PODER EJECUTIVO

PRESIDENCIA DEL CONSEJO DE MINISTROS

Decreto Supremo que aprueba el Reglamento del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo

DECRETO SUPREMO
Nº 029-2021-PCM

EL PRESIDENTE DE LA REPÚBLICA

CONSIDERANDO:

Que, a través del Decreto de Urgencia Nº 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital, se crea el referido sistema como un Sistema Funcional del Poder Ejecutivo, conformado por un conjunto de principios, normas, procedimientos, técnicas e instrumentos mediante los cuales se organizan las actividades de la administración pública y se promueven las actividades de las empresas, la sociedad civil y la academia orientadas a alcanzar los objetivos del país en materia de transformación digital;

Que, el Decreto de Urgencia Nº 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento, 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;

Que, el Decreto Legislativo Nº 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, establece el marco de gobernanza del gobierno digital para la adecuada gestión de la identidad digital, servicios digitales, arquitectura digital, interoperabilidad, seguridad digital y datos, 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, conforme a lo dispuesto en el artículo 8 del Decreto Legislativo Nº 1412, la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, es el ente rector en materia de gobierno digital, el cual comprende tecnologías digitales, identidad digital, interoperabilidad, servicio digital, datos, seguridad digital y arquitectura digital; dictando para tal efecto las normas y procedimientos en dicha materia;

Que, asimismo, la Primera Disposición Complementaria Final del referido Decreto Legislativo dispone que la Presidencia del Consejo de Ministros, mediante Decreto Supremo, aprueba el Reglamento de la Ley de Gobierno Digital;

Que, el artículo 47 del Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros, aprobado mediante Decreto Supremo Nº 022-2017-PCM, establece que la Secretaría de Gobierno Digital es el órgano de línea, con autoridad técnico normativa a nivel nacional, responsable de formular y proponer políticas nacionales y sectoriales, planes nacionales, normas, lineamientos y estrategias en materia de Informática y de Gobierno Electrónico;

Que, mediante Decreto Supremo Nº 004-2019-JUS se aprobó el Texto Único Ordenado de la Ley Nº 27444, Ley del Procedimiento Administrativo General, a través del cual se establecen las normas comunes para las actuaciones de la función administrativa del Estado y se regula los procedimientos administrativos desarrollados en las entidades, incluyendo el procedimiento administrativo electrónico y el uso de la casilla única electrónica;

Que, asimismo, los numerales 20.4 del artículo 20 y 30.4 del artículo 30 del Texto Único Ordenado de la Ley Nº 27444 disponen que mediante Decreto Supremo refrendado por la Presidencia del Consejo de Ministros, se aprueban los criterios, condiciones, mecanismos y plazos para la implementación de la casilla única electrónica, y los lineamientos para establecer las condiciones y uso de las tecnologías y medios electrónicos en los procedimientos administrativos, junto a sus requisitos, respectivamente;

De conformidad con el inciso 8) del artículo 118 de la Constitución Política del Perú, la Ley Nº 29158, Ley Orgánica del Poder Ejecutivo, el Decreto Legislativo Nº 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y el Decreto Supremo Nº 004-2019-JUS, que aprueba el Texto Único Ordenado de la Ley Nº 27444, Ley del Procedimiento Administrativo General;

DECRETA:

Artículo 1. Aprobación
Apruébase el Reglamento del Decreto Legislativo Nº 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo, el mismo que consta de ocho (08) Títulos, veintiún (21) Capítulos, ciento veintiún (121) Artículos, cincuenta y dos (52) Disposiciones Complementarias Finales, cuatro (04) Disposiciones Complementarias Transitorias, seis (06) Disposiciones Complementarias Modificatorias, una (01) Disposición Complementaria Derogatoria y un (01) Anexo, el mismo que forma parte integrante del presente Decreto Supremo.

Artículo 2. Publicación
Publícase el presente Decreto Supremo y el Reglamento, aprobado mediante el artículo precedente, en la Plataforma Digital Única para Orientación al Ciudadano (www.gob.pe), y en los portales institucionales de los ministerios cuyos titulares lo refrendan, el mismo día de su publicación en el Diario Oficial El Peruano.

Artículo 3. Financiamiento
La implementación de lo establecido en el presente Decreto Supremo se financia con cargo al presupuesto institucional de las entidades involucradas, sin demandar recursos adicionales al Tesoro Público.

Artículo 4. Refrendo
El presente Decreto Supremo es refrendado por la Presidenta del Consejo de Ministros, el Ministro de Economía y Finanzas, el Ministro de Justicia y Derechos Humanos, el Ministro del Interior, la Ministra de Defensa y el Ministro de Cultura.

Dado en la Casa de Gobierno, en Lima, a los dieciocho días del mes de febrero del año dos mil veintiuno.

FRANCISCO RAFAEL SAGASTI HOCHHAUSLER
Presidente de la República

VIOLETA BERMÚDEZ VALDIVIA
Presidenta del Consejo de Ministros

WALDO MENDOZA BELLIDO
Ministro de Economía y Finanzas

EDUARDO VEGA LUNA
Ministro de Justicia y Derechos Humanos

JOSÉ MANUEL ANTONIO ELICE NAVARRO
Ministro del Interior

NURIA ESPARCH FERNÁNDEZ
Ministra de Defensa

ALEJANDRO ARTURO NEYRA SÁNCHEZ
Ministro de Cultura

REGLAMENTO DEL DECRETO LEGISLATIVO Nº 1412, DECRETO LEGISLATIVO QUE APRUEBA LA LEY DE GOBIERNO DIGITAL, Y ESTABLECE DISPOSICIONES SOBRE LAS CONDICIONES, REQUISITOS Y USO DE LAS TECNOLOGÍAS Y MEDIOS ELECTRÓNICOS EN EL PROCEDIMIENTO ADMINISTRATIVO

TÍTULO I
DISPOSICIONES GENERALES

Artículo 1. Objeto

El presente Reglamento tiene por objeto:

1.1 Regular las actividades de gobernanza y gestión de las tecnologías digitales en las entidades de la Administración Pública en materia de Gobierno Digital, que comprende la identidad digital, interoperabilidad, servicios digitales, datos, seguridad digital y arquitectura digital, así como establecer el marco jurídico aplicable al uso transversal de tecnologías digitales en la digitalización de procesos y prestación de servicios digitales en los tres niveles de gobierno, conforme lo señalado en el Decreto Legislativo Nº 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital (en adelante la Ley), con observancia de los deberes y derechos fundamentales previstos en la Constitución Política del Perú y en los tratados internacionales de derechos humanos y otros tratados internacionales ratificados por el Perú; y,

1.2 Establecer las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo, y los criterios, condiciones, mecanismos y plazos de implementación de la casilla única electrónica, conforme lo establecido en los numerales 20.4 del artículo 20 y 30.4 del artículo 30 del Texto Único Ordenado de la Ley Nº 27444, Ley del Procedimiento Administrativo General, aprobado mediante Decreto Supremo Nº 004-2019-JUS (en adelante el TUO de la Ley Nº 27444).

Artículo 2. Ente Rector

2.1 La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, ejerce la rectoría del Sistema Nacional de Transformación Digital en el país y en las materias de Gobierno, Confianza y Transformación Digital, siendo la autoridad técnico-normativa a nivel nacional en dichas materias. Asimismo, es el Líder Nacional de Gobierno Digital responsable del proceso de transformación digital en el país y dirección estratégica del Gobierno Digital en el Estado Peruano, conforme a lo dispuesto en el artículo 8 del Decreto Supremo Nº 033-2018-PCM, Decreto Supremo que crea la Plataforma Digital Única del Estado Peruano y establecen disposiciones adicionales para el desarrollo del Gobierno Digital, para lo cual en el ejercicio de sus funciones articula acciones con las entidades de la Administración Pública, la sociedad civil, los ciudadanos la academia y el sector privado.

2.2 La materia de Gobierno Digital comprende los ámbitos de tecnologías digitales, identidad digital, interoperabilidad, servicios digitales, datos, seguridad digital y arquitectura digital, los cuales se relacionan entre sí con la finalidad de mejorar la prestación de servicios centrados en los ciudadanos, la gestión interna de las entidades de la Administración Pública y la relación entre éstas en la prestación interadministrativa de servicios públicos de manera segura para fortalecer la confianza y satisfacer las necesidades de los ciudadanos y personas en general en el entorno digital, orientado a la transformación digital del Estado.

Artículo 3. Gobernanza digital

3.1 La gobernanza digital es el conjunto de roles, estructuras, procesos, herramientas y normas para articular, dirigir, evaluar y supervisar el uso y adopción de las tecnologías digitales y datos en el Estado Peruano y el proceso de transformación digital en el país, de conformidad con el artículo 3 de la Ley. El gobierno digital es el uso estratégico de las tecnologías digitales y datos en la Administración Pública para la creación de valor público, de conformidad con lo establecido en el artículo 6 de la Ley.

3.2 La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, es la entidad responsable de ejercer la gobernanza digital del uso transversal y adopción estratégica de las tecnologías digitales y datos en el Estado Peruano, del proceso de transformación digital en el país, y de los marcos de identidad digital, interoperabilidad, servicios digitales, datos, gobernanza, gestión y reestructuración de modelos de datos, seguridad digital y arquitectura digital del Estado Peruano. Asimismo, emite las normas, lineamientos, especificaciones, guías, directivas y estándares para su aplicación por parte de las entidades de la Administración Pública.

3.3 La Secretaría de Gobierno Digital establece los mecanismos de articulación de la gobernanza digital con las entidades de la Administración Pública, los ciudadanos, la sociedad civil, la academia y el sector privado, desde un enfoque multidisciplinario, sistémico, holístico e integral en base a los desafíos de una sociedad digital, con pleno respeto de los derechos de los ciudadanos y personas en el entorno digital.

Artículo 4. Mecanismos de articulación de la Gobernanza Digital

4.1 El Comité de Alto Nivel por un Perú Digital, Innovador y Competitivo, en el marco de la Ley, es el mecanismo de articulación multisectorial para la promoción de acciones relacionadas con el desarrollo del gobierno digital y la integración de la sociedad civil, el sector privado, la academia y los ciudadanos en una sociedad digital.

4.2 El Comité de Gobierno Digital es el mecanismo de gobernanza a nivel institucional en las entidades públicas y su actuar se rige de conformidad con lo establecido en el Decreto de Urgencia Nº 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital y sus normas reglamentarias. El Comité de Gobierno Digital coordina y remite el portafolio de proyectos definido en el Plan de Gobierno Digital a la Comisión de Planeamiento Estratégico de la entidad o la que haga sus veces, para su evaluación, priorización e incorporación en sus instrumentos de gestión, tales como, el plan estratégico institucional, plan anual de contrataciones y plan operativo institucional.

4.3 El Laboratorio de Gobierno y Transformación Digital del Estado es el mecanismo de gobernanza e innovación abierta para co-crear, producir, innovar, prototipar y diseñar plataformas digitales, soluciones tecnológicas y servicios digitales con las entidades públicas, fomentar el desarrollo del talento digital, el uso de tecnologías emergentes, disruptivas y el impulso de una sociedad digital, de la información y el conocimiento con la colaboración de la academia, el sector privado, la sociedad civil y los ciudadanos.

Artículo 5. Opinión técnica previa de proyectos de tecnologías digitales de carácter transversal

5.1 Los titulares de las entidades de la Administración Pública solicitan opinión a la Secretaría de Gobierno Digital, sobre los proyectos de tecnologías digitales de carácter transversal en materia de interoperabilidad, seguridad digital, identidad digital, datos y gobernanza de datos, arquitectura digital, servicios digitales y tecnologías de la información aplicables a la materia de Gobierno Digital y transformación digital, identificando a las entidades involucradas en su gestión e implementación. Los proyectos definidos son incorporados en los portafolios de proyectos de los Planes de Gobierno Digital e instrumentos de gestión (PEI, POI) de las entidades responsables e involucradas. La Secretaría de Gobierno Digital incorpora dichos proyectos en la Agenda Digital Perú o documento equivalente vigente y supervisa la implementación.

5.2 La Secretaría de Gobierno Digital emite opinión técnica previa a fin de validar técnicamente si los proyectos referidos en el numeral 5.1, cumplen con lo establecido en la Ley, el Reglamento y normas complementarias,

así como con los criterios de: accesibilidad, usabilidad, estandarización y escalabilidad, cuando corresponda.

5.3 En el caso de aquellos servicios digitales provistos a través de ventanillas únicas, así como para la implementación de ventanillas únicas digitales, la Secretaría de Gobierno Digital emite opinión previa a fin de validar técnicamente si dichos servicios cumplen con lo establecido en la Ley, el Reglamento y normas complementarias, así como con los criterios de: accesibilidad, usabilidad, estandarización y escalabilidad.

5.4 La opinión técnica previa favorable de la Secretaría de Gobierno Digital a la que hace referencia los numerales 5.2 y 5.3 habilita a la entidad proponente continuar con la implementación del proyecto de tecnologías digitales correspondiente.

5.5 El plazo para la emisión de la referida opinión técnica es de quince (15) días hábiles. Este plazo se computa desde la fecha de cumplimiento en la presentación de la documentación requerida por la Secretaría de Gobierno Digital, pudiendo ser ampliado por un periodo similar dependiendo de la complejidad y alcance del proyecto. La Secretaría de Gobierno Digital emite los lineamientos que contienen los procedimientos y documentación para la emisión de la opinión técnica previa de proyectos de tecnologías digitales de carácter transversal.

5.6 La Secretaría de Gobierno Digital brinda asistencia técnica y acompañamiento a las entidades públicas en el proceso de formulación o diseño de proyectos de tecnologías digitales de carácter transversal de mediana o alta complejidad, a fin de asegurar una base de conocimiento y mejores prácticas.

Artículo 6. Opinión técnica vinculante

6.1 La Secretaría de Gobierno Digital emite opinión técnica vinculante cuando considera necesario aclarar, interpretar o integrar las normas que regulan la materia de gobierno digital.

6.2 La opinión técnica vinculante se emite en el marco de una consulta formulada por una entidad o de oficio. Se formaliza mediante un informe técnico en el cual se califica a la opinión técnica como vinculante determinando si sus efectos son generales o de alcance al caso en particular.

6.3 La opinión técnica vinculante de efectos generales adquiere carácter obligatorio para todas las entidades desde su publicación en la página institucional de la Presidencia del Consejo de Ministros.

6.4 La recurrencia de interpretaciones divergentes acerca del alcance de una determinada norma o la reiteración de consultas similares sobre esta, son criterios para que la Secretaría de Gobierno Digital considere calificar a una opinión técnica como vinculante.

Artículo 7. Opinión técnica especializada

7.1 La Secretaría de Gobierno Digital, en su calidad de autoridad técnico normativa del Sistema Nacional de Transformación Digital y en el marco de sus competencias, emite opinión técnica especializada sobre consultas vinculadas a la materia de Gobierno Digital que comprende los ámbitos de tecnologías digitales, identidad digital, interoperabilidad, servicio digital, datos y gobernanza de datos, seguridad digital y arquitectura digital, incluyendo consultas en materia de tecnologías emergentes, tecnologías disruptivas, tendencias tecnológicas, y riesgos tecnológicos existentes.

7.2 La emisión de la opinión técnica especializada se emite en el marco de una consulta formulada por una entidad. Constituye una instancia consultiva de soporte a la adopción de decisiones individuales de cada entidad en el marco de sus competencias.

Artículo 8. Gestión de las tecnologías digitales

Las unidades de organización de tecnologías de la información o las que hagan sus veces en las entidades públicas son responsables de la planificación, implementación, ejecución y supervisión del uso y adopción de las tecnologías digitales como habilitantes de la implementación de la cadena de valor, soluciones de negocio, modelos de negocio o similares priorizadas en el marco de los instrumentos de gestión de la entidad, con el propósito de permitir alcanzar sus objetivos estratégicos, crear valor público y cumplir con lo establecido por el Comité de Gobierno Digital institucional.

TÍTULO II
IDENTIDAD DIGITAL

CAPÍTULO I
MARCO DE IDENTIDAD DIGITAL DEL ESTADO PERUANO

Artículo 9. Marco de Identidad Digital del Estado Peruano

9.1 El Marco de Identidad Digital del Estado Peruano es dirigido, supervisado y evaluado por la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, en su calidad de ente rector de la identidad digital en el país, que emite lineamientos, especificaciones, guías, directivas, normas técnicas y estándares para la aplicación de la identidad digital por parte de las entidades de la Administración Pública a fin de garantizar la identificación y autenticación de los ciudadanos y personas en general cuando acceden a los servicios digitales.

9.2 El Marco de Identidad Digital del Estado Peruano y sus normas de desarrollo, son revisadas y aplicadas en la utilización, implementación, digitalización de procesos y prestación de servicios digitales brindados por las entidades de la Administración Pública a los ciudadanos y personas en general.

9.3 El Marco de Identidad Digital del Estado Peruano comprende la gestión de la identidad digital en los siguientes ámbitos:

a) Ámbito de la interacción de los peruanos con servicios digitales provistos por las entidades de la Administración Pública.
b) Ámbito de la interacción de los extranjeros con servicios digitales provistos por las entidades de la Administración Pública.

9.4 La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, amplía los ámbitos establecidos en función de la necesidad pública, cambio tecnológico, importancia estratégica o normativa expresa que lo demande; la misma que se hace efectiva mediante Decreto Supremo refrendado por la Presidencia del Consejo de Ministros.

9.5 La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, promueve el reconocimiento transfronterizo de la identidad digital de los peruanos en coordinación con las entidades nacionales competentes.

Artículo 10. Principios del Marco de Identidad Digital del Estado Peruano

La aplicación del Marco de Identidad Digital del Estado Peruano se desarrolla de acuerdo con los principios rectores establecidos en el artículo 5 de la Ley, y con los siguientes principios específicos:

a) Inclusión. Toda persona natural que tiene asignado un código único de identificación (CUI) o código único de extranjero (CUE) que necesite interactuar con las entidades de la Administración Pública tiene derecho a una identidad digital.

b) Identificador único. Toda persona natural que accede a un servicio digital provisto por una entidad de la Administración Pública utiliza su respectivo identificador único que le permite distinguirse de otros.

c) No discriminación. No se niega validez, ni efectos jurídicos, ni fuerza ejecutoria a la verificación de la identidad de una persona natural realizada a través de los servicios de autenticación establecidos en el Marco de Identidad Digital del Estado Peruano por la sola razón de que se presta en forma electrónica.

d) Equivalencia funcional de la verificación de la identidad. Cuando se requiera la verificación de la identidad de una persona natural, ese requisito se da por cumplido si se utiliza los servicios de autenticación

establecidos en el Marco de Identidad Digital del Estado Peruano.

Artículo 11. Modelo de Identidad Digital del Estado Peruano

11.1 El Modelo de Identidad Digital es la representación holística y sistémica de los componentes que comprende el Marco de Identidad Digital del Estado Peruano, atendiendo los principios establecidos en el artículo 10 del presente Reglamento y la Ley.

11.2 El Modelo de Identidad Digital del Estado Peruano comprende los siguientes componentes:

a) Principios
b) Ciudadanos digitales
c) Gestores de la identidad digital
d) Plataforma Nacional de Identificación y Autenticación de la Identidad Digital (ID GOB.PE)
e) Atributos de identidad digital
f) Proveedores de atributos de identidad complementarios
g) Credenciales de autenticación

Artículo 12. Ciudadano Digital

12.1 Los ciudadanos digitales son aquellas personas naturales que cumplen, como mínimo, con los siguientes requisitos obligatorios:

a) Tienen atributos de identidad inherentes.
b) Cuentan con una casilla única electrónica.
c) Cuentan con credenciales de autenticación emitidas, entregadas y/o habilitadas dentro del marco del presente Reglamento.

12.2 Los ciudadanos digitales tienen las siguientes obligaciones:

a) Desenvolverse en el entorno digital de acuerdo con las normas del derecho común y buenas costumbres.
b) Facilitar a las entidades públicas información oportuna, veraz, completa y adecuada, asumiendo responsabilidad sobre ello.
c) Resguardar, custodiar y utilizar sus credenciales de autenticación de manera diligente y manteniendo el control de éstas.
d) No afectar la disponibilidad de los servicios digitales, ni alterarlos, ni hacer uso no autorizado o indebido de los mismos.
e) Respetar las políticas de seguridad y privacidad de la información establecida por los servicios digitales.
f) Ejercer la responsabilidad sobre el uso de sus datos y acciones en su interacción con las entidades públicas en el entorno digital.
g) Otros que establezca la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital.

12.3 Los ciudadanos digitales tienen los siguientes derechos:

a) Derecho fundamental a la igualdad, garantizando su libre, igualitario y no discriminado acceso, con especial incidencia en las poblaciones vulnerables, en atención a lo previsto en el artículo 2 numeral 2 de la Constitución Política del Perú.
b) Derecho fundamental a la protección de los datos personales, previsto en el artículo 2 numeral 6 de la Constitución Política del Perú, y conforme a lo establecido en la Ley Nº 29733, Ley de Protección de Datos Personales y su Reglamento.
c) Derecho fundamental de acceder a la información considerando lo establecido sobre el secreto bancario y la reserva tributaria de acuerdo con lo previsto en el artículo 2 numeral 5 de la Constitución Política del Perú y el artículo 85 del Código Tributario.
d) Derecho fundamental al honor y a la buena reputación, intimidad personal y familiar, en atención a lo previsto en el artículo 2 numeral 7 de la Constitución Política del Perú.
e) Los demás derechos fundamentales previstos en la Constitución Política del Perú y en los tratados internacionales de derechos humanos ratificados por el Perú, atendiendo a cada situación en particular.
f) Derecho a relacionarse por canales digitales y haciendo uso de medios electrónicos con las entidades de la Administración pública, conforme al marco legal.
g) Derecho a elegir la modalidad de relacionarse con la Administración pública por medios tradicionales o digitales, siempre que la norma de la materia lo permita; ello sin perjuicio de que se establezca la obligatoriedad del uso de un canal digital en una disposición legal.
h) Derecho a no aportar datos ni presentar documentos que poseen las entidades públicas.

Artículo 13. Gestores de la Identidad Digital

13.1 Los Gestores de la Identidad Digital (GID) son las entidades que proveen servicios de identificación y autenticación de personas naturales en el entorno digital, y están constituidas por:

a) El Registro Nacional de Identificación y Estado Civil (RENIEC) que gestiona el otorgamiento, el registro y la acreditación de la identidad digital nacional de los peruanos.
b) La Superintendencia Nacional de Migraciones (MIGRACIONES) que gestiona el otorgamiento, el registro y la acreditación de la identidad digital de los extranjeros.

13.2 Para la gestión de la identidad digital los GID tienen las siguientes obligaciones:

a) Llevar a cabo el registro y la recopilación de los atributos inherentes de identidad digital, realizar actividades de comprobación y verificación de la identidad digital, y efectuar la vinculación de las credenciales de autenticación de la identidad digital.
b) Mantener actualizados los atributos inherentes de la identidad digital.
c) Administrar las credenciales de autenticación de la identidad digital de conformidad con las disposiciones establecidas en la Ley, su Reglamento y normas complementarias, en particular para: (i) la emisión, entrega y activación; (ii) la suspensión, revocación y reactivación; y (iii) la renovación y sustitución.
d) Autenticar a los ciudadanos digitales mediante los mecanismos de autenticación establecidos en el presente Capítulo.
e) Garantizar la disponibilidad, continuidad y el funcionamiento adecuado de sus servicios.
f) Divulgar información acerca de sus servicios de autenticación en sus canales digitales.
g) Brindar asistencia técnica a los Proveedores Públicos de Servicios Digitales para garantizar su integración con sus servicios de autenticación, en coordinación con la Secretaría de Gobierno Digital.
h) Coordinar con la Secretaría de Gobierno Digital y proporcionarle las herramientas e instrumentos para la supervisión y promoción de los servicios de autenticación de la identidad digital.
i) Publicar datos en formatos abiertos sobre el uso de los servicios de autenticación de la Plataforma ID GOB.PE en la Plataforma Nacional de Datos Abiertos.

13.3 En caso se produzca una falla de seguridad, caída del servicio o una pérdida de integridad que repercuta de manera considerable en el sistema de información de gestión de la identidad digital, en particular, en los atributos que se administran en él, los GID tienen las siguientes obligaciones:

a) Comunicar al Centro Nacional de Seguridad Digital la falla de seguridad o pérdida de integridad que se haya producido, conforme lo establecido en el artículo 107 del presente Reglamento.
b) Subsanar la falla de seguridad o la pérdida de integridad.
c) Suspender las credenciales de autenticación de la identidad digital que resulten afectadas hasta que se subsane la falla de seguridad o la pérdida de integridad.
d) Restablecer las credenciales de autenticación de la identidad digital que hayan resultado afectadas.

e) Revocar las credenciales de autenticación de la identidad digital que hayan resultado afectadas si la falla o la pérdida no puede subsanarse.

f) Atender las disposiciones del Título VII del presente Reglamento en lo que corresponda.

13.4 Para la gestión de la identidad digital en el país la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, desarrolla servicios de autenticación de la identidad digital en el marco de lo establecido en el presente Reglamento, para lo cual:

a) Hace uso de los servicios de información publicados en la Plataforma de Interoperabilidad del Estado (PIDE).

b) Es un Gestor de la Identidad Digital para la autenticación de la identidad digital de personas naturales.

Artículo 14. Plataforma Nacional de Identificación y Autenticación de la Identidad Digital

14.1 Créase la Plataforma Nacional de Identificación y Autenticación de la Identidad Digital (ID GOB.PE) como la plataforma digital que permite autenticar en línea la identidad de una persona natural que tiene asignado un CUI o CUE. La gobernanza y gestión de la Plataforma ID GOB.PE está a cargo de la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros.

14.2 La Plataforma ID GOB.PE está conformada, como mínimo, por dos (02) servicios:

a) El servicio de autenticación para peruanos gestionado por el RENIEC como Gestor de la Identidad Digital para los peruanos.

b) El servicio de autenticación para extranjeros gestionado por MIGRACIONES como Gestor de la Identidad Digital para los extranjeros.

14.3 La Plataforma ID GOB.PE proporciona el servicio de autenticación a todos los Proveedores Públicos de Servicios Digitales considerando los niveles de confianza en la autenticación definidos en el artículo 15 del presente Reglamento. Asimismo, puede ser utilizada para el ejercicio del voto electrónico no presencial en los procesos electorales organizados por la Oficina Nacional de Procesos Electorales.

14.4 Los servicios de autenticación de la Plataforma ID GOB.PE utilizan protocolos seguros, interoperables, flexibles y reconocidos por estándares internacionales.

14.5 La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, establece las condiciones de uso, protocolos de integración y gestión de indicadores de la Plataforma ID GOB.PE. Asimismo, emite las normas y disposiciones con respecto a la adopción de la Plataforma ID GOB.PE por parte de las entidades de la Administración Pública, así como también establece otros servicios de autenticación de la identidad digital.

Artículo 15. Niveles de Confianza en la Autenticación

Los niveles de confianza en la autenticación (NCA) con la Plataforma ID GOB.PE son:

a) **Nivel 1:** Provee un nivel de confianza básico respecto de la identidad de un ciudadano digital autenticado. 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 un ciudadano digital autenticado. Para este nivel se requiere el uso de dos (02) factores de autenticación diferentes entre sí.

c) **Nivel 3:** Provee un alto nivel de confianza respecto de la identidad de un ciudadano digital autenticado. 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.

Artículo 16. Eficacia jurídica y carga de la prueba

16.1 La eficacia jurídica de la autenticación realizada con la Plataforma ID GOB.PE es condicionada y proporcional al nivel de confianza empleado en la autenticación.

16.2 En caso de controversia con relación a autenticaciones realizadas con la Plataforma ID GOB.PE, con niveles 1 o 2 de confianza, la carga de la prueba recae en el correspondiente gestor de la identidad digital; sin embargo, cuando la controversia, sea por autenticaciones con nivel 3 de confianza, la carga de la prueba recae en quien la niegue. En caso de no utilizarse la Plataforma ID GOB.PE, la carga probatoria recae en el Proveedor Público del Servicio Digital.

Artículo 17. Atributos de Identidad Digital

17.1 Los atributos de identidad digital son aquellos datos que en conjunto individualizan y caracterizan a un ciudadano digital.

17.2 Los atributos de identidad digital se clasifican en inherentes y complementarios.

17.3 Los atributos inherentes son aquellos atributos que permiten distinguir a un ciudadano digital como distinto de otros dentro del contexto del Estado Peruano y son un requisito para ser un ciudadano digital.

17.4 Los atributos inherentes son:

a) Código único de identificación (CUI) para peruanos o código único de extranjero (CUE) para extranjeros (obligatorio).

b) Nombres y apellidos (obligatorio).

c) Fecha de nacimiento (obligatorio).

d) Lugar de nacimiento (obligatorio).

e) Nacionalidad (obligatorio).

f) Dirección (opcional).

g) Dirección de correo electrónico personal y/o número de teléfono celular (obligatorio).

