CONGRESO DE LA REPÚBLICA
ÁREA DE TRÁMITE DOCUMENTARIO

17 SEP 2018

RECIBIDO

Firma _____ Hora 12:41

"Decenio de la Igualdad de oportunidades para mujeres y hombres"
"Año del Diálogo y la Reconciliación Nacional"

Lima, 13 de setiembre de 2018

OFICIO Nº 243 -2018 -PR

Señor
DANIEL SALAVERRY VILLA
Presidente del Congreso de la República
Presente. -

Tenemos el agrado de dirigirnos a usted señor Presidente del Congreso de la República, de conformidad con lo dispuesto por el artículo 104° de la Constitución Política, con la finalidad de comunicarle que, al amparo de las facultades legislativas delegadas al Poder Ejecutivo mediante Ley N° 30823, y con el voto aprobatorio del Consejo de Ministros, se ha promulgado el Decreto Legislativo N° 1412 , Decreto Legislativo que aprueba la Ley de Gobierno Digital.

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

Atentamente,

MARTIN ALBERTO VIZCARRA CORNEJO
Presidente de la República

CÉSAR VILLANUEVA ARÉVALO
Presidente del Consejo de Ministros

196244-ATD

CONGRESO DE LA REPÚBLICA

Lima, 18 de Setiembre de 20 18

En aplicación de lo dispuesto en el inc. b) del artículo 90° del Reglamento del Congreso de la República: para su estudio PASE el expediente del Decreto Legislativo N° 1412,

a la Comisión de Constitución y Reglamento

.....

JOSÉ ABANTO VALDIVIESO
Oficial Mayor (e)
CONGRESO DE LA REPÚBLICA

2

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

REPUBLICA DEL PERU

Decreto Legislativo Nº 1412

EL PRESIDENTE DE LA REPÚBLICA

POR CUANTO:

Que, mediante Ley Nº 30823, el Congreso de la República ha delegado en el Poder Ejecutivo la facultad de legislar en materia de gestión económica y competitividad, de integridad y lucha contra la corrupción, de prevención y protección de personas en situación de violencia y vulnerabilidad y de modernización de la gestión del Estado, por el plazo de sesenta (60) días calendario;

Que, el literal d) numeral 5 del artículo 2, de la citada Ley faculta al Poder Ejecutivo para legislar en materia de modernización del Estado, a fin de implementar servicios y espacios compartidos por parte de las entidades públicas, así como establecer disposiciones para el gobierno digital y las plataformas multiservicios y de trámites que faculten a las entidades públicas para delegar la gestión y resolución de actos administrativos a otras entidades públicas bajo criterios que prioricen eficiencia, productividad, oportunidad y mejora de servicios para el ciudadano y la empresa; o a terceros, en las etapas previas a la emisión de la resolución que contenga la decisión final de la entidad;

Que, el ítem d.3) del literal d) del numeral 5 del artículo 2 de la citada norma establece la facultad de legislar para establecer el marco normativo para promover el despliegue transversal de las tecnologías digitales en las entidades del Estado; a fin de mejorar el alcance, condiciones, la prestación y el acceso de los ciudadanos a los servicios que presta el Estado;

Que, la Política 35 del Acuerdo Nacional, sobre Sociedad de la Información y Sociedad del Conocimiento, señala en el literal e) que el Estado fomentará la modernización del Estado, mediante el uso de las Tecnologías de la Información y la Comunicación (TIC), con un enfoque descentralista, planificador e integral;

Que, mediante el Decreto Supremo N° 086-2015-PCM, se declara de interés nacional las acciones, actividades e iniciativas desarrolladas en el marco del proceso de vinculación del Perú con la Organización para la Cooperación y el Desarrollo Económicos (OCDE) e implementación del Programa País, y crea la Comisión Multisectorial de naturaleza permanente para promover las acciones de seguimiento del referido proceso, y comprende la participación del Estado peruano en las actividades previstas en el Acuerdo y Memorando de Entendimiento suscritos entre la OCDE y el Gobierno del Perú, así como todas las demás actividades relacionadas con la organización, promoción, impulso y apoyo al referido proceso;

Que, las tecnologías digitales y el gobierno digital son conceptos integrados en las actividades, lenguaje y estructuras de la sociedad actual, y hacen parte del proceso de vinculación del Perú con la Organización para la Cooperación y el Desarrollo Económicos (OCDE), organización que entiende su uso estratégico como parte integral del diseño de

políticas y estrategias de modernización del gobierno, con la finalidad de crear servicios digitales de valor, seguros, confiables y accesibles para los ciudadanos y sociedad en general, lo cual se sustenta en un ecosistema compuesto por actores del sector público, sector privado, academia y otros interesados, quienes apoyan en la implementación de iniciativas y acciones para diseño, creación, producción de datos, servicios y contenidos, asegurando el pleno respeto los derechos de las personas en el entorno digital;

Que mediante Decreto Legislativo N° 604, se aprueba la Ley de Organización y Funciones del Instituto Nacional de Estadística e Informática - INEI, que crea el Sistema Nacional de Informática el cual tiene como objetivos normar las actividades de informática; coordinar, integrar y racionalizar las actividades de informática; y promover la capacitación, investigación y desarrollo de las actividades de informática;

Que, conforme lo establecido en el artículo 47 del Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros, aprobado mediante Decreto Supremo N° 022-2017-PCM, la Secretaría de Gobierno Digital - SEGDI 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. Asimismo, es el órgano rector del Sistema Nacional de Informática;

Que, dentro de este contexto, es necesario adecuar la gobernanza y gestión del gobierno digital en el Estado Peruano y mejorar la articulación en los tres niveles de gobierno, para lo cual resulta indispensable establecer el marco normativo que regule y habilite a las entidades del Estado integrar de manera intensiva las tecnologías digitales para la prestación de servicios digitales en condiciones seguras, confiables, transparentes, interoperables en un entorno de gobierno digital;

De conformidad con lo establecido en el literal d) del numeral 5 del artículo 2 de la Ley N° 30823 y el artículo 104 de la Constitución Política del Perú;

Con el voto aprobatorio del Consejo de Ministros; y,

Con cargo de dar cuenta al Congreso de la República;

Ha dado el Decreto Legislativo siguiente:

DECRETO LEGISLATIVO QUE APRUEBA LA LEY DE GOBIERNO DIGITAL

TÍTULO I

DISPOSICIONES GENERALES

Artículo 1.- Objeto

La presente Ley tiene por objeto establecer 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.

REPUBLICA DEL PERU

Decreto Legislativo

Artículo 2.- Ámbito de aplicación

2.1. La presente Ley es de aplicación a toda entidad que forma parte de la Administración Pública a que se refiere el artículo I del Título Preliminar del Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General. Sus regulaciones también alcanzan a las personas jurídicas o naturales que, por mandato legal, encargo o relación contractual ejercen potestades administrativas, y por tanto su accionar se encuentra sujeto a normas de derecho público, en los términos dispuestos por la Presidencia del Consejo de Ministros.

2.2. En el caso de las empresas que conforman la actividad empresarial del Estado, su aplicación se da en todo aquello que le resulte aplicable.

Artículo 3.- Definiciones

Para efectos de la presente Ley, se adoptan las siguientes definiciones:

1. **Tecnologías Digitales.-** Se refieren a las Tecnologías de la Información y la Comunicación - TIC, incluidos Internet, las tecnologías y dispositivos móviles, así como la analítica de datos utilizados para mejorar la generación, recopilación, intercambio, agregación, combinación, análisis, acceso, búsqueda y presentación de contenido digital, incluido el desarrollo de servicios y aplicaciones aplicables a la materia de gobierno digital.

2. **Entorno Digital.-** Es el dominio o ámbito habilitado por las tecnologías y dispositivos digitales, generalmente interconectados a través de redes de datos o comunicación, incluyendo el Internet, que soportan los procesos, servicios, infraestructuras y la interacción entre personas.

3. **Servicio Digital.-** Es aquel provisto de forma total o parcial a través de Internet u otra red equivalente, que se caracteriza por ser automático, no presencial y utilizar de manera intensiva las tecnologías digitales, para la producción y acceso a datos y contenidos que generen valor público para los ciudadanos y personas en general.

4. **Canal Digital.-** Es el medio de contacto digital que disponen las entidades de la Administración Pública a los ciudadanos y personas en general para facilitar el acceso a toda la información institucional y de trámites, realizar y hacer seguimiento a servicios digitales, entre otros. Este canal puede comprender páginas y sitios web, redes sociales, mensajería electrónica, aplicaciones móviles u otros.

5. **Ciudadano Digital.-** Es aquel que hace uso de las tecnologías digitales y ejerce sus deberes y derechos en un entorno digital seguro.

6. **Gobernanza Digital.-** Es el conjunto de procesos, estructuras, herramientas y normas que nos permiten dirigir, evaluar y supervisar el uso y adopción de las tecnologías digitales en la organización.

7. **Arquitectura Digital.-** Es el conjunto de componentes, lineamientos y estándares, que desde una perspectiva integral de la organización permiten alinear los sistemas de información, datos, seguridad e infraestructura tecnológica con la misión y objetivos estratégicos de la entidad, de tal manera que se promuevan la colaboración, interoperabilidad, escalabilidad, seguridad y el uso optimizado de las tecnologías digitales en un entorno de gobierno digital.

Artículo 4.- Finalidad

La presente Ley tiene por finalidad:

4.1 Mejorar la prestación y acceso de servicios digitales en condiciones interoperables, seguras, disponibles, escalables, ágiles, accesibles, y que faciliten la transparencia para el ciudadano y personas en general.

4.2 Promover la colaboración entre las entidades de la Administración Pública, así como la participación de ciudadanos y otros interesados para el desarrollo del gobierno digital y sociedad del conocimiento.

Artículo 5.- Principios rectores

Las disposiciones contenidas en la presente Ley, así como su aplicación se rigen por los siguientes principios rectores:

5.1 **Especialidad.-** La presente norma es aplicable a los servicios digitales prestados por las entidades de la Administración Pública en un entorno de gobierno digital, sin perjuicio de lo regulado para los procedimientos administrativos u otros que se rigen por su propia normatividad.

5.2 **Equivalencia Funcional.-** El ejercicio de la identidad digital para el uso y prestación de servicios digitales confiere y reconoce a las personas las mismas garantías que otorgan los modos tradicionales de relacionarse entre privados y/o en la relación con las entidades de la Administración Pública.

