REGLAMENTO DEL DECRETO DE URGENCIA N° 007-2020, DECRETO DE URGENCIA QUE APRUEBA EL MARCO DE CONFIANZA DIGITAL Y DISPONE MEDIDAS PARA SU FORTALECIMIENTO

TÍTULO PRELIMINAR

DISPOSICIONES GENERALES

Artículo I. Objeto

El presente Reglamento tiene por objeto desarrollar las disposiciones normativas para garantizar que las interacciones digitales de las personas con los servicios digitales prestados por las entidades públicas y organizaciones del sector privado en el territorio nacional, se desarrollen de forma veraz, predecible, ética, proactiva, transparente, segura, inclusiva y confiable, así como, fortalecer la confianza digital en las entidades públicas, las organizaciones del sector privado, la sociedad civil, la academia y la ciudadanía en general, conforme a lo establecido en el Decreto de Urgencia N° 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.

Artículo II. Finalidad

El presente Reglamento tiene por finalidad regular las siguientes medidas:

2.1 Fortalecer la seguridad digital en las entidades públicas, las organizaciones de la sociedad civil, ciudadanos, empresas y la academia, procurando con ello, el logro de la prosperidad económica y social del país.

2.2 Promover la participación activa de actores del sector público, sector privado, sociedad civil, la academia y otros interesados para garantizar la confianza digital de las personas.

2.3 Fortalecer la articulación de los ámbitos que integran el Marco de Confianza Digital.

Artículo III. Ámbito de aplicación

3.1. El presente Reglamento es aplicable a las entidades comprendidas 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 u otra norma que lo sustituya**.**

3.2. Las empresas que realizan actividad empresarial del Estado que se encuentran en el ámbito del Fondo Nacional de Financiamiento de la Actividad Empresarial del Estado (FONAFE), así como, las empresas públicas de los gobiernos regionales y locales.

3.3. Asimismo, comprende a las organizaciones de la sociedad civil, ciudadanos, empresas y la academia, que integran el Sistema Nacional de Transformación Digital, en lo que corresponda de conformidad con lo establecido en el Decreto de Urgencia N° 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital.

Artículo IV. Definiciones y Acrónimos

Para efectos del presente Reglamento se aplican las siguientes definiciones y acrónimos:

a) **Actividades Críticas:** Son aquellas soportadas en el uso de tecnologías digitales cuya disponibilidad, confidencialidad, integridad y continuidad son imprescindibles para la sociedad o, cuya ausencia por algún incidente de seguridad digital, configura

perjuicios directos o indirectos al funcionamiento de los servicios señalados en el numeral 9.1 del artículo 9 del DU N° 007-2020.

b) **ANPDP:** Autoridad Nacional de Protección de Datos Personales.
c) **ANTAIP:** Autoridad Nacional de Transparencia y Acceso a la Información Pública.
d) **CERT**: Equipo de Respuesta ante Emergencias de Ciberseguridad.
e) **CNSD**: Centro Nacional de Seguridad Digital.
f) **CCD**: Centro de Conocimiento Digital.
g) **CSIRT**: Equipo de Respuestas ante Incidentes de Seguridad Digital.
h) **DU 007-2020:** Decreto de Urgencia N° 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.
i) **HPC**: Computación de altas prestaciones.
j) **HTTPS**: Protocolo de transferencia de hipertexto.
k) **INDECOPI**: Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual.
l) **IOFE:** Infraestructura Oficial de Firma Electrónica.
m) **MINJUSDH:** Ministerio de Justicia y Derechos Humanos.
n) **MPFN**: Ministerio Público y Fiscalía de la Nación.
o) **NCA:** Nivel de Confianza en la Autenticación.
p) **OSCD**: Oficial de Seguridad y Confianza Digital.
q) **PNP**: Policía Nacional del Perú.
r) **PCM**: Presidencia del Consejo de Ministros.
s) **PSD**: Proveedor/es de Servicio/s Digital/es.
t) **SGTD-PCM**: Secretaría de Gobierno y Transformación Digital de la PCM.
u) **SOC**: Centro de Operaciones de Seguridad.
v) **SSPPEE**: Servicios Públicos Esenciales.
w) **SSTSD**: Subsecretaría de Tecnologías y Seguridad Digital.
x) **SNTD:** Sistema Nacional de Transformación Digital.

Artículo V. Principios

4.1 Son principios que rigen el Marco de Confianza Digital:

a) **Colaboración y cooperación.** Se promueve el intercambio y transferencia de información, mejores prácticas, recursos y experiencias a nivel nacional e internacional, a fin de identificar, prevenir y mitigar riesgos en el entorno digital que afecten la continuidad de funciones u operaciones de las entidades públicas, organizaciones del sector privado, el bienestar de las personas y el desarrollo sostenible del país.
b) **Gestión de Riesgos.** La gestión de riesgos se sustenta en la aplicación de estándares y mejores prácticas que permitan reducir los incidentes de seguridad. El diseño, implementación y mejora de las medidas y controles de seguridad digital se basan en la evaluación de riesgos.
c) **Integridad.** En la interacción en el entorno digital o cualquier proceso de diseño, producción, despliegue y operación de plataformas, servicios digitales o uso de la tecnología digital, las personas deben tener una conducta proba, imparcial, honesta y ética en el uso de las tecnologías digitales, contribuyendo al fortalecimiento de la confianza digital, de conformidad con las disposiciones normativas vigentes.
d) **Privacidad y Seguridad desde el diseño.** Se promueve la adopción de medidas preventivas de tipo tecnológico, organizacional, legal, humano y procedimental en todas las etapas del ciclo de vida de los servicios digitales, que preserven la disponibilidad, integridad, y confidencialidad de los datos e información y, cuando corresponda, la autenticidad y no repudio de la información proporcionada.

e) **Recuperación y Resiliencia digital**. Implica la capacidad por la que se adoptan medidas a fin de anticipar, responder, recuperarse y aprender ante incidentes de seguridad digital.
f) **Respeto de los derechos humanos.** El diseño, implementación y mantenimiento de medidas y controles de seguridad digital en los servicios digitales, deben respetar los derechos humanos, garantizando que no existan efectos adversos a derechos como la vida, la libre expresión, la autodeterminación de la persona, la igualdad de trato y la no discriminación, entre otros, establecidos en los instrumentos internacionales sobre derechos humanos.
g) **Responsabilidad.** Las entidades comprendidas en el numeral 9.1. del artículo 9 del DU 007-2020 se comprometen a rendir cuenta sobre las medidas y controles para gestionar los riesgos de la seguridad digital en base a sus capacidades y contexto.
h) **Transparencia.** Se promueve que la provisión de datos o información a través del uso de tecnologías digitales en entornos digitales sea efectiva, clara, visible, confiable, comprensible, coherente para el ciudadano y personas en general; para lo cual se busca que toda información o datos que se gestionan en sistemas o plataformas digitales sean fidedignos, completos, íntegros, coherentes, consistentes y precisos, de conformidad con las normas legales vigentes.

4.2 Los principios que sustentan el Marco de Confianza Digital, sirven de criterio interpretativo para resolver las cuestiones que puedan suscitarse en la aplicación del presente Reglamento, así como, orientan las acciones de articulación y supervisión de los actores del SNTD, desde sus distintos roles y responsabilidades.