17.5 Los atributos inherentes de los peruanos son administrados por el Registro Nacional de Identificación y Estado Civil, y los atributos inherentes de los extranjeros son administrados por la Superintendencia Nacional de Migraciones.

17.6 Los atributos complementarios son aquellos atributos que en conjunto con los atributos inherentes permiten la caracterización de una persona desde una determinada perspectiva. Los atributos complementarios son gestionados por los Proveedores de Atributos de Identidad Complementarios señalados en el artículo 18 del presente Reglamento.

17.7 El Ministerio de Relaciones Exteriores, en el marco de sus funciones y competencias, provee información sobre los atributos de identidad de un extranjero contenidos en el Carné de Identidad, Carné de Solicitante de Refugio u otros documentos similares a la Superintendencia Nacional de Migraciones, a través de servicios de información interoperables, para su inscripción en el Registro de Información de Migraciones (RIM).

Artículo 18. Proveedores de Atributos de Identidad complementarios

18.1 Los Proveedores de Atributos de Identidad (PAI) son todas las entidades de la Administración Pública que gestionan algún atributo de identidad complementario.

18.2 Los PAI son responsables de mantener la veracidad, la exactitud y la vigencia de los valores de los atributos de identidad complementarios.

18.3 Los PAI proveen atributos de identidad a los proveedores públicos de servicios digitales (PPSD) a través de la Plataforma de Interoperabilidad del Estado. Dicha provisión no requiere el consentimiento del ciudadano digital, siendo de aplicación las limitaciones al consentimiento para el tratamiento de datos personales contenidos en el numeral 1 del artículo 14 de la Ley Nº 29733, Ley de Protección de Datos Personales. Asimismo, los PAI actúan bajo el principio de divulgación de información mínima y salvaguardando lo dispuesto en la Ley Nº 27806, Ley de Transparencia y Acceso a la Información Pública y otras normas aplicables.

Artículo 19.- Credenciales de Autenticación

19.1 Una credencial de autenticación es aquella representación de la identidad digital utilizada por un

ciudadano digital para demostrar que es quien dice ser ante la Plataforma ID GOB.PE.

19.2 Una persona natural, peruana o extranjera, puede solicitar la emisión, entrega o activación de una credencial de autenticación a los Gestores de la Identidad Digital. Asimismo, las credenciales de autenticación pueden ser emitidas, entregadas o activadas por los Gestores de la Identidad Digital previa autenticación efectuada por la Plataforma IDGOBPERÚ con un NCA igual o mayor que el de la credencial de autenticación solicitada.

19.3 Las credenciales de autenticación son un requisito para ser un ciudadano digital.

CAPÍTULO II
DOCUMENTO NACIONAL DE IDENTIDAD DIGITAL

Artículo 20. Documento Nacional de Identidad Digital

20.1 El Documento Nacional de Identidad digital (DNId) es el Documento Nacional de Identidad emitido por el RENIEC en dispositivos digitales, que permite acreditar la identidad de su titular en entornos presenciales y/o no presenciales. Además, puede permitir a su titular la creación de firmas digitales dentro del marco de la Ley Nº 27269, Ley de Firmas y Certificados Digitales, su Reglamento y normas modificatorias y complementarias. Asimismo, el DNId puede ser utilizado para el ejercicio del voto electrónico primordialmente no presencial en los procesos electorales.

20.2 El DNId se constituye como una de las credenciales de autenticación de la identidad digital nacional que puede ser utilizada por su titular para demostrar que es quién dice ser en la Plataforma ID GOB.PE.

Artículo 21. Lineamientos para el Documento Nacional de Identidad Digital

El RENIEC es responsable de establecer los requisitos, características, lineamientos y procedimientos del DNId, teniendo en consideración tecnologías que garanticen su seguridad y la verificabilidad de su autenticidad e integridad.

Artículo 22. Uso y validez del Documento Nacional de Identidad Digital

22.1 Los funcionarios y servidores públicos al servicio de las entidades de la Administración Pública pueden hacer uso del DNId para el ejercicio de sus funciones en los actos de administración, actos administrativos, procedimientos administrativos y servicios digitales. El DNId sólo otorga garantía sobre la identificación de la persona natural, mas no sobre el cargo, rol, atribuciones o facultades que ostenta un funcionario o servidor público; quien es el responsable de gestionar en su entidad las autorizaciones de acceso y asignación de roles, atribuciones o facultades para hacer uso del indicado DNId en los sistemas de información que hagan uso de este.

22.2 Para efectos de identificación, ninguna persona, autoridad o funcionario puede exigir la presentación del Documento Nacional de Identidad en formato electrónico o convencional cuando su titular disponga del mismo en formato digital, siempre que se tenga al alcance un mecanismo seguro de verificación de su validez.

22.3 El tiempo de coexistencia del Documento Nacional de Identidad en formato digital, electrónico y convencional es definido por el RENIEC, los cuales pueden ser usados en la Plataforma ID GOB.PE.

TÍTULO III
SERVICIOS DIGITALES

CAPÍTULO I
MARCO DE SERVICIOS DIGITALES DEL ESTADO PERUANO

Artículo 23. Marco de Servicios Digitales del Estado Peruano

23.1 El Marco de Servicios Digitales del Estado Peruano es dirigido, supervisado y evaluado por la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, en su calidad de ente rector de servicios digitales, que emite lineamientos, especificaciones, guías, directivas, normas técnicas y estándares para su aplicación por parte de las entidades de la Administración Pública a fin de garantizar el diseño, seguridad, escalabilidad, interoperabilidad, integridad, accesibilidad, usabilidad, omnicanalidad de los servicios digitales y el adecuado uso de las tecnologías digitales.

23.2 El Marco de Servicios Digitales del Estado Peruano comprende la interacción de los ciudadanos y personas en general con los servicios digitales provistos de forma total o parcial a través de Internet u otra red equivalente por las entidades de la Administración Pública.

23.3 El Marco de Servicios Digitales del Estado Peruano y sus normas de desarrollo, son revisadas y aplicadas en el diseño, construcción, despliegue y operación de los servicios digitales prestados por las entidades de la Administración Pública a los ciudadanos y personas en general.

Artículo 24. Principios del Marco de Servicios Digitales del Estado Peruano

La aplicación del Marco de Servicios Digitales del Estado Peruano se desarrolla de acuerdo con los principios rectores establecidos en el artículo 5 de la Ley, los principios del procedimiento administrativo establecidos en el TUO de la Ley Nº 27444, y con los siguientes principios específicos:

a) Centrados en los ciudadanos. Los servicios digitales se co-crean y co-diseñan con la participación de los ciudadanos y personas en general a fin de atender y satisfacer sus demandas y/o necesidades.

b) Accesibilidad. Los servicios digitales cuentan con las características necesarias para que sean accesibles por todas las personas, en especial por las personas en situación de discapacidad.

c) Pensados para dispositivos móviles. Los servicios digitales están configurados para poder ser utilizados con un dispositivo móvil, teléfono inteligente o similar.

d) Escalabilidad. Los servicios digitales aseguran y mantienen niveles razonables de calidad ante el incremento de la demanda.

e) Innovación abierta y mejora continua. En base a las necesidades de las personas, se garantiza la mejora continua de los servicios digitales, así como el despliegue de estrategias de innovación abierta.

f) Conservación de la información. Se garantiza que las comunicaciones y documentos generados en entornos digitales, se conservan en las mismas o mejores condiciones que aquellas utilizadas por los medios tradicionales, de acuerdo con la normatividad de la materia.

g) Seguridad desde el diseño. Los servicios digitales se diseñan y desarrollan preservando la disponibilidad, integridad, confidencialidad de la información que gestiona y, cuando corresponda, la autenticidad y no repudio de la información proporcionada.

h) Interculturalidad. Los servicios digitales se desarrollan bajo un enfoque intercultural considerando las necesidades culturales y sociales de los grupos étnico-culturales del país.

Artículo 25. Proveedores Públicos de Servicios Digitales

25.1 Los proveedores públicos de servicios digitales (PPSD) son todas las entidades de la Administración Pública que proveen servicios digitales.

25.2 Los PPSD tienen las siguientes obligaciones:

a) No solicitar al ciudadano digital otras credenciales de autenticación que no sean las emitidas y/o habilitadas dentro del marco del presente Reglamento.

b) Adoptar medidas que garanticen el respeto de las normas de procedimiento aplicables y la eficacia de los actos realizados mediante los servicios digitales.

c) Determinar el NCA pertinente por cada operación o servicio digital prestado, de acuerdo con la sensibilidad

y nivel de riesgo, considerando los criterios establecidos en el artículo 106 del Título VII del presente Reglamento.

d) Gestionar adecuadamente los atributos de identidad digital obtenidos y destinarlos únicamente para los fines para los cuales fueron obtenidos.

e) Determinar los privilegios para el acceso a la información, los recursos y los servicios asociados a la identidad digital que le corresponde a un ciudadano digital después de una autenticación exitosa mediante la Plataforma ID GOB.PE.

f) Notificar y/o comunicar al ciudadano y persona en general el inicio, estado y/o resultado de su trámite a su Casilla Única Electrónica, cuando corresponda.

g) Diseñar el servicio digital a fin de que la información entregada al ciudadano y persona en general tenga un alcance acorde al ámbito de acción que tiene la entidad, y de conformidad con la Ley Nº 27806, Ley de Transparencia y Acceso a la Información Pública, y sus modificatorias.

h) Utilizar los identificadores únicos fundamentales, vocabularios básicos y vocabularios extendidos para la prestación de sus servicios digitales previstos en el presente Reglamento.

i) Garantizar que solo el ciudadano o representante legal facultado que forma parte de un procedimiento o proceso tenga acceso a los documentos que formen parte del expediente electrónico.

j) Priorizar la prestación de servicios, tramitación de procedimientos, y desarrollo de reuniones o sesiones a su cargo haciendo uso de tecnologías digitales y canales digitales.

k) Contar con una infraestructura tecnológica que permita asegurar la disponibilidad de los servicios digitales las 24 horas de los 365 días del año.

l) No solicitar al ciudadano pago por acceder a consultar digitalmente sus propios datos o información pública, salvo aquellos casos establecidos en una disposición legal.

25.3 Los PPSD otorgan las garantías para la prestación de servicios digitales, establecidos en el artículo 18 de la Ley, asegurando que los mismos:

a) Se integran con la Plataforma ID GOB.PE para autenticar en línea la identidad de un ciudadano digital, conforme a las disposiciones establecidas en el Capítulo I del Título II del presente Reglamento.

b) Se diseñan, implementan y prestan conforme a las disposiciones de seguridad digital establecidas en el Título VII del presente Reglamento y el Decreto de Urgencia Nº 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.

c) Se diseñan, implementan y prestan conforme a las disposiciones de interoperabilidad establecidas en el Título VI del presente Reglamento.

d) Se diseñan, implementan y prestan conforme a las disposiciones de arquitectura digital establecidas en el Título VIII del presente Reglamento.

e) Se diseñan o rediseñan considerando aspectos de accesibilidad, usabilidad y simplicidad, centradas en la experiencia de los usuarios, así como normas técnicas y estándares ampliamente reconocidos y habilidades blandas.

f) Se integran a la Plataforma de Pagos Digitales del Estado Peruano u otros mecanismos para realizar los pagos de derechos de tramitación conforme a las disposiciones establecidas en el artículo 89 del presente Reglamento.

g) Se diseñan, implementan y prestan atendiendo las condiciones para el tratamiento de datos personales conforme a las normas sobre la materia.

h) Garantizan la conservación de las comunicaciones y documentos electrónicos generados en su prestación, de acuerdo con las normas sobre la materia.

Artículo 26. Tipos de Servicios digitales

26.1 El servicio digital, definido en el artículo 3 de la Ley, puede ser clasificado por su nivel de complejidad y necesidad de apersonamiento del ciudadano.

26.2 Los servicios digitales, de acuerdo con su complejidad, son clasificados en cuatro (04) tipos:

a) **Servicio digital informativo.** Son aquellos de carácter netamente informativo y unidireccional.

b) **Servicio digital cercano.** Son aquellos que permiten comunicaciones bidireccionales básicas.

c) **Servicio digital optimizado.** Son aquellos que permiten comunicación bidireccional avanzada, y su utilización requiere como mínimo la autenticación de la identidad del ciudadano mediante la plataforma ID GOB.PE y un bloque básico de interoperabilidad técnica establecido en el artículo 86 del presente Reglamento.

d) **Servicio digital conectado.** Son aquellos que utilizan al menos tres (03) bloques básicos de interoperabilidad técnica establecidos en el artículo 86 del presente Reglamento.

26.3 Los servicios digitales, de acuerdo con la necesidad de apersonamiento del ciudadano, son clasificados en tres (03) tipos:

a) **Servicio digital no presencial.** Es aquel servicio provisto de forma total a través de Internet u otra red equivalente, que se caracteriza por ser no presencial (no requiere el apersonamiento del ciudadano digital en la sede de atención de la entidad) y automático (no requiere intervención humana directa para su atención) o semiautomático (requiere intervención humana para su atención). Puede ser sincrónico o asincrónico.

b) **Servicio digital semipresencial.** Es aquel servicio provisto de forma parcial a través de Internet u otra red equivalente, que se caracteriza por ser semipresencial (requiere que el ciudadano digital se apersone a la sede de atención de la entidad en alguna etapa del servicio, o viceversa).

c) **Servicio digital presencial.** Es aquel servicio provisto de forma parcial a través de equipamiento tecnológico, diseñado para el autoservicio.

26.4 Las entidades públicas determinan los tipos de servicios digitales que le corresponde proveer en base a su complejidad o la necesidad de apersonamiento del ciudadano.

Artículo 27. Ciclo de vida de la implementación de los servicios digitales

27.1 Las entidades públicas consideran las siguientes etapas en el ciclo de vida de la implementación de los servicios digitales:

a) **Alineamiento a los objetivos estratégicos.** Comprende el alineamiento y priorización del servicio digital con los objetivos estratégicos institucionales en el marco del Sistema Nacional de Planeamiento.

b) **Concepción, co-creación y diseño-** Comprende la investigación para la identificación de las necesidades del ciudadano y personas en general, su priorización, la definición de la arquitectura lógica, el diseño, el prototipado de la solución, la realización de pruebas de concepto y las pruebas de usabilidad.

c) **Construcción e integración.** Comprende el uso de herramientas, técnicas, metodologías, estándares, normas técnicas y marcos de referencia ampliamente reconocidos para la construcción del servicio digital y su integración con los bloques básicos para la interoperabilidad técnica definidos en el Título VI del presente Reglamento, en lo que corresponda.

d) **Operación.** Comprende el uso de marcos de referencia y estándares ampliamente reconocidos para la provisión de servicios digitales seguros y de valor para el ciudadano y personas en general.

e) **Mejora continua.** Comprende el desarrollo de acciones periódicas, en base a las necesidades del ciudadano y personas en general, así como los avances tecnológicos, para el mejoramiento continuo de la calidad del servicio digital. Esta etapa se basa en el uso de métodos cuantitativos y cualitativos para perfeccionar la calidad y la eficiencia de los servicios digitales, así como de otros productos de la cadena de valor.

27.2 En la formulación y evaluación de los proyectos de tecnologías digitales se aplican las normas técnicas,

parámetros, metodologías, estándares o similares que establezca la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros.

Artículo 28. Innovación de los servicios digitales

28.1 Las entidades de la Administración Pública implementan servicios digitales innovadores, haciendo énfasis en la generación de valor para los ciudadanos y personas en general, siempre que se encuentren dentro de sus competencias, atribuciones y funciones.

28.2 Todo servicio digital es supervisado permanentemente por la entidad proveedora de este, a fin de identificar, analizar, desarrollar y verificar mejoras adicionales para su prestación.

28.3 Las entidades públicas incorporan mecanismos para recolectar la percepción de los ciudadanos acerca del servicio digital utilizado, como mínimo, implementan procesos ágiles de investigación, encuestas en línea accesibles desde su sede o servicio digital. La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, emite lineamientos o guías sobre mecanismos para evaluar la percepción o nivel de satisfacción del servicio digital.

Artículo 29. Inclusión digital y centros de ciudadanía digital

29.1 Las entidades de la Administración Pública garantizan que los ciudadanos o personas en general puedan relacionarse con ellas a través de canales digitales, para lo cual ponen a su disposición la sede digital y los centros de ciudadanía digital que sean necesarios, así como los sistemas de información, plataformas, aplicativos, servicios y contenidos digitales que en cada caso se determinen. Los centros de ciudadanía digital son los centros de acceso público de gobierno digital previstos en la Ley Nº 29904, Ley de Promoción de Banda Ancha y Construcción de la Red Dorsal Nacional de Fibra Óptica y su Reglamento.

29.2 Las entidades públicas implementan, en función a sus recursos y capacidades, y conforme a las proyecciones o actividades establecidas en sus instrumentos de gestión, centros de ciudadanía digital a fin de proveer espacios para el acceso a sus servicios y contenidos digitales, siguiendo los lineamientos y normas emitidas por la Presidencia del Consejo Ministros, a través de la Secretaría de Gobierno Digital.

Artículo 30. Fecha y hora oficial

Las entidades de la Administración Pública garantizan que todos los sistemas de cómputo y sus respectivas bases de datos están sincronizados con servidores de tiempo que permitan acceder a la fecha y hora cierta para obtener la fecha y hora oficial del Perú, salvo excepciones establecidas por norma expresa o remisión de informe técnico dirigido a la Secretaría de Gobierno Digital.

CAPÍTULO II
PLATAFORMA DIGITAL ÚNICA DEL ESTADO PERUANO PARA ORIENTACIÓN AL CIUDADANO - GOB.PE

Artículo 31. Estructura funcional de la Plataforma Digital GOB.PE

31.1 La Plataforma Digital Única del Estado Peruano para Orientación al Ciudadano (Plataforma GOB.PE) es la plataforma digital que provee, como mínimo, las siguientes funcionalidades:

a) Acceder a información del Estado Peruano presentada de manera centralizada.

b) Acceder a la información institucional, catálogo digital de trámites y servicios que prestan todas las entidades públicas, así como a sus sedes digitales.

c) Realizar trámites, acceder a servicios digitales y hacer su seguimiento, incorporando mecanismos de seguridad y, cuando corresponda, mecanismos de no repudio.

d) Realizar reclamos y hacer su seguimiento mediante la plataforma Libro de Reclamaciones o la que haga sus veces, así como realizar denuncias.

e) Presentar solicitudes, escritos u otro tipo de documento en soporte digital dirigida a una entidad pública a través de la Plataforma Única de Recepción Documental del Estado Peruano.

f) Autenticar la identidad digital mediante la Plataforma ID GOB.PE.

g) Acceder a un entorno personalizado.

h) Acceder a una carpeta ciudadana.

i) Acceder a la casilla única electrónica para la recepción de notificaciones digitales y revisión de la bandeja de comunicaciones.

j) Acceder a información personal y familiar, así como a datos de educación, trabajo, electoral, tributaria conforme a los acuerdos establecidos con las entidades competentes proveedoras de dicha información, y, a través de la Plataforma de Interoperabilidad del Estado (PIDE), a datos personales de salud conforme a lo establecido en el marco legal vigente.

31.2 El acceso a las funcionalidades citadas en los literales del f) al j) del numeral 31.1 requieren la autenticación de la identidad digital del ciudadano digital titular de la información y sus datos o del representante legal que tiene la facultad de acceder a dicha información según corresponda.

31.3 La plataforma GOB.PE no almacena información o datos personales de salud provista por el Ministerio de Salud o instituciones prestadoras de servicios de salud.

31.4 Las entidades públicas despliegan obligatoriamente los servicios de información necesarios para la implementación de la estructura funcional de la Plataforma GOB.PE.

31.5 La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, define el diseño y conduce el desarrollo e implementación de la estructura funcional de la plataforma GOB.PE. Asimismo, mediante Resolución de Secretaría de Gobierno Digital amplía o modifica la estructura funcional de la Plataforma GOB.PE en función de la necesidad pública, importancia estratégica o normativa expresa que lo demande.

Artículo 32. Sede digital

32.1 La sede digital es una sede de la entidad, cuya dirección electrónica está bajo el dominio en Internet de la Plataforma GOB.PE. Su contenido a nivel de titularidad, gestión y administración corresponde a cada entidad de la administración pública. A través de la sede digital los ciudadanos y personas en general pueden acceder al catálogo digital de trámites y servicios, realizar trámites y otras actividades conforme a lo establecido en el artículo 20 de la Ley.

32.2 Las entidades de la Administración Pública son responsables de la integridad, veracidad y actualización de la información, contenidos digitales y servicios digitales que presten a través de su respectiva sede digital.

Artículo 33. Catálogo digital de trámites y servicios

33.1 El catálogo digital de trámites y servicios es un canal informativo, que forma parte de la sede digital de las entidades públicas, para el acceso a información de trámites y servicios que prestan, en cumplimiento del artículo 1 del Decreto Supremo Nº 033-2018-PCM, Decreto Supremo que crea la Plataforma Digital Única del Estado Peruano y establece disposiciones adicionales para el desarrollo del gobierno digital.

33.2 Para el caso de la información de los procedimientos administrativos, servicios prestados en exclusividad y servicios no exclusivos, el Catálogo digital de trámites y servicios integra información del Sistema Único de Trámites o instrumentos de gestión de las entidades de la Administración Pública aprobados. El catálogo contiene como mínimo la siguiente información: descripción, requisitos, etapas, plazo, autoridad que lo aprueba, tipo de procedimiento y tasa.

Artículo 34. Catálogo Oficial de Aplicativos Móviles del Estado Peruano

34.1 Créase el Catálogo Oficial de Aplicativos Móviles del Estado Peruano, bajo la cuenta oficial GOB.PE, en

las tiendas de distribución de aplicativos móviles. Es gestionado por la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital.

34.2 Las entidades públicas desarrollan sus aplicativos móviles en base a los lineamientos y directivas técnicas para el diseño, construcción y registro emitidos por la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital.

34.3 Asimismo, las entidades coordinan con la Secretaría de Gobierno Digital el registro de un aplicativo móvil nuevo o existente en el Catálogo Oficial de Aplicativos Móviles del Estado Peruano. La Secretaría de Gobierno Digital supervisa de oficio o a pedido de una entidad un aplicativo móvil a fin de verificar el cumplimiento de los lineamientos emitidos, en caso lo requiera puede solicitar opinión a otras entidades vinculadas.

TÍTULO IV
CONDICIONES, REQUISITOS Y USO DE LAS TECNOLOGÍAS Y MEDIOS ELECTRÓNICOS EN EL PROCEDIMIENTO ADMINISTRATIVO

CAPÍTULO I
DOCUMENTO ELECTRÓNICO

Artículo 35. Documento electrónico

35.1 El documento electrónico es la unidad básica estructurada de información, es susceptible de ser clasificada, transmitida, procesada o conservada utilizando medios electrónicos, sistemas de información o similares. Contiene información de cualquier naturaleza, es registrado en un soporte electrónico o digital, en formato abierto y de aceptación general, a fin de facilitar su recuperación y conservación en el largo plazo. Asimismo, tiene asociado datos que permiten su individualización, identificación, gestión y puesta al servicio del ciudadano.

35.2 El documento electrónico tiene el mismo valor legal que aquellos documentos en soporte papel, de conformidad con lo establecido en el numeral 30.3 del artículo 30 del TUO de la Ley Nº 27444.

35.3 El documento electrónico tiene un ciclo de vida que comprende la planificación, producción (creación, emisión, recepción, despacho), conservación, puesta a disposición y/o eliminación, de acuerdo con la legislación en materia de gobierno digital y las normas del Sistema Nacional de Archivos. Asimismo, siempre que sea factible se pueden emitir representaciones imprimibles de un documento electrónico.

Artículo 36. Código de verificación digital

36.1 El Código de Verificación Digital (CVD) es la secuencia alfanumérica que permite verificar la autenticidad de una representación impresa o imprimible mediante el cotejo con el documento electrónico localizado en la sede digital de la entidad. Las entidades implementan el servicio digital para realizar dicha verificación. La Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros emite los lineamientos para la gestión y el uso del CVD a fin de garantizar su seguridad e interoperabilidad.

36.2 El CVD es incorporado en las representaciones imprimibles de documentos electrónicos gestionados por una entidad. Lo señalado en el presente numeral se aplica sin perjuicio de lo dispuesto en la Tercera Disposición Complementaria Final del Decreto Supremo Nº 026-2016-PCM, Decreto Supremo que aprueba medidas para el fortalecimiento de la infraestructura oficial de firma electrónica y la implementación progresiva de la firma digital en el Sector Público y Privado.

Artículo 37. Representación imprimible

37.1 Es la representación de un documento electrónico susceptible de ser impresa en soporte papel. Es emitida en un formato digital abierto e interoperable con al menos una firma digital de agente automatizado emitido en el marco de la IOFE y un código de verificación digital (CVD). A partir de una representación imprimible pueden generarse múltiples representaciones impresas.

37.2 Las entidades de la Administración Pública remiten representaciones imprimibles de documentos electrónicos a los ciudadanos y personas en general. Dichas representaciones pueden ser enviadas a la casilla única electrónica del ciudadano o persona en general.

37.3 En caso la entidad expida una representación impresa ésta no requiere la aplicación de una firma manuscrita por parte de ningún representante de la entidad, siempre que haya sido generada a partir de una representación imprimible.

37.4 Si una entidad de la Administración Pública solicita a un ciudadano o persona en general un documento electrónico original, se entiende cumplido su mandato con la remisión por parte de este del CVD o representación imprimible, o con la presentación de una representación impresa del mismo.

Artículo 38. Exámenes y auditorías

Los documentos electrónicos firmados con cualquier modalidad de firma electrónica por las entidades públicas son válidos para cualquier revisión, incluyendo exámenes y auditorías, públicas o privadas, pudiendo ser exhibidos, ante los revisores, inspectores, auditores y autoridades competentes, de forma directa, o mediante su presentación en aplicativos que permiten su verificación, sin requerirse copia en papel, salvo que una norma, lo exprese o lo disponga.

CAPÍTULO II
EXPEDIENTE ELECTRÓNICO

Artículo 39. Expediente electrónico

39.1 El expediente electrónico es el conjunto organizado de documentos electrónicos que respetando su integridad documental están vinculados lógicamente y forman parte de un procedimiento administrativo o servicio prestado en exclusividad en una determinada entidad de la Administración Pública, conforme a lo establecido en el artículo 31 del TUO de la Ley Nº 27444. Asimismo, todas las actuaciones del procedimiento se registran y conservan íntegramente y en orden sucesivo en el expediente electrónico.

39.2 El expediente electrónico se gestiona como un documento archivístico digital, cumpliendo las disposiciones técnico normativas emitidas por la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, y las normas del Sistema Nacional de Archivos emitidas por el Archivo General de la Nación.

39.3 En caso existan documentos en soporte papel que requieran ser incorporados en el expediente electrónico, las entidades pueden aplicar lo establecido en el artículo 48 del presente Reglamento. La Secretaría de Gobierno Digital en coordinación con el Archivo General de la Nación emite las normas sobre la gestión de expedientes conformados por documentos en soporte papel y documentos electrónicos.

Artículo 40. Estructura del expediente electrónico

40.1 El expediente electrónico tiene como mínimo los siguientes componentes:

a) Número o código único de identificación.
b) Índice digital.
c) Documentos electrónicos.
d) Firma del índice digital.
e) Metadatos del expediente electrónico.
f) Categorización

40.2 Los estándares técnicos de la estructura del expediente electrónico son establecidos por la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, teniendo en consideración las normas sobre los procesos de gestión documental definidos en estándares internacionales, normas técnicas, y de archivos definidos por el Archivo General de la Nación.

Artículo 41. Número o código único de identificación

El número o código único de identificación permite la identificación unívoca del expediente electrónico dentro

de la entidad, y con ello su ubicación, acceso, control y seguimiento en cada entidad en la que se tramite o archive. Asimismo, es utilizado para el intercambio de información entre entidades o partes interesadas, y respeta los estándares técnicos para la elaboración del expediente electrónico.

Artículo 42. Índice Digital

Es el instrumento que contiene la relación y datos para la identificación de los documentos electrónicos que integran el expediente, los cuales están ordenados en forma cronológica, alfabética, numérica o mixta. El índice digital tiene un código que lo identifica y la fecha en que se genera, así como atributos para registrar la fecha de apertura y cierre del expediente. Asimismo, por cada documento electrónico contiene, como mínimo, los siguientes elementos:

a) Código único del documento.
b) Fecha de producción o fecha de incorporación.
c) Orden del documento dentro del expediente.
d) Resumen hash del documento.
e) Foliado.