5.3 **Privacidad desde el Diseño.-** En el diseño y configuración de los servicios digitales se adoptan las medidas preventivas de tipo tecnológico, organizacional, humano y procedimental.

5.4 **Igualdad de Responsabilidades.-** Las entidades de la Administración Pública responden por los actos realizados a través de canales digitales de la misma manera y con iguales responsabilidades que por los realizados a través de medios presenciales.

5.5 **Usabilidad.-** En el diseño y configuración de los servicios digitales se propenderá a que su uso resulte de fácil manejo para los ciudadanos y personas en general.

5.6 **Cooperación Digital.-** Prima el intercambio de datos e información, la interoperabilidad de los sistemas y soluciones para la prestación conjunta de servicios digitales.

5.7 **Digital desde el Diseño.-** Los servicios, de manera preferente, progresiva y cuando corresponda, se diseñan y modelan para que sean digitales de principio a fin.

5.8 **Proporcionalidad.-** Los requerimientos de seguridad y autenticación de los servicios digitales prestados por las entidades de la Administración Pública deben ser proporcionales al nivel de riesgo asumido en la prestación del mismo.

REPUBLICA DEL PERU

Decreto Legislativo

5.9 **Datos Abiertos por Defecto**.- Los datos se encuentran abiertos y disponibles de manera inmediata, sin comprometer el derecho a la protección de los datos personales de los ciudadanos. Ante la duda corresponde a la Autoridad de Transparencia definirlo.

5.10 **Nivel de protección adecuado para los datos personales.-** El tratamiento de los datos personales debe realizarse conforme a lo establecido en la Ley de Protección de Datos Personales y su Reglamento.

TÍTULO II

GOBIERNO DIGITAL

CAPÍTULO I

GOBIERNO DIGITAL

Artículo 6.- Gobierno Digital

6.1. El gobierno digital es el uso estratégico de las tecnologías digitales y datos en la Administración Pública para la creación de valor público. Se sustenta en un ecosistema compuesto por actores del sector público, ciudadanos y otros interesados, quienes apoyan en la implementación de iniciativas y acciones de diseño, creación de servicios digitales y contenidos, asegurando el pleno respeto de los derechos de los ciudadanos y personas en general en el entorno digital.

6.2. Comprende el conjunto de principios, políticas, normas, procedimientos, técnicas e instrumentos utilizados por las entidades de la Administración Pública en la gobernanza, gestión e implementación de tecnologías digitales para la digitalización de procesos, datos, contenidos y servicios digitales de valor para los ciudadanos.

Artículo 7.- Objetivos del Gobierno Digital

Los objetivos del gobierno digital son:

7.1 Normar las actividades de gobernanza, gestión e implementación en materia de tecnologías digitales, identidad digital, servicios digitales, arquitectura digital, interoperabilidad, seguridad digital y datos.

7.2 Coordinar, integrar y promover la colaboración entre las entidades de la Administración Pública.

7.3 Promover la investigación y desarrollo en la implementación de tecnologías digitales, identidad digital, servicios digitales, interoperabilidad, seguridad digital y datos.

7.4 Promover y orientar la formación y capacitación en materia de gobierno digital y tecnologías digitales en todos los niveles de gobierno.

Artículo 8.- Ente Rector en materia de Gobierno Digital

La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, es el ente rector en materia de gobierno digital que comprende tecnologías digitales, identidad digital, interoperabilidad, servicio digital, datos, seguridad digital y arquitectura digital. Dicta las normas y establece los procedimientos en materia de gobierno digital y, es responsable de su operación y correcto funcionamiento.

Artículo 9.- Funciones del ente rector en materia de gobierno digital

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

9.1 Programar, dirigir, coordinar, supervisar y evaluar la aplicación de la materia de gobierno digital.

9.2 Elaborar y proponer normas reglamentarias y complementarias que regulan la materia de gobierno digital.

9.3 Elaborar lineamientos, procedimientos, metodologías, modelos, directivas u otros estándares de obligatorio cumplimiento para la implementación de las materias de gobierno digital.

9.4 Emitir opinión vinculante sobre el alcance, interpretación e integración de normas que regulan la materia de gobierno digital.

9.5 Emitir opinión previa a fin de validar técnicamente proyectos de tecnologías digitales de carácter transversal en materia de interoperabilidad, seguridad digital, identidad digital, datos, arquitectura digital o aquellos destinados a mejorar la prestación de servicios digitales.

9.6 Brindar apoyo técnico a las entidades públicas en la gestión e implementación de tecnologías digitales.

9.7 Definir los alcances del marco normativo en materia de gobierno digital.

9.8 Supervisar y fiscalizar, cuando corresponda, el cumplimiento del marco normativo en materia de gobierno digital.

9.9 Promover mecanismos que aseguren la identidad digital como pilar fundamental para la inclusión digital y la ciudadanía digital.

9.10 Promover y gestionar la implementación de proyectos de implementación de tecnologías digitales u otros mecanismos destinados a mejorar la prestación de servicios digitales, en coordinación con las entidades públicas, según corresponda.

9.11 Promover la digitalización de los procesos y servicios a partir del uso e implementación de tecnologías digitales.

9.12 Realizar acciones de coordinación y articulación con representantes de la administración pública, ciudadanos u otros interesados con la finalidad de optimizar el uso de tecnologías digitales para el desarrollo del gobierno digital y tecnologías digitales.

CAPÍTULO II

IDENTIDAD DIGITAL

Artículo 10.- De la Identidad Digital

10.1 La identidad digital es aquel conjunto de atributos que individualiza y permite identificar a una persona en entornos digitales.

10.2 Los atributos de la identidad digital son otorgados por distintas entidades de la Administración Pública que, en su conjunto, caracterizan al individuo.

Artículo 11.- Marco de Identidad Digital del Estado Peruano

El Marco de Identidad Digital del Estado Peruano está constituido por lineamientos, especificaciones, guías, directivas, estándares e infraestructura de tecnologías digitales, que

permiten de manera efectiva la identificación y autenticación de los ciudadanos y personas en general cuando acceden a los servicios digitales.

Artículo 12.- Credencial de Identidad Digital

Es la representación de una identidad digital que comprende los atributos inherentes a la persona definidos en el Marco de Identidad Digital del Estado Peruano, a fin de facilitar la autenticación digital.

Artículo 13.- Identificación Digital

La identificación digital es el procedimiento de reconocimiento de una persona como distinta de otras, en el entorno digital. Las entidades de la Administración Pública deben establecer los procedimientos para identificar a las personas que accedan a los servicios digitales.

Artículo 14.- Autenticación Digital

La autenticación digital es el procedimiento de verificación de la identidad digital de una persona, mediante el cual se puede afirmar que es quien dice ser.

Para el acceso a un servicio digital las entidades de la Administración Pública deben adoptar los mecanismos o procedimientos de autenticación digital, considerando los niveles de seguridad a establecerse en la norma reglamentaria.

Artículo 15.- Inclusión digital

La inclusión digital es el acceso y uso de los servicios digitales por parte de los ciudadanos a través de su identidad digital, promoviendo la ciudadanía digital. Para tal fin las entidades de la Administración Pública adoptan las disposiciones que emite el ente rector para la prestación de dichos servicios.

Artículo 16.- Documento Nacional de Identidad electrónico (DNIe)

El Documento Nacional de Identidad Electrónico (DNIe) es una credencial de identidad digital, emitida por el Registro Nacional de Identificación y Estado Civil - RENIEC, que acredita presencial y no presencialmente la identidad de las personas.

Artículo 17.- Uso del Documento Nacional de Identidad electrónico

Los funcionarios y servidores públicos al servicio de las entidades de la Administración Pública pueden hacer uso del Documento Nacional de Identidad Electrónico (DNIe) para el ejercicio de sus funciones en los actos de administración, actos administrativos, procedimientos administrativos y servicios digitales.

El DNIe sólo otorga garantía sobre la identificación de la persona natural, mas no en el cargo, rol, atribuciones o facultades que ostenta un funcionario o servidor de una entidad de la Administración Pública; dicho funcionario o servidor público es el responsable de gestionar en su entidad las autorizaciones de acceso y asignación de roles, atribuciones o facultades para hacer uso del indicado DNIe en los sistemas de información que hagan uso del mismo.

CAPÍTULO III

PRESTACIÓN DE SERVICIOS DIGITALES

Artículo 18.- Garantías para la prestación de servicios digitales

Las entidades de la Administración Pública, de manera progresiva y cuando corresponda, deben garantizar a las personas el establecimiento y la prestación de los servicios digitales, comprendidos en el ámbito de aplicación de la presente Ley, debiendo para tal efecto:

18.1 Reconocer y aceptar el uso de la identidad digital de todas las personas según lo regulado en la presente Ley.
18.2 Garantizar la disponibilidad, integridad y confidencialidad de la información de los servicios digitales con la aplicación de los controles de seguridad que correspondan en la prestación de dichos servicios conforme a las disposiciones contenidas en la presente Ley y en la normatividad vigente sobre la materia.
18.3 Capacitar en temas en materia de firmas electrónicas, firmas y certificados digitales, protección de datos personales, interoperabilidad, arquitectura digital, seguridad digital, datos abiertos y gobierno digital.
18.4 Facilitar el acceso a la información requerida por otra entidad de la Administración Pública, sobre los datos de las personas que obren en su poder y se encuentren en soporte electrónico, únicamente para el ejercicio de sus funciones en el ámbito de sus competencias. Queda excluida del intercambio la información que pueda afectar la seguridad nacional o aquella relacionada con la legislación sobre Transparencia y Acceso a la Información Pública, o la que expresamente sea excluida por Ley.
18.5 Implementar servicios digitales haciendo un análisis de la arquitectura digital y rediseño funcional.
18.6 Considerar la implementación de pagos a través de canales digitales.
18.7 Facilitar a las personas información detallada, concisa y entendible sobre las condiciones de tratamiento de sus datos personales.
18.8 Garantizar la conservación de las comunicaciones y documentos generados a través de canales digitales en las mismas o mejores condiciones que aquellas utilizadas por los medios tradicionales.
18.9 Garantizar que en el diseño y configuración de los servicios digitales se adoptan las medidas técnicas, organizativas y legales para la debida protección de datos personales y la confidencialidad de las comunicaciones.

