisión Permanente para que los examine y los eleve al Congreso, una vez que éste se instale;

Que, mediante Decreto Supremo N° 165-2019-PCM, Decreto Supremo que disuelve el Congreso de la República y convoca a elecciones para un nuevo Congreso, se revocó el mandato parlamentario de los congresistas, manteniéndose en funciones la Comisión Permanente;

Que, mediante Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, se establece un marco de gobernanza del gobierno digital para la adecuada gestión de la identidad digital, servicios digitales, arquitectura digital, interoperabilidad, seguridad digital y datos, así como el régimen jurídico aplicable al uso transversal de tecnologías digitales en la digitalización de procesos y prestación de servicios digitales por parte de las entidades de la Administración Pública en los tres niveles de gobierno;

PRESIDENCIA DEL CONSEJO DE MINISTROS Secretaría de Gobierno Digital

Que, el artículo 30 del precitado Decreto Legislativo define la Seguridad Digital como 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;

PRESIDENCIA DEL CONSEJO DE MINISTROS OFICINA GENERAL DE ASESORÍA JURÍDICA V°B°

Que, asimismo, el artículo 33 del referido Decreto Legislativo, establece que la Seguridad de la Información se enfoca en la información, de manera independiente de su formato y soporte. La seguridad digital se ocupa de las medidas de la seguridad de la información procesada, transmitida, almacenada o contenida en el entorno digital, procurando generar confianza, gestionando los riesgos que afecten la seguridad de las personas y la prosperidad económica y social en dicho entorno;

Que, mediante Decreto Supremo N° 237-2019-EF, se aprueba el Plan Nacional de Competitividad y Productividad, el cual presenta un conjunto de medidas consensuadas entre el sector público y privado con miras a establecer un entorno

COPIA FIEL DEL ORIGINAL
FÉLIX PINO FIGUEROA
SECRETARIO DEL CONSEJO DE MINISTROS

favorable y competitivo que permita generar bienestar para todos los peruanos sobre la base de un crecimiento económico sostenible con enfoque territorial;

Que, del precitado Plan Nacional se entiende que las tecnologías digitales tienen un valor estratégico para reducir brechas, impulsar la innovación y apoyar en el crecimiento del país; más aún, señala que los cambios tecnológicos por los cuales atraviesa el mundo actual serían mucho más fáciles de adoptar si es que realizamos una transformación digital a lo largo del país;

Que, mediante Decreto Supremo N° 086-2015-PCM se declara de interés nacional las acciones, actividades e iniciativas desarrolladas en el marco del proceso de vinculación del Perú con la Organización para la Cooperación y el Desarrollo Económicos (OCDE) e implementación del Programa País, en esa línea, cobra relevancia las Recomendaciones para la Gestión de Riesgos de Seguridad Digital realizadas por la OCDE, entre las cuales se señala la importancia del establecimiento de Equipos de Respuestas a Incidentes de Seguridad Digital a nivel de los Estados;

Que, en el documento Gobierno Digital en el Perú "Trabajando con los ciudadanos" la OCDE señala como recomendación que el Estado Peruano debe "considerar establecer un Centro Nacional de Seguridad Digital" que busque articular acciones con los actores relevantes para gestionar incidentes de seguridad digital y fortalecer la confianza;

Que, la confianza digital es un estado que emerge como resultado de cuan veraz, predecible, seguro y confiable son las interacciones digitales que se generan entre personas, empresas, entidades públicas o cosas en el entorno digital. La confianza digital es un componente de la Transformación Digital y tiene como ámbitos la protección de datos, transparencia, seguridad digital y protección del consumidor en el entorno digital;

Que, ante ello como parte de nuestro proceso de vinculación, resulta necesario dictar medidas en materia de confianza y seguridad digital, estableciendo los mecanismos de colaboración y articulación con actores públicos, privados y sociedad civil en el entorno digital, a través de un enfoque sistémico e integral que asegure el fortalecimiento de la confianza en los servicios digitales por las personas, entidades y sociedad en general;

En uso de las facultades conferidas por el artículo 135 de la Constitución Política del Perú;

Con el voto aprobatorio del Consejo de Ministros; y,

Con cargo a dar cuenta a la Comisión Permanente para que lo examine y lo eleve al Congreso, una vez que éste se instale:

DECRETA:

CAPÍTULO I
DISPOSICIONES GENERALES

Artículo 1. Objeto

El presente Decreto de Urgencia tiene por objeto establecer las medidas que resultan necesarias para garantizar la confianza de las personas en su interacción con los servicios digitales prestados por entidades públicas y organizaciones del sector privado en el territorio nacional.

REPUBLICA DEL PERU

ES COPIA FIEL DEL ORIGINAL
FÉLIX PINO FIGUEROA
SECRETARIO DEL CONSEJO DE MINISTROS

Decreto de Urgencia

Artículo 2. Alcance

Las normas y procedimientos que rigen la materia de Confianza Digital son aplicables 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, ciudadanos, empresas y academia.

Artículo 3. Definiciones

Para la aplicación del presente Decreto de Urgencia se establece las siguientes definiciones:

a) **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.

b) **Economía digital**.- Es la innovación y la transformación de la economía basada en el uso estratégico y disruptivo de las tecnologías digitales. Desarrolla la capacidad de incrementar la eficiencia, productividad, transparencia, seguridad y eficacia de los procesos y actividades económicas y sociales, sustentada en el uso intensivo de tecnologías digitales, redes de datos o comunicación y plataformas digitales. Conlleva a la generación de beneficios económicos y sociales, prosperidad y bienestar para la sociedad.

c) **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.

d) **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, o afectan la prosperidad económica y social en general.

e) **Incidente de seguridad digital**.- Evento o serie de eventos que pueden comprometer la confianza, la prosperidad económica, la protección de las personas y sus datos personales, la información, entre otros activos de la organización, a través de tecnologías digitales.

f) **Gestión de incidentes de seguridad digital**.- Proceso formal que tiene por finalidad planificar, preparar, identificar, analizar, contener, investigar incidentes de seguridad digital, así como la recuperación y la determinación de acciones correctivas para prevenir incidentes similares.

ES COPIA FIEL DEL ORIGINAL
FÉLIX PINO FIGUEROA
SECRETARIO DEL CONSEJO DE MINISTROS

g) **Riesgo de seguridad digital.-** Efecto de la incertidumbre relacionada con el uso, desarrollo y gestión de las tecnologías digitales y datos, en el curso de cualquier actividad. Resulta de la combinación de amenazas y vulnerabilidades en el entorno digital y es de naturaleza dinámica. Puede socavar el logro de los objetivos económicos y sociales al alterar la confidencialidad, integridad y disponibilidad de las actividades o el entorno, así como poner en riesgo la protección de la vida privada de las personas. Incluye aspectos relacionados con los entornos físicos y digitales, las actividades críticas, las personas y organizaciones involucradas en la actividad y los procesos organizacionales que la respaldan.
h) **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.
i) **Servicio digital.-** Es aquel servicio provisto de forma total o parcial a través de Internet u otras redes equivalentes, que se caracteriza por ser parcial o totalmente automatizado y utilizar de manera intensiva las tecnologías digitales y datos, permitiendo, al menos una de las siguientes prestaciones: i) Adquirir un bien, servicio, información o contenido, ii) Buscar, compartir, usar y acceder a datos, contenido o información sobre productos, servicios o personas, iii) Pagar un servicio o bien (tangible o intangible) y, iv) El relacionamiento entre personas.
j) **Proveedor de servicios digitales**.- Comprende a cualquier entidad pública u organización del sector privado, independientemente de su localización geográfica, que sea responsable por el diseño, prestación y/o acceso a servicios digitales en el territorio nacional.

CAPÍTULO II
MARCO DE CONFIANZA DIGITAL

Artículo 4. Marco de Confianza Digital

4.1 El Marco de Confianza Digital se 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.

4.2 El Marco de Confianza Digital tiene los siguientes ámbitos:

a) **Protección de datos personales y transparencia**.- El Ministerio de Justicia y Derechos Humanos (MINJUSDH), quien ejerce las autoridades nacionales de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, en el marco de sus funciones y competencias, norma, dirige, supervisa y evalúa la materia de transparencia y protección de datos personales.
b) **Protección del consumidor**.- El Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI), en el marco de sus funciones y competencias, norma, dirige, supervisa y evalúa la materia de protección al consumidor.
c) **Seguridad Digital**.- 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.

ES COPIA FIEL DEL ORIGINAL
FÉLIX PINO FIGUEROA
SECRETARIO DEL CONSEJO DE MINISTROS

REPUBLICA DEL PERU

Decreto de Urgencia

Artículo 5. Ente rector del Marco de Confianza Digital

La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, es el ente rector en materia de Confianza Digital y responsable de la articulación de cada uno de sus ámbitos.

Artículo 6. Atribuciones del Ente rector

La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, en su calidad de ente rector de la Confianza Digital, tiene las siguientes funciones:

a) Formular, articular y dirigir la estrategia de Confianza Digital a nivel nacional, y supervisar su cumplimiento.
b) Emitir lineamientos, estándares, especificaciones, guías, directivas, normas técnicas y estándares en materia de Confianza digital, sin que ello afecte el equilibrio económico financiero de los proyectos digitales.
c) Evaluar las necesidades de las entidades públicas, organizaciones privadas y personas en materia de Confianza Digital.
d) Articular acciones y medidas para la implementación de la estrategia de Confianza Digital a nivel nacional con actores del sector público, sector privado, sociedad civil, academia y otros interesados, así como promover reconocimientos.
e) Mantener informado al Presidente del Consejo de Ministros sobre los resultados y avances de la Confianza Digital en el país y los incidentes de seguridad digital notificados en el Centro Nacional de Seguridad Digital cuando corresponda.

Dichas funciones se ejercen sin afectar las autonomías y atribuciones de cada sector en el marco de sus competencias.

Artículo 7. Centro Nacional de Seguridad Digital

7.1 Créase el Centro Nacional de Seguridad Digital como una plataforma digital 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 la confianza digital. Asimismo, es responsable de identificar, 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 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 en las comunicaciones y coordinaciones con otros organismos, centros o equipos nacionales e internacionales de similar naturaleza.

ES COPIA FIEL DEL ORIGINAL
FÉLIX PINO FIGUEROA
SECRETARIO DEL CONSEJO DE MINISTROS

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, de conformidad con el artículo 32 del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital.

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

CAPÍTULO III
MEDIDAS PARA FORTALECER LA CONFIANZA DIGITAL

Artículo 8. Registro Nacional de Incidentes de Seguridad Digital

8.1 Créase el Registro Nacional de Incidentes de Seguridad Digital que tiene por objetivo recibir, consolidar y mantener datos e información sobre los incidentes de seguridad digital reportados por los proveedores de servicios digitales en el ámbito nacional que puedan servir de evidencia o insumo para su análisis, investigación y solución.

8.2 El Registro Nacional de Incidentes de Seguridad Digital y la información contenida en el mismo tiene carácter confidencial, se soporta en una plataforma digital administrada por la Secretaría de Gobierno Digital, quien es responsable de su disponibilidad, confidencialidad e integridad.

8.3 El Centro Nacional de Seguridad Digital brinda información sobre los registros de incidentes de seguridad digital, a los responsables de los ámbitos del Marco de Seguridad Digital, de conformidad con el artículo 32 del Decreto Legislativo N° 1412, y del Marco de Confianza Digital debiendo observar para tal efecto la normatividad vigente en materia de protección de datos personales.

PRESIDENCIA DEL CONSEJO DE MINISTROS
Secretaría de Gobierno Digital

Artículo 9. Obligaciones del Proveedor de servicios digitales

9.1 Las entidades de la administración pública, los proveedores de servicios digitales del sector financiero, servicios básicos (energía eléctrica, agua y gas), salud y transporte de personas, proveedores de servicios de internet, proveedores de actividades críticas y de servicios educativos, deben:

PRESIDENCIA DEL CONSEJO DE MINISTROS
OFICINA GENERAL DE ASESORÍA JURÍDICA
V°B°

a) Notificar al Centro Nacional de Seguridad Digital todo incidente de seguridad digital.
b) Implementar medidas de seguridad física, técnica, organizativa y legal que permitan garantizar la confidencialidad del mensaje, contenido e información que se transmiten a través de sus servicios de comunicaciones.
c) Gestionar los riesgos de seguridad digital en su organización con fines de establecer controles que permitan proteger la confidencialidad, integridad y disponibilidad de la información.

ES COPIA FIEL DEL ORIGINAL
FÉLIX PINO FIGUEROA
SECRETARIO DEL CONSEJO DE MINISTROS

REPUBLICA DEL PERU

Decreto de Urgencia

d) Establecer mecanismos para verificar la identidad de las personas que acceden a un servicio digital, conforme al nivel de riesgo del mismo y de acuerdo a la normatividad vigente en materia de protección de datos personales.
e) Reportar y colaborar con la autoridad de la protección de datos personales cuando verifiquen un incidente de seguridad digital que involucre datos personales.
f) Mantener una infraestructura segura, escalable e interoperable.

9.2 Las organizaciones privadas toman como referencia las normas emitidas por la Secretaría de Gobierno Digital en cuanto les aplique y les genere valor e implementan de forma obligatoria aquellas que prevengan afectación a los derechos de las personas.

9.3 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.

9.4 Toda actividad crítica debe estar soportada en una infraestructura segura, disponible, escalable e interoperable.

Artículo 10. Articulación internacional

La Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros coordina con el Ministerio de Relaciones Exteriores las acciones vinculadas a la política exterior que contribuyan a fortalecer la confianza en el entorno digital cuando corresponda y en el marco de sus competencias.