Artículo 43. Generación del Índice Digital

43.1 La generación del índice digital comprende, como mínimo, las siguientes operaciones:

a) Asociar un documento electrónico a un expediente electrónico con el fin de permitir su recuperación.
b) Identificar la secuencia, orden, y cuando corresponda, la página de inicio y fin del documento electrónico que se incorpora al expediente electrónico.
c) Firmar digitalmente el índice digital al cierre del expediente electrónico, a fin de garantizar su integridad y autenticidad.

43.2 El índice digital firmado al cierre del expediente utiliza un certificado digital emitido en el marco de la IOFE.

Artículo 44. Metadatos del expediente electrónico

44.1 Los metadatos son los datos que describen el contexto, el contenido y la estructura del expediente electrónico y su gestión a lo largo del tiempo. Cuando se asegura la integridad de los metadatos, estos sirven como evidencia ante algún requerimiento de información de los operadores de justicia, tribunales o autoridades en sus procesos de supervisión, fiscalización e investigación.

44.2 La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, establece el perfil mínimo de los metadatos que contiene el expediente electrónico.

Artículo 45. Obtención de copias del expediente electrónico

45.1 Las entidades de la Administración Pública expiden una copia de todo o parte del expediente electrónico consignando en ella un Código de Verificación Digital (CVD). Las copias del expediente electrónico son entregadas en soporte digital o son remitidas a la casilla única electrónica, salvo solicitud expresa de emisión en soporte papel y siempre que sea posible, en cuyo caso se aplica lo establecido en los artículos 53 y 90 del TUO de la Ley Nº 27444, según corresponda. Dichas copias entregadas o remitidas en soporte digital tienen la misma validez que las copias certificadas o fedateadas en soporte papel, debiendo encontrarse siempre firmadas digitalmente en el marco de la IOFE por la entidad emisora de la copia o por un fedatario institucional.

45.2 En caso el expediente electrónico se encuentre conformado por uno o varios documentos en soporte papel, que no hayan podido ser digitalizados, las copias de dichos documentos atienden lo establecido en los artículos 52 y 138 del TUO de la Ley Nº 27444.

CAPÍTULO III
RECEPCIÓN DOCUMENTAL

Artículo 46. Plataforma Única de Recepción Documental del Estado Peruano

46.1 Créase la Plataforma Única de Recepción Documental del Estado Peruano (MESA DIGITAL PERÚ) como el registro digital que forma parte de la Plataforma GOB.PE, permite la recepción de escritos, solicitudes y documentos electrónicos enviados por los ciudadanos y personas en general a las entidades de la Administración Pública cumpliendo los requisitos de cada trámite, todos los días del año durante las veinticuatro (24) horas, donde los plazos para el pronunciamiento de las entidades se contabilizan a partir del primer día hábil siguiente de haber sido presentados, respetando los plazos máximos para realizar actos procedimentales dispuestos en el artículo 143 del TUO de la Ley Nº 27444.

46.2 Para la presentación de escritos, solicitudes y documentos electrónicos correspondientes a procedimientos especiales, tales como, el procedimiento sancionador, trilateral, fiscalizador, a través de la MESA DIGITAL PERÚ, los ciudadanos y personas en general observan el horario de atención establecido en las normas que las regulan, de corresponder.

46.3 Los documentos presentados:

a) Desde las 00:00 horas hasta el término del horario de atención de la entidad de un día hábil, se consideran presentados el mismo día.
b) Después del horario de atención de la entidad hasta las 23:59 horas, se consideran presentados el día hábil siguiente.
c) Los sábados, domingos, feriados o cualquier otro día inhábil, se consideran presentados al primer día hábil siguiente.

46.4 La MESA DIGITAL PERÚ se integra con los sistemas de trámite documentario, sistemas de gestión documental o sistemas de expediente electrónico u otros sistemas de información de las entidades públicas. Asimismo, se integra con los bloques básicos para la interoperabilidad técnica definidos en el artículo 87 del Título VI del presente Reglamento según corresponda.

46.5 La MESA DIGITAL PERÚ envía a la casilla única electrónica del ciudadano o persona en general un cargo de recepción de los escritos, solicitudes y documentos electrónicos presentados, con su firma digital de agente automatizado de la entidad y un sello de tiempo, consignando la fecha, hora, cantidad de folios y canal de presentación, en conformidad con el artículo 135.2 del TUO de la Ley Nº 27444. La firma digital y el sello de tiempo son generados en el marco de la Infraestructura Oficial de Firma Electrónica (IOFE). En caso la entidad realice observaciones a la documentación presentada corresponde aplicar lo establecido en el numeral 136.6 del artículo 136 del TUO de la Ley Nº 27444, realizando la comunicación a la casilla única electrónica.

46.6 La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, establece las normas para la implementación de la MESA DIGITAL PERÚ.

Artículo 47. Recepción de documentos en original y/o copia vía canal digital

47.1 Para la recepción de cualquier documento en original, independientemente del medio de soporte que lo contenga, que no se encuentre en la relación de documentos originales que pueden ser reemplazados por sucedáneos, conforme a lo establecido en el artículo 49 del TUO de la Ley Nº 27444, vía plataformas de recepción documental, mesas de parte digital o similares, las entidades pueden optar, dependiendo de la naturaleza del procedimiento o servicio, por una o alguna combinación de las siguientes alternativas:

a) Recibir un documento escaneado presentado por el ciudadano o persona en general que tenga las firmas manuscritas necesarias, debiendo la entidad firmarlo digitalmente con certificado de agente automatizado y un sello de tiempo, en el marco de la IOFE.
b) Recibir un documento electrónico presentado por el ciudadano o persona en general que utilice alguna de las modalidades de firma electrónica establecidas en el Reglamento de la Ley Nº 27269, Ley de Firmas y Certificados Digitales, aprobado mediante Decreto

Supremo Nº 052-2008-PCM y modificatorias, debiendo la entidad firmarlo digitalmente, con certificado de agente automatizado y un sello de tiempo, en el marco de la IOFE.

c) Proveer un formulario web a ser completado por el ciudadano o persona en general, a partir del cual la entidad genera un documento electrónico debiendo firmarlo digitalmente, con un certificado de agente automatizado y un sello de tiempo, en el marco de la IOFE.

47.2 En caso la entidad requiera la presentación física del documento original en una unidad de recepción documental de la entidad, luego de la presentación por el canal digital conforme lo establecido en el literal a) del numeral precedente, corresponde al ciudadano o persona en general efectuar la referida presentación en un plazo máximo de dos (02) días hábiles siguientes de la presentación vía canal digital, conforme lo establecido el numeral 136.1 del artículo 136 del TUO de la Ley Nº 27444; mientras esté pendiente dicha presentación son aplicables las reglas establecidas en los numerales 136.3.1 y 136.3.2 de dicho cuerpo normativo. De no presentarse oportunamente lo requerido resulta de aplicación lo dispuesto en el numeral 136.4 del TUO de la Ley Nº 27444.

47.3 En caso la entidad requiera la presentación de la copia de un documento original o documentos sucedáneos de los originales que se encuentran en soporte papel, el ciudadano o persona en general puede presentar dicho documento escaneado.

47.4 La presentación de documentos en original o copia vía canal digital, señalados en los numerales 47.1 y 47.3 precedentes se sujetan al principio de presunción de veracidad conforme a lo dispuesto en el numeral 1.7 del Artículo IV del Título Preliminar y a los numerales 51.1 del artículo 51, 1 y 4 del artículo 67 del TUO de la Ley Nº 27444.

47.5 Las entidades de la Administración Pública envían a la casilla única electrónica del ciudadano o persona en general, un cargo de recepción de los escritos, solicitudes y documentos electrónicos presentados vía canal digital, con su firma digital de agente automatizado y un sello de tiempo, consignando la fecha, hora y canal de presentación, en conformidad con el artículo 135.2 del TUO de la Ley Nº 27444. La firma digital y el sello de tiempo son generados en el marco de la IOFE. Asimismo, envían un mensaje al correo electrónico registrado por el ciudadano o persona en general.

47.6 Las plataformas de recepción documental, mesas de parte digital o similares registran, como mínimo, los siguientes metadatos para la recepción: fecha y hora, asunto, tipo y número de documento de identificación, domicilio, dirección de correo electrónico, número de teléfono celular, entidad destinataria y/o dependencia destinataria. La Secretaría de Gobierno Digital emite normas sobre la categorización, indexación y metadatos para la interoperabilidad entre las referidas plataformas o sistemas en el marco del artículo 8 del Decreto Legislativo Nº 1310, Decreto Legislativo que aprueba medidas adicionales de Simplificación Administrativa.

47.7 Para la presentación de documentos a través de canales digitales las entidades pueden tomar como referencia los horarios establecidos en el numeral 46.3 del artículo 46 del presente Reglamento.

Artículo 48. Digitalización de documentos en soporte papel presentados en las unidades de recepción documental

48.1 La digitalización de documentos originales en soporte papel, presentados en las unidades de recepción documental de las entidades públicas, se realiza conforme a lo siguiente:

a) Para digitalizar un documento original en soporte papel a soporte digital con valor legal es necesario el uso de una línea de digitalización y producción de microformas certificada, observando las disposiciones legales sobre la materia.

b) Para digitalizar un documento original en soporte papel a soporte digital con valor administrativo para los efectos de la entidad donde se utilizará dicho documento, el fedatario institucional autentica el documento escaneado en soporte digital, previo cotejo con el original, con su firma digital generada en el marco de la IOFE.

48.2 Para digitalizar las copias de un documento en soporte papel, presentados en las unidades de recepción documental, se utilizan equipos de captura de imágenes para su escaneo.

48.3 Para efectos de lo dispuesto en el literal b) del numeral 48.1, cada entidad elabora o actualiza una norma interna en la cual se establecen los requisitos, atribuciones y demás disposiciones relacionadas con el desempeño de las funciones del fedatario institucional en la autenticación de documentos escaneados en soporte digital, atendiendo lo establecido en el artículo 138 del TUO de la Ley Nº 27444.

CAPÍTULO IV
GESTIÓN ARCHIVÍSTICA DIGITAL

Artículo 49. Documento archivístico digital

49.1 Es aquel documento electrónico que contiene información en soporte o medio digital y es conservado de manera segura como evidencia y/o activo de información, respetando su integridad documental. Es producido por una persona natural, persona jurídica o una entidad pública, en el ejercicio de sus actividades, procesos, funciones y/o competencias.

49.2 Las características de un documento archivístico digital son:

a) Autenticidad.
b) Fiabilidad.
c) Integridad.
d) Disponibilidad.
e) Usabilidad.

49.3 El documento archivístico digital tiene como mínimo los siguientes metadatos: código único del documento, nombre del documento, tipo y serie documental, fecha y hora, volumen (tamaño y formato) y nombre del productor.

Artículo 50. Repositorio archivístico digital institucional

50.1 El repositorio archivístico digital institucional cuenta con:

a) Principios y políticas.
b) Procedimientos del documento archivístico digital, como mínimo, para la captura, almacenamiento, preservación y acceso.
c) Metadatos.
d) Infraestructura tecnológica y de seguridad digital.
e) Plan de Capacidad.

50.2 El repositorio archivístico digital institucional es administrado y regulado por el Archivo Central de la entidad pública. Sin perjuicio de ello, las acciones relacionadas a la infraestructura tecnológica y seguridad digital del referido repositorio pueden estar a cargo de la unidad de organización de tecnologías de la información, de otra unidad de organización de la entidad o un tercero, no siendo responsables de la gestión del contenido de dicho repositorio.

50.3 Las entidades de la Administración Pública implementan de manera obligatoria su repositorio archivístico digital institucional para administrar los documentos archivísticos digitales, y garantizar su conservación y acceso durante su ciclo de vida.

50.4 En caso las unidades de organización tengan a su cargo un sistema de información o servicio digital, éstas son responsables de la custodia y acceso al documento archivístico digital contenido en dicho sistema hasta su transferencia al repositorio archivístico digital institucional de la entidad. Los precitados sistemas de información se integran con el repositorio archivístico digital institucional.

Artículo 51. Repositorio archivístico digital nacional

51.1 El Archivo General de la Nación administra el repositorio archivístico digital nacional para conservar y resguardar los documentos archivísticos digitales con valor permanente provenientes de los repositorios archivísticos digitales institucionales de las entidades.

51.2 El Archivo General de la Nación implementa el repositorio archivístico digital nacional de manera progresiva y de acuerdo con sus recursos y capacidades asignadas.

51.3 El Archivo Central de las entidades públicas remite sus documentos archivísticos digitales al Repositorio Archivístico digital nacional en base a los protocolos, lineamientos y disposiciones establecidos por el Archivo General de la Nación en coordinación con la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital.

Artículo 52. Normas y políticas para la gestión archivística digital

52.1 La producción de documentos archivísticos digitales, la aplicación de los procesos técnicos archivísticos y registro del patrimonio digital producido en el ejercicio de las funciones de cada entidad pública atienden las normas y políticas emitidas por el Archivo General de la Nación.

52.2 Las normas y políticas para la gestión archivística digital son elaboradas por el Archivo General de la Nación en coordinación con la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital.

CAPÍTULO V
CASILLA ÚNICA ELECTRÓNICA

Artículo 53. Casilla única electrónica

53.1 La casilla única electrónica es el domicilio digital que sirve para recibir comunicaciones y/o notificaciones remitidas por las entidades de la Administración pública a los ciudadanos y personas en general, conforme se establece en el numeral 20.4 del artículo 20 del TUO de la Ley Nº 27444, y al que se refiere el artículo 22 de la Ley.

53.2 La casilla única electrónica acredita la certeza, integridad y fecha y hora cierta de una comunicación y/o notificación realizada por una entidad pública a un ciudadano o persona en general. De darse una controversia referida a la emisión o recepción de una notificación, corresponderá a la entidad responsable de la gestión de la casilla única electrónica acreditar que se produjo dicha emisión o recepción; en cualquier otro caso dicha acreditación recaerá en el emisor.

53.3 La casilla única electrónica está conformada por lo siguiente: (1) dirección electrónica, (2) buzón de notificaciones, y (3) buzón de comunicaciones.

53.4 La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, asigna una casilla única electrónica al ciudadano y persona en general. Asimismo, es responsable de garantizar su disponibilidad, continuidad y funcionamiento, atendiendo a lo establecido en el presente Capítulo, así como también asegura el acceso a las notificaciones y comunicaciones mediante la Plataforma GOB.PE.

Artículo 54. Dirección electrónica

54.1 La dirección electrónica es única y permite identificar a una casilla única electrónica. Asimismo, vincula unívocamente una casilla única electrónica con un ciudadano o persona en general.

54.2 La dirección electrónica está conformada por el Código Único de Domicilio (CUD) y tiene el formato "cud@peru.gob.pe". El valor del CUD es:

a) Para el caso de los peruanos, el Código Único de Identificación asignado por el Registro Nacional de Identificación y Estado Civil.

b) Para el caso de los extranjeros, el Código Único de Extranjero asignado por la Superintendencia Nacional de Migraciones.

c) Para el caso de personas jurídicas, el Número de Partida Registral, asignado por la Superintendencia Nacional de Registros Públicos.

54.3 Para el caso de entidades públicas, así como de sujetos sin personería jurídica que no cuenten con un valor para el CUD, la Secretaría de Gobierno Digital le asigna un código identificatorio a fin de cumplir lo establecido en la Ley y el presente Reglamento.

Artículo 55. Buzón de notificaciones

55.1 Es aquel buzón donde se depositan las notificaciones de actos administrativos, así como actos de administración emitidos en el marco de cualquier actuación administrativa, remitidas por las entidades de la Administración Pública a los ciudadanos y personas en general.

55.2 En el caso del depósito de una notificación, retorna al emisor una constancia de depósito y envía al correo electrónico personal del destinatario mensajes de alerta de la llegada de la notificación. Asimismo, puede enviar al teléfono celular del destinatario mensajes de texto alertando la llegada de una notificación o realizar alertas mediante llamadas telefónicas.

55.3 Las alertas realizadas al correo electrónico personal, teléfono celular, llamadas telefónicas o similares no constituyen parte del procedimiento de notificación vía casilla única electrónica, tampoco afecta la validez de ésta ni de los actos administrativos o actos de administración que se notifican.

55.4 El buzón de notificaciones almacena las notificaciones recibidas por un periodo no menor a un (01) año.

55.5 El buzón de notificaciones guarda evidencias que permiten demostrar el depósito de una notificación.

Artículo 56. Buzón de comunicaciones

56.1 Es un mecanismo lógico con capacidad de reenviar de forma automatizada las comunicaciones que llegan a la casilla única electrónica hacia el correo electrónico personal del destinatario. Las comunicaciones pueden contener mensajes, documentos y/o avisos. Asimismo, pueden enviar al teléfono celular del destinatario mensajes de texto de alerta de la llegada de la comunicación.

56.2 El buzón de comunicaciones puede almacenar las comunicaciones recibidas de forma temporal.

56.3 El buzón de comunicaciones guarda evidencias que permiten demostrar la llegada de una comunicación.

Artículo 57. Acceso a la casilla única electrónica

57.1 Para el caso de la casilla única electrónica de personas naturales, el titular accede a la misma, a través de la Plataforma GOB.PE, previa autenticación de su identidad ante la plataforma ID GOB.PE. El titular puede delegar a uno o más representantes el acceso a un buzón de la casilla para la recepción de las notificaciones, siempre que exista manifestación expresa de su voluntad mediante la Plataforma GOB.PE, de acuerdo con los formularios que se implementen para tal fin.

57.2 Para el caso de la casilla única electrónica de personas jurídicas, su representante legal accede a la misma, a través de la Plataforma GOB.PE, previa autenticación de su identidad ante la Plataforma ID GOB.PE. El representante legal puede delegar a otros representantes el acceso a un buzón de la casilla única electrónica de la persona jurídica para la recepción de las notificaciones, siempre que exista manifestación expresa de su voluntad mediante la Plataforma GOB.PE, de acuerdo con los formularios que se implementen para tal fin.

57.3 La delegación a la que hace referencia los numerales 57.1 y 57.2 se realiza por cada procedimiento del cual sea parte el ciudadano o persona en general, siendo válida únicamente durante dicho procedimiento y en tanto no se comunique su variación. La designación, así como el término o cambio de la delegación se realiza de acuerdo con los formularios que se implementen para tal fin.

Artículo 58. Plataforma Casilla Única Electrónica del Estado Peruano

58.1 Créase la Plataforma Casilla Única Electrónica del Estado Peruano (CASILLA ÚNICA PERÚ) como la plataforma digital que administra la casilla única electrónica de todos los ciudadanos y personas en general.

58.2 La Plataforma CASILLA ÚNICA PERÚ es gestionada por la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital.

58.3 Las comunicaciones y notificaciones a través de la Plataforma CASILLA ÚNICA PERÚ se realizan entre emisores y destinatarios, donde:

a) **Emisores.** Son aquellas entidades públicas plenamente identificadas que utilizan la plataforma CASILLA ÚNICA PERÚ para efectuar comunicaciones y/o notificaciones a un ciudadano o persona en general.

b) **Destinatarios.** Son los ciudadanos o personas en general que acceden a su casilla única electrónica para revisar las comunicaciones y las notificaciones efectuadas por los emisores.

58.4 La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, establece los protocolos de integración, así como los lineamientos para garantizar su confidencialidad, integridad, autenticidad, no repudio y fecha y hora cierta de las operaciones y transacciones, en conformidad con el marco normativo correspondiente. Asimismo, establece las reglas, criterios, plazos y condiciones para el uso, delegación, suspensión e implementación de la casilla única electrónica, y publica datos en formatos abiertos sobre su uso en la Plataforma Nacional de Datos Abiertos.

58.5 Las entidades de la Administración Pública que no cuenten con ningún mecanismo de notificación, a través de tecnologías y medios digitales o electrónicos, están obligadas a utilizar la Plataforma CASILLA ÚNICA PERÚ para la emisión de comunicaciones y notificaciones digitales a los ciudadanos y personas en general.

58.6 Las entidades de la Administración Pública que cuenten con habilitación legal, mediante una norma con rango de Ley, no están obligadas a utilizar la Plataforma CASILLA ÚNICA PERÚ, salvo que opten hacerlo voluntariamente o sea dispuesto por ley. Asimismo, las notificaciones electrónicas efectuadas por dichas entidades se regulan conforme lo establece la norma con rango de ley que la habilita.

58.7 Las comunicaciones y/o solicitudes sobre procedimientos enmarcados en los contratos de Asociación Público - Privada son notificadas bajo la modalidad prevista en ellos; salvo que, en el marco de dichos contratos, las partes acuerden utilizar la Plataforma CASILLA ÚNICA PERÚ u otra modalidad que así estimen conveniente.

CAPÍTULO VI
NOTIFICACIÓN DIGITAL

Artículo 59. Notificación digital

59.1 Es aquella modalidad de notificación electrónica que es efectuada a la casilla única electrónica del ciudadano o persona en general para la notificación de actos administrativos, así como actuaciones emitidas en el marco de cualquier actividad administrativa, en concordancia con lo establecido en el artículo 20 del TUO de la Ley Nº 27444, y de lo dispuesto en la Tercera Disposición Complementaria Final de la Ley Nº 30229, Ley que adecúa el Uso de las Tecnologías de Información y Comunicaciones en el Sistema de Remates Judiciales y en los servicios de notificaciones de las resoluciones judiciales, y que modifica la Ley Orgánica del Poder Judicial, el Código Procesal Civil, el Código Procesal Constitucional y la Ley Procesal del Trabajo.

59.2 Las notificaciones digitales se realizan de manera obligatoria a la casilla única electrónica del ciudadano o persona en general, sin requerir su consentimiento o autorización expresa. Excepcionalmente, y sólo en caso de que una notificación no se pueda realizar de manera digital, se realiza en forma física, atendiendo lo establecido en el artículo 20 del TUO de la Ley Nº 27444.

59.3 La notificación digital puede ser remitida a la casilla única electrónica de un tercero, siempre que el ciudadano o persona en general lo haya autorizado expresamente al inicio o durante del procedimiento. La autorización a la que se refiere el presente numeral se realiza por cada procedimiento del cual sea parte el ciudadano o persona en general, siendo válida únicamente durante dicho procedimiento y en tanto no se comunique su variación. La autorización, así como el término o cambio de este se realiza de acuerdo con los formularios que se implementen para tal fin a través de la Plataforma CASILLA ÚNICA PERÚ.

59.4 Las notificaciones digitales tienen la misma validez y eficacia jurídica que las notificaciones realizadas por medios físicos tradicionales, para lo cual cumplen con las siguientes exigencias: oportunidad, suficiencia y debido procedimiento. La notificación digital efectuada forma parte del expediente electrónico.

59.5 Las notificaciones digitales permiten comprobar su depósito en el buzón electrónico de la casilla única electrónica, el cual contiene datos referidos a: la propia notificación, a la fecha del depósito, a quien la recibe y al contexto tecnológico utilizado.

59.6 Las notificaciones digitales se realizan en día y hora hábil conforme a lo establecido en el numeral 18.1 del artículo 18 del TUO de la Ley Nº 27444. La notificación digital se considera efectuada y surte efectos al día hábil siguiente a la fecha de su depósito en la casilla única electrónica. Las entidades depositan una copia del documento en el que consta el acto administrativo o actos de administración generados durante el procedimiento en el buzón de notificaciones de la casilla única electrónica. En caso la notificación digital se realice en día u hora inhábiles ésta surte efecto al primer día hábil siguiente a la fecha de su depósito en la casilla única electrónica.

59.7 El cómputo de los plazos expresados en días se inicia a partir del día hábil siguiente de aquel en que la notificación vía casilla única electrónica se considera efectuada, salvo que se señale una fecha posterior en el mismo acto notificado, en cuyo caso el cómputo de plazos es iniciado a partir de esta última.

Artículo 60. Dispensa de la notificación digital

60.1 La entidad queda dispensada de efectuar una notificación digital si y solo sí permite que el ciudadano o persona en general tome conocimiento del acto respectivo mediante el acceso directo y espontáneo a una copia de su expediente electrónico en su sede digital, dejando evidencia y constancia de esta situación en el referido expediente.

60.2 El ciudadano o persona en general accede a la documentación del expediente electrónico o acto que haya sido emitido por la entidad pudiendo descargarlo.

Artículo 61. Régimen de la notificación digital

61.1 Cuando una notificación digital tiene un único destinatario se realiza a la casilla única electrónica del mismo.

61.2 Cuando sean varios los destinatarios de una notificación digital, el acto es notificado a la casilla única electrónica de cada destinatario, salvo sí actúan bajo una misma representación o si han elegido la casilla única electrónica de uno de los destinatarios, en cuyo caso se remite la notificación a dicha casilla.

Artículo 62. Obligaciones de los titulares de la casilla única electrónica

Los ciudadanos y personas en general son los titulares de la casilla única electrónica, y tienen las siguientes obligaciones:

a) Revisar frecuentemente la casilla única electrónica asignada, a efectos de tomar conocimiento de los actos administrativos y actuaciones administrativas que se le notifique.

b) Adoptar las medidas de seguridad en el uso de la casilla única electrónica que se le asigne.

c) Informar a la Secretaría de Gobierno Digital el fin o cese de la delegación del acceso de terceros a la casilla única electrónica asignada conforme a lo establecido en el numeral 57.3 del presente Reglamento.

d) Informar a la Secretaría de Gobierno Digital el cese de la autorización para la remisión de la notificación digital a la casilla única electrónica de un tercero conforme a lo establecido en el numeral 59.3 del presente Reglamento.

e) Cumplir las condiciones establecidas y normas emitidas por la Secretaría de Gobierno Digital para el uso de la casilla única electrónica.

CAPÍTULO VII
REUNIÓN DIGITAL

Artículo 63. Reuniones digitales

63.1 Las reuniones que lleven a cabo los funcionarios o servidores públicos con los ciudadanos, personas en general u otros funcionarios o servidores públicos, pueden realizarse de manera no presencial, utilizando tecnologías digitales tales como las videoconferencias, audioconferencias, teleconferencias o similares.

63.2 Las entidades de la Administración pública realizan las coordinaciones correspondientes para confirmar la identidad de las personas que participan en una reunión digital, la disponibilidad de tecnologías digitales, el tipo de reunión a realizar y las condiciones o supuestos previstos conforme al ordenamiento jurídico.

Artículo 64. Reunión digital en el marco del procedimiento administrativo

64.1 Las reuniones digitales pueden ser aplicadas en las sesiones o asambleas de órganos colegiados, audiencias como medio de prueba o actividades de fiscalización que realicen las entidades públicas conforme a lo establecido en los artículos 109, 177 y numeral 240.2 del artículo 240 del TUO de la Ley Nº 27444 respectivamente, garantizando el principio del debido procedimiento.

64.2 Las partes adoptan las medidas pertinentes para contar con los equipos y condiciones necesarias para la realización de las sesiones, asambleas, audiencias o actividades de fiscalización cuando se realicen a través de reuniones digitales. Las reuniones digitales pueden ser grabadas para posterior revisión, evidencia o en cumplimiento del marco normativo del procedimiento administrativo. Asimismo, cuando corresponda se debe comunicar al ciudadano dicha grabación atendiendo lo establecido en la Ley Nº 27933, Ley de Protección de Datos Personales y su Reglamento.

Artículo 65. Acta de reunión digital

65.1 Las actas o acuerdos emitidos como resultado de una reunión digital, en el marco de actividades de coordinación entre entidades de la Administración pública, pueden ser generados como documentos electrónicos firmados con alguna modalidad de firma electrónica establecida en la Ley Nº 27269, Ley de Firmas y Certificados Digitales. Las entidades de la Administración pública participantes acuerdan la modalidad de firma a utilizar.

65.2 Las actas o acuerdos emitidos como resultado de una reunión digital a cargo de una entidad de la administración pública, en el marco de un procedimiento administrativo, pueden ser generados como documentos electrónicos firmados conforme a lo siguiente:

a) Acta de reunión firmada por el funcionario, esta se cumple con la firma digital del funcionario más un sello de tiempo, generados en el marco de la IOFE.

b) Acta de reunión firmada por las partes, esta se cumple utilizando la firma digital de las partes, generada en el marco de la IOFE, o alguna modalidad de firma electrónica distinta a la firma digital, de conformidad con la Cuarta Disposición Complementaria Final del Decreto Supremo Nº 026-2016-PCM, que aprueba medidas para el fortalecimiento de la Infraestructura Oficial de Firma Electrónica y la implementación progresiva de la firma digital en el sector público y privado.