TÍTULO I

CONFIANZA DIGITAL

CAPÍTULO I

MARCO DE CONFIANZA DIGITAL

Artículo 1. Marco de Confianza Digital

1.1 El Marco de Confianza Digital es el conjunto de principios, modelos, políticas, normas, procesos, roles, personas, empresas, entidades públicas, infraestructura tecnológica, tecnologías y estándares mínimos que permiten asegurar y mantener la confianza en el entorno digital, de conformidad con lo establecido en el artículo 4 del DU 007-2020.

1.2 Las acciones de las entidades comprendidas en el numeral 9.1. del artículo 9 del DU 007-2020 se orientan a fortalecer la continuidad, disponibilidad y resiliencia frente a incidentes de seguridad digital, ya sean accidentales o intencionados, en los procesos y servicios digitales.

1.3 Es dirigido, supervisado y evaluado por la SGTD-PCM, en su calidad de ente rector de la confianza digital en el país, procurando con ello el logro de la prosperidad económica y social.

1.4 El Marco de Confianza Digital orienta la identificación y establecimiento de condiciones mínimas y razonables de seguridad en el uso de las tecnologías digitales y de las redes de comunicaciones, datos y/o información, a efectos de promover la confianza digital en las entidades públicas, organizaciones de la

sociedad civil, empresas, la academia y la ciudadanía en general, sustentados en la gestión de riesgos de seguridad digital.

1.5 El Marco de Confianza Digital tiene por finalidad articular los ámbitos que lo integran y orientar las actividades en materia de confianza digital de los integrantes del SNTD, para impulsar el proceso de transformación digital a nivel nacional.

Artículo 2. Rectoría del Marco de Confianza Digital

La SGTD-PCM es el ente rector en materia de confianza digital en el país, y es responsable de articular los ámbitos de protección de datos personales y transparencia, protección del consumidor y seguridad digital, de acuerdo a lo establecido en el artículo 5 del DU 007-2020.

Artículo 3. Atribuciones del Ente Rector

La SGTD-PCM, adicionalmente a las funciones señaladas en el artículo 6 del DU 007-2020, tiene las siguientes atribuciones:

a) Promover la colaboración y cooperación, así como, celebrar acuerdos de colaboración para promover la confianza digital con los integrantes del SNTD.
b) Administrar y mantener actualizado el registro nacional de incidentes de seguridad digital.
c) Promover campañas de difusión y promoción que generen interacciones digitales confiables, en coordinación con los entes rectores que conforman el Marco de Confianza Digital.
d) Promover los sellos de calidad y confianza digital, y el reconocimiento de los territorios digitales confiables.
e) Promover una cultura de confianza digital en la ciudadanía.
f) Fortalecer el desarrollo de capacidades y competencias en materia de confianza digital en el marco del impulso del talento digital en el país.

Artículo 4. Componentes del Modelo de Confianza Digital

El Modelo de Confianza Digital comprende los siguientes componentes:

a) Principios rectores.
b) Responsables de los ámbitos del Marco de Confianza Digital.
c) Proveedores de Servicios Digitales.
d) Servicios Digitales.
e) Actores del Ecosistema Digital.
f) Ciudadanía.

Artículo 5. Proveedores de Servicios Digitales

5.1 Los PSD son los que suministran y/o gestionan un servicio digital a través de Internet u otras redes equivalentes en el territorio nacional, a favor de la ciudadanía o persona en general.

5.2 Los terceros que operen como intermediarios de Internet, proveedores de servicios de nube, alojamiento de contenido, de alojamiento, procesamiento, disponibilidad, continuidad, seguridad y soporte al servicio digital, o permitan mejorar su desempeño, usabilidad o acceso no son considerados PSD.

5.3 Los PSD aseguran el cumplimiento de las obligaciones establecidas en el DU 007-2020 y en el presente Reglamento, en los contratos o acuerdos contractuales que suscriban con terceros.

5.4 El cumplimiento de las disposiciones contenidas en el DU 007-2020 y el presente Reglamento por parte de los PSD no los exonera de la observancia de las obligaciones establecidas en las normas legales vigentes que regulan los ámbitos que integran el Marco de Confianza Digital.

CAPÍTULO II

ÁMBITOS DEL MARCO DE CONFIANZA DIGITAL

Artículo 6. Articulación de los ámbitos de Confianza Digital

6.1. La SGTD-PCM, como ente rector del Marco de Confianza Digital, es la encargada de la articulación de los siguientes ámbitos:

1. **Protección de Datos Personales y Transparencia**
   Ámbito a cargo del MINJUSDH, a través de la ANPDP y de la ANTAIP, en el marco de sus funciones y competencias; ambas autoridades norman, dirigen, supervisan y evalúan las acciones relacionadas con las materias de protección de datos personales y de transparencia en el entorno digital, respectivamente.

2. **Protección al Consumidor**
   El INDECOPI, en el marco de sus funciones y competencias, norma, dirige, supervisa y evalúa las acciones relacionadas con la materia de protección al consumidor.

3. **Seguridad Digital**
   La SGTD-PCM, en su calidad de ente rector en materia de seguridad digital en el país, dirige, evalúa, promueve, orienta, articula y supervisa su operación y correcto funcionamiento.

6.2. La SGTD-PCM, brinda asistencia y acompañamiento técnico al MINJUSDH, para el cumplimiento de sus funciones y desarrollo de acciones conjuntas para el diseño de campañas de difusión que involucren la materia de Protección de Datos Personales en el entorno digital, conforme a lo dispuesto en la Ley Nº 29733, Ley de Protección de Datos Personales. Asimismo, en coordinación con la ANPDP, propone protocolos de colaboración e intercambio de información sobre notificaciones de incidentes de seguridad digital, cuando estos involucren datos personales.

6.3. La SGTD-PCM, brinda asistencia y acompañamiento técnico al INDECOPI, para el cumplimiento de sus funciones y desarrollo de acciones conjuntas, para el diseño de campañas de difusión que involucren las materias de protección al consumidor y confianza digital en el entorno digital.

TÍTULO II

SEGURIDAD DIGITAL

CAPÍTULO I

MEDIDAS PARA LA SEGURIDAD DIGITAL EN LA ADMINISTRACIÓN PÚBLICA

Artículo 7. Marco de Seguridad Digital del Estado Peruano

7.1 Las disposiciones de seguridad digital establecidas en el presente Reglamento se articulan con el Marco de Seguridad Digital del Estado Peruano que se desarrolla en el Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y su Reglamento, aprobado por Decreto Supremo N° 029-2021-

PCM, en lo que respecta a la Administración Pública en los tres niveles de gobierno.

7.2 La SGTD-PCM emite normas y lineamientos basados en estándares internacionales y mejores prácticas. Las entidades de la administración pública implementan el marco de seguridad digital institucional de forma progresiva.

Artículo 8. Actividades Críticas y Funciones Críticas en la Administración Pública

8.1 Las actividades críticas se soportan en las funciones críticas, que comprenden al conjunto de personas, procesos, recursos, datos y activos que interactúan articuladamente para soportar el funcionamiento continuo y efectivo de actividades críticas y servicios básicos. Estas actividades son prestadas por entidades públicas u organizaciones privadas relacionadas con la IOFE, con el CNSD, con el SNTD y con el ecosistema de pagos digitales.

Las funciones críticas incluyen como mínimo los procesos de gestión, seguridad y mantenimiento de los sistemas de información, plataformas digitales, infraestructura tecnológica y activos de tecnologías de información, relevantes para la provisión de la actividad crítica o servicio público esencial que proporciona la entidad u organización.

8.2 Los PSD que participan en la prestación de los servicios básicos descritos en el artículo 9 del DU 007-2020 son responsables de establecer medidas para la ejecución continua y efectiva de las actividades críticas de dichos servicios; así como, de identificar, valorar y gestionar adecuadamente los riesgos de seguridad digital que los afecten.

