DIARIO OFICIAL DEL BICENTENARIO

El Peruano

FUNDADO EL 22 DE OCTUBRE DE 1825 POR EL LIBERTADOR SIMÓN BOLÍVAR

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 en 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