Artículo 19.- Conservación de los documentos electrónicos firmados digitalmente

Para conservar documentos electrónicos y garantizar la perdurabilidad en el tiempo de la firma digital incorporada en aquellos se emplean sellos de tiempo y mecanismos basados en estándares internacionalmente aceptados que permitan verificar el estado del certificado digital asociado.

Cuando dicho tipo de documentos electrónicos, y sus respectivos formatos que aseguran la característica de perdurabilidad de la firma digital, deban ser conservados de modo permanente, éstos se archivarán observando las disposiciones legales sobre la materia.

Artículo 20.- Sede Digital

La sede digital es un tipo de canal digital, a través del cual pueden acceder los ciudadanos y personas en general a un catálogo de servicios digitales, realizar trámites, hacer seguimiento de los mismos, recepcionar y enviar documentos electrónicos, y cuya

REPUBLICA DEL PERU

Decreto Legislativo

titularidad, gestión y administración corresponde a cada entidad de la Administración Pública en los tres niveles de gobierno.

Artículo 21.- Registro Digital

Las sedes digitales de las entidades de la Administración Pública cuentan con un registro digital para recibir documentos, solicitudes, escritos y comunicaciones electrónicas dirigidas a dicha entidad.

Artículo 22.- Domicilio Digital

Es uno de los atributos de la identidad digital que se constituye en el domicilio habitual de un ciudadano en el entorno digital, el cual es utilizado por las entidades de la Administración Pública para efectuar comunicaciones o notificaciones.

CAPÍTULO IV

GOBERNANZA DE DATOS

Artículo 23.- Datos

23.1 Los datos son la representación dimensionada y descifrable de hechos, información o concepto, expresada en cualquier forma apropiada para su procesamiento, almacenamiento, comunicación e interpretación.

23.2 Las entidades de la Administración Pública administran sus datos como un activo estratégico, garantizando que estos se recopilen, procesen, publiquen, almacenen y pongan a disposición durante el tiempo que sea necesario y cuando sea apropiado, considerando las necesidades de información, riesgos y la normatividad vigente en materia de gobierno digital, seguridad digital, transparencia, protección de datos personales y cualquier otra vinculante.

Artículo 24.- Infraestructura Nacional de Datos

La Infraestructura Nacional de Datos se define como el conjunto articulado de políticas, normas, medidas, procesos, tecnologías digitales, repositorios y bases de datos destinadas a promover la adecuada recopilación, procesamiento, publicación, almacenamiento y puesta a disposición de los datos que gestionan las entidades de la Administración Pública.

Artículo 25.- Marco de Gobernanza y Gestión de Datos del Estado Peruano

El Marco de Gobernanza y Gestión de Datos del Estado Peruano está constituido por instrumentos técnicos y normativos que establecen los requisitos mínimos que las entidades de la Administración Pública deben implementar conforme a su contexto legal, tecnológico y estratégico para asegurar un nivel básico y aceptable para la recopilación, procesamiento, publicación, almacenamiento y apertura de los datos que administre.

CAPÍTULO V

INTEROPERABILIDAD

Artículo 26.- Interoperabilidad

La Interoperabilidad es la capacidad de interactuar que tienen las organizaciones diversas y dispares para alcanzar objetivos que hayan acordado conjuntamente, recurriendo a la puesta en común de información y conocimientos, a través de los procesos y el intercambio de datos entre sus respectivos sistemas de información.

Artículo 27.- Marco de Interoperabilidad del Estado Peruano

El Marco de Interoperabilidad del Estado Peruano está constituido por políticas, lineamientos, especificaciones, estándares e infraestructura de tecnologías digitales, que permiten de manera efectiva la colaboración entre entidades de la Administración Pública para el intercambio de información y conocimiento, para el ejercicio de sus funciones en el ámbito de sus competencias, en la prestación de servicios digitales inter-administrativos de valor para el ciudadano provisto a través de canales digitales.

Artículo 28.- Gestión del Marco de Interoperabilidad del Estado Peruano

El Marco de Interoperabilidad del Estado Peruano se gestiona a través de los siguientes niveles:

28.1. Interoperabilidad a nivel organizacional: Se ocupa del alineamiento de objetivos, procesos, responsabilidades y relaciones entre las entidades de la Administración Pública para intercambiar datos e información para el ejercicio de sus funciones en el ámbito de sus competencias.

28.2 Interoperabilidad a nivel semántico: Se ocupa del uso de los datos y la información de una entidad garantizando que el formato y significado preciso de dichos datos e información a ser intercambiada pueda ser entendido por cualquier aplicación de otra entidad de la Administración Pública. Dichas entidades deben adoptar los estándares definidos por el ente rector para el intercambio de datos e información.

28.3. Interoperabilidad a nivel técnico: Se ocupa de los aspectos técnicos relacionados con las interfaces, la interconexión, integración, intercambio y presentación de datos e información, así como definir los protocolos de comunicación y seguridad. Es ejecutado por personal de las Oficinas de Informática o las que hagan sus veces de las entidades de la Administración Pública, de acuerdo con los estándares definidos por el ente rector.

28.4. Interoperabilidad a nivel legal: Se ocupa de la adecuada observancia de la legislación y lineamientos técnicos con la finalidad de facilitar el intercambio de datos e información entre las diferentes entidades de la Administración Pública, así como el cumplimiento de los temas concernientes con el tratamiento de la información que se intercambia.

Artículo 29.- Reutilización de Software

Las entidades de la Administración Pública titulares de Software Público Peruano, desarrollado mediante la contratación de terceros o por personal de la entidad para soportar sus procesos o servicios, adoptan las medidas necesarias a fin de obtener la titularidad exclusiva sobre los derechos patrimoniales del referido Software Público Peruano.

Todas las entidades de la Administración Pública deben compartir Software Público Peruano bajo licencias libres o abiertas que permitan (i) usarlo o ejecutarlo, (ii) copiarlo o reproducirlo, (iii) acceder al código fuente, código objeto, documentación técnica y manuales

REPUBLICA DEL PERU

Decreto Legislativo

de uso, (iv) modificarlo o transformarlo en forma colaborativa, y (v) distribuirlo, en beneficio del Estado Peruano.

CAPÍTULO VI

SEGURIDAD DIGITAL

Artículo 30.- De la Seguridad Digital
La seguridad digital es el estado de confianza en el entorno digital que resulta de la gestión y aplicación de un conjunto de medidas proactivas y reactivas frente a los riesgos que afectan la seguridad de las personas, la prosperidad económica y social, la seguridad nacional y los objetivos nacionales en dicho entorno. Se sustenta en la articulación con actores del sector público, sector privado y otros quienes apoyan en la implementación de controles, acciones y medidas.

Artículo 31.- Marco de Seguridad Digital del Estado Peruano
El Marco de Seguridad Digital del Estado Peruano se constituye en el conjunto de principios, modelos, políticas, normas, procesos, roles, tecnología y estándares mínimos que permitan preservar la confidencialidad, integridad, disponibilidad de la información en el entorno digital administrado por las entidades de la Administración Pública.

CONSEJO DE MINISTROS Secretaría de Gobierno Digital

Artículo 32.- Gestión del Marco de Seguridad Digital del Estado Peruano
El Marco de Seguridad Digital del Estado Peruano tiene los siguientes ámbitos:

a. Defensa: El Ministerio de Defensa (MINDEF) en el marco de sus funciones y competencias dirige, supervisa y evalúa las normas en materia de ciberdefensa.

b. Inteligencia: La Dirección Nacional de Inteligencia (DINI) como autoridad técnica normativa en el marco de sus funciones emite, supervisa y evalúa las normas en materia de inteligencia, contrainteligencia y seguridad digital en el ámbito de esta competencia.

c. Justicia: El Ministerio de Justicia y Derechos Humanos (MINJUS), el Ministerio del Interior (MININTER), la Policía Nacional del Perú (PNP), el Ministerio Público y el Poder Judicial (PJ) en el marco de sus funciones y competencias dirigen, supervisan y evalúan las normas en materia de ciberdelincuencia.

d. Institucional: Las entidades de la Administración Pública deben establecer, mantener y documentar un Sistema de Gestión de la Seguridad de la Información (SGSI).

Artículo 33.- Articulación de la Seguridad Digital con la Seguridad de la Información
El Marco de Seguridad Digital del Estado Peruano 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 de la Información se enfoca en la información, de manera independiente de su formato y soporte. La seguridad digital se ocupa de las medidas de la seguridad de la información procesada, transmitida, almacenada o contenida en el entorno digital, procurando generar confianza, gestionando los riesgos que afecten la seguridad de las personas y la prosperidad económica y social en dicho entorno.

Artículo 34.- Financiamiento

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

Artículo 35.- Refrendo

El presente Decreto Legislativo es refrendado por el Presidente del Consejo de Ministros y el Ministro de Justicia y Derechos Humanos.

DISPOSICIONES COMPLEMENTARIAS FINALES

PRIMERA.- Reglamentación

La Presidencia del Consejo de Ministros, mediante Decreto Supremo, aprueba el Reglamento del presente Decreto Legislativo en un plazo máximo de ciento ochenta (180) días, contados a partir del día siguiente de su publicación en el Diario Oficial El Peruano.

SEGUNDA.- Normas sobre Identidad Digital Nacional

El Registro Nacional de Identificación y Estado Civil (RENIEC) en el ámbito de sus funciones y competencias emitirá las normas que resulten pertinentes para el otorgamiento, registro y acreditación de la identidad digital nacional. La Identidad Digital Nacional proporciona el mismo valor legal que el Documento Nacional de Identidad.

TERCERA.- Fortalecimiento de capacidades

La Autoridad Nacional del Servicio Civil (SERVIR) en el ámbito de sus funciones y competencias, en coordinación con la Secretaría de Gobierno Digital, promueve el fortalecimiento de capacidades en materia de gobierno digital y tecnologías digitales a los funcionarios y servidores de las entidades de la Administración Pública.

CUARTA.- Registro de Centros de Acceso Público

Las entidades de la Administración Pública que implementan progresivamente, en función a sus recursos y capacidades, espacios o centros de acceso público, previstos en la Ley de Promoción de Banda Ancha y Construcción de la Red Dorsal Nacional de Fibra Óptica, con miras a fortalecer capacidades y facilitar el proceso de inclusión digital de los ciudadanos y personas en general el acceso a los servicios digitales deben comunicarlo a la Secretaría de Gobierno Digital para el registro respectivo.