TÍTULO V
DATOS

CAPÍTULO I
MARCO DE GOBERNANZA Y GESTIÓN DE DATOS DEL ESTADO PERUANO

Artículo 66. Marco de Gobernanza y Gestión de Datos del Estado Peruano

66.1 El Marco de Gobernanza y Gestión de Datos del Estado Peruano es dirigido, supervisado y evaluado por la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, en su calidad de ente rector en gobierno de datos, que emite lineamientos, especificaciones, guías, directivas, normas técnicas y estándares para la aplicación de la gobernanza y gestión de datos por parte de las entidades de la Administración Pública a fin de garantizar un nivel básico y aceptable para la recopilación, producción, procesamiento, analítica, publicación, almacenamiento, distribución y puesta a disposición de los datos gubernamentales, haciendo uso de tecnologías digitales y emergentes.

66.2 El Marco de Gobernanza y Gestión de Datos del Estado Peruano y sus normas de desarrollo, son revisadas y aplicadas en la implementación de iniciativas de gobierno digital y prestación de servicios digitales brindados a los ciudadanos y personas en general, salvo aquellos datos que se rijan por norma expresa.

66.3 El Marco de Gobernanza y Gestión de Datos del Estado Peruano comprende los siguientes niveles:

a) Gobernanza y gestión de datos del Estado Peruano.
b) Gestión de datos sectoriales.
c) Gestión de datos institucionales.

Artículo 67. Principios específicos del Marco de Gobernanza y Gestión de Datos

La aplicación del Marco de Gobernanza y Gestión de Datos se desarrolla de acuerdo con los principios rectores establecidos en el artículo 5 de la Ley, y con los siguientes principios específicos:

a) Liderazgo y estrategia. El liderazgo y compromiso de la alta dirección en la gobernanza de datos orienta al uso eficiente de datos para el cumplimiento de los objetivos institucionales.

b) Valoración de datos. Se reconoce a los datos gubernamentales como un activo estratégico para la toma efectiva de decisiones, atención oportuna de solicitudes de información y prestación de servicios.

c) Cultura de datos. Se promueve una cultura impulsada por datos para la toma de decisiones estratégicas basadas en la interpretación, recopilación, organización y análisis de los datos para generar valor público para los ciudadanos.

d) Responsabilidad de todos. La gestión de datos gubernamentales es una responsabilidad compartida entre los propietarios de los datos y los responsables de la recopilación, procesamiento, almacenamiento y distribución.

e) Cumplimiento y riesgo. Los datos gubernamentales son cuidadosamente gestionados como cualquier otro activo, asegurando su protección, seguridad, privacidad, calidad, estandarización, uso apropiado y cumplimiento regulatorio.

f) Calidad de datos. Los datos gubernamentales preservan características de exactitud, actualización y completitud fundamentales para satisfacer las necesidades de digitalización y despliegue del gobierno digital.

Artículo 68. Roles para la gobernanza y gestión de datos

68.1 El Comité de Gobierno Digital es el responsable de la gobernanza y uso estratégico de los datos en la entidad, estableciendo las políticas y directrices

institucionales en la materia, en cumplimiento de los lineamientos y normas emitidas por la Secretaría de Gobierno Digital. Asimismo, el Comité impulsa una cultura basada en datos e iniciativas que aseguren la calidad, uso adecuado e interoperabilidad de los datos.

68.2 El Oficial de Gobierno de Datos es el rol responsable de asegurar el uso ético de las tecnologías digitales y datos en la entidad pública, proponer iniciativas de innovación basadas en datos, fomentar una cultura basada en datos, articular y gestionar el uso de datos gubernamentales, y asegurar la calidad e integridad de datos que contribuya a la creación de valor público. Asimismo, es responsable impulsar y coordinar el modelamiento, procesamiento, análisis y desarrollo de servicios de información de datos gubernamentales y datos abiertos con los responsables de los procesos correspondientes, así como de coordinar la implementación del Modelo de Referencia de Datos de la entidad.

68.3 El Oficial de Gobierno de Datos reporta al Comité de Gobierno Digital institucional y, a la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros la implementación y aplicación de las normas en materia de gobernanza y gestión de datos.

68.4 La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, emite el perfil y responsabilidades del Oficial de Gobierno de Datos en la Administración Pública. El titular de la entidad designa al Oficial de Gobierno de Datos institucional y comunica a la Secretaría de Gobierno Digital dicha designación.

68.5 Los dueños de los procesos o en su defecto los responsables de las unidades de organización de la entidad son los propietarios de los datos que están bajo su responsabilidad, en cumplimiento de sus funciones o responsabilidades, y se encargan de cumplir con la regulación y los estándares de calidad que les aplican, así como coordinar con el Oficial de Gobierno de Datos toda iniciativa de mejora en su proceso basada en datos.

68.6 El Oficial de Datos Personales es el rol responsable de velar por el cumplimiento de las normas en materia de protección de datos personales en su entidad. Dicho rol es ejercido por un funcionario o servidor público designado por la máxima autoridad administrativa de la entidad, el mismo que puede recaer en el titular de la oficina de asesoría jurídica de la entidad o en el titular de la oficina de tecnologías de la información de la misma, o quienes hagan sus veces. El Oficial de Datos Personales actúa como enlace con la Autoridad Nacional de Protección de Datos Personales, coopera y sigue los lineamientos y directivas que emita dicha Autoridad en los ámbitos de su competencia, así como aquellos establecidos en el Decreto de Urgencia Nº 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento. Su designación se realiza en un plazo máximo diez (10) días hábiles posterior a la publicación del presente Reglamento y se comunica de manera inmediata a la Autoridad Nacional de Protección de Datos Personales.

CAPÍTULO II
INFRAESTRUCTURA NACIONAL DE DATOS

Artículo 69. Infraestructura Nacional de Datos

69.1 La Infraestructura Nacional de Datos comprende el conjunto articulado de políticas, normas, medidas, procesos, tecnologías digitales, datos gubernamentales, repositorios y bases de datos destinadas a promover la adecuada recopilación, producción, procesamiento, analítica, publicación, almacenamiento, distribución y puesta a disposición de los datos que gestionan las entidades de la Administración Pública, así como el Marco de Gobernanza y Gestión de Datos y Estrategia Nacional de Datos que siguen las mismas. La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, en su calidad de ente rector en gobierno de datos, es responsable de la gobernanza y gestión de la Infraestructura Nacional de Datos, y en el ejercicio de su rectoría establece relaciones de coordinación con los actores correspondientes, conforme a la normatividad vigente en materia de protección de datos personales.

69.2 La Infraestructura Nacional de Datos comprende los siguientes ámbitos:

a) **Estadística**, a cargo del Instituto Nacional de Estadística e Informática (INEI) quien orienta, promueve y conduce la producción estadística oficial.

b) **Espacial o Georreferenciada**, a cargo de la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, quien orienta, promueve y coordina el intercambio y uso de datos y servicios de información espacial o georreferenciada.

c) **Privados o Personales**, a cargo del Ministerio de Justicia y Derechos Humanos (MINJUSDH), a través de la Autoridad Nacional de Protección de Datos Personales, la que orienta, promueve y conduce la materia de protección de datos personales.

d) **Datos Abiertos**, a cargo de la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, quien orienta, norma, promueve y conduce la materia de datos abiertos.

69.3 La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, amplía los ámbitos establecidos en el numeral precedente en función de la necesidad pública, cambio tecnológico, importancia estratégica o normativa expresa que lo demande; la misma que se hace efectiva mediante Resolución de Secretaría de Gobierno Digital. Asimismo, en coordinación con los actores competentes desarrolla las normas complementarias para la adecuada gobernanza y gestión de datos gubernamentales.

Artículo 70. Datos gubernamentales

70.1 Los datos gubernamentales son aquellos datos que las entidades públicas recopilan, producen, procesan, analizan, publican, almacenan, distribuyen y ponen a disposición en el ejercicio de sus funciones y cuando corresponda atendiendo las normas en materia de transparencia, datos personales y datos abiertos. Los datos gubernamentales se organizan en datos maestros y datos complementarios.

70.2 Los datos maestros son un conjunto organizado de datos gubernamentales que representan objetos o elementos claves de las entidades, son utilizados en el ejercicio de sus funciones, procesos o prestación de servicios, están vinculados con su misión y procesos misionales, y tienen asignado un identificador único.

70.3 Los datos complementarios son aquellos que en conjunto con los datos maestros describen los elementos que las entidades públicas utilizan en el ejercicio de sus funciones, procesos o prestación de servicios.

70.4 Las entidades públicas identifican y mantienen sus datos maestros, sus atributos y relaciones, y desarrollan un modelo de referencia de datos; dicho modelo se basa en estándares internacionales reconocidos, vocabularios y términos descriptivos que le dan contexto y facilitan su intercambio, interpretación y reutilización.

Artículo 71. Plataforma Nacional de Datos abiertos

71.1 Las entidades de la Administración Pública publican datos gubernamentales producidos, procesados, almacenados y/o recolectados en plataformas digitales, cuya publicidad no se encuentre excluida por normas específicas en materia de transparencia, en formatos abiertos en la Plataforma Nacional de Datos Abiertos, priorizando aquellos que son de interés nacional o estratégicos para la implementación de políticas de Estado y políticas de gobierno. Para ello la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, coordina con los ministerios rectores de los sectores dicha priorización y publicación obligatoria.

71.2 Las entidades de la Administración Pública implementan mecanismos que permitan que los datos publicados en la Plataforma Nacional de Datos Abiertos sean legibles por las personas y procesables por máquina, conforme a los lineamientos que emita la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros.

71.3 Las entidades de la Administración Pública aplican herramientas o técnicas de disociación y anonimización de datos personales u otra información que se encuentre excluida por la normativa de transparencia conforme a la normatividad vigente en materia de datos personales, antes de su publicación en la Plataforma Nacional de Datos Abiertos, y cuando corresponda.

71.4 Mediante Resolución de Secretaría de Gobierno Digital se puede disponer la publicación de datos abiertos por parte de las entidades de la Administración Pública para fines de investigación científica, seguridad ciudadana, estadísticas demográficas, educación, diseño de políticas públicas, investigación en salud, iniciativas de gobierno digital, productividad y competitividad, transporte inteligente, análisis económico, comercio o situaciones de emergencia. Asimismo, la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, aprueba la Estrategia Nacional de Datos Abiertos.

Artículo 72. Identificadores únicos fundamentales

72.1 Los identificadores únicos fundamentales son un conjunto de códigos o números que permiten distinguir un objeto o elemento de otros, con características y atributos comunes, en el entorno digital. Son de carácter estratégico y transversal, para facilitar la interoperabilidad y estandarización en la Administración pública.

72.2 Se establecen como identificadores únicos fundamentales para la prestación de servicios digitales o trámites, cuando correspondan, los siguientes:

a) Código Único de Identificación de personas naturales, a cargo del RENIEC.

b) Código Único de Identificación de extranjeros, a cargo de MIGRACIONES.

c) Número de Partida Registral de personas jurídicas y Número de la placa única nacional de rodaje del vehículo, a cargo de la Superintendencia Nacional de Registros Públicos (SUNARP).

d) Código de ubicación geográfica (UBIGEO), Clasificador de Actividades Económicas, Código de Ocupaciones y Código de Carreras e Instituciones Educativas de Educación Superior y Técnico Productivas, Clasificador Nacional de Programas e Instituciones de Educación Superior Universitaria, Pedagógica, Tecnológica y Técnico Productiva, a cargo del Instituto Nacional de Estadística e Informática (INEI).

72.3 Las entidades a cargo de los identificadores únicos fundamentales establecen las normas de gestión de estos. Asimismo, aseguran la interoperabilidad entre ellos con la finalidad de prestar servicios digitales centrados en la persona.

72.4 La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, emite las normas para la adopción de los identificadores únicos fundamentales por parte de las entidades de la Administración Pública, y amplía los establecidos en el numeral 72.2 precedente, en función de la necesidad pública, importancia estratégica o normativa expresa que lo demande.

Artículo 73. Vocabularios

73.1 Los vocabularios son grupos de datos que permiten unificar la interpretación y el significado de un objeto o elemento para hacer posible la interoperabilidad entre sistemas de información.

73.2 Los vocabularios básicos para la prestación de servicios digitales son los relativos a: persona natural, persona jurídica, vehículo, predio y trámite. La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, mediante Resolución de Secretaría de Gobierno Digital amplía los vocabularios básicos.

73.3 Los vocabularios forman parte del Modelo de Referencia de Datos establecido en el numeral 118.2 del artículo 118 del presente Reglamento.

Artículo 74. Perfil mínimo de metadatos

La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, en coordinación con los responsables de los ámbitos de la Infraestructura Nacional de Datos establece los perfiles mínimos de metadatos en cada uno de sus ámbitos, para asegurar el entendimiento de los datos y garantizar su disponibilidad, accesibilidad, conservación, integración e interoperabilidad.

Artículo 75. Lineamientos para la calidad, uso y aprovechamiento de datos gubernamentales

La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, emite los lineamientos, procedimientos, estándares y estrategias para asegurar la calidad, uso adecuado y aprovechamiento de datos gubernamentales en materia de ciencia de datos, inteligencia artificial, registros distribuidos u otras tecnologías.

Artículo 76. Datos para la producción estadística digital

76.1 Toda entidad pública que disponga de datos gubernamentales sistematizados y digitalizados los publica como datos o conjunto de datos abiertos, a través de la Plataforma Nacional de Datos Abiertos, para fines de producción estadística oficial por parte del Instituto Nacional de Estadística e Informática.

76.2 El Instituto Nacional de Estadística e Informática en función de sus capacidades y recursos realiza actividades estadísticas oficiales a través de Internet; para tal fin puede utilizar los bloques básicos para la interoperabilidad técnica establecidos en el artículo 87 del presente Reglamento, cuando corresponda.

CAPÍTULO III
DATOS GEORREFERENCIADOS

Artículo 77. Plataforma Nacional de Datos Georreferenciados

77.1 Créase la Plataforma Nacional de Datos Georreferenciados, denominada GEOPERÚ, como la plataforma digital única de integración de datos espaciales o georreferenciados y estadísticos, que armoniza las bases de datos de las entidades de la Administración Pública, para el análisis de datos y la toma de decisiones con enfoque territorial. GEOPERÚ es administrada por la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, bajo el dominio www.geoperu.gob.pe.

77.2 GEOPERÚ contiene categorías de información relacionadas, de manera no limitativa, a la cartografía, infraestructura, pobreza, proyectos de inversión pública, programas sociales, salud, educación, economía, agrario, turismo, cultural, ambiental, conflictos sociales, y violencia de género del país. Puede ser usado como plataforma de geovisualización e incorporación de datos georreferenciados para entidades que no posean herramientas.

77.3 Las entidades de la Administración Pública comparten y/o publican datos georreferenciados y servicios de información georreferenciada en la Plataforma GEOPERÚ a fin de garantizar la disponibilidad de los datos necesarios para la toma de decisiones estratégicas. La Secretaría de Gobierno Digital emite los lineamientos para la gestión de la Plataforma GEOPERU y articula esfuerzos con el sector privado, la sociedad civil y la academia para la utilización de la información georreferenciada en beneficio del país.

Artículo 78. Catálogo Nacional de Metadatos Espaciales

78.1 Créase el Catálogo Nacional de Metadatos Espaciales para la búsqueda, evaluación y acceso a los datos, servicios y aplicaciones espaciales producidos y mantenidos por las entidades de la Administración Pública. Es parte de la Infraestructura Nacional de Datos Espaciales del Perú (IDEP) y es administrado por la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital.

78.2 Las entidades de la Administración Pública registran los metadatos de sus servicios de información espacial o georreferenciada en el Catálogo Nacional de

Metadatos Espaciales. La Secretaría de Gobierno Digital emite los lineamientos para la gestión de metadatos de los servicios de información espacial o georreferenciada.

78.3 Las entidades de la Administración Pública verifican en el Catálogo Nacional de Metadatos Espaciales la existencia de algún tipo de información georreferenciada disponible antes de crear un servicio de información espacial o georreferenciado, o para su reutilización en el desarrollo de nuevos productos espaciales o georreferenciados.

78.4 Asimismo, las entidades son responsables de asegurar la disponibilidad, continuidad y funcionamiento de los servicios de información espacial o georreferenciada que son de su competencia.

TÍTULO VI
INTEROPERABILIDAD

CAPÍTULO I
MARCO DE INTEROPERABILIDAD DEL ESTADO PERUANO

Artículo 79. Marco de Interoperabilidad del Estado Peruano

79.1 El Marco de Interoperabilidad del Estado Peruano es dirigido, supervisado y evaluado por la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, en su calidad de ente rector de la interoperabilidad, que emite políticas, lineamientos, especificaciones, guías, directivas, normas técnicas y estándares para su aplicación por parte de las entidades de la Administración Pública a fin de garantizar la interoperabilidad de los procesos y sistemas de información en los ámbitos correspondientes.

79.2 El Marco de Interoperabilidad del Estado Peruano y sus normas de desarrollo, son revisadas y aplicadas en la utilización, implementación y prestación de servicios digitales brindados a los ciudadanos y personas en general.

79.3 El Marco de Interoperabilidad del Estado Peruano comprende la gestión de la interoperabilidad en la interacción entre procesos y sistemas de información de las entidades de la Administración Pública.

Artículo 80. Principios específicos del Marco de Interoperabilidad del Estado Peruano

La aplicación del Marco de Interoperabilidad del Estado Peruano se desarrolla de acuerdo con los principios rectores establecidos en el artículo 5 de la Ley, y con los siguientes principios específicos:

a) **Cooperación y colaboración.** Se promueve la cooperación y colaboración para intercambiar y compartir datos, información, experiencias y recursos a fin de diseñar, implementar y desplegar servicios digitales que permitan alcanzar el bienestar de las personas y el desarrollo sostenible del país.

b) **Reutilización**. Se promueve la reutilización de datos, información, conocimiento y recursos existentes, evitando duplicar esfuerzos, y permitiendo ahorrar tiempo y dinero.

c) **Interoperabilidad desde el diseño.** Los sistemas de información que soportan servicios digitales se diseñan atendiendo los objetivos acordados, los requisitos de interoperabilidad y la posible reutilización de datos y servicios.

d) **Seguridad.** El intercambio de datos, información y recursos entre las entidades de la Administración Pública no afecta su integridad, disponibilidad o confidencialidad.

e) **Apertura**. Asegurar y dar preferencia al uso de software público o de código abierto, así como al uso de estándares abiertos para el diseño y construcción de los sistemas de información.

f) **Enfoque participativo.** No se restringe la participación de ninguna entidad de la Administración Pública para el consumo y publicación de los servicios de información disponibles, salvo excepciones establecidas por norma expresa.

g) **Independencia tecnológica.** Los sistemas de información de las entidades de la Administración Pública se comunican entre sí, independientemente de la plataforma y arquitectura tecnológica en las que fueron implementados.

Artículo 81. Modelo de Interoperabilidad del Estado Peruano

81.1 El Modelo de Interoperabilidad es la representación holística y sistémica de los componentes que comprende el Marco de Interoperabilidad del Estado Peruano, aplicable a todos los sistemas de información de las entidades de la Administración Pública que interoperan entre ellos, atendiendo los principios establecidos en el artículo 80 del presente Reglamento y aquellos establecidos en la Ley.

81.2 El Modelo de Interoperabilidad del Estado Peruano comprende los siguientes componentes:

a) Principios.
b) Procesos de la interoperabilidad.
c) Niveles para la interoperabilidad.
d) Bloques básicos para la interoperabilidad técnica.
e) Servicios digitales conforme a lo establecido en el Título III.
f) Entidades de la Administración pública.
g) Ciudadanos y personas en general.

CAPÍTULO II
GESTIÓN DEL MARCO DE INTEROPERABILIDAD DEL ESTADO PERUANO

Artículo 82. Gestión del Marco de Interoperabilidad del Estado peruano

La gestión del Marco de Interoperabilidad del Estado Peruano comprende los niveles o perspectivas establecidas en el artículo 28 de la Ley, los cuales se consideran en el diseño de un servicio digital.

Artículo 83. Interoperabilidad a nivel Legal

83.1 Las entidades públicas a solicitud de la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros informan el avance de cumplimiento de las políticas de Estado, políticas de gobierno en materia digital y de interoperabilidad.

83.2 Las iniciativas o acciones de interoperabilidad que promuevan las entidades públicas son realizadas en cumplimiento del Marco de Interoperabilidad del Estado Peruano y normas específicas sobre la materia.

83.3 La Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros evalúa y propone acuerdos de interoperabilidad transfronteriza en materia de gobierno digital.

Artículo 84. Interoperabilidad a nivel Organizacional

84.1 Las entidades públicas articulan sus planes y demás instrumentos de gestión con las políticas de Estado y de gobierno en materia digital, de manera que aseguren la implementación y mantenimiento de servicios digitales accesibles, seguros e interoperables.

84.2 Las entidades públicas cuentan con una estructura organizacional y procesos que les permita desarrollar y mantener capacidades para interoperar y reutilizar servicios de información, software u otros recursos.

84.3 Las entidades públicas identifican al dueño del proceso, órgano o unidad orgánica responsable de asegurar la exactitud, actualización y completitud de los datos provistos a través de servicios de información.

84.4 Las entidades proveedoras de servicios de información establecen y suscriben las condiciones de acceso y uso de sus servicios con la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros, en base a los instrumentos, procedimientos y mecanismos definidos para dicho fin.

84.5 Las entidades consumidoras solicitan el acceso y uso de servicios de información a la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros, en base a los instrumentos, procedimientos y mecanismos definidos por ésta.

Artículo 85. Interoperabilidad a nivel Semántico

85.1 Los vocabularios a los que hace referencia el artículo 73 del presente Reglamento, son instrumentos para ser usados por todas las entidades públicas en el diseño de sus sistemas de información, bases de datos, formatos electrónicos o iniciativas de interoperabilidad. Estos vocabularios son simples, reutilizables y extensibles.

85.2 Las entidades públicas extienden los vocabularios básicos con los datos maestros y complementarios que resulten necesarios para crear formatos electrónicos destinados al intercambio de datos e información con propósitos específicos, en base a los lineamientos que defina la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros, y conforme a lo siguiente:

a) Los Ministerios en coordinación con sus organismos públicos, programas y proyectos elaboran y mantienen vocabularios extendidos que resulten necesarios para la interoperabilidad en su sector y con otros sectores.

b) Los Organismos Constitucionales Autónomos elaboran vocabularios extendidos que resulten necesarios para la adecuada prestación de servicios digitales e interoperabilidad con otras entidades públicas.

c) Los Gobiernos Regionales elaboran vocabularios extendidos que resulten necesarios para la adecuada prestación de servicios digitales en su ámbito territorial; sin perjuicio de ello pueden reutilizar algún otro vocabulario desarrollado.

d) Las demás entidades en función de sus necesidades y contexto elaboran y mantienen vocabularios extendidos para la adecuada prestación de servicios digitales.

85.3 La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, asigna a cada entidad de la Administración Pública, y a todo aquello que requiera ser distinguido, un identificador de objetos (OID) que permita asegurar la interoperabilidad en el Estado Peruano.

Artículo 86. Interoperabilidad a nivel Técnico

86.1 Las entidades públicas utilizan obligatoriamente estándares técnicos abiertos, y excepcionalmente y de forma complementaria, estándares técnicos no abiertos en aquellas circunstancias en las que no se disponga de un estándar técnico abierto que satisfaga la funcionalidad necesaria, y sólo mientras dicha disponibilidad no se produzca.

86.2 La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, en coordinación con las entidades de la Administración Pública promueven las actividades de adopción y normalización con el fin de facilitar la disponibilidad de los estándares técnicos abiertos relevantes para sus necesidades.

86.3 Los criterios para la determinación de un estándar técnico abierto son:

a) Ser mantenido por una organización sin fines de lucro.

b) Haber sido desarrollado dentro de un proceso inclusivo y abierto a todas las partes interesadas.

c) Estar disponible de forma gratuita o a un costo mínimo.

d) No estar sujeto a ningún tipo de pago o tasa, por derechos de propiedad intelectual u otros.

e) Tener múltiples implementaciones, sin favorecer o proveer derechos exclusivos a un vendedor particular o a una marca específica.

86.4 La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, administra y mantiene un Catálogo de Estándares Abiertos que contiene una relación de estándares técnicos para facilitar la interoperabilidad de datos, aplicativos y servicios digitales en el Estado Peruano.

86.5 Los bloques básicos para la interoperabilidad técnica son recursos tecnológicos que forman parte del Marco de Interoperabilidad del Estado Peruano.

Artículo 87. Bloques básicos para la Interoperabilidad técnica

87.1 Son aquellos recursos tecnológicos reutilizables que permiten la definición, diseño, desarrollo y prestación de servicios digitales de forma eficiente, efectiva y colaborativa.

87.2 Los bloques básicos para la interoperabilidad técnica son:

a) Plataforma de Interoperabilidad del Estado (PIDE).

b) Plataforma de Pagos Digitales del Estado Peruano (PÁGALO.PE).

c) Plataforma Nacional de Identificación y Autenticación de la Identidad Digital (ID GOB.PE), creada en el artículo 14 del Título II del presente Reglamento.

d) Plataforma Casilla Única Electrónica del Estado Peruano (CASILLA ÚNICA PERÚ), creada en el artículo 58 del Título IV del presente Reglamento.

e) Plataforma Única de Recepción Documental del Estado Peruano (MESA DIGITAL PERÚ), creada en el artículo 46 del Título IV del presente Reglamento.

f) Plataforma Nacional de Software Público Peruano (PSPP).

g) Plataforma Nacional de Firma Digital (FIRMA PERÚ).

h) Infraestructura Tecnológica y Plataforma como Servicio (NUBE PERÚ).

87.3 Las entidades públicas utilizan de manera obligatoria los bloques básicos para la interoperabilidad técnica en el diseño, construcción y prestación de sus servicios digitales, así como en el desarrollo de sus procesos o procedimientos de gestión interna y actuaciones administrativas provistas a través de Internet, Extranet o Intranet, según corresponda.

87.4 El uso de los bloques básicos para la interoperabilidad técnica por parte de las entidades públicas no requiere la suscripción de convenios de colaboración o similares con las entidades a cargo de un determinado bloque. La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, aprueba los instrumentos, acuerdos de nivel de servicio, procedimientos y disposiciones para el uso de los bloques básicos para la interoperabilidad técnica.

87.5 Las entidades a cargo de un determinado bloque básico para la interoperabilidad técnica están obligadas a ponerlos a disposición de todas las entidades de la Administración pública conforme a los instrumentos aprobados por la Secretaría de Gobierno Digital para su uso, sin requerir la suscripción de un convenio de colaboración o documento similar. Asimismo, las referidas entidades suscriben con la Secretaría de Gobierno Digital un acuerdo de nivel de servicio sobre las capacidades de disponibilidad, escalabilidad y seguridad del bloque a su cargo.

87.6 La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, amplía los bloques básicos para la interoperabilidad técnica establecidos en el numeral 87.2 en función de la necesidad pública, cambio tecnológico, importancia estratégica o normativa expresa que lo demande; la misma que se hace efectiva mediante Resolución de Secretaría de Gobierno Digital.

Artículo 88. Plataforma de Interoperabilidad del Estado

88.1 La Plataforma de Interoperabilidad del Estado (PIDE) es una infraestructura tecnológica que facilita la implementación de servicios digitales en la Administración Pública. Se constituye en la capa de intercambio seguro y verificable de datos entre procesos y sistemas de información de las entidades públicas.

88.2 La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, administra la Plataforma de Interoperabilidad del Estado y establece sus condiciones de uso y mecanismos de integración.

88.3 El intercambio de datos e información a través de la Plataforma de Interoperabilidad del Estado se realiza entre entidades consumidoras y proveedoras de servicios de información, donde:

a) Las entidades proveedoras de servicios de información son aquellas entidades que publican un servicio de información en la PIDE en función de la regulación, acuerdos y necesidades de digitalización o transformación digital del Estado.

b) Las entidades consumidoras de servicios de información son aquellas entidades que consumen un servicio de información de la PIDE como parte de la prestación de un servicio digital.

c) Un servicio de información es aquel que provee datos e información que las entidades públicas gestionan en sus sistemas de información e intercambian a través de la PIDE.

88.4 La Plataforma de Interoperabilidad del Estado integra varios servicios de información publicados en ella, que por su ámbito, contenido o naturaleza resulten necesarios para satisfacer de manera ágil y eficiente las necesidades de las entidades consumidoras de servicios de información.

88.5 La Plataforma de Interoperabilidad del Estado puede proveer infraestructura tecnológica como servicio para la implementación de servicios de información de un determinado sector o grupo de entidades en función de la necesidad pública, importancia estratégica o normativa expresa que lo demande. El uso de la referida plataforma es obligatorio por parte de todas las entidades de la Administración Pública de los tres niveles de gobierno, como mínimo, en el intercambio, orquestación, composición, integración de datos, información o conocimiento entre procesos y sistemas de información de dos o más entidades, quedando prohibido el desarrollo, adquisición, contratación de plataformas similares o equivalentes que tengan el mismo fin a partir de la publicación de la presente norma.