PRESIDENCIA DEL CONSEJO DE MINISTROS Secretaría de Gobierno Digital

Artículo 11. Articulación en Materia de Comunicaciones

La Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros coordina con el Ministerio de Transportes y Comunicaciones las acciones vinculadas a la materia de comunicaciones en el marco de sus competencias.

PRESIDENCIA DEL CONSEJO DE MINISTROS SECRETARÍA GENERAL DE ASESORÍA JURÍDICA V°B°

CAPÍTULO IV
USO ÉTICO DE LAS TECNOLOGIAS DIGITALES Y DE LOS DATOS

Artículo 12. Datos como activos estratégicos

12.1 Las entidades públicas y las organizaciones del sector privado administran los datos, en especial los datos personales, biométricos y espaciales, como activos estratégicos, garantizando que estos se generen, compartan, procesen, accesen, publiquen, almacenen, conserven y pongan a disposición durante el tiempo que sea necesario y cuando sea apropiado, considerando las necesidades de información, uso ético, transparencia, riesgos y el estricto cumplimiento de la normatividad en materia de protección de datos personales, gobierno digital y seguridad digital.

ES COPIA FIEL DEL ORIGINAL
FELIX PINO FIGUEROA
SECRETARIO DEL CONSEJO DE MINISTROS

12.2 Las entidades públicas y las organizaciones del sector privado promueven y aseguran el uso ético de tecnologías digitales, el uso intensivo de datos, como internet de las cosas, inteligencia artificial, ciencia de datos, analítica y procesamiento de grandes volúmenes de datos.

12.3 El tratamiento de datos personales debe cumplir la legislación de la materia emitida por la Autoridad Nacional de Protección de Datos Personales.

Artículo 13. Centro Nacional de Datos

13.1 Créase el Centro Nacional de Datos como una plataforma digital 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 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.

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.

Artículo 14. Financiamiento

La implementación de lo establecido en el presente Decreto de Urgencia se financia con cargo al presupuesto institucional de las entidades involucradas, sin demandar recursos adicionales al Tesoro Público.

Artículo 15. Refrendo

El presente Decreto de Urgencia es refrendado por el Presidente del Consejo de Ministros y la Ministra de Justicia y Derechos Humanos.

DISPOSICIONES COMPLEMENTARIAS FINALES

PRIMERA. Reglamentación

El Poder Ejecutivo, dentro de los noventa (90) días hábiles siguientes a la entrada en vigencia de la presente norma, aprueba su reglamento mediante Decreto Supremo refrendado por el Presidente del Consejo de Ministros.

SEGUNDA. Registro Nacional de Incidentes de Seguridad Digital

En un plazo no mayor a noventa (90) días hábiles, posterior a la publicación del presente Decreto de Urgencia, la Presidencia del Consejo de Ministros implementa el Registro Nacional de Incidentes de Seguridad Digital y dicta normas, lineamientos y directivas para su correcto funcionamiento.

REPUBLICA DEL PERU

ES COPIA FIEL DEL ORIGINAL
FÉLIX PINO FIGUEROA
SECRETARIO DEL CONSEJO DE MINISTROS

Decreto de Urgencia

TERCERA. Gestión e Impulso de la Red Nacional de Estado Peruano (REDNACE) y la Red Nacional de Investigación y Educación (RNIE)

La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, se encarga de la gestión e impulso de la Red Nacional de Estado Peruano (REDNACE) y la Red Nacional de Investigación y Educación (RNIE) a las que se refiere la Ley N° 29904 a fin de coadyuvar al logro de las políticas nacionales, el fortalecimiento de una sociedad digital y la transformación digital del Estado. La contratación de los servicios para la conectividad de la REDNACE es realizada por cada entidad de la Administración Pública, de conformidad con lo dispuesto en el artículo 19 de dicha Ley.

CUARTA. Aplicación de la Norma

La presente norma se aplica a los proyectos de asociación público privada, contratos de concesión, proyectos incorporados al proceso de promoción de la inversión privada u otros proyectos y plataformas sobre transformación digital que se diseñen, inicien o gestionen a partir de la entrada en vigencia de la misma.

PRESIDENCIA DEL CONSEJO DE MINISTROS · Secretaría de Gobierno Digital

PRESIDENCIA DEL CONSEJO DE MINISTROS · Oficina General de Asesoría Jurídica · VºBº

Dado en la Casa de Gobierno, en Lima, a los ocho días del mes de enero del año dos mil veinte.

MARTÍN ALBERTO VIZCARRA CORNEJO
Presidente de la República

ANA TERESA REVILLA VERGARA
Ministra de Justicia y Derechos Humanos

VICENTE ANTONIO ZEBALLOS SALINAS
Presidente del Consejo de Ministros

EXPOSICIÓN DE MOTIVOS

DECRETO DE URGENCIA QUE APRUEBA EL MARCO DE LA CONFIANZA DIGITAL Y DISPONE MEDIDAS PARA SU FORTALECIMIENTO

I. FUNDAMENTO

A. Necesidad y Urgencia

1.1 En el Perú se ha tomado la decisión de garantizar la transformación digital del Estado para el logro de los objetivos del país[1] en el marco de la Política General de Gobierno cuyos pilares se centran en integridad y lucha contra la corrupción; fortalecimiento institucional para la gobernabilidad; crecimiento económico equitativo, competitivo y sostenible; desarrollo social y bienestar para la población y descentralización efectiva para el desarrollo. La transformación digital del país es fundamental para el logro de estos objetivos.

1.2 De igual manera, el Perú tomó la decisión de adherirse al Convenio de Budapest o Convenio contra la Ciberdelincuencia reconociendo la necesidad de fortalecer la regulación en materia de seguridad digital dado el avance de la digitalización y el crecimiento de los delitos cometidos en Internet. El Convenio de Budapest es el primer tratado internacional que busca hacer frente a los delitos informáticos y los delitos en Internet mediante la armonización de leyes entre naciones, la mejora de las técnicas de investigación y el aumento de la cooperación entre las naciones firmantes[2]. Dicha adhesión establece plazos perentorios para adecuar la regulación digital en torno a los riesgos digitales y fortalecer la confianza digital de los ciudadanos.

1.3 Bajo ese objetivo, la necesidad de emitir el presente Decreto de Urgencia durante el interregno se fundamenta en las siguientes razones:

a. Durante el 2018 y 2019 el avance de las tecnologías digitales ha sido exponencial. En medio de este avance, se ha verificado el crecimiento de los ciberataques, el robo de datos, los delitos contra niños y adolescentes, suplantación, ingeniería social, entre otros delitos en Internet. Ello ha ocasionado pérdidas económicas tanto en el sector público como en el sector privado y, sobre todo, ha afectado a millones de ciudadanos. Esta situación, que va en franco incremento, nos brinda un pronóstico bastante negativo respecto al cual la normativa resulta insuficiente y revela la necesidad de emitir una norma de rango legal para su resolución.

b. El impacto de los ciberataques afecta la credibilidad y confianza en el país, impacta la competitividad, la productividad, las condiciones para hacer negocios en el país, la productividad en las regiones y la seguridad de las personas. De igual manera, los delincuentes comunes utilizan las redes y el Internet para facilitar sus delitos: acosan a sus víctimas por redes sociales, ingresan a cámaras de vigilancia y a cualquier dispositivo de los hogares, hacen seguimiento a las víctimas rastreando maliciosamente Por ello, existe la urgencia de establecer un marco regulatorio con el fin primario de salvaguardar los **derechos fundamentales** de las personas y ciudadanos en el **entorno digital**[3], especialmente en materia de intimidad personal, familiar y seguridad, así como también atender el deber constitucional del Estado peruano de proteger a la población de las amenazas contra su seguridad[4], incluyendo aquellas que provienen por agentes perjudiciales en el referido entorno digital. Si bien, la aprobación de la Ley de Gobierno

[1] Discurso Presidencial del 28 de Julio de 2019: https://www.gob.pe/institucion/presidencia/mensajes-a-la-nacion
[2] https://www.oas.org/juridico/english/cyb_pry_convenio.pdf
[3] 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
[4] Artículo 44 de la Constitución Política del Perú de 1993.

Digital constituye un gran paso para este objetivo, el gobierno digital solo implica acciones al interior del Estado, lo cual resulta insuficiente. Revertir esta situación es urgente. Para ello debe garantizarse la articulación público privada y que el Estado emita lineamientos para los servicios y plataformas digitales públicas y privadas que se implementen para lograr estos objetivos.

c. La Política General de Gobierno tiene metas definidas que deben ser cumplidos antes del 28 de julio de 2021. Es así que la lucha contra la corrupción y la generación de bienestar social; así como la competitividad y productividad tienen un componente La transformación digital es un proceso fundamental para el logro de los objetivos de dicha Política en beneficio de los ciudadanos y empresas. Por ello, la Política General de Gobierno y la adhesión del Perú al Convenio de Budapest se constituyen en un componente normativo que establece metas sobre la materia a ser cumplidas a corto plazo.

Ahora, la confianza digital NO solo tiene como pilar la seguridad digital, sino también la protección de los datos personales y la protección del consumidor en el entorno digital, por ello, considerando que el plazo para el cumplimiento de **la Política General de Gobierno vence el 2021**, se hace urgente establecer mecanismos y normas que permitan luchar contra la corrupción en el entorno digital, robo y venta de datos personales, clonación de tarjetas de identidad, robo por internet, estafa por internet, etc. En esa línea, Perú no dispone de una norma legal de alto nivel (Norma con rango de Ley) que establece un marco de articulación acorde con las necesidades y demandas de la transformación digital y uso de tecnologías digitales, tal cual se viene dando en países desarrollados, Reino Unido, Estados Unidos, Dinamarca, Estonia, así como nuestros vecinos en América Latina **(Colombia, Brasil, Uruguay y Chile).**

En ese sentido, para revertir el estado de cosas hasta la fecha de vencimiento de la Política de General de Gobierno al 2021, es necesario que a la brevedad se incorporen nuevos estándares a nivel legal. Como puede apreciarse, este escenario debe ser revertido antes del referido plazo, por lo cual es imperioso que se incorporen nuevos estándares a nivel legal que coadyuven en dicha tarea.

Por tal motivo, aguardar hasta la instalación del nuevo Congreso implicaría dejar de contar con tiempo valioso para la aprobación de la ley correspondiente, la realización de las acciones operativas a nivel de las instituciones involucradas en la medida (como emisión de directivas, actos de difusión y capacitación, entre otros), lo cual impediría la aplicación de la norma a la brevedad, manteniendo un estado de cosas que repercuten negativamente sobre un sector de la población en situación de vulnerabilidad. Por el contrario, la aprobación del presente decreto de urgencia permitirá revertir esta situación de manera progresiva, de tal manera que a la fecha de vencimiento de la Política General de Gobierno al 2021 se podrá contar con un marco normativo idóneo para la resolución progresiva del problema y generar un mejor escenario que garantice el fortalecimiento de la confianza digital.

Al respecto, y si bien a través del Decreto Legislativo N° 1412, se aprobó la Ley de Gobierno Digital, que configura un Marco de Seguridad Digital para el Estado Peruano, la estadística que veremos a continuación nos permite apreciar que esta norma no resulta aún del todo eficaz en la prevención y solución de la problemática en esta materia particular, máxime cuando su alcance solo comprende al sector público, lo cual hace necesaria la emisión de una norma que permita un despliegue más efectivo y enfocado en dicho aspecto, en particular para articular no sólo con las entidades públicas sino también con actores privados, academia y sociedad civil, esto eso, como país frente a las amenazas que como veremos se ciernen sobre el proceso de transformación digital que nuestro país ha decido adoptar.

12

En dicho sentido, se aprecia que la prestación de servicios digitales por parte de entidades públicas y organizaciones privadas en el país ha crecido de manera exponencial en los últimos años, siendo utilizados por miles de personas en sus actividades económicas, sociales, educativas, entre otros; no obstante, con ello también se ha incrementado de manera alarmante los ataques y riesgos digitales que afectan la seguridad, tranquilidad y privacidad de las personas, sin que hasta la fecha se establezcan medidas efectivas para su prevención o atención.

Empero, y a la par de lo antes indicado, durante 2018 y 2019 se verifica el alto nivel de crecimiento de los ciberataques en el país, como también las pérdidas económicas resultado de ciberataques, problemática que se encuentra en escalada.

- **Somos el segundo país con mayor cantidad de variantes de RANSOMWARE, software malicioso que captura el sistema para chantajear.**

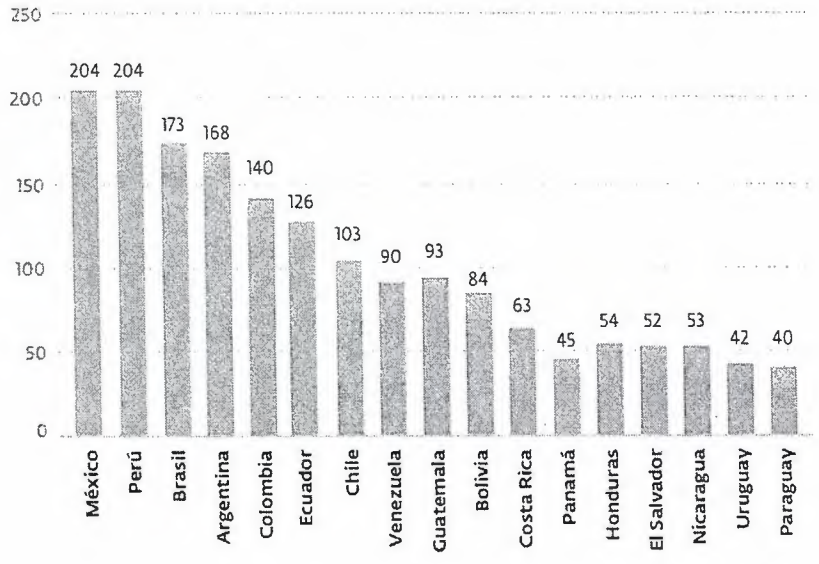


Tabla 1. Cantidad de variantes de Ransomware por país
Fuente: ESET Security Report Latinoamérica 2019

- **Alto nivel de crecimiento de los ciberataques en el país en los últimos 02 años**

ESET Security Report - Latinoamérica 2019

- Según el reporte de ESET Security Report - Latinoamérica 2019[5] el **Perú es el segundo país de América Latina más afectado por incidentes de seguridad**, 71% de los incidentes en América Latina se concentraron en nuestro país, solo nos supera México con un 72%. Asimismo, es el **segundo país** con mayor presencia de variantes de Ransomware (204).
- Ahora bien, entre los **principales incidentes** reportados por las empresas en América Latina tenemos: El acceso indebido (61%), el robo de información (58%) y la privacidad de la información (48%).