Entiéndase que toda referencia a los Centros de Acceso Ciudadano previstos en el Reglamento de la Ley de Firmas y Certificados Digitales se entenderá hecha al Centro de Acceso Público previsto en la presente norma.

QUINTA.- Vigencia

El presente Decreto Legislativo entra en vigencia a partir del día siguiente de su publicación, con excepción de lo previsto en los artículos 11, 12, 14, 15, 19, 20, 21, 22, 25, 27, 31 y numerales 18.1, 18.5, 18.6 y 18.8 del artículo 18, que entrarán en vigor con la norma reglamentaria correspondiente.

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

REPUBLICA DEL PERU

Decreto Legislativo

DISPOSICIONES COMPLEMENTARIAS TRANSITORIAS

PRIMERA.- Credencial de Identidad Digital

Las entidades de la Administración Pública pueden hacer uso de los mecanismos existentes para la autenticación de las personas en entornos digitales dentro de un contexto determinado, conforme a los lineamientos, progresividad y plazos a establecerse en el reglamento del presente Decreto Legislativo.

SEGUNDA.- Servicios Digitales

Las entidades de la Administración Pública que a la fecha de entrada en vigencia del presente Decreto Legislativo hayan implementado y brinden servicios digitales adoptan y adecuan las disposiciones de los mismos de manera progresiva conforme a sus recursos, capacidades, lineamientos y plazos a establecerse en el reglamento de la presente Ley, sin perjuicio de lo establecido en el numeral 5.1 del artículo 5 del presente Decreto Legislativo.

CONSEJO DE MINISTROS Secretaría de Gobierno Digital

POR TANTO:

Mando se publique y cumpla, dando cuenta al Congreso de la República.

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

MARTÍN ALBERTO VIZCARRA CORNEJO
Presidente de la República

CÉSAR VILLANUEVA ARÉVALO
Presidente del Consejo de Ministros

VICENTE ANTONIO ZEBALLOS SALINAS
Ministro de Justicia y Derechos Humanos

EXPOSICIÓN DE MOTIVOS

DECRETO LEGISLATIVO QUE APRUEBA LA LEY DE GOBIERNO DIGITAL

I. CONTEXTO NORMATIVO

- Ley Nº 30823, Ley que delega en el Poder Ejecutivo la facultad de legislar en materia de gestión económica y competitividad, de integridad y lucha contra la corrupción, de prevención y protección de Personas en situación de violencia y vulnerabilidad y de modernización de la gestión del Estado.
- Ley Nº 27658, Ley Marco de Modernización de la Gestión del Estado, mediante la cual se declara al Estado Peruano en proceso de modernización en sus diferentes instancias, dependencias, entidades, organizaciones y procedimientos, con la finalidad de mejorar la gestión pública y construir un Estado democrático, descentralizado y al servicio del ciudadano. La finalidad de la norma es la obtención de mayores niveles de eficiencia del aparato estatal, de manera que se logre una mejor atención a la ciudadanía, priorizando y optimizando el uso de los recursos públicos.
- Texto Único Ordenado de la Ley N° 27444 - Ley del Procedimiento Administrativo General, aprobado mediante el Decreto Supremo Nº 006-2017-JUS, que contiene las normas comunes para las actuaciones de la función administrativa del Estado en su relación con los administrados y regula todos los procedimientos administrativos desarrollados en las entidades, incluyendo los procedimientos especiales.
- La Ley N° 26497, Ley Orgánica del Registro Nacional de Identificación y Estado Civil (RENIEC), establece que el RENIEC es la entidad encargada de organizar y mantener el Registro Único de Identificación de las Personas Naturales e inscribir los hechos y actos relativos a su capacidad y estado civil. Con tal fin desarrollará técnicas y procedimientos automatizados que permitan un manejo integrado y eficaz de la información. Teniendo como una de sus funciones el emitir el documento único que acredita la identidad de las personas.
- La Ley Nº 29158, Ley Orgánica del Poder Ejecutivo, que establece el nuevo rol del Gobierno Nacional y dispone las normas y principios para reordenar la estructura y organización del Poder Ejecutivo, en virtud del mismo. Esta norma reconoce a la Presidencia del Consejo de Ministros como responsable de la coordinación de las políticas nacionales y sectoriales del Poder Ejecutivo, teniendo entre sus competencias el formular y aprobar las políticas nacionales de modernización de la Administración Pública y las relacionadas con la estructura y organización del Estado, así como dirigir la modernización de éste.
- Ley N° 27291 que modifica el Código Civil permitiendo la utilización de medios electrónicos para la comunicación de la manifestación de voluntad, particularmente mediante la utilización de la firma electrónica.
- Ley N° 27269, Ley de Firmas y Certificados Digitales que regula en el país la utilización de la firma digital. Su reglamento vigente es el Decreto Supremo N° 052-2008-PCM modificado por el Decreto Supremo N° 070-2011-PCM y Decreto Supremo Nº 105-2012-PCM, mediante el cual se otorga a la firma digital emitida dentro de la Infraestructura Oficial de Firma Electrónica la misma validez y eficacia jurídica que el uso de una firma manuscrita, garantizando de este modo la seguridad jurídica en las transacciones electrónicas, así mismo, establece la Estructura Jerárquica de Certificación Digital para el Estado Peruano para la realización de transacciones de gobierno electrónico.
- Ley N° 29733, Ley de Protección de Datos Personales y su Reglamento aprobado mediante Decreto Supremo N° 003-2013-JUS. La Ley tiene por objeto garantizar el derecho fundamental a la protección de datos, previsto en el artículo 2 numeral 6 de la Constitución Política del Perú, a través de su adecuado tratamiento.
- Decreto Supremo Nº 004-2013-PCM, mediante el cual se aprobó la Política Nacional de Modernización de la Gestión Pública (PNMGP), la cual deja sin efecto al Decreto Supremo Nº 025-2010-PCM que estableció la "Política Nacional de Simplificación Administrativa" toda vez que sus objetivos se recogen en la PNMGP.

16

- Decreto Supremo Nº 081-2013-PCM, mediante el cual se aprueba la Política Nacional de Gobierno Electrónico 2013 – 2017 la cual enmarca dentro de la estrategia de modernización de la gestión pública 2012-2016 y su respectiva Política Nacional al 2021, así como con el Plan Bicentenario y sus seis ejes de desarrollo alineadas en la Agenda Digital 2.0, la cual plantea para el desarrollo del Gobierno Electrónico en el país los siguientes lineamientos estratégicos, a saber: Transparencia, e-Inclusión, e-Participación, e-Servicios, Tecnología e Innovación, Seguridad de la Información e Infraestructura, destacándose la necesidad de habilitar los medios electrónicos necesarios al ciudadano para que pueda acceder a los servicios públicos por medios electrónicos seguros, a través del uso de su identidad digital.
- Decreto Legislativo Nº 681, mediante el cual se dictaron normas que regulan el uso de tecnologías avanzadas en materia de archivo de documentos e información aplicable tanto respecto a la documentación e información elaborada en forma convencional, como la producida mediante procedimientos informáticos en computadoras. Mediante la Ley Nº 26612 se modificó el Decreto Legislativo Nº 681, mediante el cual se regulaba el uso de tecnologías avanzadas en materia de archivo de documentos e información, incluyéndose a las personas jurídicas de derecho público interno del Sector Público dentro de los alcances del Decreto Legislativo 681. Por Decreto Supremo Nº 009-92-JUS se aprobó el Reglamento del Decreto Legislativo Nº 681. Y por Decreto Legislativo Nº 827 se amplió los alcances del Decreto Legislativo Nº 681 a las entidades públicas a fin de modernizar el sistema de archivos oficiales.
- Decreto Supremo N° 016-2017-PCM, mediante el cual se aprueba la "Estrategia Nacional de Datos Abiertos Gubernamentales del Perú 2017 - 2021" y el "Modelo de Datos Abiertos Gubernamentales del Perú"
- Decreto Supremo Nº 066-2011-PCM, por el que se aprueba el Plan de Desarrollo de la Sociedad de la Información en el Perú - La Agenda Digital Peruana 2.0.
- Decreto Supremo Nº 022-2017-PCM, por el cual se aprueba el Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros.
- Decreto Supremo N° 033-2018-PCM, mediante el cual se crea la Plataforma Digital Única del Estado Peruano y establecen disposiciones adicionales para el desarrollo del Gobierno Digital.
- Decreto Supremo N° 050-2018-PCM, mediante el cual se aprueba la definición de Seguridad Digital en el Ámbito Nacional.
- Decreto Supremo N° 051-2018-PCM, mediante el cual se crea el Portal de software Público Peruano y establece disposiciones adicionales sobre el software Público Peruano.
- Decreto Supremo N° 080-2018-PCM, mediante el cual se dispone la presentación de la Declaración de Intereses de los funcionarios y servidores públicos del Poder Ejecutivo.
- Resolución Ministerial N° 004-2016-PCM, mediante el cual se aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática.
- Resolución Ministerial N° 166-2017-PCM, mediante la cual se modifica el artículo 5 de la R.M. N° 004-2016-PCM referente al Comité de Gestión de Seguridad de la Información.
- Resolución Ministerial N° 119-2018-PCM, mediante el cual se dispone la creación de un Comité de Gobierno Digital en cada entidad de la Administración Pública.

17

II. FUNDAMENTACIÓN

El progreso desde finales del pasado siglo XX y el exponencial uso y desarrollo de las *tecnologías digitales*[1] en el presente siglo XXI permite emplearlas en un nuevo entorno, la administración pública, sobre todo, para la realización de transacciones y nuevas formas de interacción con los ciudadanos y personas, entre otros; lo cual configura un nuevo ámbito, el denominado *Gobierno Digital*[2], empero, a su vez, acarrea toda una serie de retos para los Estados como son los de mejorar su accionar y articulación entre los diferentes entes y niveles de la administración pública, así como los de generar confianza y seguridad a fin que dichas tecnologías puedan ser efectivamente aprovechadas por todas las personas procurando mejora de su calidad de vida, aprovechamiento de su tiempo y ahorro de dinero, esto es, propiciando "*valor público*"[3].