8.3 La SGTD-PCM elabora y aprueba la lista de las actividades y funciones críticas para el CNSD y la SNTD, a través de Resoluciones de Secretaría de Gobierno y Transformación Digital

Artículo 9. Gestión de Riesgos de Seguridad Digital

9.1 La gestión de riesgos de seguridad digital es el conjunto de actividades que permiten la identificación, el análisis, la valoración, el tratamiento, el monitoreo, documentación y la revisión de riesgos a los procesos, activos digitales, datos, información, servicios digitales y actividades en el entorno digital que afecten el logro de los objetivos de la organización. Comprende la evaluación que relaciona a los actores, procesos y activos, con las correspondientes amenazas, vulnerabilidades y controles, generando informes y mapas de riesgos donde se detallan todos los riesgos identificados, sus valoraciones, las decisiones tomadas para su tratamiento y los procesos de gestión de incidentes relacionados con ellos.

9.2 Las entidades públicas implementan el proceso de gestión de riesgos de seguridad digital el cual es evaluado con una periodicidad anual por dichas entidades. Los resultados de la referida evaluación se conservan como información en la entidad, en soporte físico o digital, a fin de garantizar su idoneidad y permitir su análisis.

9.3 La SGTD-PCM, emite las normas y lineamientos para la gestión de riesgos de seguridad digital y su adopción por parte de las entidades públicas. Cuando estos involucran los ámbitos de protección de datos personales y protección al consumidor, coordina para tales efectos, con las autoridades competentes en dichas materias.

9.4 El CNSD, identifica, evalúa y valora los riesgos de seguridad digital de las entidades públicas y organizaciones del sector privado.

Artículo 10. Cooperación Internacional y Alianzas Estratégicas

10.1 La SGTD-PCM es responsable de establecer y determinar las alianzas estratégicas con los actores nacionales del sector público con la finalidad de establecer espacios y plataformas para el intercambio de experiencias y buenas prácticas.

10.2 La SGTD-PCM promueve la participación de la sociedad civil, la academia, el sector privado, la cooperación internacional y otros actores, en alianzas estratégicas específicas para gestionar los incidentes de seguridad digital y garantizar la continuidad de actividades de transcendencia nacional.

10.3 La SGTD-PCM establece, coordina y promueve actividades de concientización y eventos a fin de promocionar el desarrollo del ámbito de la Seguridad Digital y el Marco de Confianza Digital, además, aprueba la Estrategia de formación de Capacidades en materia de Confianza Digital, de manera articulada con las entidades públicas, organizaciones del sector privado, sociedad civil y la academia que conforman el SNTD.

Artículo 11. Oficial de Seguridad y Confianza Digital

11.1 El Oficial de Seguridad y Confianza Digital de la entidad pública es responsable de coordinar la implementación y mantenimiento de acciones estratégicas y técnicas en materia de seguridad digital, así como los procesos del Sistema de Gestión de Seguridad de la Información (SGSI). Asimismo, es responsable de coordinar con el CSIRT institucional el registro y notificación obligatoria al CNSD de cualquier incidente de seguridad digital, e intercambio de información en materia de seguridad digital, conforme lo señalado en los artículos 31, 32, 33 y 34 del presente Reglamento.

11.2 El Oficial de Seguridad y Confianza Digital, para el cumplimiento de sus responsabilidades, coordina con el Oficial de Datos Personales en todas las cuestiones relativas al diseño e implementación de controles para la protección de los datos personales a fin de fortalecer la confianza en el entorno digital.

CAPÍTULO II

MEDIDAS PARA LA SEGURIDAD DIGITAL EN EL SECTOR PRIVADO

Artículo 12. Marco de Seguridad Digital en el Sector Privado

12.1. Las disposiciones de seguridad digital establecidos en el presente Reglamento, son aplicables a las organizaciones del sector privado que presten los servicios señalados en el numeral 9.1 del artículo 9 del DU 007-2020 en un entorno digital.

12.2. Las organizaciones del sector privado que no se encuentren comprendidos en los alcances del DU 007-2020 consideran como referenciales estas disposiciones y aquellos protocolos y lineamientos que se emitan en base al presente Reglamento.

Artículo 13. Actividades Críticas y Funciones Críticas en el Sector Privado

13.1. Las actividades críticas en el sector privado son, además de las señaladas en el numeral 9.1. del artículo 9 del DU 007-2020, aquellas relacionadas con la IOFE en

las que tengan participación, con el CNSD, con el SNTD y el ecosistema de pagos digitales.

13.2 Las actividades críticas en el sector privado se soportan en las funciones críticas, que comprenden al conjunto de personas, procesos, recursos, datos y activos que interactúan articuladamente para soportar el funcionamiento continuo y efectivo de las actividades críticas.

Las funciones críticas incluyen como mínimo los procesos de gestión, seguridad y mantenimiento de los sistemas de información, plataformas digitales, infraestructura tecnológica y activos de tecnologías de información relevantes para la provisión de la actividad crítica o servicio público esencial que proporciona la entidad u organización.

13.3 Los PSD son responsables de establecer medidas para garantizar el funcionamiento continuo y efectivo de las funciones críticas que soportan las actividades críticas y servicios que prestan; así como, de identificar, valorar y gestionar adecuadamente los riesgos de seguridad digital que los afecten.

Artículo 14. Gestión de Riesgos de Seguridad Digital

14.1 Las organizaciones del sector privado implementan la gestión de riesgos de seguridad digital en los términos establecidos en el numeral 9.1 del artículo 9 del presente Reglamento.

14.2 Las organizaciones del sector privado cuyas actividades se encuentren comprendidas en el numeral 9.1 del artículo 9 del DU 007-2020, implementan el proceso de gestión de riesgos de seguridad digital; asimismo, realizan una evaluación periódica del proceso de gestión de riesgos de seguridad digital. Los resultados de la referida evaluación se conservan como información en la entidad, en soporte físico y/o digital, a fin de garantizar su idoneidad y permitir su análisis.

14.3 Las organizaciones del sector privado que brinden servicios en un entorno digital, pueden tomar como referencia e implementar las mejores prácticas, normas técnicas peruanas y estándares internacionales ampliamente reconocidos en materia de gestión de riesgos de seguridad digital, en cuanto les genere valor para el logro de sus objetivos estratégicos, contribuyendo con la implementación del Marco de Confianza Digital.

Artículo 15. Oficial de Seguridad y Confianza Digital en el Sector Privado

15.1 Las funciones desarrolladas por el Oficial de Seguridad y Confianza Digital de la Entidad Privada se rigen de acuerdo a lo establecido en el artículo 11 del presente Reglamento.

CAPÍTULO III

MEDIDAS DE LOS PROVEEDORES DE SERVICIOS DIGITALES

Artículo 16. Implementación de Normas Técnicas Peruanas, Estándares Internacionales y/o mejores prácticas

Los PSD pueden adoptar medidas de seguridad y confianza digital mediante la implementación de Normas Técnicas Peruanas, estándares internacionales y/o mejores prácticas ampliamente reconocidas en materia de seguridad digital, seguridad de la

información, ciberseguridad, accesibilidad, protección de datos personales y prácticas de protección al consumidor.