Kaspersky

- De acuerdo con reportes de Kaspersky, los ataques en Perú se han incrementado hasta en un 39%, y las ciber amenazas llegan a 3,7 millones por día solo en Latinoamérica, teniendo como objetivo datos sensibles y dinero. En el caso de nuestro país, la modalidad

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

13

más forzada desde la delincuencia digital es el secuestro de información o ransomware, una modalidad que exige un pago de dinero para liberar los datos o los equipos secuestrados, a cambio de no borrar la información dentro de la PC infectada.

Casos Perú

- 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).
- Incremento en un 600% de los ciberataques según la Asociación de Bancos del Perú (ASBANC)[6].
- Ataque cibernético al Banco de Crédito del Perú (BCP) en el año 2018, en el cual accedieron a datos de identificación personal de clientes de dicho banco (números de L
- La División de Investigación de Delitos de Alta Tecnología (DIVINDAT) conforme los casos atendidos viene **evidenciando el incremento de delitos en el entorno digital**, de entre los cuales ha identificado como los más frecuentes: clonación de tarjetas, acoso, espionaje, robo de información a través de páginas falsa, chantaje, extorsión, difamación y estafa a organizaciones del sector público y privado través de internet.

- **Bajo nivel de gestión de la seguridad digital**

Ahora bien, con respecto a la gestión de la seguridad digital el Perú ocupa el último lugar de los países de América Latina en implementar prácticas de gestión de para la seguridad del país. Solo un 42% de las organizaciones encuestadas afirma disponer de una Política de Seguridad de la Información y, peor aún, solo un 8% de las entidades clasifica la información.

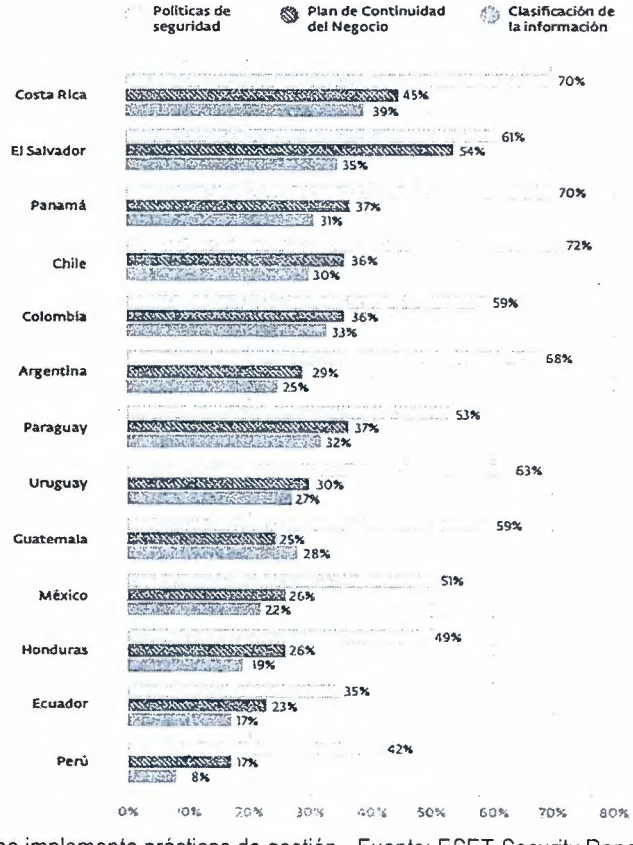


Tabla 1. Perú no implementa prácticas de gestión - Fuente: ESET Security Report Latinoamérica 2019

[6] Ver: https://gestion.pe/economia/empresas/ciberataques-empresas-peruanas-aumentaron-600-ultimos-12-meses-242114-noticia/

14

Falta de articulación entre actores públicos y privados

De otro lado, una problemática adicional en esta materia es que nuestro país **NO cuenta** con una entidad y marco articulador en materia de confianza digital que permitan coordinar y articular acciones entre entidades públicas y privadas con el fin de gestionar los riesgos e incidentes en el entorno digital que afecte los objetivos, procesos y servicios de dichas organizaciones, tal como se señaló precedentemente el Decreto Legislativo N° 1412 tiene como alcance sólo al sector público, y sus disposiciones sólo alcanzan a las entidades públicas. Cabe señalar que pese a los esfuerzos desplegados por la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, aún las acciones para atender los riesgos en el entorno digital son desarticulados, no existe una entidad o mecanismo que centralice los reportes de incidentes de seguridad digital a nivel nacional que permita desarrollar soluciones para su atención.

Actualmente, las organizaciones privados gestionan sus riesgos e incidentes de manera independiente, de manera desarticulada con el sector público, lo anterior evidencia la falta de articulación para atender este tema complejo (distintos actores con diversas necesidades), puesto que un mismo incidente de seguridad digital puede afectar los activos digitales tanto a entidades públicas y organizaciones privadas, sin distinción.

Ahora, los países más desarrollados a nivel mundial han abordado esta problemática institucionalizando un ente articulador, implementando un centro nacional de seguridad digital, definiendo obligaciones para las entidades públicas y privadas; y, sobre todo, estableciendo un marco de confianza en el que se establezca los responsables en el entorno digital y obligaciones para aquellos que prestan servicios digitales. Dichos países tienen determinado:

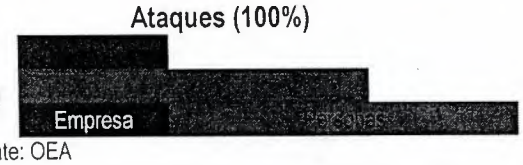
- ¿Quién protege al ciudadano "consumidor" en el entorno digital?
- ¿Quién protege los datos personales de los ciudadanos?
- ¿Quién articula la gestión de un incidente en el entorno digital?
- ¿Cómo se articula acciones con los operadores de justicia?
- ¿Cómo se recopila evidencia digital (correo, mensaje, dato, etc.) que sirva para atender un caso de ciberestafa, ciberespionaje, ciberacoso, etc.?

Lo anterior, exige un abordamiento integral e inmediato, no solo basta con castigar el delito o el mal comportamiento en internet o el mal 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, ello con miras a evitar pérdidas humanas, financieras y reputacionales. Por lo tanto, **resulta urgente** establecer un marco de articulación entre entidades públicas y privados, que permita un intercambio de información rápido para desarrollar soluciones integrales que ayuden a todos los actores del ecosistema digital, asimismo, se hace necesario establecer obligaciones mínimas a los proveedores de servicios digitales conforme las buenas prácticas y experiencia internacional.

Pérdidas económicas resultado de ciberataques

La Organización de los Estados Americanos (OEA) ha indicado en el "Estudio de Ciberseguridad en América Latina y el Caribe" alrededor del 37% de los ciberataques que se concretan están dirigidos a bancos y entidades financieras, mientras que el resto va dirigido a personas, proveedores o clientes.

Ataques a entidades financieras **(37%)**
Ataques a personas o clientes (**63%**)
Total de ataques (100%)



Ataques [7] - Fuente: OEA

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

Asimismo, en el caso del sector financiero se han identificado alrededor de 18 millones de dólares en pérdidas económicas **y aproximadamente 17 millones de dólares de pérdidas económicas en servicios públicos y energía.**

Pérdidas en Millones de Dólares [8] - Fuente: OEA

Lo anterior, impacta directamente a la competitividad y productividad de nuestras empresas y entidades, **resultando urgente** el establecimiento de un marco de articulación público y privado para hacer frente a esta problemática, países como Colombia, Estonia, Uruguay, Reino Unido y Estados Unidos, han establecido normas con rango de Ley para promover la colaboración entre entidades públicas y privadas, implementar centros 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.

Deficiencias de la actual regulación

En el caso peruano no disponemos de una norma con rango de ley en materia de confianza digital que establezca disposiciones obligatorias para públicos y privados en dicho ámbito, así como mecanismos de articulación para una gestión preventiva y atención de incidentes digitales; como se ha mencionado el Decreto Legislativo N° 1412, que aprueba la Ley de Gobierno Digital establece un Marco de Seguridad Digital solo alcanza a entidades del sector público, por lo que no resulta del todo eficaz en la prevención y solución de la problemática en esta materia particular, faltando el componente de articulación con el sector privado, sociedad civil y academia para una gestión oportuna de los riesgos e incidentes de seguridad digital, desarrollo de capacidades, entre otros, así como la definición de obligaciones para todos los actores que presten servicios digitales.

Más aún, con la emisión del Decreto de Urgencia se estaría fortaleciendo el accionar de las entidades responsables en materia de protección de datos personales, seguridad digital y protección al consumidor en el entorno digital, a fin de asegurar la confianza del ciudadano en los servicios digitales.

Diferente, es el caso Europeo donde existe un consenso sobre la materia de confianza digital, contando con normas con rango de ley que permiten la adecuada articulación y enfoque integral y sistémico del problema de la desconfianza en el entorno digital. Los países más desarrollados en materia de confianza y seguridad digital han aprobado normas con rango de Ley para atender la compleja problemática sobre los riesgos y confianza en el entorno digital.

1. **Estonia,** tiene Ley de Ciberseguridad[9]
2. **Dinamarca,** tiene un Centro Nacional de Ciberseguridad y una Estrategia[10] para la seguridad de la información y ciberseguridad danesa.

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

[9] Ver: https://www.riigiteataja.ee/en/eli/523052018003/consolide

[10] Ver: https://digst.dk/media/16943/danish_cyber_and_information_security_strategy_pdfa.pdf

16

3. **Australia,** tiene un Centro Nacional de Ciberseguridad[11], una Estrategia Nacional de Ciberseguridad y ha establecido una red de intercambio de información de confianza[12] para atender los incidentes de seguridad digital a actividades e infraestructuras relevantes para las operaciones del país.
4. **Chile,** Política Nacional de Ciberseguridad[13].
5. **Colombia,** Política de Confianza y Seguridad digital[14].

De otro lado, el Estado Peruano mediante el **Decreto Supremo N° 086-2015-PCM**, declaró de interés nacional las acciones, actividades e iniciativas desarrolladas en el marco del proceso de vinculación del Perú con la **OCDE** e implementación del Programa País y crea la Comisión Multisectorial de naturaleza permanente para promover las acciones de seguimiento del referido proceso. En línea con ello, mediante el **Decreto Supremo N° 118-2018-PCM**, se declaró de interés nacional el desarrollo del **Gobierno Digital, la innovación y la economía digital** con enfoque territorial, lo cual se sustenta en las recomendaciones de la OCDE en materia de Gobierno Digital contenidas en el Estudio de Gobernanza Perú (**OCDE, 2016**)[15].

El año 2015, la OCDE emite el documento "Recomendaciones sobre **gestión de riesgos de seguridad digital** para la prosperidad económica y social", en **el cual busca ser una guía en la formulación de estrategias integrales y sistémicas para abordar los riesgos en el entorno digital desde un alto nivel**. Conforme lo anterior, el Estado Peruano ha optado por abordar los riesgos, delitos, actos ilícitos, operaciones militares en el entorno digital mediante un marco integral, holístico y sistémico, definido en la Ley de Gobierno Digital como Marco de Seguridad Digital del Estado, dentro del cual ya comprende a la **ciberseguridad** como una capacidad que refleja la **perspectiva técnica de la Seguridad Digital**. Así, en la propuesta de DU se establece una definición de ciberseguridad y su articulación con el Marco de Seguridad Digital del Estado peruano. Sobre el Consejo de Seguridad y Defensa Nacional, señalar que **el artículo 13 de la Ley N° 30999**, Ley de Ciberdefensa, **señala** que la PCM, en su calidad de miembro del Consejo de Seguridad y Defensa Nacional, a través de la **Secretaría de Gobierno Digital, establece los protocolos de escalamiento** para atender los incidentes de seguridad digital.

No obstante, a lo indicado precedentemente, se tiene la necesidad de fortalecer y asegurar mecanismos de articulación en materia de política exterior que contribuyan en la confianza en el entorno digital, para lo cual se debe prever articular acciones con el Ministerio de Relaciones Exteriores a fin de atender dicha necesidad.

Asimismo, en el caso del Perú, la norma propuesta incorpora como factor clave, el uso ético de las tecnologías digitales como la inteligencia artificial, bigdata entre otros, a fin de proteger al ciudadano en todas las perspectivas. Cabe indicar que el uso ético de datos y tecnologías digitales se introduce con miras a generar un marco tal como lo tiene Reino Unido[16] y Australia, países desarrollados en materia de servicios digitales, así como también siguiendo las recomendaciones de la OCDE para un uso ético de los mismos, puesto que se debe fortalecer que la ética debe estar presente en todo el ciclo de vida del dato: captación, gestión, privacidad y uso, así como en el uso de la tecnología para el bienestar de la población. Este esfuerzo debe ser articulado con la Autoridad Nacional de Protección de Datos Personales.