En esa línea, el Estado mediante la creación del Sistema Nacional de Informática[4] , la constitución de la Secretaría de Gobierno Digital en el ámbito de la Presidencia del Consejo de Ministros[5] , así como su designación de Líder Nacional de Gobierno Digital[6], ha sentado las bases para dirigir, evaluar y supervisar el desarrollo de Gobierno Digital y toda iniciativa de transformación digital en todo el sector público, siendo ello, a su vez, concordante con la Política 35 del Acuerdo Nacional[7], sobre Sociedad de la Información y Sociedad del Conocimiento, la misma que señala en el literal e) que el Estado fomentará la modernización del Estado, mediante el uso de las TIC, con un enfoque descentralista, planificador e integral.

De otra parte, cabe señalar que las aludidas tecnologías digitales están originando los llamados derechos humanos o fundamentales de "*cuarta generación*" que vienen a resguardar de un lado la libertad de expresión de las personas en las redes telemáticas, empero también "*...la universalidad de acceso a las mismas porque es eficaz para el criterio social de eficacia operativa, porque va a aumentar el volumen de intercambios a través del comercio electrónico, porque va a abrir nuevos mercados de distribución de bienes y servicios, porque va a dar al ciudadano una mayor sensación de proximidad con respecto al Estado, y por tanto de participación democrática, etc.*"[8], dando pie al concepto de **ciudadanía digital** que adquiere un sentido pleno en la era de Internet en tanto que favorece la participación de las personas, en cualquiera de sus roles: ciudadano (**persona natural**) o representante de una entidad pública, empresa privada u organización (**persona jurídica**) a ejercer sus derechos y deberes en un entorno digital a través de una gran variedad de mecanismos (**dispositivos digitales**) y formas (**presenciales y no presenciales**).

Así, el acceso y uso de las tecnologías digitales ofrece nuevos canales de comunicación innovadores que permiten dar voz a los que antes no la tenían, a través de redes y la creación de redes generando ***sociedades del conocimiento*** que se basan en "*cuatro pilares: la libertad de expresión, el acceso universal a la información y al conocimiento, el respeto a la diversidad cultural y lingüística, y la educación de calidad para todos*"[9].

---

[1] "Se refieren a las Tecnologías de la Información y la Comunicación - TIC, incluidos Internet, las tecnologías y dispositivos móviles, así como la analítica de datos utilizados para mejorar la generación, recopilación, intercambio, agregación, combinación, análisis, acceso, búsqueda y presentación de contenido digital, incluido el desarrollo de servicios y aplicaciones", según lo dispuesto por el numeral 5, del artículo 2° del Decreto Supremo N° 033-2018-PCM, por el que se crea la Plataforma Digital Única del Estado Peruano y establecen disposiciones adicionales para el desarrollo del Gobierno Digital.

[2] Definido como "...el uso de las tecnologías digitales como parte integral de las estrategias de modernización de los gobiernos para crear valor público. Se basa en un ecosistema de gobierno digital conformado por actores gubernamentales, organizaciones no gubernamentales, empresas, asociaciones de ciudadanos y personas que apoyan la producción de datos, servicios y contenido y tienen acceso a los mismos a través de interacciones dentro del gobierno", en: Perú: Gobernanza Integrada para un crecimiento Inclusivo, OCDE 2016, P 249, cuya versión integra puede ser consultada en: https://goo.gl/DSZjUB.

[3] Entendido como los "diversos beneficios para la sociedad que pueden variar según la perspectiva o los actores, incluidos los siguientes: 1) bienes o servicios que satisfacen los deseos de los ciudadanos y clientes; 2) elecciones de producción que cumplan con las expectativas ciudadanas de justicia, equidad, eficiencia y efectividad; 3) instituciones públicas ordenadas y productivas que reflejen los deseos y preferencias de los ciudadanos; 4) equidad y eficiencia de la distribución; 5) uso legítimo del recurso para lograr propósitos públicos; y 6) innovación y adaptabilidad a las preferencias y demandas cambiantes", en Recomendación del Consejo sobre Estrategias de Gobierno Digital, adoptado por el Consejo de la OCDE el 15 de julio de 2014, documento que puede ser consultado en: http://www.oecd.org/gov/digital-government/Recommendation-digital-government-strategies.pdf

[4] Ver: Decreto Legislativo N° 604, de fecha 30ABR1990 -: http://m.inei.gob.pe/media/archivos/5073_1.pdf

[5] Ver: Decreto Supremo N° 022-2017-PCM, de fecha 28FEB2017- https://bit.ly/2OXxDAj

[6] Ver: Decreto Supremo N° 033-2018-PCM, de fecha 23MAR2018 - https://bit.ly/2IbQBjl

[7] Ver: https://bit.ly/2NcODSO

[8] BUSTAMANTE DONAS, Javier; "COOPERACIÓN EN EL CIBERESPACIO: BASES PARA UNA CIUDADANÍA DIGITAL", en Revista Argumentos de Razón Técnica, N° 10, 2007, Universidad Complutense, Madrid, p. 324.

[9] En "*Sociedades del conocimiento: el camino para construir un mundo mejor*", según la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (**UNESCO**), en documento que puede ser consultado en: https://es.unesco.org/about-us/introducing-unesco.

18

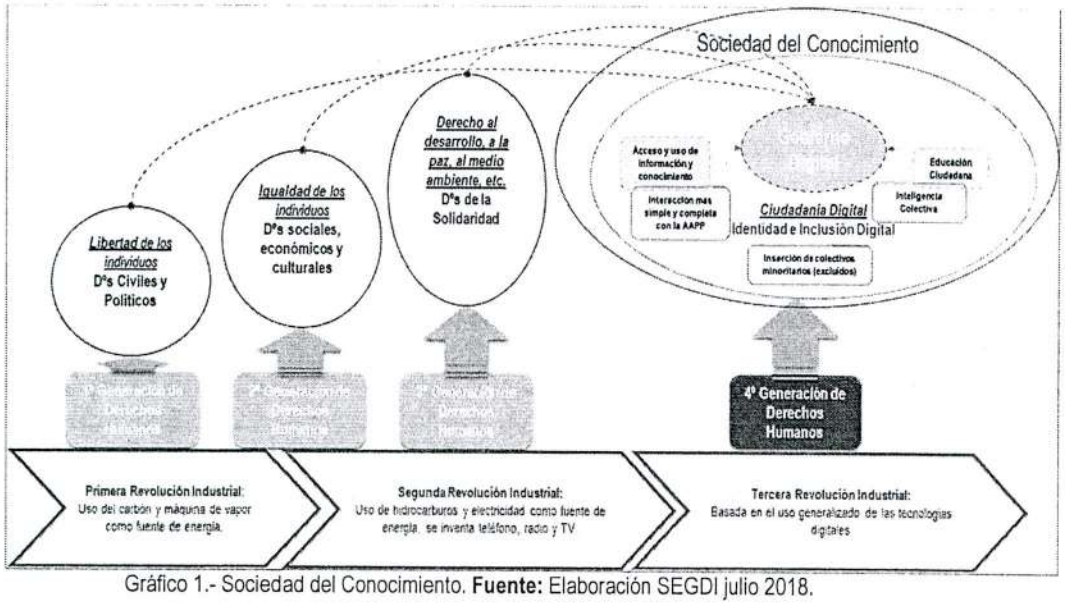

Gráfico 1.- Sociedad del Conocimiento. **Fuente:** Elaboración SEGDI julio 2018.

En efecto, hasta ahora se ha tenido como noción a la "*sociedad de la información*" basada en los avances tecnológicos; empero, el cambio de concepto se apoya en que las "*sociedades del conocimiento comprende dimensiones sociales, éticas y políticas mucho más vastas*"[10], donde la anotada evolución de las tecnologías digitales no sólo nos lleve, "*–en virtud de un determinismo tecnológico estrecho y fatalista– a prever una forma única de sociedad posible*"[11], sino a una "*sociedad del conocimiento*" donde se garantice el aprovechamiento compartido del saber y en que la educación juega un rol determinante, empero también que a través de las diferentes entidades públicas se establezcan las condiciones necesarias para la prestación de servicios públicos; en esa línea el Estado viene propiciar no sólo dichas "sociedades del conocimiento" sino también nuevas posibilidades de desarrollo.

No obstante, el trabajo realizado resulta aún insuficiente para lograr niveles adecuados de digitalización, por un lado, según cifras del Foro Económico Mundial (FEM) en su estudio "Reporte Global sobre las Tecnologías de la Información 2016", el Perú se ubica en el *puesto noventa (90) de ciento cuarenta y tres (143) economías;* lo cual implica que no tenemos la capacidad de aprovechar las Tecnologías de la Información y Comunicación para impulsar el progreso económico de nuestro país; por otro lado, según el estudio de la Organización de las Naciones Unidas sobre Gobierno Electrónico[12], el Perú se ubica en el puesto setenta y *siete (77) de ciento noventa y tres (193) países*; más aún según cifras reportadas en "El fin del Trámite Eterno: Ciudadanos, Burocracia y Gobierno Digital[13]", documento elaborado por el Banco Interamericano de Desarrollo (BID,2018), en el Perú un trámite *requiere 8.6 horas, solo el 29% de ciudadanos completa su trámite en una sola visita, y solo el 17% de trámites son catalogados como fáciles, es decir, se realizan en una sola interacción y en menos de 02 horas*; por otro lado, existe a la fecha más de 200 normas de distinto rango y naturaleza[14] (leyes, decretos legislativos, decretos supremos), sobre diferentes aspectos del uso de las tecnologías digitales por parte de la administración en sus procesos y servicios en ámbitos tales como interoperabilidad, identidad digital, datos abiertos, seguridad, notificaciones electrónicas, etc. Lo cual limita en última instancia los procesos de simplificación administrativa, modernización y digitalización de los servicios y trámites que se prestan a la ciudadanía no generándose "valor público" que facilite la cercanía del Estado.