88.6 Los servicios de información publicados en la Plataforma de Interoperabilidad del Estado implementan métodos o interfaces entre aplicaciones, en modalidades síncrona o asíncrona respectivamente, para retornar la información firmada digitalmente utilizando un certificado digital de agente automatizado, observando las disposiciones legales sobre la materia y lo establecido en los estándares aprobados por la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros.

88.7 Todas las entidades públicas que pongan a disposición algún servicio de información, aseguran que en su diseño y desarrollo se hayan implementado las medidas y controles que permitan proteger adecuadamente la seguridad de los datos mediante el uso de protocolos seguros de almacenamiento y comunicación, algoritmos de cifrado estándar y otros aspectos pertinentes, de acuerdo con la normatividad vigente y las buenas prácticas que existen en materia de desarrollo de software, seguridad de la información y protección de datos personales.

88.8 Las entidades de la Administración Pública reutilizan los servicios de información publicados en el Catálogo Nacional de Servicios de Información, creado en el artículo 7 del Decreto Legislativo Nº 1211, Decreto Legislativo que aprueba Medidas para el fortalecimiento e implementación de servicios públicos integrados a través de ventanillas únicas e intercambio de información entre entidades públicas y modificatoria, de la Plataforma de Interoperabilidad del Estado que puedan satisfacer de forma total o parcial las necesidades de digitalización de sus procesos o servicios, o la mejora y actualización de los ya existentes.

88.9 La publicación y consumo de servicios de información se realiza en base a los procedimientos que defina la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros, y las normas vigentes sobre la materia. Las entidades proveedoras de servicios de información suscriben Acuerdos de Nivel de Servicio (ANS) con la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros a fin de garantizar el cumplimiento y disponibilidad del servicio, los cuales son firmados digitalmente. En el caso del consumo de servicios de información las entidades atienden los referidos Acuerdos de Nivel de Servicio.

Artículo 89. Plataforma de Pagos Digitales del Estado Peruano

89.1 La Plataforma de Pagos Digitales del Estado Peruano (PÁGALO.PE) es aquella plataforma digital que permite el pago en línea de los derechos de tramitación, conforme a lo establecido en el artículo 6 del Decreto Legislativo Nº 1246, Decreto Legislativo que aprueba diversas medidas de simplificación administrativa.

89.2 La plataforma de pagos digitales PÁGALO.PE comprende funcionalidades que aseguren su acceso a través de la web y dispositivos móviles de forma nativa; y permitan su integración directa con servicios digitales prestados por las entidades de la Administración Pública.

89.3 El Banco de la Nación administra la plataforma de pagos digitales PÁGALO.PE, establece sus condiciones de uso, mecanismos de arquitectura digital, seguridad digital e integración, y publica datos en formatos abiertos sobre el uso de la plataforma PÁGALO.PE en la Plataforma Nacional de Datos Abiertos. Asimismo, la Secretaría de Gobierno Digital emite las normas y disposiciones con respecto a la adopción de la plataforma PÁGALO.PE por parte de las entidades de la Administración Pública.

89.4 La plataforma de pagos digitales PÁGALO.PE admite cualquier modalidad de pago, incluyendo el dinero electrónico, regulado conforme a lo dispuesto en la Ley Nº 29985, Ley del Dinero Electrónico y normas reglamentarias.

89.5 La plataforma de pagos digitales PÁGALO.PE permite generar un ticket para el pago en efectivo de los derechos de tramitación en cualquier agente corresponsal del Banco de la Nación a nivel nacional, en caso el ciudadano carezca de medios de pago digitales.

89.6 Las entidades públicas pueden hacer uso de otros mecanismos o plataformas de pago digital seguras regulados por la Superintendencia de Banca, Seguros y AFP para el pago de sus derechos de tramitación, de conformidad con la normatividad del Sistema Nacional de Tesorería.

Artículo 90. Plataforma Nacional de Software Público Peruano

90.1 La Plataforma Nacional de Software Público Peruano (PSPP) es la plataforma digital que facilita el acceso y reutilización del Software Público Peruano (SPP), conforme a lo establecido en el Decreto Supremo Nº 051-2018-PCM, Decreto Supremo que crea el Portal de Software Público Peruano y establece disposiciones adicionales sobre el Software Público Peruano y normas complementarias.

90.2 El Catálogo de Software Público Peruano permite buscar, acceder y evaluar un SPP para su reutilización por parte de las entidades públicas, y es mantenido por la Presidencia del Consejo Ministros, a través de la Secretaría de Gobierno Digital.

90.3 Las entidades de la Administración Pública reutilizan los SPP disponibles en el Catálogo de Software Público Peruano que puedan satisfacer de forma total o parcial las necesidades de digitalización de sus procesos o servicios, o la mejora y actualización de los ya existentes.

90.4 La publicación y reutilización de software público peruano a través del PSPP se realiza entre entidades proveedoras y consumidoras de software público, donde:

a) **Entidades proveedoras de software público.** Son aquellas entidades que publican un software en la PSPP en función de la regulación y necesidades de digitalización o transformación digital del Estado. Son responsables de mantener actualizado la información de los SPP registrados en el Catálogo de Software Público.

b) **Entidades consumidoras de software público.** Son aquellas entidades que consumen un software de la PSPP como parte de la prestación de un servicio digital o mejoras en su gestión interna.

90.5 La publicación y/o reutilización de software público peruano por parte de las entidades públicas no requiere la suscripción de convenios de colaboración o similares con las entidades titulares de los mismos, y se realiza en base a los procedimientos establecidos

por la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros y las normas vigentes sobre la materia.

Artículo 91. Plataforma Nacional de Firma Digital

91.1 Créase la Plataforma Nacional de Firma Digital (FIRMA PERÚ) como la plataforma digital que permite la creación y validación de firmas digitales dentro del marco de la IOFE, para la provisión de los servicios digitales prestados por las entidades de la Administración Pública.

91.2 La Plataforma FIRMA PERÚ está conformada por los softwares acreditados de creación y validación de firmas digitales desarrollados o de titularidad de las entidades públicas en el marco de la Infraestructura Oficial de Firma Electrónica (IOFE). La Secretaría de Gobierno Digital establece el listado de softwares que conforman la Plataforma FIRMA PERÚ, los cuales son puestos a disposición por las entidades públicas correspondientes, sin necesidad de suscribir un convenio o similar, de conformidad con lo dispuesto en el artículo 29 de la Ley. Dichas entidades son responsables de asegurar la disponibilidad de los referidos softwares.

91.3 La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, amplía la lista de software que conforman la Plataforma FIRMA PERÚ en función de la necesidad o avance tecnológico, la misma que se hace efectiva mediante Resolución de Secretaría de Gobierno Digital.

91.4 La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, establece las condiciones de uso, instrumentos, procedimientos, protocolos de integración y gestión de indicadores de la Plataforma FIRMA PERÚ; así como también emite las normas y disposiciones con respecto a la adopción progresiva de la Plataforma FIRMA PERÚ y el uso de la firma digital por parte de las entidades de la Administración Pública.

Artículo 92. Infraestructura tecnológica y plataforma como servicio

92.1 La infraestructura tecnológica y plataforma tecnológica como servicio (NUBE PERÚ) habilita el acceso a un conjunto de recursos computacionales compartidos (dispositivos de red, servidores y almacenamiento, software) de forma segura, bajo demanda y a través de Internet. Los recursos son adquiridos y liberados con un esfuerzo administrativo exiguo o mínima interacción con el proveedor del servicio.

92.2 Las entidades de la Administración Pública que requieran infraestructura o plataformas tecnológicas para el ejercicio de sus funciones en el ámbito de sus competencias y despliegue de sus servicios digitales utilizan de forma preferente infraestructuras tecnológicas o plataformas provistas por proveedores de servicios en la nube.

92.3 Las entidades de la Administración Pública que cuentan con infraestructura tecnológica o plataforma tecnológica propia, para el ejercicio de sus funciones en el ámbito de sus competencias, pueden:

a) Compartirla con otras entidades públicas de su sector en función de sus necesidades, proyectos y objetivos en común.

b) Ampliar las capacidades de su infraestructura tecnológica o plataforma tecnológica como servicio para compartir con sus proyectos, programas u órganos desconcentrados, en función de sus necesidades y objetivos en común.

92.4 La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, dicta las directivas o lineamientos para la determinación, adquisición y uso de las infraestructuras tecnológicas provistas en la modalidad de infraestructura como servicio o plataforma como servicio.

92.5 En el caso de las municipalidades pertenecientes a ciudades principales tipo F y G, conforme a la clasificación realizada por el Ministerio de Economía y Finanzas, en el marco del Programa de Incentivos a la Mejora de la Gestión Municipal, la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, provee la infraestructura tecnológica o plataformas tecnológicas como servicio para la prestación de sus servicios digitales, sistemas de información o catálogos de servicios de información geográfica, para lo cual emite las disposiciones que regulen dicha prestación. Asimismo, la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, puede proveer la infraestructura tecnológica o plataformas tecnológicas como servicio a las municipalidades no pertenecientes a esta clasificación siempre que lo requieran, manifiesten y sustenten técnicamente conforme a la regulación que se emita para dicho fin.

Artículo 93. Datos maestros para la interoperabilidad

Los datos maestros para la interoperabilidad son datos maestros que son reutilizados por las entidades de la Administración Pública para facilitar la interoperabilidad. Utilizan los identificadores únicos fundamentales establecidos en el artículo 72 del presente Reglamento y son fuente de información básica de persona natural, persona jurídica, vehículo, predio y trámite.

TÍTULO VII
SEGURIDAD DIGITAL

CAPÍTULO I
MARCO DE SEGURIDAD DIGITAL DEL ESTADO PERUANO

Artículo 94. Marco de Seguridad Digital del Estado Peruano

94.1 El Marco de Seguridad Digital del Estado Peruano es dirigido, supervisado y evaluado por la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, en su calidad de ente rector de la seguridad digital, que emite lineamientos, especificaciones, guías, directivas, normas técnicas y estándares para su aplicación por parte de las entidades de la Administración Pública a fin de fortalecer la confianza de los ciudadanos, entidades públicas y personas en general en el entorno digital.

94.2 El Marco de Seguridad Digital del Estado Peruano integra aquellas normas que conforman los ámbitos de defensa, inteligencia, justicia e institucional, establecidos en el artículo 32 de la Ley y se articula y sustenta en las normas, procesos, roles, responsabilidades y mecanismos regulados e implementados a nivel nacional en materia de Seguridad de la Información. La seguridad digital es un ámbito del Marco de Confianza Digital establecido en el Decreto de Urgencia Nº 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.

94.3 La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, es la encargada de: (1) definir, articular y dirigir la política, estrategia y planes para el desarrollo de la Seguridad Digital del Estado Peruano, (2) emitir lineamientos, especificaciones, guías, directivas, normas técnicas y estándares en Seguridad Digital, (3) supervisar su cumplimiento, (4) evaluar las necesidades de las entidades, ciudadanos y personas en general en dicho ámbito, (5) asesorar el Consejo de Seguridad y Defensa Nacional sobre los aspectos relacionados a seguridad digital, (6) impulsar campañas de sensibilización sobre los riesgos de seguridad digital de la ciudadanía, (7) promover contenidos digitales para la formación de talento digital en seguridad y, (8) comunicar al Presidente del Consejo de Ministros los resultados y avances del mismo, a fin de garantizar de manera efectiva la seguridad digital en el país.

Artículo 95. Principios del Marco de Seguridad Digital del Estado Peruano

La aplicación del Marco de Seguridad Digital del Estado Peruano se desarrolla de acuerdo con los principios rectores establecidos en el artículo 5 de la Ley, y con los siguientes principios específicos de la seguridad digital:

a) Seguridad desde el diseño. Los servicios digitales se diseñan y crean atendiendo las necesidades de disponibilidad, integridad y confidencialidad de los datos e información que capturan, procesan y distribuyen.

b) Gestión de riesgos. La gestión de riesgos de seguridad en el entorno digital está integrada en la toma de decisiones, diseño de controles de seguridad en los servicios digitales y procesos de la entidad. Es responsabilidad de la alta dirección dirigirla, mantenerla e incorporarla en la gestión integral de riesgos de la entidad.

c) Colaboración y cooperación. Se promueve el intercambio de información, mejores prácticas y experiencias a fin de identificar y prevenir riesgos de seguridad digital; así como detectar, responder y recuperarse ante incidentes en el entorno digital que afecten la continuidad de las entidades, bienestar de las personas y el desarrollo sostenible del país.

d) Participación responsable. El Estado y la sociedad en su conjunto tienen responsabilidad en la protección de sus datos personales y gestión de riesgos en el entorno digital, en función de sus roles, contexto y su capacidad de actuar, teniendo en cuenta el impacto potencial de sus decisiones con respecto a otros.

e) Protección de datos e información. Se promueve la implementación de medidas y controles de seguridad organizativos, técnicos y legales para preservar la disponibilidad, integridad y confidencialidad de los datos e información que capture, procese, almacene y distribuya una entidad, así como en cualquier otra forma de actividad que facilite el acceso o la interconexión de los datos.

f) Enfoque nacional. La Seguridad Digital es un componente de la seguridad nacional, respalda el funcionamiento del Estado, la sociedad, la competitividad, la economía y la innovación.

g) Enfoque integral. La Seguridad Digital es entendida como un proceso integral y holístico constituido por todos los elementos técnicos, humanos, materiales y organizativos relacionados con una entidad.

Artículo 96. Modelo de Seguridad Digital

96.1 El Modelo de Seguridad Digital es la representación holística y sistémica de los componentes que comprende el Marco de Seguridad Digital del Estado Peruano, atendiendo los principios establecidos en el artículo 95 del presente Reglamento, aquellos establecidos en la Ley, el Decreto de Urgencia Nº 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento, y las normas en materia de Seguridad de la Información en el Estado Peruano.

96.2 El Modelo de Seguridad Digital comprende los siguientes componentes:

a) Responsables de los ámbitos del Marco de Seguridad Digital.
b) Centro Nacional de Seguridad Digital.
c) Redes de confianza en Seguridad Digital.
d) Oficial de Seguridad Digital.
e) Sistemas de Gestión de Seguridad de la Información.
f) Ciudadano o persona en general.
g) Autoridad Nacional de Protección de Datos Personales.

Artículo 97. Articulación normativa en materia de Seguridad Digital

Las políticas, lineamientos, directrices y planes en los ámbitos de defensa, inteligencia, justicia e institucional previstos en el artículo 32 de la Ley, se articulan con las políticas, estrategias y planes en materia de Seguridad Digital del Estado Peruano que establezca la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital.

CAPÍTULO II
GESTIÓN DEL MARCO DE SEGURIDAD DIGITAL DEL ESTADO PERUANO

Artículo 98. Ámbito de Defensa

98.1 La ciberdefensa es gestionada por el Ministerio de Defensa, quien articula con sus órganos ejecutores el planeamiento y conducción de operaciones militares en y mediante el ciberespacio conforme los objetivos y lineamientos de la Política de Seguridad y Defensa Nacional aprobados por el Consejo de Seguridad y Defensa Nacional (COSEDENA) y de manera articulada con los objetivos de seguridad digital.

98.2 El Comando Conjunto de las Fuerzas Armadas está a cargo de la ciberdefensa de los activos críticos nacionales y recursos claves, cuando la capacidad de protección de sus operadores y/o sector responsable de cada uno de ellos o de la Dirección Nacional de Inteligencia o quien haga sus veces, sean sobrepasadas, y se vea afectada la seguridad nacional.

98.3 La Presidencia del Consejo de Ministros, en su calidad de miembro del Consejo de Seguridad y Defensa Nacional, establece los protocolos de escalamiento, coordinación, intercambio y activación para lo indicado en la Ley Nº 30999, Ley de Ciberdefensa. Esta función se ejerce a través de la Secretaría de Gobierno Digital en su calidad de ente rector del Sistema Nacional de Transformación Digital y de seguridad y confianza digital en el país, quien emite los lineamientos y las directivas correspondientes.

Artículo 99. Ámbito de Inteligencia

La inteligencia y contrainteligencia en este ámbito es gestionada, en el marco de sus competencias, por la Dirección Nacional de Inteligencia (DINI), quien articula con la Secretaría de Gobierno Digital Presidencia del Consejo de Ministros y los órganos competentes, el planeamiento y conducción de operaciones de inteligencia para asegurar los activos críticos nacionales.

Artículo 100. Ámbito de Justicia

100.1 Las acciones para garantizar la lucha eficaz contra la ciberdelincuencia es dirigida por el Ministerio del Interior (MININTER) y la Policía Nacional del Perú (PNP), quienes articulan con el Ministerio de Justicia y Derechos Humanos (MINJUSDH), el Instituto Nacional Penitenciario (INPE), el Ministerio Público - Fiscalía de la Nación, el Tribunal Constitucional, Academia de la Magistratura, la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros y el Poder Judicial (PJ), conforme a lo dispuesto en la Ley Nº 30096, Ley de Delitos Informáticos, y los convenios aprobados y ratificados por el Estado Peruano en esta materia.

100.2 La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, en coordinación con la División de Investigación de Delitos de Alta Tecnología (DIVINDAT) de la Policía Nacional del Perú y el Ministerio Público - Fiscalía de la Nación proponen los protocolos de colaboración y comunicación para el reporte de casos de violencia sexual contra niños, niñas y adolescentes en el entorno digital, la cual se hace efectiva mediante Resolución de la Secretaría de Gobierno Digital.

Artículo 101. Ámbito Institucional

El ámbito institucional es dirigido, evaluado y supervisado por la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, quien articula con las entidades de la Administración Pública la implementación de las normas, directivas y estándares de Seguridad Digital, Ciberseguridad y Seguridad de la Información, y supervisa su cumplimiento.

Artículo 102. Articulación de ámbitos

La Secretaría de Gobierno Digital dirige y articula acciones para la gestión de incidentes y riesgos de seguridad digital que afecten a la sociedad con los responsables de los ámbitos de Defensa, Inteligencia y Justicia, conforme lo establece el Decreto de Urgencia Nº 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento y su Reglamento.

Artículo 103. Adopción de estándares y buenas prácticas

Las entidades de la Administración Pública pueden adoptar normas técnicas peruanas o normas y/o estándares técnicos internacionales ampliamente

reconocidos en materia de gestión de riesgos, gestión de incidentes, seguridad digital, ciberseguridad y seguridad de la información en ausencia de normas o especificaciones técnicas nacionales vigentes.

CAPÍTULO III
EQUIPO DE RESPUESTAS ANTE INCIDENTES DE SEGURIDAD DIGITAL

Artículo 104. Equipo de Respuestas ante Incidentes de Seguridad Digital

104.1 Un Equipo de Respuestas ante Incidentes de Seguridad Digital es aquel equipo responsable de la gestión de incidentes de seguridad digital que afectan los activos de una entidad pública o una red de confianza. Su implementación y conformación se realiza en base a las disposiciones que determine la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros.

104.2 Las entidades de la Administración pública conforman un Equipo de Respuestas ante Incidentes de Seguridad Digital de carácter institucional. Dichos Equipos forman parte de los órganos o unidades orgánicas de Tecnologías de la Información de la entidad o de la unidad de organización especializada en seguridad de la información o similar prevista en su estructura orgánica o funcional. Su conformación es comunicada a la Secretaría de Gobierno Digital mediante los mecanismos dispuestos para tal fin.

104.3 La Secretaría de Gobierno Digital, en su calidad de ente rector de la seguridad digital en el país, emite opinión técnica especializada a pedido de una entidad a fin de revisar o validar aspectos técnicos sobre la conformación de un Equipo de Respuesta ante incidentes de Seguridad Digital, conforme a lo establecido en el presente Reglamento y normas complementarias.

104.4 La red de confianza es el conjunto de entidades públicas e interesados que articulan acciones para el intercambio de información sobre incidentes de seguridad digital, vulnerabilidades, amenazas, medidas de mitigación, herramientas, mejores prácticas o similares en materia de seguridad digital. Se conforman en función de un sector, territorio o para atender un objetivo específico.

104.5 Las entidades públicas pueden conformar una red de confianza en base a las disposiciones establecidas por la Secretaría de Gobierno Digital. Asimismo, la Secretaría de Gobierno Digital en función de los objetivos nacionales, políticas de estado o aspectos estratégicos promueve la conformación de redes de confianza.

Artículo 105. Obligaciones de las entidades en Seguridad Digital

Las entidades públicas tienen, como mínimo, las siguientes obligaciones:

a) Implementar y mantener un Sistema de Gestión de Seguridad de la Información (SGSI).
b) Comunicar al Centro Nacional de Seguridad Digital los incidentes de seguridad digital atendiendo lo establecido en el artículo 107 del presente Reglamento.
c) Adoptar medidas para la gestión de riesgos e incidentes de seguridad digital que afecten a los activos de la entidad.
d) Difundir alertas tempranas, avisos e información sobre riesgos e incidentes de seguridad digital en su entidad y red de confianza.
e) Asegurar acciones de investigación y cooperación efectiva, eficiente y segura con el Centro Nacional de Seguridad Digital.
f) Proveer los recursos y medidas necesarias para asegurar la efectiva gestión de incidentes de seguridad digital.
g) Requerir a sus proveedores de desarrollo de software el cumplimiento de estándares, normas técnicas y mejores prácticas de seguridad ampliamente reconocidos.

Artículo 106. Criterios para determinar el impacto significativo de un incidente

Para determinar el impacto significativo de un incidente de seguridad digital se consideran, como mínimo, los siguientes criterios:

a) Perjuicio a la reputación.
b) Pérdida u obligación financiera.
c) Interrupción de las operaciones, procesos o actividades de la entidad.
d) Divulgación no autorizada de datos personales o información reservada, secreta o confidencial.
e) Daños personales (físico, psicológico o emocional).

Artículo 107. Comunicación de un incidente

La comunicación de un incidente de seguridad digital se realiza conforme a lo establecido en el Decreto de Urgencia Nº 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento, su Reglamento y normas complementarias.

Artículo 108. Incidentes de Seguridad Digital relativos a Datos Personales

Las entidades públicas comunican y colaboran con la Autoridad Nacional de Protección de Datos Personales ante la identificación de incidentes de seguridad digital que hayan afectado los datos personales, comunicándose en un plazo máximo de 48 horas, a partir de la toma de conocimiento de la brecha de seguridad.

CAPÍTULO IV
SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Artículo 109. Sistema de Gestión de Seguridad de la Información

109.1 El Sistema de Gestión de Seguridad de la Información (SGSI) comprende el conjunto de políticas, lineamientos, procedimientos, recursos y actividades asociadas, que gestiona una entidad con el propósito de proteger sus activos de información, de manera independiente del soporte en que estos se encuentren. Asimismo, contempla la gestión de riesgos e incidentes de seguridad de la información y seguridad digital, la implementación efectiva de medidas de ciberseguridad, y acciones de colaboración y cooperación.

109.2 El diseño, implementación, operación y mejora del SGSI atiende a las necesidades de todas las partes interesadas de la entidad; asimismo, responde a los objetivos estratégicos, estructura, tamaño, procesos y servicios de la entidad. El SGSI comprende al Equipo de Respuesta ante Incidentes de Seguridad Digital.

109.3 Las entidades de la Administración Pública implementan un SGSI en su institución, teniendo como alcance mínimo sus procesos misionales y aquellos que son relevantes para su operación.

109.4 Se gestiona la implementación de controles y medidas de seguridad a nivel organizacional, técnico y legal, basadas en riesgos, a fin de garantizar la disponibilidad, integridad y confidencialidad de los datos personales que sean tratados, procesados, almacenados y compartidos a una entidad, así como en cualquier otra forma de actividad que facilite el acceso o intercambio de datos.

Artículo 110. Gestión de Riesgos de Seguridad Digital

Las entidades de la Administración Pública gestionan sus riesgos de seguridad digital, conforme a lo establecido en el Decreto de Urgencia Nº 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento y sus normas reglamentarias.

Artículo 111. Roles para la Seguridad de la Información

111.1 El titular de la entidad es responsable de la implementación del SGSI.

111.2 El Comité de Gobierno Digital es responsable de dirigir, mantener y supervisar el SGSI de la entidad.

111.3 El Oficial de Seguridad Digital es el rol responsable de coordinar la implementación y mantenimiento del SGSI en la entidad, atendiendo las normas en materia de seguridad digital, confianza digital y gobierno digital.

La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, emite el perfil del Oficial de Seguridad Digital en la Administración Pública.

Artículo 112. Deberes y obligaciones del personal de la entidad

112.1 Las entidades públicas capacitan e informan a su personal sobre sus deberes y obligaciones en materia de seguridad de la información y seguridad digital, siendo estos últimos responsables de su aplicación en el ejercicio de sus funciones y actividades. Asimismo, las entidades fortalecen las competencias de su personal en el uso adecuado, eficiente y seguro de las tecnologías digitales, para lo cual pueden solicitar el soporte de la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital.

112.2 El personal de la entidad que accede a datos e información a través de aplicativos informáticos, sistemas de información o herramientas informáticas usa credenciales que permitan determinar: su identidad en un ámbito determinado, los tipos de derecho o privilegio de uso y accesos asignados, las actividades realizadas, a fin de establecer responsabilidades cuando corresponda.

Artículo 113. Auditorías de Seguridad de la Información

113.1 Las entidades públicas de manera permanente realizan como mínimo una auditoría externa anual a su SGSI. Los resultados de las auditorías constan como información documentada por la entidad.

113.2 La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, solicita a las entidades públicas informes de las auditorías realizadas o sobre la aplicación efectiva de las normas en materia de seguridad de la información o seguridad digital, en el marco de sus funciones de supervisión o cuando lo considere necesario para prevenir o resolver incidentes de seguridad digital.

Artículo 114. Seguridad de los servicios digitales

Los servicios digitales se implementan considerando los controles y medidas de seguridad de la información que permitan garantizar su disponibilidad, integridad y confidencialidad, así como atendiendo las disposiciones establecidas en el Decreto de Urgencia Nº 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento y sus normas reglamentarias.

Artículo 115. Pruebas para evaluar vulnerabilidades

115.1 Las entidades públicas planifican y realizan pruebas para evaluar vulnerabilidades a los siguientes activos: aplicativos informáticos, sistemas, infraestructura, datos y redes, que soportan los servicios digitales, procesos misionales o relevantes de la entidad. La ejecución de dichas pruebas se realiza, como mínimo, una vez al año. El Centro Nacional de Seguridad Digital solicita a la entidad información sobre las pruebas realizadas o coordina con ella la realización de dichas pruebas.

115.2 Los resultados de las pruebas realizadas constan como información documentada por la entidad. La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, solicita dichos resultados en el marco de sus funciones de supervisión o cuando lo considere necesario para la gestión de un incidente de seguridad digital.

TITULO VIII
ARQUITECTURA DIGITAL

CAPÍTULO I
MARCO DE LA ARQUITECTURA DIGITAL DEL ESTADO

Artículo 116. Marco de la Arquitectura Digital del Estado Peruano

116.1 El Marco de la Arquitectura Digital del Estado Peruano es dirigido, supervisado y evaluado por la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, en su calidad de ente rector en arquitectura digital, que emite lineamientos, especificaciones, guías, directivas, normas técnicas y estándares para su aplicación por parte de las entidades de la Administración Pública que aseguren el alineamiento entre los objetivos estratégicos nacionales e institucionales con el uso optimizado de las tecnologías digitales.

116.2 El alineamiento comprende las inversiones en tecnologías de la información, activos de tecnologías de la información, datos y seguridad digital, para optimizar el uso de recursos y prestación de servicios digitales en el Estado.

116.3 El Marco de la Arquitectura Digital del Estado Peruano comprende las siguientes perspectivas: desempeño, organizacional, datos, aplicaciones, tecnológico y seguridad.

Artículo 117. Principios del Marco de la Arquitectura Digital del Estado Peruano

La aplicación del Marco de la Arquitectura Digital del Estado Peruano se desarrolla de acuerdo con los principios rectores establecidos en el artículo 5 de la Ley, y con los siguientes principios específicos:

a) Neutralidad tecnológica: En la evaluación, adopción o adquisición de tecnología prima la neutralidad, no debiendo orientarse o limitarse a un determinado tipo de tecnología.

b) Valor ganado: Las inversiones en tecnologías de la información generan valor para la entidad mediante la eficiencia en sus procesos, optimización de costos, riesgos y beneficios cuantificables.

c) Reusabilidad: Se promueve la reutilización de componentes, datos, información, activos de tecnologías de la información y soluciones tecnológicas en la entidad.

d) Automatización: Se facilita la automatización de los procesos permitiendo lograr un alto rendimiento, modelando cada uno de ellos hasta elevarlos a un nivel óptimo de calidad.

e) Seguridad de la información: Permite la definición, implementación y la gestión adecuada de la confidencialidad, integridad y disponibilidad de los activos de información independientemente del soporte que los contenga.