Artículo 17. Niveles de Confianza en la Autenticación

17.1 Los NCA pueden ser:

a) Nivel 1: Provee un nivel de confianza básico respecto de la identidad de una persona autenticada. Para este nivel se requiere el uso de por lo menos un (01) factor de autenticación.
b) Nivel 2: Provee un nivel de confianza razonable respecto de la identidad de una persona autenticada. Para este nivel se requiere el uso de dos (02) factores de autenticación diferentes entre sí.
c) Nivel 3: Provee un nivel de confianza alto respecto de la identidad de una persona autenticada. Para este nivel se requiere el uso de dos (02) factores de autenticación diferentes entre sí, debiendo uno de ellos estar basado en un módulo criptográfico resistente a manipulaciones.

17.2 Los PSD, para autenticar digitalmente a las personas naturales, implementarán los NCA considerando el nivel de riesgo del servicio digital.

Artículo 18. Obligaciones de los Proveedores de Servicios Digitales

18.1 Las entidades públicas, los proveedores de servicios digitales del sector financiero, servicios básicos (energía eléctrica, agua y gas, entre otros), salud y transporte de personas, proveedores de servicios de Internet, proveedores de actividades críticas y de servicios educativos que lo brindan en el entorno digital, tienen las siguientes obligaciones:

a) Notificar al CNSD los incidentes de seguridad digital de su organización mediante los protocolos, canales y en los plazos establecidos.
b) Implementar controles y medidas de seguridad en la provisión de sus servicios digitales, conforme a su evaluación de riesgos, estándares internacionales y prácticas ampliamente reconocidas.
c) Gestionar los riesgos de seguridad digital para generar valor en su organización.
d) Establecer mecanismos de autenticación para verificar la identidad de las personas que acceden a un servicio digital, considerando los NCA establecidos en el numeral 17.1 del artículo 17 del presente Reglamento, y de acuerdo con la Ley Nº 29733, Ley de Protección de Datos Personales, y las normas de seguridad digital que se aprueben.
e) Reportar y colaborar con la ANPDP, cuando verifiquen un incidente de seguridad digital que involucre el tratamiento indebido de datos personales.
f) Mantener una infraestructura segura, escalable e interoperable, con la finalidad de garantizar la confidencialidad, disponibilidad e integridad de los servicios digitales.
g) Coordinar con los terceros la atención oportuna de todo incidente de seguridad digital.
h) Disponer de servicios de pago digital o electrónico con mecanismos de seguridad adecuados, cuando corresponda.
i) Realizar pruebas para evaluar vulnerabilidades de los servicios digitales de manera proactiva que permitan identificar los riesgos de seguridad digital.
j) Promover la innovación digital como un elemento integral para reducir los riesgos a la seguridad digital a un determinado nivel aceptable.

18.2 Los PSD que se encuentran regulados por Ley o norma especial deben cumplir con la normativa correspondiente a su sector, y se rigen supletoriamente en todo lo no previsto por el presente Reglamento.

18.3 Las organizaciones del sector privado que prestan servicios en el marco de lo establecido en el numeral 9.1 del artículo 9 del DU 007-2020 se sujetan a lo establecido en el numeral 9.2 del artículo 9 de la norma antes señalada.

Artículo 19. Monitoreo y Supervisión del Cumplimiento de las Obligaciones del ámbito de Seguridad Digital

La SGTD-PCM realiza acciones de monitoreo y supervisión sobre el cumplimiento de obligaciones de los proveedores de servicios digitales, de conformidad con lo establecido en el artículo 9 del DU 007-2020 y el artículo 18 del presente Reglamento.

Las acciones de supervisión se realizan de forma presencial o digital y tienen un enfoque basado en riesgos, que permitan las recomendaciones de mejoras o la adopción de medidas correctivas y preventivas. Para tal fin, elabora los lineamientos para la supervisión del cumplimiento de las obligaciones de seguridad digital establecidas en el presente Reglamento.

CAPÍTULO IV

CENTRO NACIONAL DE SEGURIDAD DIGITAL

Artículo 20. Centro Nacional de Seguridad Digital

20.1. El CNSD es una plataforma digital gestionada por la SSTSD, que se encarga de gestionar, dirigir, articular y supervisar la operación, educación, promoción, colaboración y cooperación de la seguridad digital a nivel nacional. Asimismo, el CNSD identifica, protege, detecta, responde, recupera, recopila y gestiona la información sobre incidentes de seguridad digital en el ámbito nacional.

20.2. El CNSD contribuye al fortalecimiento de la seguridad y confianza en el entorno digital a través de los siguientes roles, llevados a cabo a través de la SSTSD:

a) **Articulador.** En el CNSD se integran obligatoriamente las plataformas digitales de datos de las entidades del sector público y privado, bajo el ámbito del DU 007-2020; asimismo, de forma facultativa, pueden integrarse las plataformas digitales de datos de las demás entidades del sector privado que operan en el mercado.
b) **Supervisor.** A través del CNSD, la SSTSD vigila la adecuada gestión de los datos que son procesados en las plataformas digitales del sector público y privado. Asimismo, verifica la calidad de los datos y de advertir la vulneración de normas generales, comunica dichos incidentes a las entidades competentes.
c) **Capacitador**. La SSTSD realiza actividades de sensibilización y promoción sobre la adecuada gestión de los datos y el cumplimiento normativo como medio para alcanzar y sostener la Confianza Digital.

20.3. La SGTD-PCM se encarga de elaborar y emitir los lineamientos que aseguren el cumplimiento de lo señalado en el numeral 20.2 del presente artículo.

Artículo 21. Acciones del Centro Nacional de Seguridad Digital

El CNSD, a través de la SSTSD, desarrolla las siguientes acciones:

a) Gestiona los incidentes de seguridad digital a nivel nacional, del Registro Nacional de Incidentes de Seguridad Digital y de las redes de confianza.

b) Articula acciones para la gestión de riesgos e incidentes de seguridad digital, que afecten a la sociedad o a los servicios públicos esenciales, con los responsables de los ámbitos del Marco de Confianza Digital.
c) Promover una cultura de seguridad digital en la ciudadanía.
d) Realizar evaluaciones sectoriales de exposición al riesgo en las materias de seguridad y confianza digital, mediante la ejecución de pruebas de penetración o intrusión controlada, en coordinación con las autoridades competentes, de ser el caso.
e) Desarrollar y fortalecer políticas, estrategias, acciones, actividades, instrumentos, lineamientos, planes, directivas e iniciativas en materia de seguridad y confianza digital; así como, supervisar su cumplimiento y mejora continua.
f) Brindar soporte y asesoría a los actores del ecosistema digital en acciones relacionadas con la gestión de riesgos de seguridad digital.
g) Promover la colaboración y cooperación, así como, implementar acuerdos de colaboración, confianza y cooperación en materia de seguridad digital con otros centros de similar naturaleza del sector privado, la academia, centros de investigación, sociedad civil del ámbito nacional y con otros países, organizaciones y actores internacionales de similar naturaleza.
h) Fortalecer el desarrollo de capacidades y competencias en materia de seguridad digital en el marco del impulso del talento digital; así como, el desarrollo de contenidos y transferencia de conocimiento en materia de seguridad y confianza digital.
i) Impulsar, participar y gestionar la creación de comunidades y espacios de colaboración en los que se genere, comparta e intercambie información y conocimiento sobre mejores prácticas y experiencias relativas a investigación, innovación y desarrollo en materia de seguridad y confianza digital.
j) Implementar los protocolos de comunicaciones, escalamiento, coordinación, intercambio y activación para la atención y gestión de los incidentes de seguridad digital a nivel nacional.
k) Supervisar y evaluar el cumplimiento de las obligaciones en materia de seguridad digital por parte de las entidades públicas y de los proveedores de servicios digitales señalados en el numeral 9.1 del artículo 9 del DU 007-2020, y cuando corresponda, el incumplimiento al ordenamiento jurídico se pone en conocimiento de la autoridad de control y supervisión competente, a fin que se establezca las responsabilidades que pudiera haber.
l) Diseñar y analizar indicadores sobre el avance y desempeño de la seguridad digital a nivel nacional, para así, monitorear y elaborar anualmente publicaciones en dicho ámbito.
m) Evaluar y recomendar las propuestas de activos críticos nacionales que impliquen un componente digital para asegurar la seguridad y confianza digital, y que generen un impacto en la transformación digital del país.
n) Colaborar con la PNP y MPFN, a solicitud de estos, en la atención de un incidente de seguridad digital o investigación de un potencial delito informático.
o) Asistir y colaborar con los operadores de servicios esenciales y actividades críticas para la gestión de incidentes de seguridad digital y evaluación de riesgos de seguridad digital.
p) Colaborar con otros Centros Nacionales de Seguridad Digital o Ciberseguridad, a nivel nacional o internacional, en el desarrollo de sus políticas en gestión de riesgos de seguridad digital o gestión de incidentes de seguridad digital.
q) Coordinar con los operadores de actividades críticas, ejercicios de manera preventiva para identificar riesgos de seguridad digital que los puedan afectar.
r) Otras que determine la SGTD-PCM.