Sin embargo, y mediante el ítem d.3) del literal d) del numeral 5 del artículo 2 de la Ley N° 30823[15], se delega al Poder Ejecutivo la facultad de legislar con miras a "*establecer el marco normativo para*

[10] Hacia las sociedades del conocimiento — ISBN 92-3-304000-3 — © UNESCO 2005, P. 17.
[11] Hacia las sociedades del conocimiento, Op. Cit., P. 17.
[12] Ver: https://bit.ly/2pYDkW3
[13] BID. 2018. El fin del trámite eterno: ciudadanos, burocracia y gobierno digital / Benjamin Roseth, Angela Reyes, Carlos Santiso, editores. Ver: https://bit.ly/2MOZDss
[14] Ver: Análisis de la normatividad en TIC y recomendaciones de mejora, consultoría solicitada por el Consejo Nacional de Competitividad
[15] Ver: https://bit.ly/2N6InNC

19

promover el despliegue transversal de las tecnologías digitales en las entidades del Estado; a fin de mejorar el alcance, condiciones, la prestación y el acceso de los ciudadanos a los servicios que presta el Estado", lo cual conlleva a que la Secretaría de Gobierno Digital - SEGDI en coordinación con los actores relevantes en esta materia, tales como la Secretaría de Gestión Pública - SGP y el Registro Nacional de Identificación y Estado Civil - RENIEC) y otros interesados, presente la siguiente propuesta normativa que, sustentado en recomendaciones de la Organización para la Cooperación y el Desarrollo Económico - OCDE, estudios en materia de tecnologías digitales realizado por organismos supranacionales (Foro Económico Mundial - FEM, OCDE, Banco Mundial - BM, Banco Interamericano de Desarrollo -BID entre otros), estándares internacionales (básicamente los emitidos por la International Organization for Standardization - ISO), normas técnicas, marcos de referencia y buenas prácticas ampliamente reconocidas en materia de gobierno, gestión y despliegue de las tecnologías digitales; tiene por objeto materializar un *marco normativo 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.*

1. RECOMENDACIONES DE LA OCDE Y ORGANISMOS INTERNACIONALES EN MATERIA DE GOBIERNO DIGITAL

Con la finalidad de aprovechar las anotadas tecnologías digitales, nuestro país viene siguiendo las recomendaciones de la Organización para la Cooperación y el Desarrollo Económicos (OCDE)[16], contenidas en el documento Perú, Gobernanza Integrada para un crecimiento Inclusivo, OCDE 2016[17], donde dicho organismo menciona que el "*...hecho de que el gobierno esté desarrollando y desplegando TIC dentro de una perspectiva de procedimientos, legalista y técnica podrá presagiar una deficiencia potencial en el Perú. El enfoque actual podría estar subestimando los beneficios potenciales que podrían derivarse de la digitalización de la reforma del sector público en la práctica política actual. Por lo tanto, se necesita un marco estratégico de política de gobierno digital y gobernanza consistente con la definición anterior, de la mano con la revisión del enfoque estratégico sobre el uso de las TIC en el sector público con el fin de generar ventajas claras y un* ***gran valor público*** *en todo el ecosistema de gobierno digital*"[18] (énfasis agregado).

En la misma línea, y como lo consideran los *Objetivos de Desarrollo Sostenible* – ODS[19], acordados por los países miembros de las Naciones Unidas[20], la tecnología es un medio para alcanzar el desarrollo (bienestar) sostenible (para el presente y el futuro); en efecto, es evidente que las tecnologías pueden aportar en los planes de desarrollo, por ejemplo, con computadoras en las escuelas, sistemas de información en las entidades de la Administración Pública, entre otros. Pero más allá de lo antes indicado es donde aparece el verdadero sentido de las tecnologías digitales en función con el desarrollo, esto es el de la innovación para la transformación digital de la sociedad, donde en tal contexto ya no es tan importante la cantidad sino la "**calidad de los servicios**" que se prestan a las personas desde las escuelas hasta los servicios digitales que aportan y generan valor público. En tal sentido, las **tecnologías digitales** son una herramienta para mejorar la calidad de vida de las generaciones presentes y para garantizar una mejor gestión de los recursos para las venideras.

Aquí es donde es decisivo el papel del Poder Ejecutivo, así como de los gobiernos regionales y locales, para abrir las puertas desde las políticas públicas para orientarnos hacia las *ciudades inteligentes* y las *ciudadanías del conocimiento*.

---

[16] Conocida como OECD por las siglas en inglés de Organisation for Economic Co-operation and Development, organismo que tiene como misión "promover políticas que mejoren el desarrollo económico y el bienestar social de las personas en todo el mundo", en http://www.oecd.org.

[17] Perú: Gobernanza integrada para un crecimiento inclusivo, OCDE 2016, Op. Cit.

[18] Perú: Gobernanza Integrada para un crecimiento Inclusivo, OCDE 2016, Op. Cit., P 249.

[19] "También conocidos como Objetivos Mundiales, son un llamado universal a la adopción de medidas para poner fin a la pobreza, proteger el planeta y garantizar que todas las personas gocen de paz y prosperidad. Estos 17 Objetivos se basan en los logros de los Objetivos de Desarrollo del Milenio, aunque incluyen nuevas esferas como el cambio climático, la desigualdad económica, la innovación, el consumo sostenible y la paz y la justicia, entre otras prioridades", información obtenida en: http://www.undp.org/content/undp/es/home/sustainable-development-goals.html.

[20] Los Objetivos de Desarrollo Sostenible (ODS) se gestaron en la Conferencia de las Naciones Unidas sobre el Desarrollo Sostenible, celebrada en Rio de Janeiro en 2012, información obtenida en: http://www.undp.org/content/undp/es/home/sustainable-development-goals/background.html.

20

Sobre lo anterior, referir que cada dos años el Departamento de Asuntos Económicos y Sociales de la ONU elabora el Estudio de Gobierno Electrónico, en los que evalúa a todos sus Estados miembros (193) en materia de desarrollo de gobierno electrónico. Así, para dicho estudio la ONU define un indicador, conocido como el ***«Índice de Desarrollo de Gobierno Electrónico (IDGE)»***, el cual es el promedio ponderado de tres (3) subíndices normalizados, los cuales corresponden a tres dimensiones: 1. Servicios en Línea (Online Service), 2. Infraestructura de Telecomunicaciones (Telecommunication Infrastructure) y 3. Capital Humano (Human Capital).

Así, tenemos que, a la fecha de hoy para el caso de nuestro país, en el referido índice nos ubicamos en el puesto setenta y siete (77) de ciento noventa y tres (193) países, habiendo subido cuatro (04) posiciones en la última evaluación, de cuyo análisis se desprende que debemos trabajar en mejorar las políticas, normas y lineamientos con miras a establecer el marco normativo para promover el despliegue transversal de las tecnologías digitales en las entidades del Estado.

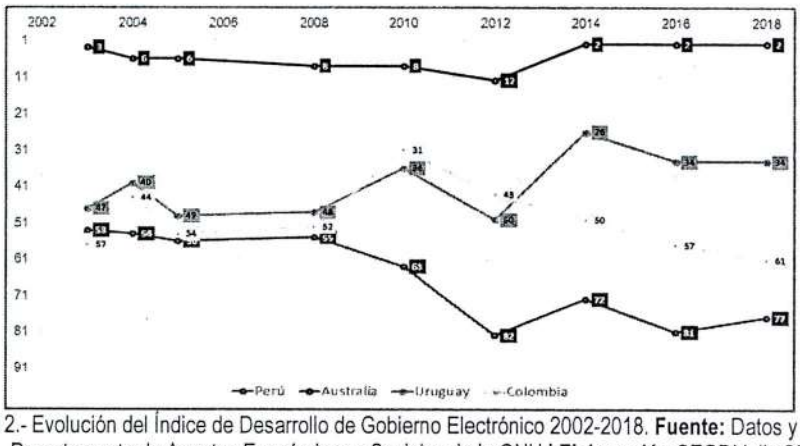

Gráfico 2.- Evolución del Índice de Desarrollo de Gobierno Electrónico 2002-2018. **Fuente:** Datos y estudios del Departamento de Asuntos Económicos y Sociales de la ONU | **Elaboración** SEGDI julio 2018.

Por otro lado, el Foro Económico Mundial (WEF, por sus siglas en inglés), en coordinación con la Escuela de Negocios INSEAD[21] desde el 2002, anualmente evalúa la capacidad que tienen las economías por aprovechar las Tecnologías de la Información y Comunicación (TIC) e impulsar el progreso económico de sus países. Cabe indicar que el referido estudio desarrolla el Índice de Capacidad de Respuesta en Red (Networked Readiness Index - NRI, por su denominación en inglés), el cual es un indicador compuesto por 4 subíndices, 10 subcategorías y 53 indicadores que evalúan el entorno y condiciones de la economía miembro para soportar el emprendimiento y desarrollo de las TIC, así como el grado de preparación, adopción e impacto económico y social del uso de las Tecnologías de la Información y Comunicación.

Más aún, el referido índice se encuadra en un marco de referencia, el cual comprende los siguientes ámbitos: "Entorno", "Preparación", "Uso o adopción" e "Impacto", y para cada uno de los cuales hay una serie de sub-índices e indicadores.

1. Entorno, ámbito que mide el grado en el que el marco regulatorio y Condiciones de Mercado soportan el emprendimiento, innovación y desarrollo de las TI.
2. Preparación, ámbito que mide Grado de preparación del País que apoyan la adopción de las TIC (Infraestructura, Capacidades y Asequibilidad).
3. Uso o adopción, ámbito que mide el grado de adopción por los Principales Interesados (individuos, Empresas y Gobierno).
4. Impacto, ámbito que mide el impacto económico y social del uso de las TIC.