Artículo 118. Modelos de referencia de la Arquitectura Digital

118.1 Los modelos de referencia de la Arquitectura Digital permiten un análisis integral de la entidad, desde diferentes perspectivas, para identificar necesidades, problemas y brechas asociadas con los procesos, servicios, sistemas de información, infraestructura tecnológica, gestión de datos y seguridad digital, así como identificar oportunidades de mejora para satisfacer las necesidades de información de la entidad y ciudadano, en el tiempo presente, inmediato y futuro.

118.2 Los modelos de referencia de la Arquitectura Digital son:

a) **Modelo de referencia de Desempeño:** Permite describir los mecanismos e indicadores utilizados para alinear, evaluar y medir las inversiones en tecnologías de la información, proyectos y servicios de gobierno digital; conforme a los objetivos institucionales y objetivos estratégicos de desarrollo nacional.

b) **Modelo de referencia Organizacional:** Permite analizar la visión, misión, objetivos estratégicos, estructura, funciones, servicios y procesos establecidos en los instrumentos de gestión y documentos de gestión organizacional de la entidad y el nivel de alineamiento con las disposiciones de gobierno digital, donde se plasma el presente, lo inmediato y el futuro organizacional.

c) **Modelo de referencia de Aplicaciones:** Permite describir las aplicaciones y sistemas de información que brindan soporte a las funciones, procesos y servicios de la entidad, las cuales se pueden compartir o reutilizar.

d) **Modelo de referencia de Datos:** Permite describir los datos, su estructura y significado en el contexto de la

entidad, para facilitar su descripción, clasificación, calidad, apertura, acceso, reutilización y gestión en general.

e) **Modelo de referencia Tecnológico:** Permite describir los activos de tecnologías de la información necesarios para gestionar los datos e información y, brindar soporte a las aplicaciones y sistemas de información en la entidad.

f) **Modelo de referencia de Seguridad:** Permite describir las medidas de seguridad de información en la entidad, para garantizar la confidencialidad, disponibilidad e integridad de sus activos de información, así como fortalecer la confianza en los servicios digitales.

118.3 La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, establece las normas, guías, directivas y lineamientos para la aplicación de los Modelos de referencia de desempeño, organizacional, aplicaciones, datos, tecnológico y seguridad.

118.4 Los modelos de referencia de la Arquitectura Digital pueden ser utilizados para analizar y alinear los sistemas de información, datos, seguridad e infraestructura tecnológica con los objetivos estratégicos institucionales, regionales, sectoriales, o de un sistema funcional o administrativo, con perspectiva futura.

Artículo 119. Plataforma Nacional de Gobierno Digital

119.1 Créase la Plataforma Nacional de Gobierno Digital la cual comprende el conjunto de componentes tecnológicos, lineamientos y estándares para facilitar e impulsar la digitalización de servicios y procesos en las entidades de la Administración pública, promoviendo su colaboración, integración, un uso eficiente de los recursos y el alineamiento con los objetivos estratégicos nacionales.

119.2 La Plataforma Nacional de Gobierno Digital es dirigida, supervisada y evaluada por la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros.

119.3 La referida plataforma comprende, de manera no limitativa, a los bloques básicos de interoperabilidad técnica, la Plataforma GOB.PE, plataforma de Información de la Arquitectura Digital del Estado, Inventario de Activos Digitales del Estado Peruano, así como aquellos recursos, herramientas, instrumentos o servicios digitales a cargo de la Secretaría de Gobierno Digital que faciliten la transformación digital del Estado.

119.4 La Secretaría de Gobierno Digital es la responsable de gestionar los requerimientos de las entidades de la Administración pública sobre el uso de los componentes de la Plataforma Nacional de Gobierno Digital, que incluyen la recepción, habilitación, deshabilitación, renovación u otras acciones necesarias.

Artículo 120. Plataforma Nacional de Gobierno de Datos

120.1 Créase la Plataforma Nacional de Gobierno de Datos (DATOS PERÚ) la cual comprende, de manera no limitativa, la Plataforma Nacional de Datos Abiertos, la Plataforma GEOPERU y las fuentes disponibles en datos espaciales o georreferenciados. Asimismo, implementa tecnologías digitales para la analítica de grandes volúmenes de datos, inteligencia artificial u otras tecnologías emergentes a fin de facilitar la disponibilidad de tableros de gestión y toma de decisiones e intervenciones estratégicas en la Administración Pública.

120.2 La Plataforma Nacional de Gobierno de Datos es administrada por la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, que promueve su uso eficiente para el logro de los objetivos estratégicos nacionales, cuyo dominio en Internet es www.datos.gob.pe.

Artículo 121. Roles y Plataforma de Información de la Arquitectura Digital del Estado

121.1 El Comité de Gobierno Digital es el responsable del uso de los modelos de referencia de la arquitectura digital en su entidad y, la actualización de la información en la Plataforma de Información de la Arquitectura Digital del Estado.

121.2 El titular de la entidad en función de sus capacidades, presupuesto y recursos puede designar un Arquitecto Digital como rol responsable de coordinar el uso y documentación de los modelos de referencia de la Arquitectura Digital. Dicha designación se hace de conocimiento a la Secretaría de Gobierno Digital para las coordinaciones y acciones correspondientes.

121.3 Créase la Plataforma de Información de la Arquitectura Digital del Estado como la plataforma que permite (i) automatizar la gestión de la arquitectura digital del Estado Peruano, (ii) almacenar datos para la gestión y evaluación de los proyectos de gobierno digital, y (iii) proporcionar información para la mejora continua de la arquitectura digital del Estado. Es administrada por la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros, cuyo dominio en internet es www.arquitecturadigital.gob.pe.

121.4 La Plataforma de Información de la Arquitectura Digital del Estado contiene información de las entidades, como mínimo, sobre:

a) Visión, misión y objetivos estratégicos.
b) Procesos de la entidad.
c) Proyectos de TI o tecnologías digitales.
d) Aplicaciones, sistemas de información y activos de tecnologías de la información.
e) Inversiones en tecnologías de la información.
f) Información sobre el personal de tecnologías de la información.

121.5 Las entidades de la Administración Pública registran y/o validan la información descrita en el numeral precedente en la Plataforma de Información de la Arquitectura Digital del Estado, para ello toma como referencia la información de su Plan de Gobierno Digital aprobado e instrumentos de gestión institucional.

121.6 La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, realiza anualmente la Encuesta Nacional de Activos Digitales del Estado para elaborar y mantener el Inventario de Activos Digitales del Estado Peruano, en concordancia con lo dispuesto en la Ley, el presente Reglamento y las normas en materia de gobierno digital.

DISPOSICIONES COMPLEMENTARIAS FINALES

Primera. Normas complementarias

La Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros dicta las normas complementarias para la implementación del presente Reglamento.

Segunda. Implementación de la Plataforma ID GOB.PE

La implementación de la plataforma ID GOB.PE se realiza en tres (03) fases:

a) Fase 1: la implementación del servicio de autenticación para peruanos se encuentra a cargo del RENIEC, y se realiza en los siguientes plazos:

i) Con nivel 1 de confianza en la autenticación, en un plazo no mayor a noventa (90) días calendario, contados a partir de la publicación del presente Reglamento.

ii) Con nivel 2 de confianza en la autenticación, en un plazo no mayor a seis (06) meses, contados a partir de la publicación del presente Reglamento.

iii) Con nivel 3 de confianza en la autenticación, en un plazo no mayor a nueve (09) meses, contados a partir de la publicación del presente Reglamento.

b) Fase 2: la implementación del servicio de autenticación para extranjeros, con al menos un nivel de seguridad, se realiza en un plazo no mayor a doce (12) meses, contados a partir de la publicación del presente Reglamento, a cargo de MIGRACIONES.

c) Fase 3: la implementación del servicio de autenticación para personas naturales, con al menos un nivel de seguridad, se realiza en un plazo no mayor a seis

(06) meses, contados a partir de la publicación del presente Reglamento, a cargo de la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros.

La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, en un plazo no mayor a noventa (90) días hábiles contados a partir de la publicación del presente Reglamento, mediante Resolución Secretarial, emite las normas, condiciones de uso y protocolos de integración de la Plataforma ID GOB.PE. Así como, las normas y disposiciones con respecto a la adopción de la Plataforma ID GOB.PE por parte de las entidades de la Administración Pública.

El Ministerio de Relaciones Exteriores en un plazo no mayor a noventa (90) días hábiles, contados a partir de la publicación del presente Reglamento, publica en la Plataforma de Interoperabilidad del Estado los servicios de información de los atributos de identidad de un extranjero contenidos en el Carné de Identidad y/o Carné de Solicitante de Refugio para el consumo exclusivo de la Superintendencia Nacional de Migraciones, así como de otras entidades autorizadas expresamente por Relaciones Exteriores. Hasta la publicación de los referidos servicios de información el Ministerio de Relaciones Exteriores remite los atributos de identidad correspondientes a la Superintendencia Nacional de Migraciones, a través de los mecanismos que acuerden y establezcan para dicho fin, para su inscripción en el Registro de Información de Migraciones (RIM).

Tercera. Adecuación de la Plataforma Digital GOB.PE

La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, en un plazo no mayor a ciento ochenta (180) días calendario, contados a partir de la publicación del presente Reglamento, realiza progresivamente las adecuaciones necesarias a la Plataforma Digital Única del Estado Peruano para Orientación al Ciudadano - GOB.PE, en base a la estructura funcional establecida en el artículo 31 y demás disposiciones del presente Reglamento.

Las entidades públicas en un plazo no mayor a noventa (90) días calendario, contados a partir de la publicación del presente Reglamento, proporcionan los servicios de información que defina la Secretaría de Gobierno Digital para las adecuaciones de la Plataforma GOB.PE

Cuarta. Integración de la Plataforma GOB.PE y la Plataforma ID GOB.PE

En un plazo no mayor de noventa (90) días hábiles, contados a partir de la publicación del presente Reglamento, la Plataforma GOB.PE se integra con la Plataforma ID GOB.PE para verificar la identidad de las personas que requieren acceder y utilizar los servicios digitales prestados a través de la Plataforma GOB.PE, así como acceder a un entorno personalizado conforme a los literales f) y g) del numeral 31.1 del artículo 31 del presente Reglamento.

Quinta. Aplicativos Móviles del Estado Peruano

La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, emite los lineamientos y directivas para el diseño, construcción y registro de aplicativos móviles en el Catálogo Oficial de Aplicativos Móviles en un periodo no mayor a ciento ochenta (180) días hábiles, contados a partir de la publicación del presente Reglamento.

En un plazo no mayor a dos (02) años posterior a la emisión de los referidos lineamientos, las entidades que cuenten con aplicativos móviles existentes a la entrada en vigencia de la presente norma realizan las adecuaciones que correspondan y solicitan su registro en el Catálogo Oficial de Aplicativos Móviles.

Sexta. Registro de aplicativos móviles en las tiendas de distribución

A partir del 01 de julio del 2021 el registro de aplicaciones móviles de las entidades públicas en tiendas de distribución se realiza únicamente a través del Catálogo Oficial de Aplicativos Móviles del Estado Peruano, bajo la cuenta oficial GOB.PE.

Séptima. Normas para procesos técnicos archivísticos en soporte digital

El Archivo General de la Nación en coordinación con la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, dictan las normas para los procesos técnicos archivísticos en soporte digital, en un plazo no mayor a ciento ochenta (180) días hábiles contados a partir de a la publicación del presente Reglamento.

Las referidas normas serán aplicables a los documentos electrónicos que se hayan generado a la entrada en vigencia del presente Reglamento.

Octava. Implementación de la Plataforma Única de Recepción Documental del Estado Peruano

En un plazo no mayor a un (01) año, posterior a la publicación del presente Reglamento, la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, implementa la Plataforma Única de Recepción Documental del Estado Peruano y establece los lineamientos y requisitos de integración.

Novena. Plazos para la integración con la Plataforma Única de Recepción Documental del Estado Peruano

Las entidades de la Administración Pública, posterior a la implementación de la Plataforma Única de Recepción Documental del Estado Peruano se integran con la misma conforme a los siguientes plazos:

a) Poder Ejecutivo hasta seis (06) meses.
b) Organismos Constitucionales Autónomos hasta seis (06) meses.
c) Gobiernos regionales y universidades públicas hasta seis (06) meses.
d) Gobiernos locales Tipo A y Tipo C hasta un (01) año.
e) Gobiernos locales Tipo B hasta dieciocho (18) meses.
f) Las empresas públicas de los gobiernos regionales, locales, o bajo el ámbito del Fondo Nacional de Financiamiento de la Actividad Empresarial del Estado (FONAFE) hasta un (01) año.

Las demás entidades en función de sus capacidades y recursos pueden integrar sus sistemas de información con la Plataforma Única de Recepción Documental del Estado Peruano.

La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, amplía los plazos de integración en función de las capacidades y recursos de las entidades; la misma que se hace efectiva mediante Resolución de Secretaría de Gobierno Digital.

Décima. Plazos para la integración de servicios digitales con las plataformas PIDE, ID GOB.PE y PSPP

Las entidades de la Administración Pública integran sus servicios digitales con las plataformas PIDE, ID GOB.PE y PSPP en lo que corresponda, conforme a los siguientes plazos:

a) Poder Ejecutivo hasta un (01) año, contado desde la publicación del presente Reglamento.
b) Organismos Constitucionales Autónomos hasta un (01) año, contado desde la publicación del presente Reglamento.
c) Gobiernos regionales y universidades públicas hasta dieciocho (18) meses, contado desde la publicación del presente Reglamento.
d) Gobiernos locales Tipo A, Tipo B y Tipo C hasta dieciocho (18) meses, contado desde la publicación del presente Reglamento.
e) Las empresas públicas de los gobiernos regionales, locales, o bajo el ámbito del Fondo Nacional de Financiamiento de la Actividad Empresarial del Estado (FONAFE) hasta dieciocho (18) meses.

Las demás entidades en función de sus capacidades y recursos pueden integrar sus servicios digitales con las Plataformas PIDE, ID GOB.PE y PSPP.

La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, amplía los plazos de

integración en función de las capacidades y recursos de las entidades; la misma que se hace efectiva mediante Resolución de Secretaría de Gobierno Digital.

Décima Primera. Lineamientos e implementación de la Plataforma Casilla Única Electrónica del Estado Peruano

La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, implementa la Plataforma Casilla Única Electrónica del Estado Peruano, en las siguientes fases y plazos:

a) Fase 1: Dirección electrónica y buzón de comunicaciones, conforme a:

i) Personas naturales peruanas en un plazo no mayor a seis (06) meses, posterior a la implementación de la fase 1 a la que se refiere la Segunda Disposición Complementaria Final del presente Reglamento.
ii) Personas naturales extranjeras en un plazo no mayor a seis (06) meses, posterior a la implementación de la fase 2 a la que se refiere la Segunda Disposición Complementaria Final del presente Reglamento.
iii) Personas jurídicas en un plazo no mayor a doce (12) meses, posterior a la implementación del servicio de información al que se refiere la Cuadragésima Sexta Disposición Complementaria Final del presente Reglamento.

b) Fase 2: Buzón de notificaciones, conforme a:

i) Personas naturales peruanos en un plazo no mayor a doce (12) meses, posterior a la culminación de la Fase 1.
ii) Personas naturales extranjeras en un plazo no mayor a doce (12) meses, posterior a la culminación de la Fase 1.
iii) Personas jurídicas en un plazo no mayor a dieciocho (18) meses, posterior a la culminación de la Fase 1.

Asimismo, la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros mediante Resolución de Secretaría de Gobierno Digital, en un plazo no mayor a un (01) año, posterior a la publicación del presente Reglamento, establece las condiciones, requisitos, uso y gestión de la casilla única electrónica, así como las normas para la adopción e integración de la Plataforma Casilla Única Electrónica por parte de las entidades públicas.

Hasta la culminación de la implementación de la Plataforma Casilla Única Electrónica del Estado Peruano las notificaciones se realizan conforme a lo previsto en el artículo 20 del TUO de la Ley Nº 27444.

Décima Segunda. Plazos para la integración de la Plataforma Casilla Única Electrónica del Estado Peruano

Las entidades de la Administración Pública, posterior a la implementación de la Plataforma Casilla Única Electrónica del Estado Peruano, se integran con la misma conforme a los siguientes plazos:

a) Poder Ejecutivo hasta seis (06) meses.
b) Organismos Constitucionales Autónomos hasta seis (06) meses.
c) Gobiernos regionales y universidades públicas hasta un (01) año.
d) Gobiernos locales Tipo A y Tipo C hasta un (01) año.
e) Gobiernos locales Tipo B hasta dieciocho (18) meses.
f) Las empresas públicas de los gobiernos regionales, locales, o bajo el ámbito del Fondo Nacional de Financiamiento de la Actividad Empresarial del Estado (FONAFE) hasta un (01) año.

Las demás entidades en función de sus capacidades y recursos pueden integrar sus sistemas de información con la Plataforma Casilla Única Electrónica del Estado Peruano.

La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, amplía los plazos de integración en función de las capacidades y recursos de las entidades; la misma que se hace efectiva mediante Resolución de Secretaría de Gobierno Digital.

Décima Tercera. Gestión de la entidad de certificación nacional del Estado peruano y Directiva de la Plataforma Nacional de Firma Digital

En un plazo no mayor a seis (06) meses, posterior a la publicación del presente Reglamento, el Registro Nacional de Identificación y Estado Civil (RENIEC) transfiere el acervo documentario, activos físicos, activos lógicos, así como todo aquello que se requiera para la adecuada transferencia de la Entidad de Certificación Nacional para el Estado Peruano a la Presidencia del Consejo de Ministros. La PCM incorpora en sus documentos de gestión los objetivos, acciones y actividades necesarias para la implementación de la presente disposición.

En un plazo no mayor a seis (06) meses, posterior a la publicación del presente Reglamento, la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, emite las normas sobre el uso de la firma digital por parte de las entidades de la Administración Pública, así como la directiva sobre la Plataforma Nacional de Firma Digital.

El RENIEC, en un plazo no mayor a treinta (30) días calendario contados a partir de la publicación del presente Reglamento, pone a disposición de la Presidencia del Consejo de Ministros el software acreditado de validación y generación de firmas digitales de su titularidad, incluyendo como mínimo los ejecutables, los identificadores, la documentación asociada, y todo aquello que sea necesario para iniciar la implementación de la Plataforma FIRMA PERÚ, de conformidad con lo previsto en la Ley y el presente Reglamento.

La Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros solicita a cualquier entidad de la Administración Pública la entrega del software acreditado de validación y generación de firmas digitales de su titularidad, incluyendo como mínimo los ejecutables, los identificadores, la documentación asociada a fin de dar cumplimiento a lo dispuesto en el presente Reglamento.

Décima Cuarta. Plazos para la integración de la plataforma FIRMA PERÚ

La Secretaría de Gobierno Digital en un plazo no mayor a dos (02) meses, contados a partir de la información entregada por el RENIEC a la que se refiere la Décima Tercera Disposición Complementaria Final, implementa la Plataforma FIRMA PERÚ.

Las entidades de la Administración Pública, posterior a la emisión de la directiva de la Plataforma FIRMA PERÚ, se integran con la misma conforme a los siguientes plazos:

a) Poder Ejecutivo hasta seis (06) meses.
b) Organismos Constitucionales Autónomos hasta seis (06) meses.
c) Gobiernos regionales y universidades públicas hasta un (01) año.
d) Gobiernos locales Tipo A y Tipo C hasta un (01) año.
e) Gobiernos locales Tipo B hasta dieciocho (18) meses.

Las demás entidades en función de sus capacidades y recursos pueden integrar sus sistemas de información con la Plataforma FIRMA PERÚ.

La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, amplía los plazos de integración en función de las capacidades y recursos de las entidades; la misma que se hace efectiva mediante Resolución de Secretaría de Gobierno Digital.

Décima Quinta. Registro de tasas en la plataforma PÁGALO.PE

Las entidades de la Administración Pública registran todas las tasas y los pagos por derechos de tramitación de sus servicios y trámites en la plataforma PÁGALO.PE; los cuales deben encontrarse en sus instrumentos de gestión vigente. Los plazos para el registro, a partir de la publicación del presente Reglamento, son:

a) Poder Ejecutivo hasta un (01) año.

b) Organismos Constitucionales Autónomos hasta un (01) año.
c) Gobiernos regionales y universidades públicas hasta un (01) año.
d) Gobiernos locales Tipo A y Tipo C hasta un (01) año.
e) Gobiernos locales Tipo B hasta dos (02) años.
f) Las empresas públicas de los gobiernos regionales, locales, o bajo el ámbito del Fondo Nacional de Financiamiento de la Actividad Empresarial del Estado (FONAFE) hasta un (01) año.

La aplicación de la presente disposición corresponde a las entidades públicas que efectúan la recaudación de sus ingresos a través del Banco de la Nación, sin perjuicio de lo indicado en el numeral 89.6 del artículo 89 del presente Reglamento.
La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, amplía los plazos de registro en función de las capacidades y recursos de las entidades; la misma que se hace efectiva mediante Resolución de Secretaría de Gobierno Digital.

Décima Sexta. Ampliación de la plataforma PÁGALO.PE
En un plazo no mayor a un (01) año, posterior a la publicación del presente Reglamento, el Banco de la Nación implementa el mecanismo necesario que permite la integración directa de la plataforma PÁGALO.PE con los servicios digitales prestados por las entidades públicas para el pago en línea de sus derechos de tramitación de forma automática y en tiempo real.

Décima Séptima. Integración de los servicios digitales con la plataforma PÁGALO.PE
Las entidades de la Administración Pública, posterior a la implementación del mecanismo al que hace referencia la Décima Sexta Disposición Complementaria Final, integran sus servicios digitales con la plataforma PÁGALO.PE para el pago en línea de sus derechos de tramitación de forma automática y en tiempo real, teniendo en consideración las disposiciones establecidas por el Banco de la Nación, y en los siguientes plazos:

a) Poder Ejecutivo, Organismos Constitucionales Autónomos hasta seis (06) meses.
b) Gobiernos regionales y universidades públicas hasta un (01) año.
c) Gobiernos locales Tipo A y Tipo C hasta dieciocho (18) meses.
d) Gobiernos locales Tipo B hasta dos (02) años.
e) Las empresas públicas de los gobiernos regionales, locales, o bajo el ámbito del Fondo Nacional de Financiamiento de la Actividad Empresarial del Estado (FONAFE) hasta dieciocho (18) meses.

Las demás entidades públicas en función de sus capacidades y recursos pueden integrarse con la referida plataforma PÁGALO.PE, sin perjuicio de lo indicado en el numeral 89.6 del artículo 89 del presente Reglamento.
La aplicación de la presente disposición corresponde a las entidades públicas que efectúan la recaudación de sus ingresos a través del Banco de la Nación.
La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, amplía los plazos de integración en función de las capacidades y recursos de las entidades; la misma que se hace efectiva mediante Resolución de Secretaría de Gobierno Digital.

Décima Octava. Infraestructura tecnológica y plataforma tecnológica como servicio para gobiernos locales
La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, en un periodo no mayor a un (01) año, posterior a la publicación del presente Reglamento, implementa lo dispuesto en el numeral 92.5 del artículo 92 del presente Reglamento.

Décima Novena. Vocabularios básicos para la interoperabilidad
La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, en coordinación con el Registro Nacional de Identificación y Estado Civil, la Superintendencia Nacional de Migraciones, la Superintendencia Nacional de Registros Públicos, Superintendencia Nacional de Aduana y Administración Tributaria y el Instituto Nacional de Estadística e Informática, en un periodo no mayor a un (01) año, posterior a la publicación del presente Reglamento, elaboran los vocabularios básicos de los datos maestros para la interoperabilidad.

Vigésima. Gestión de Identificadores de Objetos
La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, es la entidad responsable de la gestión y asignación de identificadores de objetos (OID) para el ámbito nacional, bajo la rama {joint-iso-itu-t(2) country(16) pe(604)}, y realiza las acciones necesarias para su implementación. Asimismo, coordina con el Instituto Nacional de la Calidad (INACAL) y el Ministerio de Transportes y Comunicaciones (MTC), la comunicación a la Organización Internacional de Estandarización (ISO) y a la Unión Internacional de Telecomunicaciones (UIT) para el reconocimiento correspondiente, en un plazo no mayor a tres (03) meses posteriores a la publicación del presente Reglamento.

Vigésima Primera. Portal de Software Público Peruano, Portal Nacional de Datos Abiertos, Oficial de Seguridad de la Información, ID PERÚ y Encuesta Nacional de Recursos Informáticos de la Administración Pública
Para todo efecto la mención al Portal de Software Público Peruano, Portal Nacional de Datos Abiertos, Oficial de Seguridad de la Información, ID PERÚ y Encuesta Nacional de Recursos Informáticos de la Administración Pública que se efectúe en cualquier disposición, norma o documento de gestión debe entenderse a la Plataforma Nacional de Software Público Peruano, Plataforma Nacional de Datos Abiertos, Oficial de Seguridad Digital, ID GOB.PE y Encuesta Nacional de Activos Digitales del Estado respectivamente.

Vigésima Segunda. Opiniones técnicas
La Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros, en un periodo no mayor a tres (03) meses, posterior a la publicación del presente Reglamento, aprueba la norma que contiene los procedimientos, criterios y requisitos para la emisión de la opinión técnica previa de los proyectos de tecnologías digitales de carácter transversal al que se refiere el artículo 5 de la presente norma. Asimismo, en los referidos lineamientos se establecerán los plazos para la emisión de la opinión técnica vinculante y opinión técnica especializada a los que se refieren los artículos 6 y 7 respectivamente del presente Reglamento.
El artículo 5 del presente Reglamento no será aplicable a los proyectos de tecnologías digitales de carácter transversal iniciados con anterioridad a la entrada en vigencia de esta norma, a los proyectos de inversión pública que se encuentren aprobados o en ejecución, así como a los proyectos de inversión privada desarrollados al amparo del Decreto Legislativo Nº 1362, Decreto Legislativo que regula la Promoción de la Inversión Privada mediante Asociaciones Público - Privadas y Proyectos en Activos. Asimismo, tampoco será aplicable a las ventanillas únicas digitales que se encuentren en operación o hayan sido creadas a la entrada en vigencia de esta norma.

Vigésima Tercera. Soluciones de firma digital adquiridas o desarrolladas
Aquellas entidades que hayan adquirido, desarrollado o reutilizado una solución de firma digital en el marco de la IOFE, con anterioridad a la publicación del presente reglamento, pueden integrarse con la plataforma FIRMA PERÚ.

Vigésima Cuarta. Prohibición de usar mecanismos alternativos a los bloques básicos para la interoperabilidad técnica
A partir del 01 de enero del 2022 las entidades públicas quedan prohibidas de adquirir, desarrollar o utilizar

aplicativos, plataformas, recursos o servicios que posean las mismas funcionalidades provistas por los bloques básicos para la interoperabilidad técnica establecidos en el artículo 87 del presente Reglamento. El MINCETUR, en su calidad de administrador de la Ventanilla Única de Comercio Exterior, utiliza dicha plataforma e implementa progresivamente el uso de las plataformas ID GOB. PE, CASILLA ÚNICA PERÚ, MESA DIGITAL PERÚ y PAGALO.PE de acuerdo con sus estrategias y planes institucionales.

Asimismo, la SUNAT utiliza su sistema informático SUNAT Operaciones en Línea y la Clave SOL, e implementa progresivamente el uso de las plataformas ID GOB.PE, CASILLA ÚNICA PERÚ, MESA DIGITAL PERÚ, PAGALO.PE y FIRMA PERÚ de acuerdo con sus estrategias y planes institucionales.

La presente disposición no será aplicable a los proyectos de inversión pública que se encuentren aprobados o en ejecución a la entrada en vigencia de esta norma. Finalizado el proyecto de inversión pública las entidades responsables del mismo planifican su integración progresiva con los referidos bloques básicos para la interoperabilidad técnica, en lo que corresponda, en coordinación con la Secretaría de Gobierno Digital.

Vigésima Quinta. Mesa de partes digital institucional y Plataforma Única de Recepción Documental del Estado Peruano

Las mesas de partes digitales o similares puestas a disposición por las entidades públicas a través de sus sedes digitales coexisten con la Plataforma Única de Recepción Documental del Estado Peruano hasta la culminación del proceso de integración a la misma, conforme los plazos establecidos en la Novena Disposición Complementaria Final.

Vigésima Sexta. Estándares para datos y metadatos estadísticos

El Instituto Nacional de Estadística e Informática (INEI) es responsable de definir y establecer los formatos y estándares para el intercambio de datos y metadatos estadísticos en el Estado peruano.