Artículo 22. Líneas de acción del Centro Nacional de Seguridad Digital

La SSTSD desarrolla las siguientes líneas de acción que rigen el funcionamiento del CNSD:

a) **Planificación:** Comprende los objetivos, estrategias y planes de acción a mediano y largo plazo para dirigir y guiar las actividades del CNSD.
b) **Operación:** Comprende los procesos de análisis e intercambio de información, gestión y tratamiento de riesgos, prevención y gestión de incidentes de seguridad digital, así como, la vigilancia y monitoreo continuo de los servicios esenciales, actividades críticas y los activos digitales que se consideren relevantes y/o críticos.
c) **Fortalecimiento de Competencias Digitales:** Comprende el desarrollo de contenidos digitales, así como, la generación y transferencia de conocimiento en materia de confianza digital dirigida a la ciudadanía, PSD y aliados estratégicos en el marco del impulso del talento digital para fortalecer la confianza digital en el país.
d) **Promoción de una Cultura de Seguridad Digital:** Comprende campañas de difusión y comunicación de contenidos sobre seguridad digital, así como, de las actividades del propio CNSD.
e) **Colaboración y Cooperación:** Comprende el establecimiento de relaciones bilaterales o multilaterales de cooperación con los CSIRT, SOC, CERT y otros actores de similar naturaleza, tanto a nivel nacional como internacional, con el propósito de fortalecer la confianza y transformación digital, así como, la articulación y coordinación con las entidades públicas para el eficiente y oportuno desarrollo de las actividades y líneas de acción del CNSD. Asimismo, cuando corresponda, brindar asistencia en el desarrollo de políticas en materia de gestión de riesgos y gestión de incidentes de seguridad digital.

Artículo 23. Procesos Operativos del Centro Nacional de Seguridad Digital

El CNSD conforme a sus líneas de acción, tiene los siguientes procesos operativos:

a) **Gestión de Incidentes de Seguridad Digital**: Está a cargo del CSIRT Nacional. Comprende las actividades de planificación, preparación, identificación, análisis, contención e investigación de los incidentes de seguridad digital, para su prevención oportuna y resolución efectiva. Asimismo, comprende las actividades de identificación, análisis y comunicación de alertas sobre incidentes de seguridad digital, producidos en el ámbito nacional e internacional, así como, de apoyo, coordinación y articulación con otros equipos de similar naturaleza en el ámbito nacional e internacional, para atender los incidentes de seguridad digital, ciberseguridad y seguridad de la información.
b) **Gestión del Sistema de Gestión de Seguridad de la Información:** Comprende las actividades de asistencia en los procesos de actualización, mantenimiento de los controles y análisis de riesgos de seguridad digital, para la implementación, operación y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI), para preservar la seguridad y fortalecer la confianza y transformación digital; en cumplimiento del Marco de Seguridad Digital del Estado Peruano.
c) **Gestión de Monitoreo**: Comprende actividades de prevención, monitoreo y control de la seguridad en las redes y en Internet. Adicionalmente, incluye la ciber resiliencia de los sistemas en las entidades públicas y actúa de forma preventiva utilizando diversas herramientas de monitoreo, seguimiento y análisis para proteger la información y los sistemas.
d) **Gestión de Servicios e Infraestructura**: Comprende las actividades de planificación, implementación y mantenimiento de los recursos, sistemas**,** plataformas y entorno digital, con la finalidad de asegurar la disponibilidad y continuidad de los procesos del CNSD.

Artículo 24. Plataforma Nacional de Talento Digital

Se crea la Plataforma Nacional de Talento Digital, a cargo de la SSTSD, que permite el acceso a cursos, programas, talleres y otras modalidades formativas para crear capacidades en confianza digital, con la finalidad de desarrollar competencias, concientización y talento en dicha materia. La SGTD-PCM emite los lineamientos para regularla.

Artículo 25. Alertas, Comunicados y Campañas de Difusión de Seguridad Digital

25.1 Como parte de la gestión de los incidentes de seguridad digital, la SGTD-PCM, en coordinación con las entidades responsables de los ámbitos del Marco de Seguridad Digital, emite alertas integradas y comunicados de seguridad digital en el ámbito nacional, las que son gestionadas por la SSTSD.

25.2 Las alertas integradas de seguridad digital comprenden información de naturaleza técnica sobre riesgos en el entorno digital, están dirigidas a las áreas técnicas de las entidades públicas, organizaciones del sector privado y a la ciudadanía interesada, con fines de prevención de suplantación de identidad, estafas o diferentes delitos informáticos, vulnerabilidades recientemente identificadas, nuevos vectores de ciberataques y/o cualquier otro riesgo asociado a la ciberdelincuencia. Son publicadas en la Plataforma Digital Única del Estado Peruano para Orientación al Ciudadano (Plataforma GOB.PE).

25.3 Los comunicados de seguridad digital comprenden información sobre vulnerabilidades, ataques o medidas que se han realizado para mitigar un riesgo de seguridad digital, están dirigidos a la ciudadanía en general en un lenguaje sencillo y comprensible, y son publicados en la Plataforma GOB.PE, y en otros canales digitales que determine la SGTD-PCM. Dicha información se brinda guardando un razonable equilibrio y ponderación, a fin de no perjudicar o poner en riesgo de un modo irrazonable y desproporcionado la confidencialidad, reputación u operaciones de los PSD que lo comunican.

25.4 Asimismo, la SGTD-PCM, coordina con el MINJUSDH, INDECOPI, el Ministerio del Interior (MININTER), la PNP, el MPFN, el Poder Judicial (PJ) y demás entidades competentes, el diseño de las acciones de sensibilización y capacitación dirigidos a la ciudadanía. Las acciones de sensibilización y capacitación son programadas y ejecutadas de acuerdo a la planificación realizada por cada entidad en el marco de sus competencias.

25.5. Estas acciones de sensibilización y capacitación tienen por finalidad prevenir amenazas en el entorno digital que afecten la seguridad y bienestar de las personas a nivel nacional. Las campañas o iniciativas referidas a la materia de confianza digital, que realicen las entidades públicas en mérito a competencias relacionadas con dicha materia deben ser coordinadas previamente con la SGTD-PCM, a través del CNSD, según corresponda, a fin de articular esfuerzos y optimizar el uso de recursos públicos.