[21] Ver: https://www.insead.edu/

21

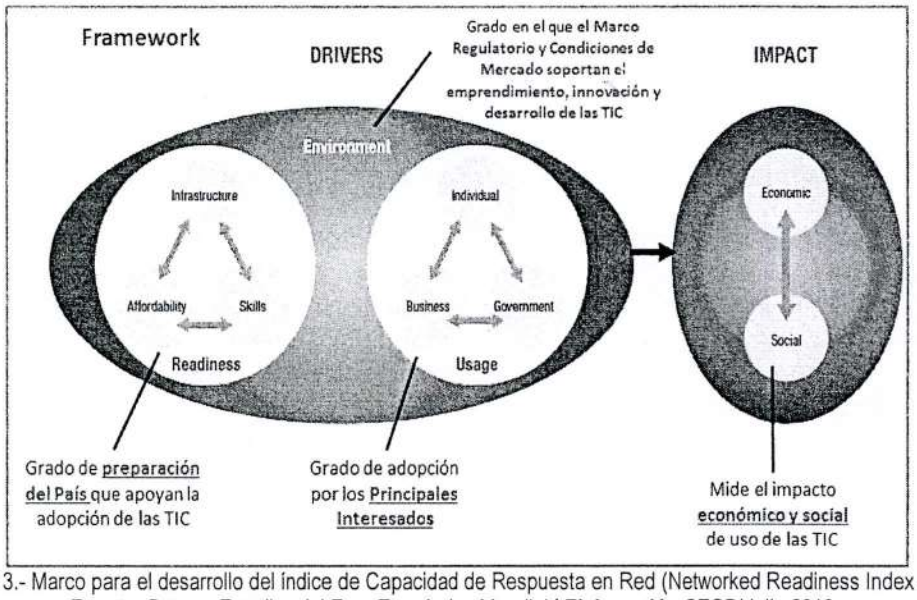

Gráfico 3.- Marco para el desarrollo del índice de Capacidad de Respuesta en Red (Networked Readiness Index - NRI). **Fuente:** Datos y Estudios del Foro Económico Mundial | **Elaboración** SEGDI julio 2018.

En esa línea, como se muestra en el Gráfico ***"Evolución del índice de Capacidad de Respuesta en Red (Networked Readiness Index - NRI)"*** los indicadores desde el 2012 para nuestro país no son nada favorables, nos encontramos en el puesto 90 de 143 economías, lo cual se explica, en sus diferentes estudios, en parte por lo siguiente:

- Entorno político y normativo débil.
- Una infraestructura TIC insuficientemente desarrollada y costosa.
- Sistema educativo de baja calidad
- Bajo uso de las TIC por parte de los actores (ciudadano, empresa y gobierno)
- Deficientes condiciones para aprovechar la innovación
- Un número excesivo de días para abrir nuevas empresas.
- Una economía que no puede ofrecer muchos empleos intensivos en conocimiento.

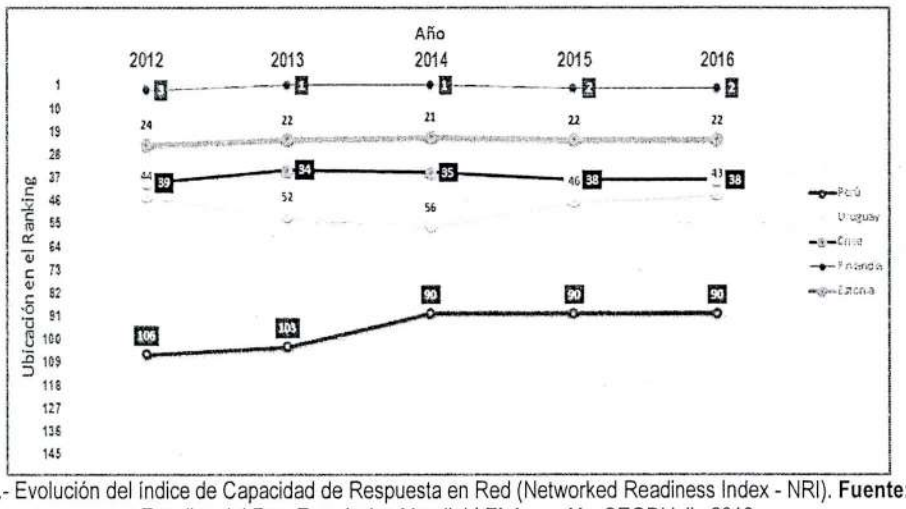

Gráfico 4.- Evolución del índice de Capacidad de Respuesta en Red (Networked Readiness Index - NRI). **Fuente:** Datos y Estudios del Foro Económico Mundial | **Elaboración** SEGDI julio 2018.

De otro lado, el Banco Interamericano de Desarrollo (BID) en el documento "El fin del Trámite Eterno: Ciudadanos, Burocracia y Gobierno Digital[22]" señala que implementar una reforma de simplificación y digitalización de trámites en un país de América Latina no es fácil, existen diferentes factores que influyen negativamente en la adopción e implementación de ese tipo de reformas, entre ellos, la baja

[22] Op. Cit Capítulo 3

22

coordinación interinstitucional, la complejidad regulatoria y técnica, un gobierno alejado del ciudadano. Es por ello, que para obtener resultados destacables recomienda 3 lecciones:

- ***Promover un cambio de paradigma que oriente el Estado hacia el ciudadano.***
- ***Empoderar a una entidad rectora con las competencias y recursos suficientes para impulsar cambios en todo el gobierno.***
- ***Establecer un modelo de gobernanza que facilite la implementación efectiva.***

Como se puede ver el tema del uso estratégico y transversal de las tecnologías digitales no es un asunto meramente técnico, normativo o de mercado, es un tema de carácter multisectorial que tiene impacto directo en el desarrollo de la economía del país, procurando con ello su desarrollo económico y social ("Prosperidad Económica y Social", por la OCDE); por tanto, si se ha delegado el desarrollo de un "***marco normativo para promover el despliegue transversal de las tecnologías digitales en las entidades del Estado; a fin de mejorar el alcance, condiciones, la prestación y el acceso de los ciudadanos a los servicios que presta el Estado***", este debe comprender o abarcar ámbitos que le permitan a las entidades en sus diferentes procesos o servicios usar de manera ágil, fiable y eficiente las tecnologías digitales con miras a:

1. Prestar un servicio digital en condiciones de accesibilidad y usabilidad.
2. Intercambiar información con otras entidades haciendo uso intensivo de las tecnologías digitales.
3. Emprender iniciativas de transparencia y datos abiertos.
4. Mantener los riesgos relacionados con las tecnologías digitales en un nivel aceptable.

Así, la OCDE en el antes reseñado documento Perú, Gobernanza Integrada para un crecimiento Inclusivo, OCDE 2016 menciona la necesidad que nuestro país adopte un enfoque más amplio de Gobierno Digital que el de Gobierno Electrónico, el cual implica desarrollar una visión integrada en la que la naturaleza transversal de las tecnologías digitales, debidamente posicionadas, faciliten el cambio a la transición digital y al uso estratégico de las tecnología digitales en el desarrollo del ecosistema digital en los tres niveles de gobierno, coadyuvando al logro de los objetivos nacionales establecidos en la agenda de gobierno, así como en la generación de "valor público" para los ciudadanos, recomendación que nuestro país a través de la Presidencia del Consejo de Ministros - PCM ha recogido en las funciones que ha encomendado a la Secretaría de Gobierno Digital[23].

Efectivamente, la Secretaría de Gobierno Digital (en adelante la SEGDI, anteriormente denominada Oficina Nacional de Gobierno Electrónico e Informática - ONGEI), se constituye en el ente rector del Sistema Nacional de Informática, establecido por el Decreto Legislativo N° 604[24], lo cual es recogido en el Reglamento de Organización y Funciones de la PCM aprobado el 28FEB2017, siendo responsable de emitir normas, lineamientos, guías, estándares, entre otros para promover el desarrollo del gobierno digital en el Perú, a través de servicios públicos digitales, seguridad digital, regulación digital, digitalización de pagos, interoperabilidad, entre otros en las entidades de la Administración Pública.

Sin embargo, y si bien todo lo antes indicado evidencia la predisposición y la preparación de nuestro país para tener una agenda inclusiva en línea con los referidos Objetivos de Desarrollo Sostenible (ODS)[25] y el acogimiento de las recomendaciones de la OCDE, se hace necesario fortalecer las capacidades de la Secretaría de Gobierno Digital para su adecuada función rectora del Sistema Nacional de Informática, de modo que permita dar cabida a la transición digital y al uso estratégico de las tecnología digitales a fin que se constituyan en el centro de la reforma y acompañen el proceso de modernización del Estado.

---

[23] Contenidas en el Reglamento de Organización y Funciones – ROF de la Presidencia del Consejo de Ministros, aprobado mediante Decreto Supremo N° 022-2017-PCM.

[24] El Decreto Legislativo N° 604 crea el Sistema Nacional de Informática, el cual define en su artículo 3 como ámbito de competencia: "*La instrumentalización jurídica y de mecanismos técnicos para el ordenamiento de los recursos de cómputo y de la actividad informática del Estado, así como toda la documentación asociada; la operación y explotación de los bancos de datos y archivos magnéticos de información al servicio de la gestión pública. Corresponde a este desarrollo la planeación sistemática de procesos, métodos y técnicas apoyadas en ciencia y técnica aplicada, que se establecen con el fin de usar, procesar y transportar información*".

[25] Ver: https://bit.ly/2qk9f28

Gráfico 5.- Recomendaciones de la OCDE. **Fuente**: Estudio de Gobernanza Pública del Perú. Elaboración SEGDI julio 2018.

Adicionalmente, un aspecto relevante es acerca de los **Servicios Digitales**, según CEPAL los Servicios Electrónicos (e-servicios) *"se refiere a la entrega de mejores servicios a los ciudadanos, como los trámites interactivos (peticiones de documentos, emisión de certificados, pagos hacia y desde los organismos públicos)"*[26].

Asimismo, según lo indicado por la División de Administración Pública y Gestión del Desarrollo de Naciones Unidas se entiende por "**E-SERVICE:** cuando los servicios públicos son ofrecidos de forma total o parcial a través de plataformas que utilizan TICs".

En esa línea, el Estudio de las Naciones Unidas sobre el Gobierno Electrónico[27], en el cual define etapas para los servicios digitales en base al grado de interactividad de dichos servicios con los usuarios o ciudadanos, los cuales son "*Servicios de Información Emergente*" el cual consiste en la difusión en sus sitios web de las entidades públicas de información general y estática, en este nivel no existe tipo alguno de interactividad; "*Servicios de Información Mejorada*" donde los sitios web de las entidades públicas la comunicación bidireccional o unidireccional mejorada como la búsqueda de documentos, descarga de formularios, entre otros; "*Servicios Transaccionales*" que se caracteriza por una mayor interactividad, en este nivel se exigen alguna forma de autenticación de la identidad del ciudadano, los servicios procesan además de transacciones financieras (pagos digitales) otro tipo de transacciones como declaración de impuestos, solicitud de certificados, licencias, entre otros; y finalmente "*Servicios Conectados o Integrados*" donde la información, datos y conocimiento se transfiere entre entidades públicas mediante aplicaciones integradas, en esta etapa se proporcionan además servicios personalizados pensados en la experiencia del ciudadano.