---

[11] Ver: https://www.cyber.gov.au/

[12] Ver: https://www.tisn.gov.au/Pages/default.aspx

[13] Ver: https://www.ciberseguridad.gob.cl/media/2017/05/PNCS-CHILE-FEA.pdf

[14] Ver: https://estrategia.gobiernoenlinea.gov.co/623/w3-article-106311.html

[15] Ver: http://bit.ly/2SCyк7e

[16] Por ejemplo el Data Ethics Framework del Reino Unido se crea dentro de la unidad de servicios digitales - http://bit.ly/364YGmv.

17

Como parte de los Principios recomendados por la OCDE en materia de adopción de Inteligencia Artificial en sus economías miembro, se ha identificado que existe una preocupación por el uso ético de tecnologías digitales y datos al momento de diseñar servicios y políticas. En esa línea, se ha indicado que le compete, a cada país miembro, asegurarse de que el diseño de los sistemas de Inteligencia Artificial respete nuestros valores y leyes, de forma que las personas puedan confiar en que su seguridad y privacidad serán objeto de una consideración prioritaria. Estos principios, se constituyen en un referente global para una IA confiable, de modo que las oportunidades que brinda redunden en los mejores resultados para todos. http://bit.ly/2MDFZhL

Adicionalmente a lo anterior, el presente decreto de urgencia debe de cumplir con requisitos formales, tanto previos como posteriores a su promulgación. Así, el requisito ex ante está constituido por el refrendo del Presidente del Consejo de Ministros (inciso 3 del artículo 123 de la Constitución Política del Perú), mientras que el requisito ex post lo constituye la obligación del Ejecutivo de dar cuenta a la Comisión Permanente par que lo examine y lo eleve al Congreso una vez que este se instale, de acuerdo a lo señalado en el artículo 135 de la Constitución. En ese sentido, la presente norma cuenta con la rúbrica del Presidente de la República y el refrendo del Presidente del Consejo de Ministros, la Ministra de Justicia y Derechos Humanos y la Ministra de Economía y Finanzas, de acuerdo a lo señalado en el Decreto de Urgencia.

De otro lado, debe tenerse presente que la norma constituye un decreto de urgencia, cuyo origen se encuentra en la aplicación de los artículos 134 y 135 de la Constitución Política del Perú, encontrándose habilitado el Poder Ejecutivo para legislar mediante decretos de urgencia durante el interregno. Así, durante este periodo del interregno el Poder Ejecutivo se encuentra habilitado para emitir decretos de urgencia que no se encuentren limitados únicamente sobre temas económicos y financieros, lo contrario llevaría a sostener que durante el interregno y ante la inexistencia de una órgano legislativo, el Poder Ejecutivo se encuentra impedido de regular situaciones de atención urgente que no correspondan únicamente a estas materias. Como resulta claro, esto último no puede resultar amparable en un Estado de Derecho ya que pondría en grave riesgo el goce de derechos fundamentales y objetivos y deberes constitucionales, como lo que se buscan a través de la presente norma.

Así las cosas, la propuesta de Decreto de Urgencia también responde al cumplimiento de políticas y planes de cara al 2021:

- **Política de General de Gobierno 2021**

  Mediante **Decreto Supremo N° 056-2018-PCM**, se aprueba la **Política General de Gobierno al 2021**, la cual establece en como uno de sus lineamientos la "Lucha contra la corrupción", en esa línea, disponer de un marco de confianza digital que articule el actuar de las entidades públicas y empresa, aboga a que los ciudadanos identifiquen una respuesta integral frente a este problema toda vez que serán estos actores que intercambiaran información digital de manera inmediata para atender un incidente que impacte la seguridad de las personas y empresas.

  Ahora, la confianza digital **NO solo tiene como pilar la seguridad digital**, sino también la protección de los datos personales y la protección del consumidor en el entorno digital, por ello, considerando que el plazo para el cumplimiento de la Política General de Gobierno vence el 2021, se hace urgente establecer mecanismos y normas que permitan luchar contra la corrupción en el entorno digital, robo y venta de datos personales, clonación de tarjetas de identidad, robo por internet, estafa por internet, etc. En esa línea, Perú no dispone de una norma legal de alto nivel (Norma con rango de Ley) que establece un marco de articulación

18

acorde con las necesidades y demandas de la transformación digital y uso de tecnologías digitales, tal cual se viene dando en países desarrollados, Reino Unido, Estados Unidos, Dinamarca, Estonia, así como nuestros vecinos en América Latina **(Colombia, Brasil, Uruguay y Chile).**

El Decreto de Urgencia cuenta con un plazo de reglamentación de noventa (90) días hábiles, asimismo, se han considerado las siguientes actividades a realizar con anterioridad a la instalación del nuevo congreso:

ID	ACCIÓN URGENTE	2020					
		ENERO	FEBRERO	MARZO	ABRIL	MAYO	JUNIO
1	Formular el Reglamento del DU de Confianza Digital						
2	Implementar el Registro Nacional de Incidentes de Seguridad Digital						
3	Implementar el Centro Nacional de Seguridad Digital						
4	Implementar el Centro Nacional de Datos						
5	Emitir lineamientos, estándares, especificaciones, guías, directivas, normas técnicas y estándares en materia de Confianza digital						
6	Adecuación de normas para implementación Convenio de Budapest						
7	Articular estrategia de Confianza Digital a nivel nacional, y supervisar su cumplimiento						
8	Plan de difusión en materia de Confianza Digital						

- **Convenio de Ciberdelincuencia**

  El Perú ratificó, mediante Decreto Supremo N° 010-2019-RE, su adhesión al "Convenio de Ciberdelincuencia", también conocido como Convenio de Budapest; suscrito el 23 de noviembre de 2001, por el Consejo de Ministros de Europa, compuesto por Ministros del Interior de los Estados que conforman la Unión Europea, conjuntamente con Estados Unidos de Norteamérica, Sudáfrica, Canadá y Japón, al cual se han adherido diversos países a la fecha. Entre los objetivos de este Convenio se encuentran:

  - Armonizar leyes penales sustantivas aplicables a las conductas delictivas con entorno informático.
  - Proveer reglas de procedimiento, normas procesales, persecución del delito t rastreo
  - Establecer un régimen de cooperación internacional, esto es, la colaboración entre Estados para perseguir los delitos informáticos.

  Se observa que, entre las consideraciones más relevantes del Convenio de Ciberdelincuencia, se establece como cuestión prioritaria la política penal común respecto de la protección de la sociedad contra los delitos informáticos, aprobando legislación apropiada y fomento de la cooperación internacional. El Convenio no sólo establece lineamientos en cuestión de un país en particular, sino en función de una normativa con miras a establecer el carácter globalizado para combatir el ciberdelito. Entre otros, establece la preocupación de los Estados suscriptores

ante el riesgo que las redes informáticas y la información electrónica puedan también, ser utilizadas para cometer delitos y que las pruebas relacionadas con dichos delitos puedan ser almacenadas y transferidas por estas redes.

En esa línea, el Perú requiere fortalecer su legislación para atender lo establecido en el referido Convenio, definir un mecanismo de cooperación con los Estados y el sector privado para reducir los riesgos de seguridad digital e intercambio de información de incidentes de seguridad digital.

Cabe indicar que el referido Convenio de Budapest entró en **entró en vigor en nuestro país el 01 de diciembre** del año 2019, en consecuencia, se precisa realizar la adecuación de las normas que resulten necesarias para la implementación efectiva del referido convenio ello en la medida que de sufrir ataques que afecten la seguridad digital, en particular en lo referido a ciberdelincuencia, ello podría en devenir en **daños irreparables en aquellos que se vean afectados así como en la confianza en la gestión que realice nuestro país en dicha materia.**

- **Política Nacional de Inclusión Financiera**

Mediante Decreto Supremo N° 255-2019-EF, se aprueba la Política Nacional de Inclusión Financiera, la cual establece en como uno de sus objetivos prioritarios 4 *"Desarrollar infraestructura de telecomunicaciones y plataformas digitales para incrementar la cobertura de servicios financieros. Lo cual se sustenta en desarrollar infraestructura de telecomunicaciones para facilitar que los servicios financieros se encuentren al alcance de todos los segmentos de la población, así como en desarrollar plataformas digitales a fin de favorecer la colaboración, interoperabilidad, autenticación,* ***seguridad digital*** *y el uso optimizado de las tecnologías digitales".*

Consistente con ello, se estableció como uno de sus lineamientos "Desarrollar plataformas digitales a fin de favorecer la colaboración, interoperabilidad, autentificación, **seguridad digital** y el uso optimizado de las tecnologías digitales."

En esa línea, resulta urgente fortalecer la **regulación y plataformas** que permitan desplegar servicios digitales para promover la inclusión financiera, en un marco de confianza digital. En esa línea, **resulta urgente** establecer una norma que permita articular acciones en materia de seguridad digital como parte del marco de seguridad digital, las acciones se coordinarán con actores públicos y privados. Adicionalmente, es importante que asegurar que las plataformas digitales recojan las disposiciones emitidas por la Autoridad Nacional de Protección de Datos Personales y el INDECOPI en su calidad de protector del consumidor. Ahora bien, para preservar la seguridad digital se hace necesario que se establezcan obligaciones mínimas a los proveedores de servicios digitales, tal cual lo desarrolla Estonia, Colombia, Reino Unido, Dinamarca, etc.

Cabe señalar que la OCDE, en el año 2019, publicó el estudio "**Digital Government in Perú: Working Closely with Citizens**"[17]recomienda:

a. Considere establecer un Centro Nacional para gestionar los riesgos e incidentes de seguridad digital, conforme las mejores prácticas y las Recomendación de la OCDE sobre Gestión de riesgos de seguridad digital para la prosperidad económica y social (OCDE, 2015).

[17] Obtenido de OECD (2019), Digital Government in Peru: Working Closely with Citizens, OECD Digital Government Studies, OECD Publishing, Paris, https://doi.org/10.1787/0c1eb85b-en

20

b. Buscar la cooperación con el sector privado y otros actores relevantes en este entorno.

B. Estado del Arte

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 y 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[18].

Adicionalmente, según datos del Instituto Nacional de Estadística e Informática (INEI) a setiembre 2019[19] en el Perú la población de 06 años a más de edad que hace uso de internet es de 59.8%, con respecto al grupo etario se sabe que el 76.8% corresponde a adolescentes de 12 a 18 años de edad, el 88.5% a jóvenes de 19 a 24 años, y el 72.5% a adultos entre los 25 y 40 años, siendo estos grupos la población que más accede a este Internet. Un aspecto **importante a considerar es el porcentaje de población que hace uso de Internet a través del teléfono celular 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, se incrementan las transacciones, las ventas y compras, lo cual es producto de una mayor conectividad y que tanto entidades públicas como empresas han apert urado canales digitales para ello. No obstante, se requiere dictar medidas que aseguren la confianza digital en la interacción de las personas con dichos servicios, más aun considerando que a la fecha nuestro país ha evidenciado la voluntad política y social por acoger la denominada transformación digital.

Indicador	Resultado
Confianza en el Estado Peruano	El 40% de los encuestados desconfía del Estado Peruano
Manera preferida para realizar gestiones	El 67 % de encuestados lo realiza de manera presencial El 24 % de encuestados lo realiza a través de internet El 9 % de encuestados lo realiza por teléfono
Trámites con alguna entidad por internet	9 de cada 10 encuestados no ha realizado ningún trámite a través de la página web de la entidad

Tabla 1.- Algunos Indicadores sobre satisfacción ciudadana | Fuente: Encuesta Nacional de Satisfacción Ciudadana 2017

Más aún, el Foro Económico Mundial (FEM) señala en su "Informe Global sobre Riesgos 2018" [20] (Global Risk Report, su denominación en inglés) que uno de los cinco (05) 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.

En esa línea, se ha urgente emitir disposiciones específicas para establecer una norma que genera el Marco de Confianza digital, así como crear un Centro Nacional de Seguridad Digital, un Registro

[18] Ver: https://www.ecommercenews.pe/ecommerce-insights/2019/crecimiento-del-comercio-electronico-en-peru.html

[19] Ver: https://www.inei.gob.pe/media/MenuRecursivo/boletines/ticdiciembre.pdf

[20] El documento puede ser consultado en: https://www.weforum.org/reports/the-global-risks-report-2018

21

Nacional de Incidentes de Seguridad Digital y la constitución del dato como un activo estratégico refleja la voluntad del Estado por atender las preocupaciones y riesgos de las personas en el entorno digital, velar por su tranquilidad y asegurar confianza en los servicios digitales, aspecto que no puede esperar.

Estudios internacionales

Al respecto, en el 2018 Microsoft publicó el documento denominado "Global Cyber Risk Perception Survey"[21], un estudio que proporciona una perspectiva sobre el estado de la gestión del riesgo cibernético en organizaciones a nivel mundial, concluyendo que estas 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 **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 2018 nuestro país está ubicado en el puesto 95 de 193 economías evaluadas.**

Confianza Digital

En esa línea, la **adecuada satisfacción** de las expectativas y la atención de las demandas y necesidades de los ciudadanos cuando realizan transacciones, consultas compras, descarga de información, etc., configura lo que denominados **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.