Artículo 26. Redes de confianza digital

26.1 Las redes de confianza digital son el conjunto de organizaciones conformadas por entidades públicas, organizaciones privadas, la academia, sociedad civil, nacionales o internacionales o una combinación de éstas, en función de un territorio, negocio, sector o para atender un objetivo específico, previa suscripción de un acuerdo u otro documento de similar naturaleza.

26.2 Las redes de confianza digital articulan acciones para el intercambio y procesamiento de información y conocimiento sobre incidentes, riesgos, medidas

de mitigación, herramientas, mejores prácticas o similares en materia de seguridad digital.

26.3 Las entidades de la administración pública coordinan en el ámbito de sus competencias con la SGTD-PCM, la cual lidera y articula las redes de confianza digital a nivel nacional y participa a nivel internacional en su calidad de único punto de contacto en las comunicaciones y coordinaciones con otros organismos, centros o equipos de similar naturaleza.

26.4 La SGTD-PCM, a través del CNSD, establece una red de confianza digital con los operadores de actividades críticas y funciones críticas a nivel nacional para la gestión de sus riesgos e incidentes de seguridad digital, previa suscripción de un acuerdo u otro documento de similar naturaleza.

CAPÍTULO V
INCIDENTES DE SEGURIDAD DIGITAL

Artículo 27. Equipo de Respuesta a Incidentes de Seguridad Digital Nacional

27.1 El CSIRT nacional es el componente del CNSD responsable de prevenir, detectar, manejar, analizar, recopilar información y desarrollar soluciones estratégicas para gestionar, contener, articular y atender los incidentes de seguridad digital en el ámbito nacional.

27.2 Asimismo, el CSIRT nacional es responsable de la coordinación para la gestión y articulación de respuesta a incidentes de seguridad digital, así como de la cooperación y colaboración ante la ocurrencia de incidentes de seguridad digital a nivel internacional.

Artículo 28. Responsabilidades del CSIRT Nacional

El CSIRT Nacional tiene las siguientes funciones:

a) Gestionar la contención, respuesta y recuperación ante incidentes de seguridad digital de las entidades públicas y, cuando resulte aplicable, de las organizaciones del sector privado en el ámbito nacional.
b) Coordinar y articular acciones con otros equipos nacionales e internacionales de similar naturaleza, para atender los incidentes de seguridad digital y, en el caso de las organizaciones del sector privado, cuando estos lo soliciten y conforme a sus capacidades.
c) Brindar soporte y asesoramiento a las entidades públicas en acciones relacionadas con la gestión de incidentes y riesgos de seguridad digital.
d) Otras establecidas por la SGTD-PCM o regulación específica.

Artículo 29. Registro Nacional de Incidentes de Seguridad Digital

29.1 El Registro Nacional de Incidentes de Seguridad Digital es un registro informativo que tiene por objetivo recibir, consolidar y centralizar los datos e información sobre los incidentes de seguridad digital a nivel nacional, notificados por las entidades públicas, que puedan servir para la generación de datos que sirvan de evidencia, o insumo para su análisis, investigación y solución de incidentes de seguridad digital. Asimismo, registra las alertas de los incidentes de seguridad digital que afectan la seguridad nacional.

29.2 Las organizaciones del sector privado que presten servicio en entorno digital, y no estén comprendidas en el artículo 9 del DU 007-2020, pueden notificar los

incidentes de seguridad digital al Registro Nacional de Incidencias de Seguridad Digital, sin perjuicio de cumplir con las normas legales vigentes.

29.3 El CNSD implementa medidas y controles de seguridad sobre la información recibida y registrada en el Registro Nacional de Incidentes de Seguridad Digital, con especial énfasis en aquella considerada restringida o de divulgación limitada, que ponga en riesgo la confidencialidad, reputación u operaciones de la entidad pública u organización del sector privado que la comunica.

29.4 El CNSD implementa reglas de cifrado, protocolos y medidas de control para compartir información sobre incidentes y riesgos de seguridad digital, medidas de mitigación, eventos, mejores prácticas o notificaciones urgentes recibidas con los responsables de los ámbitos del Marco de Seguridad Digital, debiendo observar para tal efecto, la normativa vigente en materia de protección de datos personales, transparencia y acceso a la información pública.

Artículo 30. Protocolos para la Notificación de Incidentes de Seguridad Digital

30.1 Los protocolos para la notificación de incidentes de seguridad digital permiten establecer controles o medidas para que la información comunicada sea compartida solo con la red de confianza establecida. Dichos protocolos deben ser legibles para seres humanos y adecuados para su uso mediante plataformas digitales o aplicaciones informáticas que automaticen el intercambio de información.

30.2 Asimismo, los protocolos para la notificación de incidentes de seguridad digital a través de reuniones, comprenden reglas que permiten utilizar la información compartida sin vulnerar la confidencialidad en dichas reuniones en las que participan las entidades públicas previa suscripción de un acuerdo de confidencialidad.

30.3 La SSTSD evalúa y habilita el protocolo para escalar los incidentes de seguridad digital del ámbito nacional para cooperación y apoyo internacional, cuando corresponda, articulando con las autoridades competentes.

30.4 En el caso de incidentes de seguridad digital que comprometen la seguridad nacional, se ejecuta el protocolo de escalamiento, coordinación, intercambio y activación, mediante el cual la SGTD-PCM, a través del CNSD, interactúa de manera directa e inmediata con el Comando Conjunto de las Fuerzas Armadas, de conformidad con lo dispuesto en el artículo 13 de la Ley N° 30999, Ley de Ciberdefensa.

30.5. La SGTD-PCM 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.

Artículo 31. Canales Oficiales para la Notificación de Incidentes de Seguridad Digital

31.1 Los canales oficiales para la notificación de incidentes de seguridad digital al CNSD, por parte de los PSD son los siguientes:

a) Plataforma digital que automatiza el registro de incidentes de seguridad digital e intercambio de información, previo registro del Oficial de Seguridad y Confianza Digital y asignación de usuario, siendo este el canal de notificación recomendado.

b) Correo electrónico, la comunicación debe estar cifrada.
c) Comunicaciones por teléfono, previa identificación, siguiendo los protocolos que se emitan para tal efecto.
d) Otros canales que determine la SGTD-PCM, publicados a través de la sede digital de la PCM en la Plataforma GOB.PE.

31.2 La información a notificar al CNSD comprende, como mínimo: descripción del incidente, clasificación e impacto. Adicionalmente, notifican información sobre el tipo de dato afectado, las medidas o respuestas inmediatas adoptadas, indicadores de compromiso o detalles operativos, estén o no relacionados directamente con el incidente de seguridad digital; así como, otras que defina la SGTD-PCM, mediante Resolución de Secretaría de Gobierno y Transformación Digital.

31.3 Cuando la SSTSD tome conocimiento de un incidente de seguridad digital que involucre una posible afectación a los datos personales, comunica el mismo a la ANPDP, para que actúe conforme a sus atribuciones y competencias, y en el marco de los protocolos determinados para tal fin.

Artículo 32. Plazos para la Notificación de Incidentes de Seguridad Digital

32.1 Los incidentes de seguridad digital clasificados con nivel crítico son notificados al CNSD, de manera obligatoria, dentro de un plazo máximo de cuarenta y ocho (48) horas, contado desde que el PSD toma conocimiento del incidente.