Vigésima Séptima. Servicios de información espacial o georreferenciada

En un plazo no mayor a dieciocho (18) meses, posterior a la publicación del presente reglamento, las entidades del Poder Ejecutivo y gobiernos regionales implementan servicios de información espacial o georreferenciada correspondientes a los datos espaciales que producen en el marco de sus competencias. La información de dichos servicios se registra en el Catálogo Nacional de Metadatos Espaciales y publica en la Plataforma Digital GEOPERÚ.

Vigésima Octava. Implementación de la Plataforma Digital de Información de la Arquitectura Digital del Estado

En un plazo no mayor a nueve (09) meses, posterior a la publicación del presente reglamento, la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros habilita la Plataforma Digital de Información de la Arquitectura Digital del Estado. La referida Plataforma Digital toma como base el desarrollo del aplicativo informático para el registro del Plan de Gobierno Digital.

Vigésima Novena. Modelos de Referencia de la Arquitectura Digital del Estado

En un plazo no mayor a doce (12) meses, posterior a la publicación del presente Reglamento, la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, aprueba las Guías de los Modelos de Referencia de la Arquitectura Digital.

Trigésima. Aprobación de estándares y guías de acreditación para servicios de firma digital remota y servicios de preservación digital

En un plazo no mayor a ciento ochenta (180) días calendario, contados a partir de la publicación del presente Reglamento, la Autoridad Administrativa Competente de la IOFE aprueba los estándares técnicos relacionados con los servicios de firma digital remota y con los servicios de preservación digital; y, en un plazo no mayor a un (01) año aprueba las guías de acreditación correspondientes para aquellos Prestadores de Servicios de Certificación Digital que opten por brindar cada uno de los referidos servicios.

Trigésima Primera. Implementación del servicio de información de recursos humanos del sector público

En un plazo no mayor a seis (06) meses, posterior a la publicación del presente Reglamento, el Ministerio de Economía y Finanzas (MEF) implementa y publica en la PIDE el servicio de información que retorna datos sobre los recursos humanos del sector público registrados en el "Aplicativo Informático para el Registro Centralizado de Planillas y de Datos de los Recursos Humanos del Sector Público" en situación activa o inactiva. El servicio de información provee, como mínimo, los siguientes datos por cada consulta: a) Número de documento de identidad, b) Nombres y apellidos, c) Sector según corresponda, d) Pliego según corresponda, e) Entidad, f) Cargo funcional, g) Fecha de inicio, y, h) Fecha de fin.

Trigésima Segunda. Reconocimiento transfronterizo de la identidad digital

La Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros, en coordinación con el Ministerio de Relaciones Exteriores, promueve la suscripción de acuerdos de cooperación para el reconocimiento transfronterizo de la identidad digital de los ciudadanos peruanos en el extranjero, prioritariamente con los países que conforman el Mercado Común del Sur (MERCOSUR), Comunidad Andina y la Alianza del Pacífico (AP).

Trigésima Tercera. Actualización de normas internas para el gobierno digital

Las entidades comprendidas en el alcance incorporan en sus Planes Operativos Institucionales, Planes Estratégicos Institucionales, Plan de Desarrollo de Personas, Plan Anual de Contrataciones y demás instrumentos los objetivos, acciones y actividades necesarias para la implementación del presente Reglamento.

Asimismo, dichas entidades, posterior a la publicación del presente Reglamento, realizan las modificaciones correspondientes en sus normas internas a fin de soportar el flujo documental digital en todos sus procesos, en los siguientes plazos:

a) Poder Ejecutivo hasta un (01) año.
b) Organismos Constitucionales Autónomos hasta un (01) año.
c) Gobiernos regionales hasta un (01) año.
d) Gobiernos locales Tipo A y Tipo C hasta un (01) año.
e) Gobiernos locales Tipo B hasta dieciocho (18) meses.
f) Las empresas públicas de los gobiernos regionales, locales, o bajo el ámbito del Fondo Nacional de Financiamiento de la Actividad Empresarial del Estado (FONAFE) hasta dieciocho (18) meses.

Trigésima Cuarta. Planes de apertura de datos

Las entidades de la Administración Pública, posterior a la publicación del presente Reglamento, aprueban y publican planes de apertura de datos, en los siguientes plazos:

a) Poder Ejecutivo, Organismos Constitucionales Autónomos y empresas del Estado hasta seis (06) meses.
b) Gobiernos regionales, universidades públicas y gobiernos locales tipo A y C hasta un (01) año.

Los demás gobiernos locales proceden a la apertura de sus datos en función de sus capacidades y recursos.

Trigésima Quinta. Estrategia Nacional de Gobierno de Datos e Inteligencia Artificial, Estrategia Nacional de Seguridad y Confianza Digital y Estrategia Nacional de Talento e Innovación Digital

La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, aprueba una Estrategia Nacional de Gobierno de Datos e

Inteligencia Artificial, una Estrategia Nacional de Seguridad y Confianza Digital, y una Estrategia Nacional de Talento e Innovación Digital, en un plazo no mayor a ciento ochenta (180) días hábiles, posterior a la publicación del presente Reglamento, las cuales se actualizan cada dos (02) años, y se elaboran con la participación del sector público, la academia, sector privado y sociedad civil.

Trigésima Sexta. Apertura por defecto de datos económicos y de contrataciones

Los datos disponibles en el Portal de Transparencia Económica del Ministerio de Economía y Finanzas, así como los datos obtenidos a partir de información registrada en el Sistema Electrónico de Contrataciones del Estado (SEACE); se publica automáticamente y por defecto en la Plataforma Nacional de Datos Abiertos, en un plazo no mayor a seis (06) meses, posterior a la publicación del presente Reglamento, con excepción de la información calificada como secreta, reservada o confidencial y los datos personales, en observancia de las normas legales vigentes.

Trigésima Séptima. Competencias y talento digital para el acceso y uso de servicios digitales

La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, en coordinación con los actores del Sistema Nacional de Transformación Digital promueven las acciones para el desarrollo del talento digital de los ciudadanos y personas en general, a fin de asegurar el ejercicio de ciudadanía digital, así como el desarrollo de competencias digitales para el acceso y uso a contenidos y servicios digitales provistos por el sector público y privado.

Trigésima Octava. Nombres de dominio de la Administración Pública

La estandarización y validación de los nombres de dominio de la Administración Pública y empresas públicas se encuentra a cargo de la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, quien emite las normas correspondientes.

Trigésima Novena. Fiscalización y Supervisión

La Contraloría General de la República, a través de los órganos de control institucional de cada entidad de la Administración Pública, conforme a sus competencias, verifican de oficio que los funcionarios y servidores cumplan con implementar las disposiciones y plazos previstos en el presente Reglamento. Asimismo, corresponde a Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, en el ejercicio de sus funciones de supervisión y fiscalización, realizar las gestiones conducentes para hacer efectiva la responsabilidad de los funcionarios en la implementación del presente Reglamento, para lo cual reporta a la Contraloría General de la República para las acciones correspondientes.

El incumplimiento de lo dispuesto en el presente Reglamento genera responsabilidad administrativa disciplinaria pasible de sanción en observancia a las normas del régimen disciplinario y procedimiento sancionador de la Ley Nº 30057, Ley del Servicio Civil y su Reglamento General, aprobado por Decreto Supremo Nº 040-2014-PCM. Corresponde a la máxima autoridad administrativa de cada entidad asegurar el cumplimiento de la presente disposición.

Cuadragésima. Interoperabilidad de las firmas electrónicas cualificadas

La Entidad de Certificación Nacional para el Estado Peruano, en un plazo no mayor a un (01) año, posterior a la publicación del presente Reglamento, emite los lineamientos para la generación, uso, validación y verificación de las firmas electrónicas cualificadas para su interoperabilidad en el marco del modelo de gestión documental.

La interoperabilidad internacional a través de la VUCE para asuntos de comercio exterior se realiza conforme a los acuerdos o convenios internacionales suscritos por el Perú.

Cuadragésima Primera. Condiciones tecnológicas para gobiernos locales

La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, en un plazo no mayor a seis (06) meses, posterior a la publicación del presente Reglamento, emite las disposiciones sobre las condiciones tecnológicas mínimas y plazos para la implementación del presente Reglamento por parte de los gobiernos locales. La presente disposición no se aplica a los gobiernos locales de Lima Metropolitana y Callao ni aquellos que son capitales de provincia.

La Secretaría de Gobierno Digital provee el soporte técnico y herramientas para la adopción de los bloques básicos para la interoperabilidad técnica por parte de las municipalidades pertenecientes a ciudades principales tipo F y G.

Cuadragésima Segunda. Aprobación de normas para el Documento Nacional de Identidad digital

El Registro Nacional de Identificación y Estado Civil, en un plazo no mayor a dos (02) años, posterior a la publicación del presente Reglamento, aprueba los requisitos, características, lineamientos y procedimientos del Documento Nacional de Identidad digital, la cual se hace efectiva mediante Resolución Jefatural.

Cuadragésima Tercera. Estándares, lineamientos y perfiles técnicos sobre el expediente electrónico

En un plazo no mayor a un (01) año, posterior a la publicación del presente Reglamento, la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, emite el perfil mínimo de metadatos del expediente electrónico, los lineamientos para su gestión y los estándares técnicos de su estructura.

Cuadragésima Cuarta. Normas para la determinación, adquisición y uso de NUBE PERÚ

En un plazo no mayor a seis (06) meses, posterior a la publicación del presente Reglamento, la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, emite las normas para la determinación, adquisición y uso de infraestructuras tecnológicas y plataformas tecnológicas provistas en la modalidad de infraestructura y plataforma como servicio (NUBE PERÚ).

Cuadragésima Quinta. Uso de la Plataforma IDGOB PERÚ para el acceso a sistemas de información de las entidades públicas

La Plataforma ID GOB.PE es utilizada para proveer el acceso de funcionarios y servidores públicos a los sistemas de información de las entidades públicas accesibles desde Internet, para el ejercicio de sus funciones o actuaciones a su cargo. Asimismo, la referida plataforma es utilizada para proveer el acceso a los sistemas de información de usuarios autorizados o representantes legales de personas jurídicas que requieran interactuar con las entidades públicas.

La Plataforma ID GOB.PE sólo otorga garantía sobre la identificación de la persona natural, mas no sobre el cargo, rol, atribuciones o facultades que ostenta un funcionario o servidor de una entidad de la Administración Pública, o usuario autorizado o representante legal de una persona jurídica.

La entidad pública es responsable de gestionar las autorizaciones de acceso y asignación de roles, atribuciones o facultades en los referidos sistemas de información.

Cuadragésima Sexta. Implementación del servicio de información de representante legal

En un plazo no mayor a nueve (09) meses, posterior a la publicación del presente Reglamento, la Superintendencia Nacional de Registros Públicos (SUNARP) en coordinación con la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros, desarrolla, implementa y publica en la PIDE el servicio de información que retorna datos sobre los representantes legales de personas jurídicas inscritas. El servicio de información tiene como parámetros de entrada el número de documento de identidad, y provee, como mínimo, los siguientes datos por cada

consulta: a) Denominación o razón social y b) Número de partida registral.

Hasta la implementación del servicio de información del representante legal de una persona jurídica, las entidades pueden utilizar el número del RUC otorgado por la SUNAT como identificador para la prestación de servicios digitales.

Cuadragésima Séptima. Código de Verificación Digital

La Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros, en un plazo no mayor a tres (03) meses, posterior a la publicación del presente Reglamento, emite las normas para la generación y uso del Código de Verificación Digital.

Cuadragésima Octava. Conformación de Equipos de Respuestas ante Incidentes de Seguridad Digital

La Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros en un plazo no mayor a tres (03) meses, posterior a la publicación del presente Reglamento, emite las normas para la implementación y conformación de Equipos de Respuestas ante Incidentes de Seguridad Digital y Redes de Confianza.

Las entidades de la Administración Pública, posterior a la publicación de las normas a las que se hace referencia en el párrafo precedente, conforman sus Equipos de Respuestas ante Incidentes de Seguridad Digital conforme a los siguientes plazos:

a) Poder Ejecutivo y Organismos Constitucionales Autónomos hasta seis (06) meses.

b) Gobiernos regionales y universidades públicas hasta un (01) año.

c) Gobiernos locales Tipo A y Tipo C hasta dieciocho (18) meses.

d) Gobiernos locales Tipo B hasta dos (02) años.

e) Las empresas públicas de los gobiernos regionales, locales, o bajo el ámbito del Fondo Nacional de Financiamiento de la Actividad Empresarial del Estado (FONAFE) hasta un (01) año.

Las demás entidades en función de sus capacidades y recursos pueden conformar los referidos Equipos de Respuestas ante Incidentes de Seguridad Digital.

La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, amplía los plazos de conformación en función de las capacidades y recursos de las entidades, la misma que se hace efectiva mediante Resolución de Secretaría de Gobierno Digital.

Cuadragésima Novena. Interconexión de sistemas de trámite documentario o equivalentes

Las entidades de la Administración Pública, de conformidad con lo establecido en el artículo 8 del Decreto Legislativo Nº 1310, Decreto Legislativo que aprueba medidas adicionales de Simplificación Administrativa, interconectan e integran sus sistemas de trámite documentario o equivalentes para el envío automático de documentos electrónicos con otras entidades, a través de la Plataforma de Interoperabilidad del Estado, en los siguientes plazos:

a) Organismos Constitucionales Autónomos, gobiernos regionales, universidades públicas, gobiernos locales Tipo A, Tipo B y Tipo C, y empresas públicas de los gobiernos regionales, locales, o bajo el ámbito del Fondo Nacional de Financiamiento de la Actividad Empresarial del Estado (FONAFE) hasta el 31 de diciembre de 2021.

b) Gobiernos locales Tipo D, Tipo E, Tipo F y Tipo G hasta el 31 de julio de 2022.

Los gobiernos locales tipo D, E, F y G que no intervienen como administrados en un procedimiento administrativo pueden presentar documentos electrónicos vía plataformas de recepción documental, mesas de partes digital o similares aplicando las alternativas señaladas en el numeral 47.1 del artículo 47 del presente Reglamento, hasta la culminación de la interconexión de sus sistemas de trámite documentario a la que se refiere el párrafo precedente.

La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, amplía los plazos de implementación en función de las capacidades y recursos de las entidades, la misma que se hace efectiva mediante Resolución de Secretaría de Gobierno Digital.

Quincuagésima. Interoperabilidad a favor de los gobiernos regionales

Las entidades del Poder Ejecutivo a las que se refiere el artículo 1 del Decreto Supremo Nº 002-2018-MINAGRI, Decreto Supremo que exonera del pago de tasas y cualquier otro derecho de trámite ante diversas entidades del Poder Ejecutivo a los Gobiernos Regionales en el ejercicio de la función descrita en el literal n) del artículo 51 de la Ley Nº 27867, Ley Orgánica de Gobiernos Regionales, de manera progresiva y gratuita publican información en la Plataforma de Interoperabilidad del Estado para el consumo de los gobiernos regionales a cargo del ejercicio de la función descrita en el literal n) del artículo 51 de la Ley Nº 27867, Ley Orgánica de Gobiernos Regionales.

Quincuagésima Primera. Aplicación normativa

Los procedimientos y servicios tramitados a través de la Ventanilla Única de Comercio Exterior (VUCE) se efectúan en concordancia con lo establecido en la Ley Nº 30860, Ley de Fortalecimiento de la Ventanilla Única de Comercio Exterior y su Reglamento, siendo aplicable de manera supletoria lo dispuesto en el Capítulo I, II, III, V y VI del Título IV y Título II del presente Reglamento en lo que corresponda.

Los procedimientos, actos o actuaciones que se realizan en virtud de las competencias otorgadas por el Código Tributario, la Ley General de Aduanas y demás normas que atribuyen competencia a las Administraciones Tributarias, SUNAT y el Tribunal Fiscal, incluyendo aquellos casos en los que además se requiere la suscripción de un convenio interinstitucional conforme lo previsto en el tercer párrafo del artículo 5 de la Ley Nº 29816, Ley de Fortalecimiento de la SUNAT o en una norma con rango de ley o decreto supremo que lo establezca, se regulan por sus normas especiales, siendo que, en lo no previsto en estas, resulta aplicable supletoriamente lo dispuesto en los Títulos II y IV del presente Reglamento en lo que corresponda. Sin perjuicio de ello las mencionadas entidades pueden optar voluntariamente por integrarse con la plataforma ID GOB.PE, CASILLA ÚNICA PERÚ y MESA DIGITAL PERÚ, para lo cual aprobarán las normas correspondientes.

La SUNAT puede utilizar en su relación con los administrados los sistemas, aplicaciones móviles y otros productos informáticos desarrollados en virtud de las facultades que le otorga la normativa que la regula, como es el caso del sistema informático SUNAT Operaciones en Línea y la Clave SOL, incluyendo la utilización de esta para generar la firma electrónica, asimismo, implementa progresivamente el uso de los bloques básicos de interoperabilidad técnica de acuerdo con sus estrategias y planes institucionales.

Sin perjuicio de lo indicado precedentemente tanto la VUCE como el sistema informático SUNAT Operaciones en Línea (SOL) interoperan progresivamente en lo que corresponda con los bloques básicos de interoperabilidad técnica.

La regulación y supervisión de los sistemas, productos y servicios supervisados por la Superintendencia de Banca, Seguros y AFP se rigen en virtud del principio de especialidad normativa por la Ley Nº 26702, Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros.

Quincuagésima Segunda. Glosario de términos

Se incluye el Glosario de Términos para el adecuado entendimiento del presente Reglamento, conforme al Anexo adjunto a la presente norma.

DISPOSICIONES COMPLEMENTARIAS TRANSITORIAS

Primera. Adecuación y registro en el Catálogo Oficial de Aplicativos Móviles

Las entidades de la Administración Pública que cuentan con aplicativos registrados en los repositorios de distribución de aplicativos móviles implementan las adecuaciones correspondientes y solicitan su registro en el Catálogo Oficial de Aplicativos Móviles en un periodo no mayor a dos (02) años, contado a partir de la emisión de los lineamientos a los que hace referencia la Quinta Disposición Complementaria Final.

Segunda. Obligatoriedad de la implementación de los servicios digitales

Las entidades comprendidas en el alcance incorporan anualmente en sus instrumentos de gestión, acciones o actividades para la implementación de servicios digitales no presenciales o semipresenciales conforme lo dispuesto en el presente Reglamento, salvo aquellas entidades que dispongan de todos sus procedimientos o servicios accesibles a través de canales digitales.

La implementación de la digitalización de procesos de comercio exterior se efectúa de manera progresiva en concordancia con lo señalado en el artículo 5 del Decreto Legislativo Nº 1492, Decreto Legislativo que aprueba Disposiciones para la Reactivación, Continuidad y Eficiencia de las Operaciones vinculadas a la Cadena Logística de Comercio Exterior y su Reglamento.

Tercera. Mecanismos existentes de casilla electrónica

Las entidades públicas que hayan implementado algún mecanismo de notificación haciendo uso de tecnologías y medios electrónicos (casillas electrónicas, sistemas de notificación electrónica, buzones electrónicos o similares) se adaptan e integran de manera progresiva con la plataforma Casilla Única Perú, hasta el 31 de diciembre del 2022; sin perjuicio, de continuar con la utilización de los referidos mecanismos de notificación durante dicho período.

Las entidades a las que se hace referencia en el numeral 58.6 del presente Reglamento quedan exceptuadas de la presente disposición.

Cuarta. Reconocimiento de Prestadores de Servicios de Valor Añadido en la modalidad de sistema de creación de firma remota

Las empresas que cuenten con acreditación nacional o certificación internacional vigente como proveedores de servicios de creación de firma remota o equivalentes pueden prestar sus servicios a entidades públicas y privadas sin encontrarse acreditadas como tales ante la Autoridad Administrativa Competente (AAC), previo cumplimiento del procedimiento de reconocimiento que disponga la AAC, hasta por un plazo no mayor a dieciocho (18) meses, posterior a la publicación del presente Reglamento. Tales empresas ponen en conocimiento de la AAC, a través de sus representantes en el país, de ser el caso, sus operaciones en el ámbito nacional para su incorporación en el Registro Oficial de Prestadores de Servicios de Certificación Digital como Prestadores de Servicios de Valor Añadido reconocidos en la modalidad de sistema de creación de firma remota. En dicho plazo las referidas empresas concluyen su proceso de acreditación ante la AAC. Si cumplido el plazo del reconocimiento, la empresa no hubiese obtenido la acreditación ante la AAC, ésta la retira del Registro Oficial de Prestadores de Servicios de Certificación Digital.

DISPOSICIONES COMPLEMENTARIAS MODIFICATORIAS

Primera. Incorporación de los artículos 1A y 2A en el Reglamento de la Ley Nº 27269, Ley de Firmas y Certificados Digitales, aprobado por Decreto Supremo Nº 052-2008-PCM

Incorpóranse los artículos 1A y 2A en el Reglamento de la Ley Nº 27269, Ley de Firmas y Certificados Digitales, aprobado por Decreto Supremo Nº 052-2008-PCM, en los siguientes términos:

"Artículo 1A.- Modalidades de la firma electrónica

Se reconocen las siguientes tres (03) modalidades de firma electrónica:

a) Firma Electrónica Simple. Es un dato en formato electrónico anexo a otros datos electrónicos o asociado de manera lógica con ellos, que utiliza un firmante para firmar.

b) Firma Electrónica Avanzada. Es aquella firma electrónica simple que cumple con las siguientes características: (i) está vinculada al firmante de manera única, (ii) permite la identificación del firmante, (iii) ha sido creada utilizando datos de creación de firmas que el firmante puede utilizar bajo su control, y (iv) está vinculada con los datos firmados de modo tal que cualquier modificación posterior de los mismos es detectable.

c) Firma Electrónica Cualificada. La firma electrónica cualificada o firma digital es aquella firma electrónica avanzada que cumple con lo establecido en el capítulo II del presente Reglamento.

Artículo 2A.- Carga de la prueba de la firma electrónica

Para cada modalidad de firma electrónica la aplicación de la carga de la prueba varía conforme a lo siguiente:

a) En caso de controversia sobre la autoría de la firma electrónica simple o avanzada, la carga de la prueba recae en quien la invoque como auténtica.

b) En caso de controversia, en la utilización de la firma electrónica cualificada, la carga de la prueba se invierte debiendo quien niegue la autoría, demostrar que la firma es apócrifa.

(...)".

Segunda. Modificación de los artículos 6, 8, 10, 15, 16, 29, 33, 35, 36, 45, 46, 47, 48, 57, 60, Octava y Décima Cuarta Disposición Complementaria Final del Reglamento de la Ley Nº 27269, Ley de Firmas y Certificados Digitales, aprobado por Decreto Supremo Nº 052-2008-PCM y modificatorias

Modifícanse los artículos 6, 8, 10, 15, 16, 29, 33, 35, 36, 45, 47, 48, el literal a) del artículo 46, el literal h) del artículo 57, artículo 60, la Octava Disposición Complementaria Final y el octavo término de la Décima Cuarta Disposición Complementaria Final del Reglamento de la Ley Nº 27269, Ley de Firmas y Certificados Digitales, aprobado por Decreto Supremo Nº 052-2008-PCM y modificatorias, en los siguientes términos:

"Artículo 6.- Firma digital

Es aquella firma electrónica que utilizando una técnica de criptografía asimétrica, permite la identificación del signatario y ha sido creada por medios, incluso a distancia, que garantizan que éste mantiene bajo su control con un elevado grado de confianza, de manera que está vinculada únicamente al signatario y a los datos a los que refiere, lo que permite garantizar la integridad del contenido y detectar cualquier modificación ulterior, tiene la misma validez y eficacia jurídica que el uso de una firma manuscrita, siempre y cuando haya sido generada por un Prestador de Servicios de Certificación Digital debidamente acreditado que se encuentre dentro de la Infraestructura Oficial de Firma Electrónica, y que no medie ninguno de los vicios de la voluntad previstos en el Título VIII del Libro IV del Código Civil.

(…)

Artículo 8.- Presunciones

Tratándose de documentos electrónicos firmados digitalmente a partir de certificados digitales generados dentro de la Infraestructura Oficial de Firma Electrónica, se aplican las siguientes presunciones:

a) Que el suscriptor del certificado digital tiene el control de la clave privada asociada, con un elevado grado de confianza, incluso cuando la misma es gestionada por un Prestador de Servicios de Valor Añadido acreditado en la modalidad de sistema de creación de firma remota.

(…)

Artículo 10.- Obligaciones del suscriptor

Las obligaciones del suscriptor son:

a) Entregar información veraz bajo su responsabilidad.

b) Generar por sí mismo la clave privada, o autorizar

su generación a distancia por parte de un Prestador de Servicios de Valor Añadido acreditado en la modalidad de sistema de creación de firma remota, y firmar digitalmente mediante los procedimientos señalados por la Entidad de Certificación.

c) Mantener el control y la reserva de la clave privada bajo su responsabilidad, sin perjuicio de la responsabilidad del Prestador de Servicios de Valor Añadido acreditado en la modalidad de sistema de creación de firma remota que genere la clave privada para el servicio de firma remota.

(…)

Artículo 15.- Obligaciones del titular

Las obligaciones del titular son:

(…)

c) Solicitar la cancelación de su certificado digital en caso de que la reserva sobre la clave privada se haya visto comprometida, bajo responsabilidad, excepto cuando dicha clave sea gestionada por un Prestador de Servicios de Valor Añadido acreditado en la modalidad de sistema de creación de firma remota.

d) Cumplir permanentemente las condiciones establecidas por la Entidad de Certificación para la utilización del certificado y, en su caso, por el Prestador de Servicios de Valor Añadido acreditado en la modalidad de sistema de creación de firma remota.

Artículo 16.- Contenido y vigencia

Los certificados emitidos dentro de la Infraestructura Oficial de Firma Electrónica contienen como mínimo, además de lo establecido en el artículo 7 de la Ley, lo siguiente:

a) Para personas naturales:

• Nombres y apellidos completos
• Número de documento oficial de identidad
• Tipo de documento
• Dirección electrónica de los servicios donde consultar el estado de validez del certificado
• Dirección electrónica del certificado de la entidad de certificación emisora
• Identificador de la política de certificación bajo la cual fue emitido el certificado

b) Para personas jurídicas (suscriptor):

• Denominación o razón social
• Número del Registro Único de Contribuyentes (RUC) de la organización
• Nombres y apellidos completos del suscriptor
• Número de documento oficial de identidad del suscriptor
• Tipo de documento del suscriptor
• Dirección electrónica de los servicios donde consultar el estado de validez del certificado
• Dirección electrónica del certificado de la entidad de certificación emisora
• Identificador de la política de certificación bajo la cual fue emitido el certificado

c) Para personas jurídicas (titular):

• Denominación o razón social
• Número del Registro Único de Contribuyentes (RUC) de la organización
• Nombre del sistema de información o sistema de cómputo
• Dirección electrónica de los servicios donde consultar el estado de validez del certificado
• Dirección electrónica del certificado de la entidad de certificación emisora
• Identificador de la política de certificación bajo la cual fue emitido el certificado

(…)

Artículo 29.- Funciones

Las Entidades de Registro o Verificación tienen las siguientes funciones:

a) Identificar a los titulares y/o suscriptores del certificado digital mediante el levantamiento de datos y la comprobación de la información brindada por aquél. La identificación y comprobación debe efectuarse: (i) en presencia física del solicitante, o (ii) a distancia, mediante el uso de los certificados digitales del solicitante entregados en su Documento Nacional de Identidad electrónico o digital, o (iii) a distancia, utilizando métodos de identificación aprobados por la Autoridad Administrativa Competente que provean una seguridad equivalente en términos de fiabilidad a la presencia física.

(...)

Artículo 33.- Funciones

Los Prestadores de Servicios de Valor Añadido tienen las siguientes funciones:

(…)

d) Ofrecer servicios de gestión de claves privadas y creación de firmas digitales remotas de usuarios finales asociados a la prestación de servicios de valor añadido de firma remota.

(…)

Artículo 35.- Modalidades del Prestador de Servicios de Valor Añadido con firma digital del usuario final

Los Prestadores de Servicios de Valor Añadido que realizan procedimientos con firma digital del usuario final, pueden a su vez adoptar tres modalidades:

a) Sistema de Intermediación Digital cuyo procedimiento concluye con una microforma o microarchivo.

b) Sistema de Intermediación Digital cuyo procedimiento no concluye en microforma o microarchivo.

c) Sistema de creación de firma remota, que permite efectuar operaciones de creación de firma digital utilizando claves privadas que se encuentran localizadas remotamente y son gestionadas por un tercero.

(...)