Ahora bien, sobre la materia de confianza y sus componentes, se han realizado estudios para conocer el Estado del Arte, entre los cuales resaltan:

MasterCard presentó el Índice de Evolución Digital 2017[22] (de sus siglas en inglés DEI 17), donde se propone un **Marco de la confianza digital** compuesto por cuatro habilitadores que ayudan a esbozar sobre la confianza digital y su importancia, siendo los siguientes:

Figura 4.- Habilitadores de la Confianza Digital – Fuente: DEI 17

- *Donde el **entorno y experiencia** es responsabilidad de las empresas, instituciones y gobierno. Ahora bien, el entorno se relaciona con la **seguridad**, los sistemas de responsabilidad y la **privacidad**. La **experiencia** se caracteriza por cuan sencillo y predecible es para los usuarios interactuar con el entorno digital.*

[21] El documento puede ser consultado en https://bit.ly/2EFzKUX

[22] Digital Evolution Index 2017, MasterCard and The Fletcher School, https://globalrisk.mastercard.com/wp-content/uploads/2017/07/Mastercard_DigitalTrust_PDFPrint_FINAL_AG.pdf

22

- *Las actitudes y el comportamiento son dimensiones relacionadas con los consumidores. La actitud corresponde a usuarios con niveles de auto-informados sobre tecnología, las transacciones en línea y la capacidad del gobierno para mantener sus datos seguros. El comportamiento es una medida de cómo los usuarios interactúan con el mundo digital.*

Consistente con lo anterior, podemos referir que cuando **MasterCard** aborda el ámbito de confianza entiende aspectos vinculados a privacidad **(protección de datos personales, seguridad digital y protección de las personas en el entorno digital)**

Ahora bien, según el informe, el **Perú** se encuentra en el puesto **49 de 60 países** en la calificación de su evolución digital (estado de digitalización), por lo que se tiene mucho trabajo por hacer, en términos de desarrollo de infraestructura como de innovación.

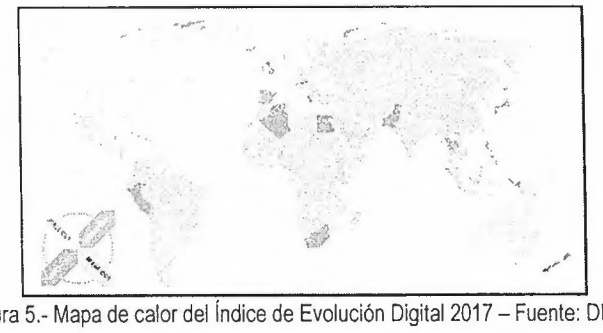


Figura 5.- Mapa de calor del Índice de Evolución Digital 2017 – Fuente: DEI 17

DELOITTE **Insights**, en su informe del Desarrollo de la Confianza Digital: La Tecnología puede liderar el camino[23], propone cuatro (04) pilares de la confianza, las cuales se describen a continuación:

1. **Ética y Responsabilidad**: A medida que las innovaciones tecnológicas plantean cuestiones éticas al dar a las organizaciones más poder, su disposición a trabajar por el bienestar de su cliente, puede generar mayores niveles de credibilidad y confianza.
2. **Privacidad y Control**: Las organizaciones que respetan las preferencias de los clientes sobre qué datos recopilar y cómo se manejan esos datos, pueden recibir mayores permisos para manejar la información de su cliente y proporcionar servicios personalizados.
3. **Transparencia y Accesibilidad**: La transparencia en torno a las prácticas comerciales digitales junto con divulgaciones fáciles de entender pueden ayudar a generar confianza en las intenciones de una organización y su promesa de ofrecer productos y servicios digitales de calidad.
4. **Seguridad y Confiabilidad**: Con una mayor conciencia sobre los riesgos cibernéticos y una mayor dependencia de los dispositivos inteligentes, los clientes cada vez más eligen organizaciones que utilizan la última tecnología para mantener los productos y servicios seguros y confiables.

De lo anterior, se deduce que la tecnología, por sí sola, no puede construir confianza, la confianza se soporta en **cuatro (04)** pilares integrados, los cuales abordan aspectos de **protección de datos personales, transparencia, seguridad digital y protección de las personas en el entorno digital.**

[23] Mayor información en "Building digital trust: Technology can lead the way", Deloitte 2019, https://www2.deloitte.com/content/dam/insights/us/articles/6320_Building-digital-trust/DI_Building-digital-trust.pdf

C. Problema

La confianza digital es un problema complejo que comprende diversos actores (público, privado, academia y sociedad civil) con diferentes intereses, pero un solo afectado que son las personas. En esa línea, la urgencia de establecer un Marco de confianza responde a:

- Vulneración de los derechos fundamentales del ciudadano en el entorno digital.
- Falta de una norma con rango de ley que establezca un marco de articulación entre actores públicos y privados para atender incidentes de seguridad digital a nivel nacional.
- No existe un registro unificado de los incidentes de seguridad digital en el Estado
- Pérdidas económicas como resultado de los ciberataques
- No se tiene un Centro Nacional de Seguridad Digital que gestione la respuesta en el ámbito nacional, interactuando con actores públicos y privados.

II. PROPUESTA O ALTERNATIVA DE SOLUCIÓN

Consistente con lo analizado, la propuesta de Decreto de Urgencia responde a motivaciones de naturaleza estratégica, económica, social, política y técnica, con miras a promover la confianza de los ciudadanos en el entorno digital, asegurando su desenvolvimiento con las mismas garantías que en el entorno digital.

La propuesta normativa tiene como primer aspecto a relevar aquel referido a Disposiciones Generales, las cuales establecen disposiciones sobre el "**Objeto**", "**Alcance**" y "**Definiciones**" que allana la comprensión e interpretación de las disposiciones sustantivas de la norma.

3.1 Objeto de la norma

El Decreto de Urgencia tiene por objeto establecer las medidas que resulten necesarias para garantizar la confianza de las personas en su interacción con los servicios digitales prestados por entidades públicas y organizaciones del sector privado en el territorio nacional.

3.2 Alcance de la propuesta

El Decreto de Urgencia comprende como alcance: "*Las normas y procedimientos que rigen la materia de Confianza Digital son aplicables 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 Nº 004-2019-JUS y, a las organizaciones de la sociedad civil, ciudadanos, empresas y academia*", esto en conformidad de las recomendaciones establecidas por la OCDE, buenas prácticas internacionales y contexto internacional[24].

3.3 Definiciones

Conforme estándares y buenas prácticas internacionales se establecen un conjunto de definiciones con miras a entender de manera integral la propuesta normativa, los términos definidos son: Confianza Digital, Economía digital, Entorno Digital[25], Actividad crítica, Incidente de seguridad digital, Gestión de incidentes de seguridad digital, Riesgo de seguridad digital, Ciberseguridad, Servicio digital y Proveedor de servicios digitales.

---

[24] Conforme se recomienda en el libro "Best Practices for Establishing a National CSIRT", 2016, OEA

[25] La definición de "entorno digital" toma como base lo establecido en el numeral 2 del artículo 3 del Decreto Legislativo N° 1412.

24

3.4 Marco de Confianza Digital

Conforme el análisis del contexto normativo, tendencias y el impacto que la confianza en el entorno digital tiene en la confianza en el gobierno, emprendimiento, uso de servicios digitales, se establecen disposiciones en materia de confianza digital, las cuales se integran en tres ámbitos **1.** Marco de Confianza Digital y **2**. Medidas para fortalecer la confianza digital y **3**. Uso ético de las tecnologías digitales y de los datos.

Así, considerando las investigaciones y estudios revisados (**Mastercard, Deloitte, ISG y la OCDE**) sobre la **confianza digital**, se constituye el Marco de Confianza Digital indicando que es 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*.

Asimismo, se establece que el **Marco de Confianza Digital** tiene los siguientes ámbitos:

a. **Protección de datos personales y transparencia**.- El Ministerio de Justicia y Derechos Humanos (MINJUSDH), en el marco de sus funciones y competencias, norma, dirige, supervisa y evalúa la materia de transparencia y protección de datos personales.
b. **Protección del consumidor**.- El Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI), en el marco de sus funciones y competencias, norma, dirige, supervisa y evalúa la materia de protección al consumidor.
c. **Seguridad Digital**.- 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.

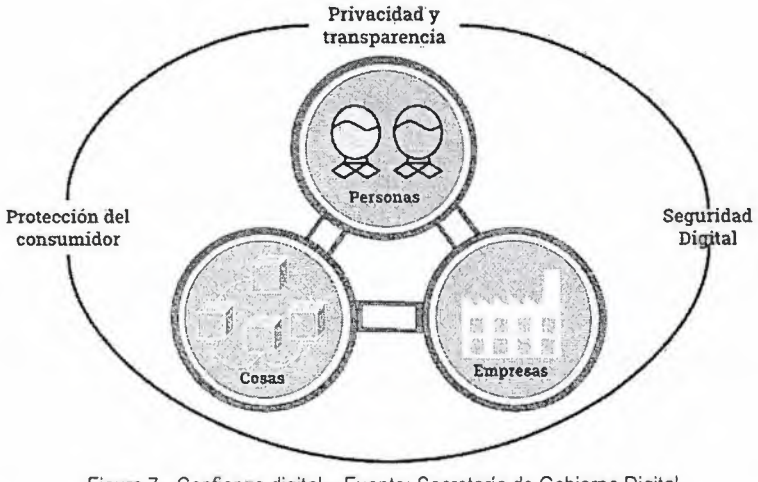


Figura 7.- Confianza digital – Fuente: Secretaría de Gobierno Digital

Consistente con lo anterior, y entendiendo que este ámbito requiere un actor articulador se establece que *la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, es el ente rector en materia de Confianza Digital en el país y responsable de la articulación de cada uno de sus ámbitos.* Cabe resaltar que la PCM es responsable de la coordinación de las políticas nacionales de carácter sectorial y multisectorial del Poder Ejecutivo y de la coordinación con los demás Poderes del Estado, organismos constitucionales autónomos, gobiernos regionales, gobiernos locales, y sociedad civil, conforme lo establece el artículo 2 de su Reglamento de Organización y Funciones y la Ley Orgánica del Poder Ejecutivo, artículos 17 y 18. En ese sentido, el posicionamiento y la autoridad de la Presidencia del Consejo de Ministros, resulta un factor determinante en el cumplimiento de las mismas.

En esa línea, se le confiere una serie de atribuciones en su calidad de ente rector, las cuales son tomadas de las recomendaciones y estándares internacionales, las cuales son las siguientes:

a. *Formular, articular y dirigir la estrategia de Confianza Digital a nivel nacional, y supervisar su cumplimiento.*
b. *Emitir lineamientos, estándares, especificaciones, guías, directivas, normas técnicas y estándares en materia de Confianza digital, sin que ello afecte el equilibrio económico financiero de los proyectos digitales.*
c. *Evaluar las necesidades de las entidades públicas, organizaciones privadas y personas en materia de Confianza Digital.*
d. *Articular acciones y medidas para la implementación de la estrategia de Confianza Digital a nivel nacional con actores del sector público, sector privado, sociedad civil, academia y otros interesados, así como promover reconocimientos.*
e. *Mantener informado al Presidente del Consejo de Ministros sobre los resultados y avances de la Confianza Digital en el país y los incidentes de seguridad digital notificados en el Centro Nacional de Seguridad Digital cuando corresponda.*

Dichas funciones se ejercen sin afectar las autonomías y atribuciones de cada sector en el marco de sus competencias

Adicionalmente, conforme las recomendaciones de la OCDE señaladas en el documento "Gobierno Digital en el Perú – Trabajando de cerca con los ciudadanos", y de conformidad con el Marco de Seguridad Digital creado en el Decreto Legislativo N° 1412, Ley de Gobierno Digital, se dispone la creación del *Centro Nacional de Seguridad Digital como una plataforma digital 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 la confianza y bienestar de las personas en el entorno digital. Asimismo, es responsable de identificar, proteger, detectar, responder, recuperar y recopilar información sobre incidentes de seguridad digital en el ámbito nacional para gestionarlos.*

En esa línea, se establece que el Centro Nacional de Seguridad Digital 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 en las comunicaciones y coordinaciones con otros organismos, centros o equipos nacionales e internacionales de similar naturaleza.

Asimismo, se establece que el referido Centro Nacional de Seguridad Digital incorpora al Equipo de Respuesta a Incidentes de Seguridad Digital Nacional como 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.

Otro aspecto a relevar es su capacidad de articular e intercambiar información con los responsables de los ámbitos del Marco de Seguridad Digital, de conformidad con el artículo 32 del Decreto Legislativo N° 1412, que aprueba la Ley de Gobierno Digital.

26

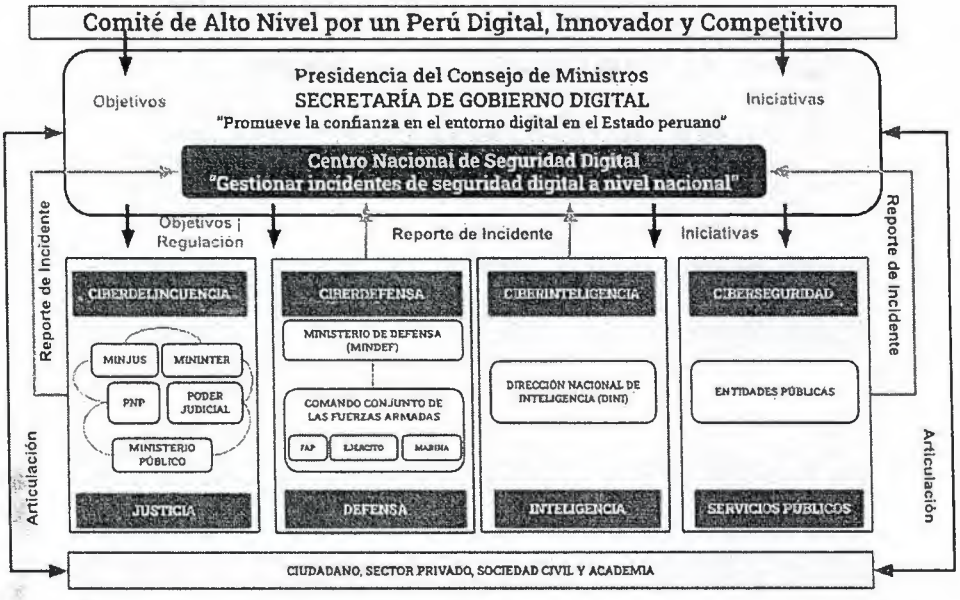


Figura 8.- Marco de Gobernanza de Seguridad Digital – Fuente: Secretaría de Gobierno Digital

3.5 Medidas para fortalecer la confianza digital

Entendiendo que la seguridad digital es un ámbito de la confianza digital y que siendo consistente con su definición es una tarea de intensa cooperación, colaboración y articulación con actores públicos, privados y sociedad civil, se plantea la creación de un Registro Nacional de incidentes de seguridad digital, que tiene por finalidad recibir, consolidar y mantener datos e información sobre los incidentes de seguridad digital reportados por los proveedores de servicios digitales en el ámbito nacional que puedan servir de evidencia o insumo para su análisis, investigación y solución.