32.2 Los incidentes de seguridad digital con una clasificación diferente al nivel crítico son notificados en los plazos establecidos por la SGTD-PCM en la Clasificación de los Incidentes de Seguridad Digital.

Artículo 33. Clasificación de los Incidentes de Seguridad Digital

33.1 Comprende la clasificación de los tipos de incidentes de seguridad digital y la determinación de su nivel de peligrosidad previo análisis de riesgos, siendo su aplicación obligatoria para la notificación del incidente al CNSD.

33.2 Las entidades públicas clasifican sus incidentes de seguridad digital conforme a la Clasificación de los Incidentes de Seguridad Digital.

33.3 Los PSD que sean organizaciones del sector privado pueden tomar como referencia la Clasificación de Incidentes de Seguridad Digital publicada por la SGTD-PCM.

Artículo 34. Notificación de incidentes de seguridad digital

34.1 Los incidentes de seguridad digital son notificados al CNSD y se incorporan en el Registro Nacional de Incidentes de Seguridad Digital, mediante los protocolos, canales, plazos y clasificación establecidos para la notificación, de conformidad con lo señalado en los artículos 29, 30, 31, 32 y 33 del presente Reglamento.

34.2 El CNSD, a través de la SSTSD, comparte con la red de confianza digital, información relevante sobre los incidentes de seguridad digital; dicha información es compartida en función del territorio, tipo de negocio, sector u objetivo específico, y conforme los canales de notificación, protocolos y plazos definidos conforme el presente Reglamento, garantizando la confidencialidad, integridad y disponibilidad de la información.

34.3 El CNSD comparte, a través de la SSTSD, la información de los incidentes de seguridad digital con las entidades de la administración pública, considerando para ello la naturaleza del incidente, y las funciones y ámbito de competencias de la entidad o las entidades, cumpliendo los protocolos que se emitan para dicho fin, y garantizando la confidencialidad, integridad y disponibilidad de la información.

34.4 Los PSD establecen los lineamientos a fin de que los terceros que les brinden servicios cumplan con comunicarles los incidentes de seguridad digital que se encuentren bajo su dominio y responsabilidad, siendo los PSD los encargados de notificar el incidente de seguridad digital al CNSD.

Artículo 35. Gestión de Incidentes de Seguridad Digital

35.1 El CNSD brinda asistencia técnica a las entidades públicas, de acuerdo a las condiciones técnicas y tecnológicas disponibles, con el propósito de prevenir, contener y mitigar los incidentes de seguridad digital, así como, mejorar, preservar y restaurar la disponibilidad de los servicios, plataformas digitales o sistemas de información afectados.

35.2 Los informes o reportes sobre la atención de incidentes de seguridad digital son resguardados y archivados por el CNSD. El CNSD, a través de la SSTSD, es el encargado de informar semestralmente a la SGTD-PCM, las acciones realizadas en el marco de la gestión de incidentes de seguridad digital.

35.3 Los PSD vinculados con la prestación de los servicios señalados en el artículo 9 del DU 007-2020 colaboran con el CNSD de forma célere y oportuna para que, en la medida de sus capacidades técnicas, puedan apoyar en la gestión de los incidentes de seguridad digital que afecten a los servicios prestados.

35.4 Las entidades del sector financiero tienen habilitado un canal digital en la Plataforma GOB.PE, para publicar información en un lenguaje claro y sencillo, de todo incidente que deba ser comunicado a los ciudadanos. La publicación realizada en la Plataforma GOB.PE, no limita o restringe las publicaciones que realicen las entidades del sector financiero en sus canales.

Artículo 36. Reportes de Incidentes de Seguridad Digital por la Ciudadanía

36.1 Cualquier persona que tome conocimiento vinculado a incidentes de seguridad digital puede reportarlo al CNSD, previa validación de su identidad, a través de los canales establecidos por SGTD-PCM, publicado a través de la sede digital de la Presidencia del Consejo de Ministros en la Plataforma GOB.PE.

36.2 Los referidos incidentes son ingresados en el Registro Nacional de Incidentes de Seguridad Digital el cual es desarrollado y administrado por la SGTD-PCM.

TÍTULO III

MEDIDAS PARA FORTALECER LA CONFIANZA DIGITAL

CAPÍTULO I

INSTRUMENTOS PARA LA CONFIANZA

Artículo 37. Confianza Digital de Nombres de Dominio

37.1 La SGTD-PCM, a través del CNSD, articula acciones y medidas con la organización a cargo de la administración del registro del código de país (ccTLD).pe, para fortalecer la confianza digital en los servicios públicos y mitigar riesgos de seguridad digital que afecten los nombres de dominio asignados a entidades de la administración pública.

37.2 Las entidades públicas y empresas del Estado comprendidas en el alcance del presente Reglamento deben registrar, únicamente, nombres de dominio de tercer nivel "*.gob.pe", "*.edu.pe", "*.mil.pe" y "*.com.pe", según corresponda. Los nombres de dominio definidos por las entidades públicas son validados por la SGTD-PCM, siguiendo las reglas de nomenclatura (tipología) y procedimientos emitidos para tales efectos.

37.3 Las entidades públicas implementan obligatoriamente protocolos de seguridad que permitan cifrar el tráfico de datos entre los usuarios y el servidor web.

37.4 La SGTD-PCM emite los lineamientos para la asignación de nombres de dominio a las entidades de la administración pública.

Artículo 38.- Sellos de confianza digital

38.1 Los sellos de confianza digital se constituyen en el reconocimiento a las buenas prácticas que miden los niveles de confiabilidad de un servicio digital prestado por una entidad pública. Se consideran como criterios, el cumplimiento de los requisitos establecidos en la normativa vigente, los estándares tecnológicos y de seguridad digital implementados y los mecanismos de mitigación y respuesta ante contingencias.

38.2 La SGTD-PCM promueve y establece los criterios para la participación, selección y reconocimiento de las entidades públicas a través del sello de confianza digital.

CAPÍTULO II

USO ÉTICO DE LAS TECNOLOGÍAS DIGITALES Y DE LOS DATOS

Artículo 39. Uso Ético de las Tecnologías Digitales y de los Datos

39.1 Se promueve la ética en todas las fases de diseño, desarrollo, implementación y uso de las tecnologías digitales; así como, el uso responsable de los datos, a fin de contribuir el bienestar de la ciudadanía, generar valor público, garantizar el progreso científico y tecnológico centrado en la persona y en la transparencia; y, asegurar el respeto de los derechos fundamentales, previstos en la Constitución Política del Perú y en los tratados internacionales sobre derechos humanos.

39.2 Los PSD promueven y gestionan el uso ético y responsable de los datos y tecnologías digitales, incluyendo las tecnologías emergentes. Para tal efecto, los PSD actúan respetando lo siguiente:

a) Sus acciones se encuentran al servicio de las personas y del medio ambiente, a fin de impulsar el crecimiento inclusivo, el desarrollo sostenible, y el bienestar económico y social.
b) Diseñan e implementan sus acciones observando el marco normativo vigente.
c) Se rigen por la transparencia, privacidad y seguridad de los datos.
d) Garantizan la calidad e integridad de los datos que contribuyan a la creación de valor público en la sociedad, en el marco de la normativa vigente.

e) Funcionan con robustez, de manera fiable y segura durante todo su ciclo de vida, evaluando los potenciales riesgos en la protección de datos, a fin de gestionarlos adecuadamente.
f) Fomentan el uso de los datos abiertos y tecnologías digitales en sectores de interés público como educación, salud, transporte, entre otros; asimismo, coadyuvan a que los datos y tecnologías puedan ser comprendidos por los ciudadanos, a fin de generar un entorno confiable.
g) Incluyen acciones para prevenir situaciones de discriminación, exclusión, prejuicios, desigualdades y brechas, así como, permiten responder ante situaciones de vulneración a los derechos humanos.
h) Aseguran la privacidad desde el diseño y, por defecto, desde las primeras etapas de su diseño y a lo largo de todos sus procesos involucrados.