Artículo 36.- Modalidad del Prestador de Servicios de Valor Añadido sin firma digital del usuario final

Los Prestadores de Servicios de Valor Añadido que realizan procedimientos sin firma digital del usuario final, pueden a su vez adoptar dos modalidades:

a) Sistema de sellado de tiempo. Consigna la fecha y hora cierta para evidenciar que un dato u objeto digital ha existido en un momento determinado del tiempo, y que no ha sido alterado desde entonces.

b) Sistema de preservación digital. Provee capacidades que permiten validar una firma digital en el largo plazo y/o pruebas de existencia de objetos digitales utilizando firmas digitales y sellos de tiempo.

(...)

Artículo 45.- Documento Nacional de Identidad Electrónico

El Documento Nacional de Identidad electrónico (DNIe) es un Documento Nacional de Identidad, emitido en una tarjeta inteligente por el Registro Nacional de Identificación y Estado Civil - RENIEC, que acredita presencial y/o electrónicamente la identidad personal de su titular, permitiendo la firma digital de documentos electrónicos y el ejercicio del voto electrónico presencial. A diferencia de los certificados digitales que pudiesen ser provistos por otras Entidades de Certificación públicas o privadas, aquellos incorporados en el Documento Nacional de Identidad Electrónico (DNIe) pueden usarse para el ejercicio del voto electrónico no presencial en los procesos electorales. El RENIEC dispone de las características y condiciones técnicas del Documento Nacional de Identidad Electrónico; así como los casos en los que no se incorporan los certificados digitales.

(...)

Artículo 46.- Estructura Jerárquica de Certificación del Estado Peruano

Las entidades que presten servicios de certificación digital en el marco de la Infraestructura Oficial de Firma Electrónica son las entidades de la administración pública o personas jurídicas de derecho público siguientes:

a) Entidad de Certificación Nacional para el Estado Peruano, la cual es la encargada de emitir los certificados subordinados para las Entidades de Certificación para el Estado Peruano que lo soliciten, además de proponer a la Autoridad Administrativa Competente, las políticas y estándares de las Entidades de Certificación para el Estado Peruano, Entidades de Registro o Verificación para el Estado Peruano y Prestadores de Servicios de Valor Añadido para el Estado Peruano, según los requerimientos de la Autoridad Administrativa Competente y lo establecido por el presente Reglamento.

(...)

d) Prestador de Servicios de Valor Añadido para el Estado Peruano acreditados por la Autoridad Administrativa Competente bajo cualquiera de las modalidades de servicio de valor añadido establecidas en el presente reglamento.

(…)

Los servicios brindados por los Prestadores de Servicios de Certificación Digital públicos se sustentan en los principios de acceso universal y no discriminación del uso de las tecnologías de la información y de comunicaciones, procurando que los beneficios resultantes contribuyan a la mejora de la calidad de vida de todos los ciudadanos. En consecuencia, las entidades públicas que presten servicios como Entidad de Certificación Nacional para el Estado Peruano, Entidades de Certificación para el Estado Peruano, Entidades de Registro o Verificación para el Estado Peruano y Prestador de Servicios de Valor Añadido para el Estado Peruano, sólo pueden considerar los costos asociados a la prestación del servicio al momento de determinar su valor a efectos de gestionar la asignación presupuestal correspondiente o determinar las tasas que garanticen su sostenibilidad en el tiempo.

Artículo 47.- Designación de las entidades responsables

Se designa a la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, como Entidad de Certificación Nacional para el Estado Peruano. La Secretaría de Gobierno Digital es responsable de la gestión de los servicios de la ECERNEP, así como también implementa y mantiene un canal digital para la difusión de sus contenidos e instrumentos, cuya dirección en Internet es www.ecernep.gob.pe.

Se designa al Registro Nacional de Identificación y Estado Civil - RENIEC como Entidad de Certificación para el Estado Peruano, Entidad de Registro o Verificación para el Estado Peruano. Los servicios a ser prestados en cumplimiento de los roles señalados están a disposición de todas las Entidades Públicas del Estado Peruano y de todas las personas naturales y jurídicas que mantengan vínculos con él, no excluyendo ninguna representación del Estado Peruano en el territorio nacional o en el extranjero. El Registro Nacional de Identificación y Estado Civil – RENIEC puede asimismo implementar y poner a disposición de las Entidades Públicas otros servicios de certificación de valor añadido contemplados en el presente reglamento.

(...)

Las demás entidades de la Administración Pública que opten por constituirse como Entidad de Certificación para el Estado Peruano, Entidad de Registro o Verificación para el Estado Peruano y/o Prestador de Servicios de Valor Añadido para el Estado Peruano cumplen con las políticas y estándares que sean propuestos por la Entidad de Certificación Nacional para el Estado Peruano y aprobadas por la Autoridad Administrativa Competente, y solicitar su acreditación correspondiente a fin de ingresar a la Infraestructura Oficial de Firma Electrónica.

Artículo 48.- Entidad de Certificación Nacional para el Estado Peruano

a) La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, es la única Entidad de Certificación Nacional para el Estado Peruano. Todos los prestadores de servicios de certificación para el Estado Peruano siguen las políticas y estándares propuestos por la Entidad de Certificación Nacional para el Estado Peruano y aprobados por la Autoridad Administrativa Competente.

b) La Entidad de Certificación Nacional para el Estado Peruano cuenta con una estructura funcional y jurídica estable y permanente dentro de la entidad que ejerce dicho rol, no cambiante en el tiempo, sólo variable en la cantidad de prestadores de servicios de certificación para el Estado Peruano que pueda tenerse bajo la Estructura Jerárquica de Certificación del Estado Peruano.

(…)

e) La Entidad de Certificación Nacional para el Estado Peruano participa como miembro con voz y voto en las comisiones, grupos de trabajo y/o órganos colegiados responsables de la gestión de la Infraestructura Oficial de la Firma Electrónica.

(...)

Artículo 57.- Funciones

La Autoridad Administrativa Competente tiene las siguientes funciones:

(...)

h) Publicar por medios telemáticos y sin restricción de acceso:

1. La relación de Prestadores de Servicios de Certificación Digital y su estado.

2. Sus procedimientos de gestión, organización y operación.

3. Los nombres de los integrantes que conforman o conformaron su estructura organizacional, técnica y operacional.

4. Todos sus documentos con carácter decisorio, así como aquellos de carácter resolutivo y administrativo (Resoluciones, ordenanzas o documentos similares).

5. Balance de gestión anual e indicadores.

i) Adoptar y aprobar el empleo de estándares técnicos internacionales dentro de la Infraestructura Oficial de Firma Electrónica, así como de otros estándares técnicos determinando su compatibilidad con los estándares internacionales; cooperar, dentro de su competencia, en la unificación de los sistemas que se manejan en los organismos de la Administración Pública, tendiendo puentes entre todos sus niveles; y, en la obtención de la interoperabilidad del mayor número de aplicaciones, componentes e infraestructuras de firmas digitales (análogos a la Infraestructura Oficial de Firma Electrónica en otros países).

(…)

Artículo 60º.- Acreditación de Entidades de Registro o Verificación

Las entidades que soliciten su acreditación y registro ante la Autoridad Administrativa Competente, como Entidades de Registro o Verificación, incluyendo las Entidades de Registro o Verificación para el Estado Peruano, deben contar con los requerimientos establecidos por la Autoridad Administrativa Competente para la prestación de sus servicios, los que tendrán que asegurar la verificación de la identidad del solicitante de un nuevo certificado digital conforme a lo establecido en el literal a) del artículo 29 del presente Reglamento.

(...)

"Octava. Plazo de Implementación de la Entidad de Certificación Nacional para el Estado Peruano, Entidad de Certificación para el Estado Peruano y Entidad de Registro o Verificación para el Estado Peruano

La Presidencia del Consejo de Ministros puede prestar sus servicios como Entidad de Certificación Nacional para el Estado Peruano (ECERNEP) sin encontrarse acreditada como tal ante la AAC, hasta el 31 de diciembre del 2022. En dicho periodo la Presidencia del Consejo de Ministros concluye su proceso de acreditación ante la AAC.

El Registro Nacional de Identificación y Estado Civil (RENIEC) tendrá un plazo hasta el 31 de julio del 2012 para iniciar los procedimientos de acreditación respectivos ante el INDECOPI. Este último contará con un plazo máximo de 120 días hábiles para culminarlos, sin perjuicio de lo dispuesto en el artículo 67 del presente Reglamento.

Autorícese al Registro Nacional de Identificación y Estado Civil (RENIEC), en su condición de Entidad de Certificación para el Estado Peruano y Entidad de Registro o Verificación para el Estado Peruano, emitir firmas y certificados digitales en tanto no esté acreditada ante la Autoridad Administrativa Competente (INDECOPI), reconociéndose a los documentos electrónicos soportados en dichos certificados digitales las presunciones legales establecidas en el artículo 8, así como, los efectos jurídicos que corresponde para los fines de los artículos 4 y 43 del presente reglamento.

A tal efecto las entidades de la Administración Pública que hagan uso de la firma digital, y de ser el caso, los Colegios de Notarios del Perú y/o la Junta de Decanos de los Colegios de Notarios del Perú, que así lo soliciten, deberán suscribir Convenios con el Registro Nacional de Identificación y Estado Civil (RENIEC), a fin de llevar un registro de los titulares y/o suscriptores de certificados digitales, así como, de los Certificados Digitales emitidos bajo esta Disposición Complementaria Final.

(…)

Décima Cuarta. Glosario de términos

(...)

***Autoridad Administrativa Competente.** Es el organismo público responsable de acreditar a las Entidades de Certificación, a las Entidades de Registro o Verificación y a los Prestadores de Servicios de Valor Añadido, públicos y privados, de reconocer los estándares tecnológicos aplicables en la Infraestructura Oficial de Firma Electrónica, de supervisar dicha Infraestructura, y las otras funciones señaladas en el presente Reglamento o aquellas que requiera en el transcurso de sus operaciones.*

(...)".

Tercera. Modificación de los artículos 3, 4 y 9 del Decreto Supremo Nº 033-2018-PCM, Decreto Supremo que crea la Plataforma Digital Única del Estado Peruano y establecen disposiciones adicionales para el desarrollo del Gobierno Digital

Modifícanse el artículo 3, 4 y 9 del Decreto Supremo Nº 033-2018-PCM, Decreto Supremo que crea la Plataforma Digital Única del Estado Peruano y establecen disposiciones adicionales para el desarrollo del Gobierno Digital, en los siguientes términos:

*"**Artículo 3.- Alcance***

*El presente Decreto Supremo es de alcance obligatorio a todas las entidades de la Administración Pública comprendidas en el artículo I del Título Preliminar del Texto Único Ordenado de la Ley Nº 27444, Ley del Procedimiento Administrativo General, aprobado mediante **Decreto Supremo Nº 004-2019-JUS**.*

(...)

Artículo 4.- Incorporación progresiva a la Plataforma GOB.PE

Las entidades comprendidas en el alcance del presente Decreto Supremo realizan las acciones necesarias para la incorporación progresiva de sus canales digitales a la Plataforma GOB.PE y las incluyen en sus instrumentos de gestión institucional. Para tal efecto, la Presidencia del Consejo de Ministros a través de la Secretaría de Gobierno Digital emite las disposiciones y plazos correspondientes.

El funcionario del Área de Comunicación o Imagen de la entidad o quien haga sus veces es el responsable del proceso de migración de los canales digitales a la Plataforma GOB.PE, reporta sus avances al Comité de Gobierno Digital de la entidad. Asimismo, el Líder de Gobierno Digital impulsa el referido proceso de migración gestionando la asignación de recursos para su implementación.

(…)

Artículo 9.- Líder de Gobierno Digital

Créase el rol del Líder de Gobierno Digital en cada una de las entidades de la Administración Pública comprendidas en el alcance del presente Decreto Supremo, quien es un funcionario o asesor de la Alta Dirección o director de un órgano de línea de la entidad. Es designado mediante acto resolutivo del titular de la entidad.

El Líder de Gobierno Digital comunica al Líder Nacional de Gobierno Digital los objetivos, acciones y medidas para la transformación digital y despliegue del Gobierno Digital establecidas en su entidad, así como el estado de la implementación de las iniciativas y proyectos priorizados por el Comité de Gobierno Digital, los avances del proceso de migración de los canales digitales a la Plataforma GOB.PE y la aplicación de lo dispuesto en el presente Decreto Supremo.

(...)".

Cuarta. Modificación del artículo 2 del Decreto Supremo Nº 051-2018-PCM, Decreto Supremo que crea el Portal de Software Público Peruano y establece disposiciones adicionales sobre el Software Público Peruano

Modifícase el artículo 2 del Decreto Supremo Nº 051-2018-PCM, Decreto Supremo que crea el Portal de Software Público Peruano y establece disposiciones adicionales sobre el Software Público Peruano, en los siguientes términos:

*"**Artículo 2.- Alcance***

El presente Decreto Supremo es de alcance obligatorio a todas las entidades de la Administración Pública comprendidas en el artículo I del Título Preliminar del Texto Único Ordenado de la Ley Nº 27444, Ley del Procedimiento Administrativo General, aprobado mediante Decreto Supremo Nº 004-2019-JUS.

(...)".

Quinta. Modificación del artículo 3 del Decreto Supremo Nº 118-2018-PCM, Decreto Supremo que declara de interés nacional el desarrollo del Gobierno Digital, la innovación y la economía digital con enfoque territorial

Modifícase el artículo 3 del Decreto Supremo Nº 118-2018-PCM, Decreto Supremo que declara de interés nacional el desarrollo del Gobierno Digital, la innovación y la economía digital con enfoque territorial, en los siguientes términos:

"***Artículo 3.- Integrantes del Comité de Alto Nivel***

3.1. El Comité de Alto Nivel estará integrado por:

a) El/a titular de la Presidencia del Consejo de Ministros o su representante, quien la preside.

b) El/a Secretario/a de Gobierno Digital, quien cumple el rol de Secretaría Técnica.

c) Un representante del Despacho Presidencial.

d) El/a titular del Ministerio de Economía y Finanzas o su representante.

e) El/a titular del Ministerio de Educación o su representante.

f) El/a titular del Ministerio de la Producción o su representante.

g) El/a titular del Ministerio de Transportes y Comunicaciones o su representante.

h) El/a titular del Ministerio de Relaciones Exteriores o su representante.

i) El/a titular del Ministerio de Comercio Exterior y Turismo.

j) El/a titular del Ministerio de Defensa.

k) Un/a representante de los Gobiernos Regionales.

l) Un/a representante de los Gobiernos Locales.

m) Un/a representante de la sociedad civil.

n) Un/a representante del sector privado.

o) Un/a representante de la academia.

3.2. Los miembros del Comité de Alto Nivel solo podrán delegar su participación a un miembro de la Alta Dirección de la entidad.

3.3. El Presidente del Comité podrá invitar a participar en sus sesiones a titulares de otras entidades públicas o privadas cada vez que en éstas se traten objetivos que tengan relación con su competencia.

3.4 El Comité promoverá políticas, iniciativas y programas para el desarrollo de la innovación, la

competitividad, la transformación digital de procesos y servicios públicos, las competencias digitales, la inclusión digital y el desarrollo de aplicaciones para la economía digital.

3.5. La participación de los integrantes del Comité de Alto Nivel es ad honorem.

3.6 La Secretaría Técnica es responsable de proponer los lineamientos para el funcionamiento del Comité de Alto Nivel, conformación de equipos técnicos y otras iniciativas para el logro de sus objetivos.

(...)".

Sexta. Modificación del artículo 6 del Decreto Supremo Nº 093-2019-PCM, Decreto Supremo que aprueba el Reglamento de la Ley Nº 30254, Ley de Promoción para el uso seguro y responsable de las Tecnologías de la Información y Comunicaciones por Niños, Niñas y Adolescentes

Modifícase el artículo 6 del Decreto Supremo Nº 093-2019-PCM, Decreto Supremo que aprueba el Reglamento de la Ley Nº 30254, Ley de Promoción para el uso seguro y responsable de las Tecnologías de la Información y Comunicaciones por Niños, Niñas y Adolescentes, en los siguientes términos:

"Artículo 6.- Miembros de la Comisión Especial

6.1 La Comisión Especial está conformada por:

a) Un/a representante de la Presidencia del Consejo de Ministros, quien la preside.

b) Un/a representante de la alta dirección del Ministerio de Educación.

c) Un/a representante de la alta dirección del Ministerio del Interior.

d) Un/a representante de la alta dirección del Ministerio de la Mujer y Poblaciones Vulnerables.

e) Un/a representante de la alta dirección del Organismo Supervisor de Inversión Privada en Telecomunicaciones (OSIPTEL).

f) Un/a representante del sector privado.

g) Un/a representante de la sociedad civil.

6.2 Las entidades que conforman la Comisión Especial cuentan con un/a representante titular y un/a alterno, quienes forman parte de la alta dirección y son designados por el Titular de la entidad o máxima autoridad, según corresponda.

6.3. Las entidades públicas designan a sus representantes para la Comisión Especial en el plazo de cinco (05) días hábiles de publicado el presente Reglamento. Dicha designación es comunicada a la Presidencia del Consejo de Ministros.

6.4. Los representantes del sector privado y de la sociedad civil son propuestos por los miembros de la Comisión Especial y designados mediante Resolución Ministerial de la Presidencia del Consejo de Ministros.

6.5. El ejercicio de las funciones de los miembros de la Comisión Especial, así como de sus miembros alternos, es ad honórem.

6.6. La Comisión Especial puede invitar a participar en las acciones que desarrolle a otras entidades públicas, privadas o de la sociedad civil, así como a profesionales especializados con la finalidad de solicitar la colaboración de los mismos en temas que sean materia de sus competencias o funciones. Asimismo, la Presidencia del Consejo de Ministros puede invitar a representantes de los gobiernos regionales y gobiernos locales en las sesiones de la Comisión Especial.

6.7. La Comisión Especial propondrá su Reglamento Interno en un plazo de treinta (30) días calendario contados desde su instalación, para su aprobación mediante Resolución Ministerial.

(...)".

DISPOSICIÓN COMPLEMENTARIA DEROGATORIA

ÚNICA. Derogación

Deróguese el Decreto Supremo Nº 065-2015-PCM, que crea la Comisión Multisectorial Permanente encargada del seguimiento y evaluación del "Plan de Desarrollo de la Sociedad de la Información en el Perú - La Agenda Digital Peruana 2.0" (CODESI), y el Decreto Supremo Nº 066-2011-PCM, que aprueba el Plan de Desarrollo de la Sociedad de la Información en el Perú - La Agenda Digital Peruana 2.0.

ANEXO
GLOSARIO DE TÉRMINOS

a) **Alfabetización digital.** Es el proceso de adquisición de competencias esenciales para interactuar en entornos digitales permanentemente; necesario para estudiar, trabajar, desenvolverse en la vida diaria, que permite ejercer la ciudadanía de manera plena y aprovechar las oportunidades que brinda el entorno.

b) **Algoritmo de resumen hash.** Es aquel algoritmo que implementa una función hash. Recibe como entrada un dato de tamaño variable y genera como salida un dato de longitud fija.

c) **Carpeta personal.** Es un espacio lógico que permite el alojamiento de documentos personales en formato digital.

d) **Ciencia de datos**. Comprende el proceso de descubrimiento de correlaciones entre variables a una escala (incluyendo volumen, velocidad y variedad) que va más allá de la cognición humana y de otros paradigmas analíticos.

e) **Ciudadanía digital**. Es el ejercicio de los deberes y derechos de un ciudadano o persona en general en un entorno digital seguro

f) **Datos abiertos**. Son aquellos datos producidos por las entidades públicas que se encuentran disponibles en la web (en formatos estandarizados y abiertos) para que cualquier persona pueda acceder a ellos, reutilizarlos, combinarlos y redistribuirlos para crear nuevos servicios, visualizaciones o realizar investigaciones a partir de ellos.

g) **Datos espaciales**. Son aquellos datos que describen la geometría, la localización o las relaciones topológicas de los objetos geográficos. Son sinónimos: dato geoespacial, dato geográfico o dato georreferenciado.

h) **Datos estadísticos.** Son los valores que se obtienen al llevar a cabo un estudio de tipo estadístico en base a registros administrativos, censos o encuestas en materia socioeconómica, demográfica u otra de especial interés para la producción estadística.

i) **Datos estadísticos oficiales.** Son los datos estadísticos producidos por el Sistema Nacional de Estadística.

j) **Descriptores archivísticos.** Son elementos necesarios para la búsqueda, control y acceso de documentos archivísticos.

k) **Digital.** Se refiere a todo aquello que es procesable por medio de un dispositivo digital. Es caracterizado por el uso de codificación binaria.

l) **Electrónico.** Se refiere a todo aquello que es procesable por medio de un dispositivo electrónico. Es caracterizado por el uso de codificación analógica o binaria.

m) **Factor de autenticación.** Es una categoría de credenciales de autenticación. Cada categoría es un factor de autenticación. Los factores de autenticación más conocidos son tres: algo que sabes, algo que tienes y algo que eres.

n) **Formato electrónico**. Documento electrónico estructurado producido y procesable por sistemas de información.

o) **Fecha y hora cierta.** Fecha y hora consignada y firmada digitalmente por un Prestador de Servicios de Valor Añadido, en la modalidad de Sistema de Sellado de Tiempo.

p) **Identidad digital.** Conjunto de atributos que individualiza y permite identificar a una persona en entornos digitales.

q) **Inteligencia artificial.** Se refiere a los sistemas que presentan comportamiento inteligente, que en base al análisis de su entorno toman decisiones, con algún grado de autonomía, para lograr metas específicas.

r) **Metadato.** Son datos estructurados que describen otros datos. Los metadatos proporcionan la

semántica necesaria para entender un dato al definirlo, contextualizarlo y describir sus características y sus relaciones, sus referencias de uso, sus formas de representación e incluso, sus valores permitidos, con la finalidad de garantizar su disponibilidad, accesibilidad, conservación e interoperabilidad con otros sistemas.

s) **Prototipado.** Actividad de la etapa de diseño y construcción del ciclo de vida de los servicios digitales, en la cual se construyen prototipos de una solución con la finalidad de evaluar su viabilidad.

t) **Proyectos de Tecnologías Digitales de carácter transversal**. Son aquellos proyectos que tienen como resultado plataformas, soluciones o servicios digitales de uso común por dos o más entidades públicas para soportar procedimientos administrativos, procesos de gestión interna, servicios públicos de cara al ciudadano o cualquier otra intervención pública que genere beneficios para la sociedad. Dichos proyectos tienen como mínimo las siguientes características: a) Atienden un objetivo estratégico nacional o política de Estado, b) Se integran con uno o más bloques básicos de interoperabilidad técnica, c) Tienen un alcance interinstitucional o multisectorial, y, d) Usan intensivamente las tecnologías digitales o datos.

Esta definición no incluye a los proyectos de carácter institucional, los cuales se encuentran vinculados con los procesos de una entidad en el ejercicio de sus funciones y competencias. Entiéndase como proyecto de carácter institucional al esfuerzo planificado, temporal y único, realizado para crear productos o servicios únicos que agreguen valor, mejoren u optimicen las condiciones de operación o mantenimiento de una institución, que provoquen un cambio beneficioso en ella y/o en sus administrados, y que requiere la participación de representantes de uno o más unidades de organización, pudiendo contar con la colaboración de los servicios que presten otras entidades públicas, así como utilizar las tecnologías disponibles en estas.

u) **Registros distribuidos.** Son un tipo de registro que es compartido, replicado y sincronizado (de manera descentralizada y distribuida) entre y por los nodos de una red.

v) **Resumen hash.** Es el valor producido por un algoritmo de resumen hash.

w) **Servicio de información.** Mecanismo de provisión de información pública que las entidades del Estado gestionan en sus sistemas de información y que se suministran entre sí a través de la PIDE.

x) **Tecnología de registros distribuidos.** Tecnología que permite que los nodos de una red propongan, validen y registren de forma segura cambios de estado (o actualizaciones) en un registro distribuido.

1929103-3

AMBIENTE

Crean Grupo de Trabajo Multisectorial denominado "Comisión de Categorización de la Zona Reservada Illescas", dependiente del SERNANP

RESOLUCIÓN MINISTERIAL
N° 031-2021-MINAM

Lima,17 de febrero de 2021

VISTOS; el Oficio Nº 313-2020-SERNANP-J del Servicio Nacional de Áreas Naturales Protegidas por el Estado; el Informe Nº 00018-2021-MINAM/SG/OGPP/OPM de la Oficina de Planeamiento y Modernización; el Memorando Nº 00072-2021-MINAM/SG/OGPP de la Oficina General de Planeamiento y Presupuesto; y el Informe Nº 00033-2021-MINAM/SG/OGAJ de la Oficina General de Asesoría Jurídica;

CONSIDERANDO:

Que, mediante el artículo 68 de la Constitución Política del Perú se establece que es obligación del Estado promover la conservación de la diversidad biológica y de las Áreas Naturales Protegidas;

Que, de conformidad con el artículo 1 de la Ley N° 26834, Ley de Áreas Naturales Protegidas, las Áreas Naturales Protegidas son aquellos espacios continentales y/o marinos del territorio nacional, expresamente reconocidos y declarados como tales, incluyendo sus categorías y zonificaciones, para conservar la diversidad biológica y demás valores asociados de interés cultural, paisajístico y científico, así como por su contribución al desarrollo sostenible del país;

Que, de acuerdo a lo previsto en el artículo 6 de la referida Ley Nº 26834, Ley de Áreas Naturales Protegidas, las Áreas Naturales Protegidas de administración nacional conforman en su conjunto el Sistema Nacional de Áreas Naturales Protegidas por el Estado - SINANPE, cuya gestión se integran las instituciones públicas del gobierno central, gobiernos descentralizados de nivel regional y local, instituciones privadas y las poblaciones locales que actúan, intervienen o participan, directa o indirectamente, en la gestión y desarrollo de dichas áreas;

Que, conforme con lo establecido en el literal h) del artículo 7 del Decreto Legislativo Nº 1013, Ley de Creación, Organización y Funciones del Ministerio del Ambiente, el Ministerio del Ambiente tiene como función específica dirigir el Sistema Nacional de Áreas Naturales Protegidas por el Estado - SINANPE, función que ejecuta a través del Servicio Nacional de Áreas Naturales Protegidas por el Estado - SERNANP, organismo público técnico especializado adscrito al Ministerio del Ambiente, ente rector del SINANPE y su autoridad técnico-normativa;

Que, en el marco de lo previsto en el artículo 35 de la Ley N° 29158, Ley Orgánica del Poder Ejecutivo, los numerales 28.1 y 28.3 del artículo 28 de los Lineamientos de Organización del Estado, aprobados mediante Decreto Supremo N° 054-2018-PCM y modificados por el Decreto Supremo N° 131-2018-PCM, establecen que los grupos de trabajo son un tipo de órgano colegiado, sin personería jurídica ni administración propia, que se crean para cumplir funciones distintas a las de seguimiento, fiscalización, propuesta o emisión de informes técnicos; agregando que se extinguen automáticamente concluido su periodo de vigencia, pudiendo ser sectoriales o multisectoriales, siendo conformados mediante Resolución Ministerial del Ministerio que lo preside;

Que, mediante Resolución Ministerial N° 251-2010-MINAM de fecha 16 de diciembre de 2010, se declara Zona Reservada Illescas la superficie de treinta y siete mil cuatrocientas cincuenta y dos hectáreas y cinco mil ochocientos metros cuadrados (37,452.58 ha), ubicada en el distrito de Sechura, provincia de Sechura, departamento de Piura;

Que, de acuerdo a lo previsto en los artículos 4 y 5 de la Resolución Ministerial Nº 251-2010-MINAM, el SERNANP, en coordinación con las autoridades competentes, tiene a cargo el proceso de categorización definitiva de la Zona Reservada Illescas, por lo cual se constituye una Comisión encargada de la formulación de la propuesta de ordenación territorial, por un plazo máximo de seis (06) meses contados a partir de la instalación;

Que, mediante Oficio Nº 313-2020-SERNANP-J, el SERNANP remite el Informe Técnico Legal N° 003-2020-SERNANP-DDE-OAJ-OPP de su Dirección de Desarrollo Estratégico, su Oficina de Asesoría Jurídica y su Oficina de Planeamiento y Presupuesto; a través de los cuales se sustenta y concluye que debido a que la Comisión de Categorización constituida mediante Resolución Ministerial N° 251-2010-MINAM no logró culminar el proceso de categorización, se requiere conformar el Grupo de Trabajo denominado "Comisión de Categorización de la Zona Reservada de Illescas", a fin culminar el proceso de categorización de la Zona Reservada Illescas, por un periodo de tres (3) meses;

Que, con Memorando Nº 00072-2021-MINAM/SG/OGPP, la Oficina General de Planeamiento y Presupuesto del Ministerio del Ambiente remite el Informe Nº 00018-2021-MINAM/SG/OGPP/OPM, con el cual se emite opinión favorable respecto a la conformación del Grupo de Trabajo denominado "Comisión de Categorización de la Zona Reservada de Illescas";