El **Registro Nacional de Incidentes de Seguridad Digital** y la información contenida en el mismo tiene carácter confidencial y se soporta en una plataforma digital, el cual es administrado por la Secretaría de Gobierno Digital, quien mantiene su disponibilidad, confidencialidad e integridad.

Cabe señalar que atendiendo la diversidad de actores que pueden aprovechar la información del registro de incidentes, es el Centro Nacional de Seguridad Digital, en su calidad de administrador quien brinda información sobre los registros de incidentes de seguridad digital, por mandato judicial o cuando corresponda, a los responsables de los ámbitos del Marco de Seguridad Digital, de conformidad con el artículo 32 del Decreto Legislativo N° 1412 y del Marco de Confianza Digital conforme a la presente norma.

En línea con lo anterior, también es necesario establecer obligaciones para los proveedores de servicios digitales. En esa línea, las entidades de la administración pública, los proveedores de servicios digitales del sector financiero, servicios básicos (energía eléctrica, agua y gas), salud y transporte de personas, proveedores de servicios de internet, proveedores de actividades críticas y proveedores de servicios educativos deben:

a. *Notificar al Centro Nacional de Seguridad Digital todo incidente de seguridad digital.*
b. *Implementar medidas de seguridad física, técnica, organizativa y legal que permitan garantizar la confidencialidad del mensaje, contenido e información que se transmiten a través de sus servicios de comunicaciones.*
c. *Gestionar los riesgos de seguridad digital en su organización con fines de establecer controles que permitan proteger la confidencialidad, integridad y disponibilidad de la información.*

27

d. *Establecer mecanismos para verificar la identidad de las personas que acceden a un servicio digital, conforme al nivel de riesgo del mismo y de acuerdo a la normatividad vigente en materia de protección de datos personales.*
e. *Reportar y colaborar con la autoridad de la protección de datos personales cuando verifiquen un incidente de seguridad que involucre datos personales.*
f. *Mantener una infraestructura segura, escalable e interoperable.*

No obstante, dichas obligaciones no comprenden a la infraestructura de telecomunicaciones a cargo de los concesionarios de servicios de internet, quienes se rigen por sus contratos de concesión vigentes.

Ahora bien, en el caso de entidades de la administración pública, en materia de seguridad digital deben cumplir con la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) y toda regulación emitida por la Secretaría de Gobierno Digital en su calidad de ente rector de la seguridad digital en el país.

Las organizaciones privadas toman como referencia las normas emitidas por la Presidencia del Consejo de Ministros en cuanto les aplique y les genere valor e implementan de forma obligatoria aquellas que prevengan afectación a los derechos de las personas.

Asimismo, se refiere que toda actividad crítica debe estar soportada en una infraestructura segura, disponible, escalable e interoperable.

Adicionalmente, se requieren mecanismos de articulación concordantes con la política exterior y que contribuyan a la confianza en el entorno digital. En esa línea, se ha previsto que la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros coordine con el Ministerio de Relaciones Exteriores las acciones vinculadas a la política exterior que contribuyan a fortalecer la confianza en el entorno digital cuando corresponda y en el marco de sus competencias

Consistente con lo anterior, la propuesta hace una mención especial a los datos, considerando que estos son activos estratégicos. En esa línea, se establece que las entidades públicas y las organizaciones del sector privado administran los datos, en especial los datos personales, los biométricos y espaciales, como activos estratégicos, garantizando que estos se generen, compartan, procesen, accedan, publiquen, almacenen, conserven y pongan a disposición durante el tiempo que sea necesario y cuando sea apropiado, considerando las necesidades de información, uso ético, transparencia, riesgos y el estricto cumplimiento de la normatividad vigente.

Así, las entidades públicas y las organizaciones del sector privado promueven y aseguran el uso ético de tecnologías digitales, el uso intensivo de datos, como internet de las cosas, inteligencia artificial, ciencia de datos, analítica y procesamiento de grandes volúmenes de datos.

Es preciso indicar que la propuesta normativa no pretende emitir regulaciones sobre contenidos en Internet, siendo esto facultad del sector privado salvo aquellos contenidos que se tipifiquen como delitos o violación de los derechos de las personas, para lo cual la autoridad competente establecerá las sanciones correspondientes en el marco de confianza digital.

Cabe señalar que en el marco de la Ley N° 29733, el tratamiento de datos personales debe cumplir la legislación de la materia emitida por la Autoridad Nacional de Protección de Datos Personales ejercida, a través del Ministerio de Justicia y Derechos Humanos.

28

Por otro lado, el artículo 17 de la Ley N° 29904, Ley de Promoción de la Banda Ancha y Construcción de la Red Dorsal Nacional de Fibra Óptica (en adelante, Ley de Banda Ancha), establece que el Estado cuenta con una Red Nacional del Estado Peruano (**REDNACE**) definida como una red de acceso que se utiliza para la conectividad a nivel nacional aspecto base para el desarrollo de una Sociedad Digital, cabe señalar que se ha establecido que se priorizara ámbitos relacionados con la educación, salud, defensa nacional, seguridad, cultura, investigación y desarrollo e innovación para cumplir con las políticas y lograr los objetivos nacionales, quedando prohibido su uso comercial.

Asimismo, el artículo 25 de la Ley de Banda Ancha establece la incorporación de todas las universidades públicas e institutos de investigación a la REDNACE, formando la Red Nacional de Investigación y Educación (RNIE), a efectos de su integración a las redes regionales de investigación y educación del mundo, con la finalidad de mejorar los procesos de investigación, desarrollo tecnológico e innovación.

Cabe señalar que la OCDE[26], ONU y el BID [27]en sus distintos informes reconocen lo importante de contar con redes de acceso y alta velocidad para promover la digitalización de la economía y sociedad.

Conforme lo anterior se puede advertir que la REDNACE y la RNIE constituyen redes estratégicas para el Estado, más aun, debido a que:

- Son un activo clave para el proceso de digitalización del Estado, de los cuales se deben gestionar sus riesgos.
- Involucra a todas las entidades de la administración pública para asegurar la conectividad de dichas entidades en la prestación de servicios en favor de la población.
- Involucra a universidades públicas e institutos de investigación los que, a través de procesos de investigación, desarrollo tecnológico e innovación, generan valor en la población.
- Sobre la REDNACE es posible configurar otras subredes por software, en base a las facilidades del IP MPLS, como son las redes de teleservicios (telesalud, teleducación, televigilancia, entre otros) con prestaciones y prioridades configurables y que permitirían proveer servicios en la nube o el uso de plataformas y aplicativos compartidos o virtualizados para una mejor gestión de los recursos del Estado.

Dada la relevancia de ambas redes, resulta preponderante que su uso y despliegue sean promovidos por un órgano que permita la adecuada articulación con las distintas entidades e instituciones involucradas, supervise su adecuado funcionamiento, así como su utilización en la implementación de servicios básicos habilitados por las tecnologías digitales en favor de la población, lo que implica una constante coordinación con los sectores involucrados en cada caso.

Siendo ello así, y en atención a las funciones que viene desempeñando la Secretaría de Gobierno Digital, respecto a la coordinación de la seguridad digital, interoperabilidad de los sistemas informáticos del Estado, la asistencia técnica para la implementación de proyectos de tecnologías de la información, así como el impulso en el proceso de desarrollo e innovación tecnológica para la mejora de la gestión pública y digitalización del Estado promoviendo la integración tecnológica,

[26] Toma como fuente el documento "Perfilando la transformación digital en América Latina". https://www.oecd-ilibrary.org/fr/science-and-technology/perfilando-la-transformacion-digital-en-america-latina_4817d61b-es

[27] Toma como fuente el "Informe anual del Índice de Desarrollo de la Banda Ancha en América Latina y el Caribe: IDBA 2018" https://publications.iadb.org/es/informe-anual-del-indice-de-desarrollo-de-la-banda-ancha-en-america-latina-y-el-caribe-idba-2018

esta Secretaría sería el ente idóneo para asumir la gestión y administración de la REDNACE y la RNIE.

Centro Nacional de Datos

La seguridad es un componente esencial para generar "confianza" y el mismo requiere contar con espacios que permitan técnicamente custodiar la información bajo un modelo efectivo de gobernanza. Es por ello, que el crear un Centro Nacional de Datos, como una plataforma digital, permitirá disponer de espacios de uso exclusivo donde las entidades públicas y privadas, mantienen y operan sus infraestructuras tecnológicas. Es ese espacio donde se pueden alojar los servidores y sistemas de almacenamiento para ejecutar las aplicaciones que procesan y almacenan datos.

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.

La Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros, 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.

Adicionalmente, en materia de gestión de proyectos de inversión privada o en relación a contratos suscritos para dicho fin, se establece que no serán afectados o comprendidos en el alcance de la presente norma. En esa línea, se ha establecido una disposición complementaria final que indica lo siguiente:

CUARTA.- Aplicación de la Norma
La presente norma se aplica a los proyectos de asociación público privada, contratos de concesión, proyectos incorporados al proceso de promoción de la inversión privada u otros proyectos y plataformas sobre transformación digital que se diseñen, inicien o gestionen a partir de la entrada en vigencia de la misma.

III. ANÁLISIS COSTO – BENEFICIO

La presente sección identifica los costos y beneficios de la propuesta. Al respecto, entre los beneficios advertidos se encuentran los siguientes:

- Mayor confianza en el uso de canales digitales por parte de la ciudadanía, al establecer obligaciones a los proveedores de servicios digitales con respecto a la implementación de medidas de seguridad físicas, técnicas, organizativas y legales, la correcta gestión de sus riesgos de seguridad digital, entre otros, que permita acceder a las personas a servicios digitales seguros, escalables y confiables.
- Fortalecer el despliegue del proceso de transformación digital de manera sostenible, al ser la confianza digital un aspecto clave para dicho proceso. La transformación digital conlleva a una serie de desafíos, algunos de los cuales pueden representar una ventaja, no obstante, otros pueden representar riesgos para la seguridad. En esa línea, contar con un Marco de Confianza Digital que comprende a actores del sector público, privado, academia y sociedad civil permitirá fortalecer las medidas que aseguren la seguridad digital, la protección de datos personales y la protección al consumidor en el entorno digital, tanto las personas, como empresas y entidades públicas deben compartir la responsabilidad de la seguridad digital.
- Garantizar la seguridad con respecto al resguardo y acceso a los datos e información que gestiona el sector público, al tener un mayor nivel de comprensión por parte de los funcionarios con respecto

30

a los datos como activo estratégico, así como al contar con un centro nacional de datos para su gobernanza. Lo anterior implica ahorros por la ocurrencia de posibles incidentes relacionados al robo de información o acceso indebido a la misma.

- Mejora en los indicadores de satisfacción ciudadana asociados al uso de los servicios digitales.
- Contar con funcionarios y servidores públicos capacitados en materia de seguridad digital, ya que la implementación del Centro Nacional de Seguridad Digital comprende acciones para el fortalecimiento de capacidades en los aspectos técnicos, legales, organizacionales de la seguridad digital.
- Contribuir al crecimiento del comercio electrónico y gobierno digital en el país al fortalecer el ecosistema digital que requiere un mayor nivel de articulación entre actores públicos y privados para asegurar la adecuada protección de las personas, en sus diferentes roles (administrado, consumidor, usuario, etc.) en el entorno digital, al favorecer el intercambio de información sobre amenazas, vulnerabilidades e incidentes.

De otro lado, con respecto a los costos que implicaría el establecimiento de un marco de confianza digital y medidas para su fortalecimiento, señalar lo siguiente:

En el año 2016, **Kaspersky Lab**[28], en conjunto con B2B International, realizó un estudio global en más de 4,000 empresas representativos de 25 países, observando sus presupuestos de seguridad informática, la complejidad de su infraestructura, la actitud que toman ante las amenazas de seguridad y soluciones, el costo real de las filtraciones de información, y los incidentes de seguridad que han sufrido. La **inversión anual promedio** por parte de las empresas varía entre **$1,000 USD** para las empresas más pequeñas y **$1,000,000 USD** en el caso de las más grandes, donde el **costo promedio de la recuperación** de un solo incidente de seguridad está estimado en $86.5 mil USD para las pequeñas y medianas empresas y $861 mil USD para las grandes.

	Empresas pequeñas	Empresas grandes
Inversión anual	**$1,000 USD**	**$1,000,000 USD**
Costo promedio de la recuperación	$86.5 mil	$861 mil USD

Tabla 3.- Costo e inversión – Fuente: Kaspersky Lab

Los ciberataques le han costado a las pequeñas y microempresas un estimado de $149,000 y a las empresas $2 millones de dólares, y los ataques dirigidos resultan en un impacto financiero de $134,000 y $1.7 millones de dólares respectivamente.