39.3 La protección de la privacidad es un elemento que se incorpora en cada acción y medida implementada por los PSD, siendo de obligatorio cumplimiento la normativa vigente en materia de protección de datos personales.

Artículo 40. Transparencia en los Algoritmos de los Servicios Digitales

40.1 Las entidades públicas evalúan los algoritmos implementados en sus servicios digitales, asegurando la privacidad, el uso ético y el respeto a los derechos humanos. Asimismo, verifican si los algoritmos gestionan adecuadamente los atributos de identidad digital obtenidos y si estos son destinados únicamente para los fines para los cuales fueron consentidos.

40.2 Las entidades públicas deben implementar un canal que permita informar a las personas naturales cuando existan decisiones automatizadas basadas en algoritmos o cuando se afecte su seguridad o sus derechos y libertades, así también, en caso se vean afectados por alguna decisión, el mecanismo a seguir a fin de que esta pueda ser corregida, siempre que no existan restricciones legales. La SGTD-PCM y la ANPDP, según corresponda, establecen lineamientos a tener en cuenta para el cumplimiento de esta medida.

40.3 Las organizaciones del sector privado pueden promover la transparencia en los algoritmos de los servicios digitales siguiendo las disposiciones establecidas en los numerales 40.1 y 40.2 del presente artículo, cuando les genere valor o les resulte aplicable conforme a Ley.

Artículo 41. Criterios para la Calidad de los Datos

41.1 La calidad de los datos implica determinadas características, tales como, completitud, conformidad, consistencia, no duplicidad, integridad y precisión, las cuales son necesarias para satisfacer las necesidades de digitalización, toma de decisiones, apertura de datos, transparencia y despliegue de la transformación y confianza digital de la sociedad.

41.2 Los PSD, sean entidades públicas u organizaciones del sector privado que forman parte del SNTD, promueven la calidad de los datos teniendo en cuenta los siguientes criterios:
a) Completitud: contienen toda la información que se requiere de ellos.
b) Conformidad: cuentan con el formato esperado y asociado con ellos.
c) Consistencia: no son contradictorios con otras versiones de sí mismos o en combinación con otros datos.
d) No duplicidad: no se ha duplicado su almacenamiento en un mismo contexto.

e) Integridad: los datos no han sido alterados de forma incongruente, inválida o que lleve al repudio, o a incumplir el criterio de consistencia y normas de propiedad intelectual o licencias.
f) Precisión o exactitud: los datos contienen los detalles precisos y exactos sobre la realidad que representan.

41.3 La SGTD-PCM coordina con las entidades públicas la publicación de datos de valor estratégico para el desarrollo de una economía basada en datos, aplicando la regulación vigente en datos abiertos, datos personales, seguridad digital y transformación digital.

Artículo 42. Gestión del Centro Nacional de Datos
El Centro Nacional de Datos es una plataforma digital gestionada por la SSTSD, en el marco de lo establecido en el artículo 13 del DU 007-2020, y comprende, de manera no limitativa, las capacidades de almacenamiento para el procesamiento, analítica, ciencia de datos y análisis de datos e información para el aprovechamiento de los datos para la toma decisiones en base a evidencias, previo establecimiento de condiciones, criterios y procedimientos aprobados por SGTD-PCM mediante Resolución de Secretaría de Gobierno y Transformación Digital.

DISPOSICIONES COMPLEMENTARIAS FINALES

PRIMERA. Normas Complementarias
La SGTD-PCM, mediante Resolución de Secretaría de Gobierno y Transformación Digital, dicta los protocolos, normas y lineamientos complementarios para la implementación del presente Reglamento.

SEGUNDA. Aprobación de Lineamientos y Protocolos propuestos por otras Entidades de la Administración Pública
Las entidades de la administración pública aprueban lineamientos y protocolos para el cumplimiento de lo dispuesto en el presente Reglamento en las materias de su competencia, siempre que sean concordantes con lo establecido en el presente Reglamento, los lineamientos y disposiciones complementarias vigentes, con la opinión previa favorable de la SGTD-PCM.

TERCERA. Aprobación de los Lineamientos para la Gestión del Centro Nacional de Datos
La SGTD-PCM, en coordinación con la ANPDP y la ANTAIP, según corresponda, aprueba mediante Resolución de Secretaría de Gobierno y Transformación Digital, los protocolos y mecanismos a través de los lineamientos y las directivas correspondientes.

CUARTA. Plan Anual de Operaciones del Centro Nacional de Seguridad Digital
El Plan Anual de Operaciones del Centro Nacional de Seguridad Digital es desarrollado por la SGTD-PCM, el cual contiene los objetivos, principales actividades, ejercicios coordinados, responsables, interesados, plazos y recursos a utilizar en el desarrollo de sus acciones. El primer Plan es desarrollado en un plazo no mayor a ciento veinte (120) días hábiles, contados a partir de la entrada en vigencia del presente Reglamento. Asimismo, los planes anuales posteriores serán presentados con una posterioridad de quince (15) días hábiles al año inicio del año correspondiente.

QUINTA. Estrategia Nacional de Confianza Digital
La SGTD-PCM, mediante Resolución de Secretaría de Gobierno y Transformación Digital, aprueba la Estrategia Nacional de Confianza Digital, que desarrolla los objetivos,

acciones estratégicas y ejes para fortalecer la confianza digital a nivel nacional; asimismo, establece la gobernanza para su implementación.

SEXTA. Clasificación Nacional de Incidentes de Seguridad Digital
La SGTD-PCM, mediante Resolución de Secretaría de Gobierno y Transformación Digital, aprueba la Clasificación Nacional de Incidentes de Seguridad Digital, en un plazo no mayor a ciento veinte (120) días hábiles, contados a partir de la entrada en vigencia del presente Reglamento.

SÉTIMA. Protocolos, canales y plazos para la Notificación de Incidentes de Seguridad Digital
La SGTD-PCM, mediante Resolución de Secretaría de Gobierno y Transformación Digital, aprueba o actualiza los protocolos y canales y establece plazos para la notificación de incidentes de seguridad digital, en un plazo no mayor a noventa (90) días hábiles, contados a partir de la entrada en vigencia del presente Reglamento.

OCTAVA. Informe sobre la situación de la Seguridad y Confianza Digital en el País
La SGTD-PCM presenta al Comité de Alto Nivel por un Perú Digital, Innovador y Competitivo informes con una periodicidad anual sobre la situación de la seguridad y confianza digital en el país.

NOVENA. Recursos Críticos de Internet
Las entidades de la administración pública y del sector privado, que gestionan recursos críticos de Internet (nombres de dominio, dirección IP), por su calidad de entidades vinculadas a la confianza digital, notifican los incidentes de seguridad digital al CNSD, conforme a lo dispuesto en el DU 007-2020 y el presente Reglamento.

FIRMA DIGITAL
PCM
PRESIDENCIA DEL CONSEJO DE MINISTROS

Firmado digitalmente por VILCHEZ INGA Cesar FAU 20168999926 soft
Motivo: Doy V° B°
Fecha: 31.03.2025 18:05:39 -05:00