Conviene indicar, que según estudios realizados por ESET SECURITY REPORT Latinoamérica 2019, en la cual participan entidades públicas, banca y finanzas, educación, entre otros, las organizaciones afrontan los retos de seguridad digital llevando acciones relacionadas a la implementación de proyectos de seguridad y actividades de educación, resaltando que el porcentaje de organizaciones que lleva a cabo actividades de educación de forma periódica y sufrió incidentes de seguridad alcanzó un 18%, mientras que aquellas en las que no se realizan este tipo de actividades alcanzó un 40%.

Ahora bien, según los estudios en materia de ciberseguridad realizados por la Organización de Estados Americanos (OEA) las pérdidas para la administración pública en materia datos e información sustraída, robada, recuperada, o alterada alcanza los 17 millones de dólares aproximadamente. Cabe indicar que esto implica aspectos reputaciones, la imagen de la entidad o empresa, la infraestructura que se ve afectada, los procesos detenidos, etc. No obstante, el costo de recuperación de un incidente de seguridad digital en la administración pública es similar que en el sector privado en términos monetarios;

[28] Mayor información en https://latam.kaspersky.com/blog/reporte-midiendo-el-impacto-financiero-de-la-seguridad-informatica-en-los-negocios/7711/

31

sin embargo, el impacto es mayor al considerarse que la información que posee el sector público puede llegar a comprender información sensible, reservada, confidencial de lo peruanos y entidades a nivel nacional.

Las disposiciones referidas a la implementación del Centro Nacional de Seguridad Digital, Registro Nacional de Incidentes de Seguridad Digital, Centro Nacional de Datos y plataforma de aprendizaje en línea se encuentran contemplados como parte de los componentes del "Proyecto de Mejoramiento y Ampliación de los Servicios de Soporte para la Provisión de los Servicios a los Ciudadanos y a las Empresas, a Nivel Nacional", que a la fecha viene ejecutando la Presidencia del Consejo de Ministros. El referido Proyecto tiene un monto de inversión de US$ 60.9 millones, siendo el monto del préstamo de US$ 50 millones y la contrapartida nacional de US$ 10.9 millones, de este monto total el porcentaje destinado a dichas implementaciones es de 20% aproximadamente.

Con respecto a las obligaciones por parte de entidades públicas y privadas que prestan servicios digitales señalar lo siguiente:

Obligaciones	Inversión
Notificar al Centro Nacional de Seguridad Digital todo incidente de seguridad digital.	PCM implementa el Registro Nacional de Incidentes de Seguridad Digital, por lo que los actores públicos y privados solo deben realizar el registro respectivo. Para ello, la SEGDI realizará capacitaciones para su registro.
Implementar medidas de seguridad física, técnica, organizativa y legal que permitan garantizar la confidencialidad del mensaje, contenido e información que se transmiten a través de sus servicios de comunicaciones.	Tanto las entidades públicas y privadas invertirán en por lo menos backup y antimalware con el presupuesto que manejan actualmente. Adicionalmente, la SEGDI realizará capacitaciones en línea.
Gestionar los riesgos de seguridad digital en su organización.	La PCM implementará una plataforma y lineamientos para la gestión de riesgos. Adicionalmente, la SEGDI realizará capacitaciones en línea.
Establecer mecanismos para verificar la identidad de las personas que acceden a un servicio digital, conforme al nivel de riesgo del mismo y de acuerdo a la normatividad vigente en materia de protección de datos personales.	Las entidades públicas usarán gratuitamente la plataforma de autenticación nacional de RENIEC , las organizaciones privadas implementarán mejoras
Reportar y colaborar con la autoridad de la protección de datos personales cuando verifiquen un incidente de seguridad que involucre datos personales.	Las acciones se encuentran a cargo del MINJUSDH quien a la fecha ya viene ejecutándolas.
Mantener una infraestructura segura, escalable e interoperable	Tanto las entidades públicas y privadas invertirán en por lo menos backup y antimalware con el presupuesto que manejan actualmente

PRESIDENCIA DEL CONSEJO DE MINISTROS
Secretaría de Gobierno Digital

Finalmente, concluir que una vez valorados los beneficios y posibles cargas que pudiera generar la implementación de la propuesta normativa, señalar que su implementación sería positiva, principalmente por promover la confianza digital en las interacciones que realizan el 59.8%[29] (más de

[29] Se realizó la consulta al "Sistema de Consulta de Base de Datos" de los "Censos Nacionales 2017: XII de Población, VII de Vivienda y III de Comunidades Indígenas" de la cual se obtuvo que la población de 0 a 18 años es de 9,704 850 personas a nivel nacional. Ver: http://censos2017.inei.gob.pe/redatam/.
De la consulta realizada al "Sistema de Consulta de Base de Datos" de los "Censos Nacionales 2017: XII de Población, VII de Vivienda y III de Comunidades Indígenas" se obtuvo la cantidad de población niños de 06 a 11 años y adolescentes de 12 a 18 años a partir, la cual es de 6,699 288 personas. A partir de dicha cantidad se ha

32

16 millones de personas aproximadamente) de la población que accede a Internet en nuestro país, así como también a las empresas (grandes, medianas, pequeñas, micro) que utiliza las tecnologías digitales fomentando una cultura preventiva de seguridad y protección de datos e información, que permita minimizar los riesgos de seguridad digital.

IV. EFECTO DE LA VIGENCIA DE LA NORMA SOBRE LA LEGISLACIÓN NACIONAL

El presente proyecto de Decreto de Urgencia se ha elaborado en cumplimiento de lo dispuesto en el artículo 74 de la Constitución Política del Estado y está en concordancia con lo dispuesto por la Ley General.

Asimismo, el proyecto de Decreto de Urgencia propuesto, no deroga ni modifica ninguna norma con rango legal vigente de nuestro ordenamiento jurídico, en razón que, lo expresado en el Decreto de Urgencia en mención, establece el Marco de la Confianza Digital y medidas adicionales para su fortalecimiento. En vista de ello, la presente exposición de motivos, promueve el crecimiento de entornos digitales seguros, íntegros y confiables, a fin de reducir la brecha entre las expectativas de las entidades de la Administración Pública y las necesidades o intereses del ciudadano, personas y empresas.

realizado el cálculo en base a los porcentajes del documento "Las Tecnologías de Información y Comunicación en los Hogares – Diciembre 2018" del INEI para obtener la cantidad de población de 06 a 11 años y de 12 a 18 años con acceso a Internet, obteniendo aproximadamente 3,817 575 niños, niñas y adolescentes a nivel nacional.

El Peruano
Firmado Digitalmente por:
EMPRESA PERUANA DE SERVICIOS
EDITORIALES S.A. - EDITORA PERU
Fecha: 09/01/2020 04:30:25

DISPOSICIÓN COMPLEMENTARIA DEROGATORIA

Única.- Norma derogatoria

Deróganse las disposiciones contenidas en el Decreto Legislativo 604 relativas al Sistema Nacional de Informática que se opongan al presente Decreto de Urgencia. Entiéndase, para todos sus efectos, que el Sistema Nacional de Transformación Digital sustituye al Sistema Nacional de Informática.

Dado en la Casa de Gobierno, en Lima, a los ocho días del mes de enero del año dos mil veinte.

MARTÍN ALBERTO VIZCARRA CORNEJO
Presidente de la República

VICENTE ANTONIO ZEBALLOS SALINAS
Presidente del Consejo de Ministros

MARÍA ANTONIETA ALVA LUPERDI
Ministra de Economía y Finanzas y
Encargada del Despacho del Ministerio de
Relaciones Exteriores

FLOR AIDEÉ PABLO MEDINA
Ministra de Educación

ANA TERESA REVILLA VERGARA
Ministra de Justicia y Derechos Humanos

ROCÍO INGRED BARRIOS ALVARADO
Ministra de la Producción

EDMER TRUJILLO MORI
Ministro de Transportes y Comunicaciones

1844001-1

DECRETO DE URGENCIA Nº 007-2020

DECRETO DE URGENCIA QUE APRUEBA EL MARCO DE CONFIANZA DIGITAL Y DISPONE MEDIDAS PARA SU FORTALECIMIENTO

EL PRESIDENTE DE LA REPÚBLICA

CONSIDERANDO:

Que, de conformidad con el artículo 135 de la Constitución Política del Perú, durante el interregno parlamentario, el Poder Ejecutivo legisla mediante decretos de urgencia de los que da cuenta a la Comisión Permanente para que los examine y los eleve al Congreso, una vez que éste se instale;

Que, mediante Decreto Supremo Nº 165-2019-PCM, Decreto Supremo que disuelve el Congreso de la República y convoca a elecciones para un nuevo Congreso, se revocó el mandato parlamentario de los congresistas, manteniéndose en funciones la Comisión Permanente;

Que, mediante Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, se establece un marco de gobernanza del gobierno digital para la adecuada gestión de la identidad digital, servicios digitales, arquitectura digital, interoperabilidad, seguridad digital y datos, así como el régimen jurídico aplicable al uso transversal de tecnologías digitales en la digitalización de procesos y prestación de servicios digitales por parte de las entidades de la Administración Pública en los tres niveles de gobierno;

Que, el artículo 30 del precitado Decreto Legislativo define la Seguridad Digital como 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;

Que, asimismo, el artículo 33 del referido Decreto Legislativo, establece que la Seguridad de la Información se enfoca en la información, de manera independiente de su formato y soporte. La seguridad digital se ocupa de las medidas de la seguridad de la información procesada, transmitida, almacenada o contenida en el entorno digital, procurando generar confianza, gestionando los riesgos que afecten la seguridad de las personas y la prosperidad económica y social en dicho entorno;

Que, mediante Decreto Supremo N° 237-2019-EF, se aprueba el Plan Nacional de Competitividad y Productividad, el cual presenta un conjunto de medidas consensuadas entre el sector público y privado con miras a establecer un entorno favorable y competitivo que permita generar bienestar para todos los peruanos sobre la base de un crecimiento económico sostenible con enfoque territorial;

Que, del precitado Plan Nacional se entiende que las tecnologías digitales tienen un valor estratégico para reducir brechas, impulsar la innovación y apoyar en el crecimiento del país; más aún, señala que los cambios tecnológicos por los cuales atraviesa el mundo actual serían mucho más fáciles de adoptar si es que realizamos una transformación digital a lo largo del país;

Que, mediante Decreto Supremo N° 086-2015-PCM se declara de interés nacional las acciones, actividades e iniciativas desarrolladas en el marco del proceso de vinculación del Perú con la Organización para la Cooperación y el Desarrollo Económicos (OCDE) e implementación del Programa País, en esa línea, cobra relevancia las Recomendaciones para la Gestión de Riesgos de Seguridad Digital realizadas por la OCDE, entre las cuales se señala la importancia del establecimiento de Equipos de Respuestas a Incidentes de Seguridad Digital a nivel de los Estados;

Que, en el documento Gobierno Digital en el Perú "Trabajando con los ciudadanos" la OCDE señala como recomendación que el Estado Peruano debe "considerar establecer un Centro Nacional de Seguridad Digital" que busque articular acciones con los actores relevantes para gestionar incidentes de seguridad digital y fortalecer la confianza;

Que, la confianza digital es un estado que emerge como resultado de cuan veraz, predecible, seguro y confiable son las interacciones digitales que se generan entre personas, empresas, entidades públicas o cosas en el entorno digital. La confianza digital es un componente de la Transformación Digital y tiene como ámbitos la protección de datos, transparencia, seguridad digital y protección del consumidor en el entorno digital;

Que, ante ello como parte de nuestro proceso de vinculación, resulta necesario dictar medidas en materia de confianza y seguridad digital, estableciendo los mecanismos de colaboración y articulación con actores públicos, privados y sociedad civil en el entorno digital, a través de un enfoque sistémico e integral que asegure el fortalecimiento de la confianza en los servicios digitales por las personas, entidades y sociedad en general;

En uso de las facultades conferidas por el artículo 135 de la Constitución Política del Perú;

Con el voto aprobatorio del Consejo de Ministros; y,

Con cargo a dar cuenta a la Comisión Permanente para que lo examine y lo eleve al Congreso, una vez que éste se instale:

DECRETA:

CAPÍTULO I
DISPOSICIONES GENERALES

Artículo 1. Objeto

El presente Decreto de Urgencia tiene por objeto establecer las medidas que resultan necesarias para garantizar la confianza de las personas en su interacción con los servicios digitales prestados por entidades públicas y organizaciones del sector privado en el territorio nacional.

Artículo 2. Alcance

Las normas y procedimientos que rigen la materia de Confianza Digital son aplicables 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, ciudadanos, empresas y academia.

Artículo 3. Definiciones

Para la aplicación del presente Decreto de Urgencia se establece las siguientes definiciones:

a) 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.

b) Economía digital.- Es la innovación y la transformación de la economía basada en el uso estratégico y disruptivo de las tecnologías digitales. Desarrolla la capacidad de incrementar la eficiencia, productividad, transparencia, seguridad y eficacia de los procesos y actividades económicas y sociales, sustentada en el uso intensivo de tecnologías digitales, redes de datos o comunicación y plataformas digitales. Conlleva a la generación de beneficios económicos y sociales, prosperidad y bienestar para la sociedad.

c) 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.

d) 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, o afectan la prosperidad económica y social en general.

e) Incidente de seguridad digital.- Evento o serie de eventos que pueden comprometer la confianza, la prosperidad económica, la protección de las personas y sus datos personales, la información, entre otros activos de la organización, a través de tecnologías digitales.

f) Gestión de incidentes de seguridad digital.- Proceso formal que tiene por finalidad planificar, preparar, identificar, analizar, contener, investigar incidentes de seguridad digital, así como la recuperación y la determinación de acciones correctivas para prevenir incidentes similares.

g) Riesgo de seguridad digital.- Efecto de la incertidumbre relacionada con el uso, desarrollo y gestión de las tecnologías digitales y datos, en el curso de cualquier actividad. Resulta de la combinación de amenazas y vulnerabilidades en el entorno digital y es de naturaleza dinámica. Puede socavar el logro de los objetivos económicos y sociales al alterar la confidencialidad, integridad y disponibilidad de las actividades o el entorno, así como poner en riesgo la protección de la vida privada de las personas. Incluye aspectos relacionados con los entornos físicos y digitales, las actividades críticas, las personas y organizaciones involucradas en la actividad y los procesos organizacionales que la respaldan.

h) 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.

i) Servicio digital.- Es aquel servicio provisto de forma total o parcial a través de Internet u otras redes equivalentes, que se caracteriza por ser parcial o totalmente automatizado y utilizar de manera intensiva las tecnologías digitales y datos, permitiendo, al menos una de las siguientes prestaciones: i) Adquirir un bien, servicio, información o contenido, ii) Buscar, compartir, usar y acceder a datos, contenido o información sobre productos, servicios o personas, iii) Pagar un servicio o bien (tangible o intangible) y, iv) El relacionamiento entre personas.

j) Proveedor de servicios digitales.- Comprende a cualquier entidad pública u organización del sector privado, independientemente de su localización geográfica, que sea responsable por el diseño, prestación y/o acceso a servicios digitales en el territorio nacional.

CAPÍTULO II
MARCO DE CONFIANZA DIGITAL

Artículo 4. Marco de Confianza Digital

4.1 El Marco de Confianza Digital se 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.

4.2 El Marco de Confianza Digital tiene los siguientes ámbitos:

a) Protección de datos personales y transparencia.- El Ministerio de Justicia y Derechos Humanos (MINJUSDH), quien ejerce las autoridades nacionales de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, en el marco de sus funciones y competencias, norma, dirige, supervisa y evalúa la materia de transparencia y protección de datos personales.

b) Protección del consumidor.- El Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI), en el marco de sus funciones y competencias, norma, dirige, supervisa y evalúa la materia de protección al consumidor.

c) Seguridad Digital.- 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.

Artículo 5. Ente rector del Marco de Confianza Digital

La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, es el ente rector en materia de Confianza Digital y responsable de la articulación de cada uno de sus ámbitos.

Artículo 6. Atribuciones del Ente rector

La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, en su calidad de ente rector de la Confianza Digital, tiene las siguientes funciones:

a) Formular, articular y dirigir la estrategia de Confianza Digital a nivel nacional, y supervisar su cumplimiento.

b) Emitir lineamientos, estándares, especificaciones, guías, directivas, normas técnicas y estándares en materia de Confianza digital, sin que ello afecte el equilibrio económico financiero de los proyectos digitales.

c) Evaluar las necesidades de las entidades públicas, organizaciones privadas y personas en materia de Confianza Digital.

d) Articular acciones y medidas para la implementación de la estrategia de Confianza Digital a nivel nacional con actores del sector público, sector privado, sociedad civil, academia y otros interesados, así como promover reconocimientos.

e) Mantener informado al Presidente del Consejo de Ministros sobre los resultados y avances de la Confianza Digital en el país y los incidentes de seguridad digital notificados en el Centro Nacional de Seguridad Digital cuando corresponda.

Dichas funciones se ejercen sin afectar las autonomías y atribuciones de cada sector en el marco de sus competencias.

Artículo 7. Centro Nacional de Seguridad Digital

7.1 Créase el Centro Nacional de Seguridad Digital como una plataforma digital 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 la confianza digital. Asimismo, es responsable de identificar, 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 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 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, de conformidad con el artículo 32 del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital.

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

CAPÍTULO III
MEDIDAS PARA FORTALECER LA CONFIANZA DIGITAL

Artículo 8. Registro Nacional de Incidentes de Seguridad Digital

8.1 Créase el Registro Nacional de Incidentes de Seguridad Digital que tiene por objetivo recibir, consolidar y mantener datos e información sobre los incidentes de seguridad digital reportados por los proveedores de servicios digitales en el ámbito nacional que puedan servir de evidencia o insumo para su análisis, investigación y solución.

8.2 El Registro Nacional de Incidentes de Seguridad Digital y la información contenida en el mismo tiene carácter confidencial, se soporta en una plataforma digital administrada por la Secretaría de Gobierno Digital, quien es responsable de su disponibilidad, confidencialidad e integridad.

8.3 El Centro Nacional de Seguridad Digital brinda información sobre los registros de incidentes de seguridad digital, a los responsables de los ámbitos del Marco de Seguridad Digital, de conformidad con el artículo 32 del Decreto Legislativo N° 1412, y del Marco de Confianza Digital debiendo observar para tal efecto la normatividad vigente en materia de protección de datos personales.

Artículo 9. Obligaciones del Proveedor de servicios digitales

9.1 Las entidades de la administración pública, los proveedores de servicios digitales del sector financiero, servicios básicos (energía eléctrica, agua y gas), salud y transporte de personas, proveedores de servicios de internet, proveedores de actividades críticas y de servicios educativos, deben:

a) Notificar al Centro Nacional de Seguridad Digital todo incidente de seguridad digital.

b) Implementar medidas de seguridad física, técnica, organizativa y legal que permitan garantizar la confidencialidad del mensaje, contenido e información que se transmiten a través de sus servicios de comunicaciones.

c) Gestionar los riesgos de seguridad digital en su organización con fines de establecer controles que permitan proteger la confidencialidad, integridad y disponibilidad de la información.

d) Establecer mecanismos para verificar la identidad de las personas que acceden a un servicio digital, conforme al nivel de riesgo del mismo y de acuerdo a la normatividad vigente en materia de protección de datos personales.

e) Reportar y colaborar con la autoridad de la protección de datos personales cuando verifiquen un incidente de seguridad digital que involucre datos personales.

f) Mantener una infraestructura segura, escalable e interoperable.

9.2 Las organizaciones privadas toman como referencia las normas emitidas por la Secretaría de Gobierno Digital en cuanto les aplique y les genere valor e implementan de forma obligatoria aquellas que prevengan afectación a los derechos de las personas.

9.3 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.

9.4 Toda actividad crítica debe estar soportada en una infraestructura segura, disponible, escalable e interoperable.

Artículo 10. Articulación internacional

La Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros coordina con el Ministerio de Relaciones Exteriores las acciones vinculadas a la política exterior que contribuyan a fortalecer la confianza en el entorno digital cuando corresponda y en el marco de sus competencias.

Artículo 11. Articulación en Materia de Comunicaciones

La Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros coordina con el Ministerio de Transportes y Comunicaciones las acciones vinculadas a la materia de comunicaciones en el marco de sus competencias.

CAPÍTULO IV
USO ÉTICO DE LAS TECNOLOGIAS DIGITALES Y DE LOS DATOS

Artículo 12. Datos como activos estratégicos

12.1 Las entidades públicas y las organizaciones del sector privado administran los datos, en especial los datos personales, biométricos y espaciales, como activos estratégicos, garantizando que estos se generen, compartan, procesen, accesen, publiquen, almacenen, conserven y pongan a disposición durante el tiempo que sea necesario y cuando sea apropiado, considerando las necesidades de información, uso ético, transparencia, riesgos y el estricto cumplimiento de la normatividad en materia de protección de datos personales, gobierno digital y seguridad digital.

12.2 Las entidades públicas y las organizaciones del sector privado promueven y aseguran el uso ético de tecnologías digitales, el uso intensivo de datos, como internet de las cosas, inteligencia artificial, ciencia de datos, analítica y procesamiento de grandes volúmenes de datos.

12.3 El tratamiento de datos personales debe cumplir la legislación de la materia emitida por la Autoridad Nacional de Protección de Datos Personales.

Artículo 13. Centro Nacional de Datos

13.1 Créase el Centro Nacional de Datos como una plataforma digital 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 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.

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.

Artículo 14. Financiamiento

La implementación de lo establecido en el presente Decreto de Urgencia se financia con cargo al presupuesto institucional de las entidades involucradas, sin demandar recursos adicionales al Tesoro Público.

Artículo 15. Refrendo

El presente Decreto de Urgencia es refrendado por el Presidente del Consejo de Ministros y la Ministra de Justicia y Derechos Humanos.

DISPOSICIONES COMPLEMENTARIAS FINALES

Primera. Reglamentación

El Poder Ejecutivo, dentro de los noventa (90) días hábiles siguientes a la entrada en vigencia de la presente norma, aprueba su reglamento mediante Decreto Supremo refrendado por el Presidente del Consejo de Ministros.

Segunda. Registro Nacional de Incidentes de Seguridad Digital

En un plazo no mayor a noventa (90) días hábiles, posterior a la publicación del presente Decreto de Urgencia, la Presidencia del Consejo de Ministros implementa el Registro Nacional de Incidentes de Seguridad Digital y dicta normas, lineamientos y directivas para su correcto funcionamiento.

Tercera. Gestión e Impulso de la Red Nacional de Estado Peruano (REDNACE) y la Red Nacional de Investigación y Educación (RNIE)

La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, se encarga de la gestión e impulso de la Red Nacional de Estado Peruano (REDNACE) y la Red Nacional de Investigación y Educación (RNIE) a las que se refiere la Ley N° 29904 a fin de coadyuvar al logro de las políticas nacionales, el fortalecimiento de una sociedad digital y la transformación digital del Estado. La contratación de los servicios para la conectividad de la REDNACE es realizada por cada entidad de la Administración Pública, de conformidad con lo dispuesto en el artículo 19 de dicha Ley.

Cuarta. Aplicación de la Norma

La presente norma se aplica a los proyectos de asociación público privada, contratos de concesión, proyectos incorporados al proceso de promoción de la inversión privada u otros proyectos y plataformas sobre transformación digital que se diseñen, inicien o gestionen a partir de la entrada en vigencia de la misma.

Dado en la Casa de Gobierno, en Lima, a los ocho días del mes de enero del año dos mil veinte.

MARTÍN ALBERTO VIZCARRA CORNEJO
Presidente de la República

VICENTE ANTONIO ZEBALLOS SALINAS
Presidente del Consejo de Ministros

ANA TERESA REVILLA VERGARA
Ministra de Justicia y Derechos Humanos

1844001-2

DECRETO DE URGENCIA Nº 008-2020

DECRETO DE URGENCIA QUE ESTABLECE NUEVOS SUPUESTOS DE CONVERSIÓN DE PENA EN LOS CASOS DE PERSONAS PRIVADAS DE LIBERTAD POR EL DELITO DE OMISIÓN DE ASISTENCIA FAMILIAR PARA PROMOVER EL PAGO DE LA REPARACIÓN CIVIL Y LA DEUDA ALIMENTICIA

EL PRESIDENTE DE LA REPÚBLICA

CONSIDERANDO:

Que, de conformidad con el artículo 135 de la Constitución Política del Perú, durante el interregno parlamentario, el Poder Ejecutivo legisla mediante decretos de urgencia, de los que da cuenta a la Comisión Permanente para que los examine y los eleve al nuevo Congreso, una vez que éste se instale;

Que, mediante Decreto Supremo N° 165-2019-PCM, Decreto Supremo que disuelve el Congreso de la República y convoca a elecciones para un nuevo Congreso, se revocó el mandato parlamentario de los congresistas, manteniéndose en funciones la Comisión Permanente;

Que, la Constitución Política del Perú señala en su artículo 4 que el Estado protege especialmente al niño, al adolescente y a la familia, reconociendo a esta última como un instituto natural y fundamental de la sociedad. Una disposición sobre la protección de niños y adolescentes que es ratificada en el artículo IX del Título Preliminar de la Ley N° 27337, Código de los Niños y Adolescentes, que establece que, en toda medida concerniente al niño y al adolescente, adoptada por el Estado, se considera el Principio del Interés Superior del Niño y del Adolescente y el respeto a sus derechos;

Que, ante las dificultades de cumplimiento de obligaciones alimentarias respecto a niños, niñas y adolescentes ocasionadas por la reclusión de los obligados; y la necesidad de atender prioritariamente los intereses y las oportunidades que requieren los niños, las niñas y los adolescentes en su condición de población vulnerable, resulta conveniente promover egresos penitenciarios de internos condenados por omisión de asistencia familiar, siempre que su otorgamiento esté expresamente condicionado al pago íntegro de las deudas pendientes; que se establezca una revocatoria inmediata por incumplimiento posterior del pago; y que el egresado continúe sancionado con una pena alternativa que permita resocializarlo. Esta medida, a su vez, logrará contrarrestar el hacinamiento penitenciario que aqueja al Sistema Penitenciario peruano a nivel nacional;

Que, la Constitución Política del Perú señala en el inciso 22 de su artículo 139, que el objeto del régimen penitenciario es la reeducación, rehabilitación y reincorporación del penado a la sociedad. Lamentablemente, la situación penitenciaria actual presenta condiciones críticas por las que, a través del Decreto Supremo N° 013-2018-JUS, Decreto Supremo que prorroga la emergencia dispuesta por el Decreto Legislativo Nº 1325, para la reestructuración del Sistema Nacional Penitenciario y el Instituto Nacional Penitenciario, se prorrogó el periodo de emergencia del Sistema Nacional Penitenciario y del Instituto Nacional Penitenciario, por veinticuatro meses adicionales, en razón a asuntos de seguridad, salud, deficiente infraestructura y hacinamiento, siendo este último el factor que problematiza íntegramente el funcionamiento regular del modelo penitenciario;

Que, actualmente nuestros establecimientos penitenciarios albergan aproximadamente 2900 internos por el delito de omisión de asistencia familiar, cuya condición de reclusión no asegura el cumplimiento de las obligaciones alimenticias impuestas y, por el contrario, lo dificulta, repercutiendo directamente en la situación de carencia o desabastecimiento que padecen los niños, niñas o adolescentes que son destinatarios legítimos de dicho pago;

En uso de las facultades conferidas por el artículo 135 de la Constitución Política del Perú;