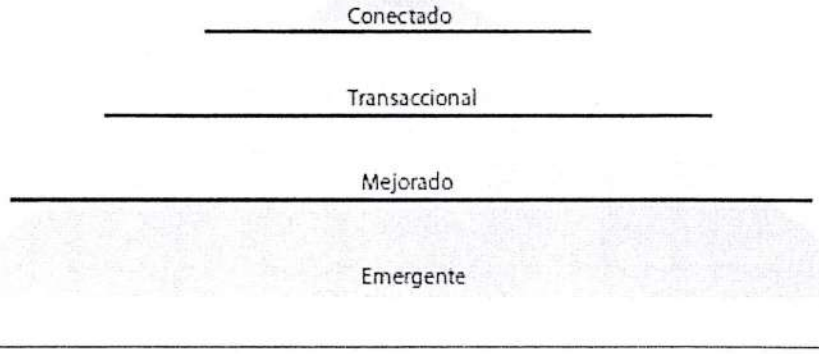

Gráfico 6.- Las cuatro etapas del desarrollo de los servicios en línea. Fuente: Naciones Unidas 2012

[26] CEPAL. El Gobierno Electrónico en la gestión pública. Ver: https://repositorio.cepal.org/bitstream/handle/11362/7330/1/S1100145_es.pdf
[27] Department of Economic and Social Aff airs. United Nations. E-Government Survey 2012 - E-Government for the People. Puede ser consultado en: https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2012-Survey/Complete-Survey.pdf

Adicionalmente, la Agenda Digital para América Latina y el Caribe (eLAC2020)[28] tiene como uno de sus objetivos de Gobierno Digital *"Establecer e impulsar estándares de **servicios digitales** que faciliten y agilicen los servicios gubernamentales y promuevan múltiples canales de acceso, favoreciendo un entorno regional interoperable de servicios digitales mediante el desarrollo de infraestructura, plataformas, arquitecturas, estándares y sistemas integrados."*

Resulta conveniente señalar que países como Colombia, Estados Unidos, Reino Unido cuentan con su propia definición de servicio digital, las cuales son:

País	Concepto	Definición
Colombia[29]	Servicios ciudadanos digitales	Es el conjunto de servicios que brindan capacidades y eficiencias para optimizar y facilitar el adecuado **acceso de los usuarios a la Administración Pública a través de medios electrónicos**. Estos servicios se clasifican en básicos y especiales.
Estados Unidos[30]	Servicios digitales	*Los servicios digitales incluyen la **entrega de la información digital y los servicios transaccionales** (por ejemplo, formularios en línea, beneficia a las aplicaciones, presentaciones tarjeta de tiempo) a través de una **variedad de plataformas, dispositivos y mecanismos de entrega** (por ejemplo, sitios web, aplicaciones móviles y las redes sociales).*
Reino Unido[31]	Servicios digitales (públicos o privados)	*Que se pueden prestar a través de la comunicación digital, por ejemplo, internet, red de telefonía móvil que puede incluir la entrega de información digital (por ejemplo, datos, contenido) y / o servicios transaccionales. Pueden ser públicos o privados, por ejemplo, el gobierno electrónico, los servicios de banca digital, el comercio electrónico, los servicios de música (por ejemplo, Spotify) y los servicios de cine y televisión (por ejemplo, Netflix).*

Tabla 1.- Definiciones de Servicios Digitales

Con respecto a lo anterior hay que indicar que tanto Colombia, Estados Unidos y Reino Unido hacen referencia al acceso a servicios o entrega de información a través de medios electrónicos, sitios web, aplicaciones móviles, entre otros.

De otro lado, resulta conveniente revisar la regulación nacional en este ámbito el Reglamento de la Ley del Impuesto a la Renta, aprobado mediante Decreto Supremo N° 122-94-EF, en su artículo 4°-A señala que *"se entiende por servicio digital a todo servicio que se pone a disposición del usuario a través del Internet o de cualquier adaptación o aplicación de los protocolos, plataformas o de la tecnología utilizada por Internet o cualquier otra red a través de la que se presten servicios equivalentes mediante accesos en línea y que se caracteriza por ser esencialmente automático y no ser viable en ausencia de la tecnología de la información. Para efecto del Reglamento, las referencias a página de Internet, proveedor de Internet, operador de Internet o Internet comprenden tanto a Internet como a cualquier otra red, pública o privada." (énfasis añadido).*

Asimismo, el Reglamento de la Ley N° 27269 – Ley de Firmas y Certificados Digitales, aprobado mediante Decreto Supremo N° 052-2008-PCM, señala en el artículo 40° que *"El ciudadano tiene derecho al acceso a los servicios públicos a través de medios electrónicos seguros para la realización de transacciones de gobierno electrónico con las entidades de la Administración Pública" (énfasis añadido)*, debiendo considerar para tal fin el uso de firmas y certificados digitales, asegurando la disponibilidad de acceso, la integridad, la autenticidad, el no repudio y la confidencialidad de las transacciones realizadas por estos medios. Asimismo, define como "Medios

[28] Sexta Conferencia Ministerial sobre la Sociedad de la Información de América Latina y el Caribe – Elac2020. Enlace: https://conferenciaelac.cepal.org/6/sites/elac2020/files/cmsi.6_agenda_digital.pdf
[29] Enlace: http://www.mintic.gov.co/portal/604/articles-59399_documento.pdf
[30] Estrategia de Gobierno Digital de Estados Unidos. Texto original: *"Digital services include the delivery of digital information (i.e. data or content) and transactional services (e.g. online forms, benefits applications) across a variety of platforms, devices and delivery mechanisms (e.g. websites, mobile applications, and social media)".*
[31] El Marco de Competencia Digital 2.0. Ver: https://ec.europa.eu/jrc/en/digcomp/digital-competence-framework

25

electrónicos" a "*los sistemas informáticos o computacionales a través de los cuales se puede generar, procesar, transmitir y archivar de documentos electrónicos*".

En esa línea, y considerando las etapas definidas por Naciones Unidas, siguiendo las definiciones y experiencias de países líderes en Gobierno Digital y organismos supranacionales, así como también la regulación nacional, para los efectos de la presente propuesta se entiende por **Servicio Digital** a aquel provisto de forma total o parcial a través de Internet u otra red equivalente, que se caracteriza por ser automático, no presencial y utilizar de manera intensiva las tecnologías digitales, para la producción y acceso a datos y contenidos que generen valor público para los ciudadanos y personas en general.

Otro aspecto a relevar es importante que la "**Arquitectura Empresarial**", cabe indicar que otro término importante en el ámbito de Gobierno Digital es el de "**Arquitectura Digital**", el cual conforme las buenas prácticas y estándares internacionales de países como Estados Unidos, Uruguay y Colombia se constituye en un *"Conjunto de componentes, lineamientos y estándares, que desde una perspectiva integral de la organización permite alinear los sistemas de información, datos, seguridad e infraestructura tecnológica con la misión y objetivos estratégicos de la entidad, de tal manera que se promuevan la colaboración, interoperabilidad, escalabilidad, seguridad y el uso optimizado de las tecnologías digitales en un entorno de Gobierno Digital".*

Es más, en cada uno de los países referidos el diseño de una **Arquitectura Digital,** ha servido para alinear los objetivos de estratégicos de la organización, entidad o país con las capacidades y potencialidades de los sistemas de información, datos e infraestructura tecnológica, en suma Tecnologías Digitales. En esa línea es bueno referir su importancia en base a lo desarrollado por otros países y lo indicado por algunas buenas prácticas.

a) **Caso Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (AGESIC) - Uruguay** [32]

Conforme lo indicado por **AGESIC**, la Arquitectura Empresarial es una metodología de mejora continua a mediano plazo. Se basa en una visión integral y permite mantener actualizada la estructura de información organizacional alineando procesos, datos, aplicaciones e infraestructura tecnológica. La misma que comprende un conjunto de estándares, políticas, productos recomendados y mejores prácticas para guiar a los organismos en el diseño de sus soluciones tecnológicas, de tal manera que se promuevan la interoperabilidad y el uso optimizado de los recursos de Tecnologías de la Información del Estado. Más aun, establece como componentes de la Arquitectura Empresarial

Compontes de la arquitectura empresarial

- **Arquitectura de información**: describe la estructura de los datos físicos y lógicos de la organización y sus modelos de gestión.
- **Arquitectura de negocio**: define la estrategia de negocio, la estructura organizacional y los procesos clave de la organización.
- **Arquitectura de aplicaciones**: provee la definición funcional para cada uno de los sistemas de información requeridos, sus interacciones y las relaciones que tienen con los procesos de negocio CORE de la organización.
- **Arquitectura tecnológica**: describe la estructura de hardware, software y comunicaciones requerida para dar soporte a la implementación de los sistemas de información.

b) **Caso Colombia**[33]**:**

El Ministerio de Tecnologías de la Información y Comunicación de Colombia especifica que la Arquitectura de Tecnologías de la Información del Estado se constituye en un componente estratégico para el uso de las tecnologías digitales de manera transversal en los sectores,

[32] Ver:https://www.agesic.gub.uy/innovaportal/v/5417/1/agesic/arquitectura-empresarial-de-gobierno.html
[33] Ver: http://www.mintic.gov.co/arquitecturati/630/w3-propertyvalue-8109.html

26

regiones y toda institución pública. Busca explicar a través de un conjunto integrado de componentes cómo los sistemas de información, los procesos, las unidades organizativas y las personas funcionan como un todo, como un sistema, como un solo país. Asimismo, especifica que la Arquitectura de Tecnologías de la Información del Estado describe la estructura y las relaciones de todos los elementos de TI de una organización. Se descompone en arquitectura de información, arquitectura de sistemas de información y arquitectura de servicios tecnológicos. Incluye además las arquitecturas de referencia y los elementos estructurales de la estrategia de TI (visión de arquitectura, principios de arquitectura, lineamientos y objetivos estratégicos).

c) **Caso Estados Unidos** [34]

En el caso de Estados Unidos, disponen de un "**Marco de Arquitectura Empresarial**", el cual describe un conjunto de herramientas para ayudar a los planificadores del gobierno a implementar un Enfoque Común en la prestación de servicios de Tecnologías de información con miras a promover mayores niveles de efectividad, reducir brechas de rendimiento, analizar inversiones en tecnologías de la información y aumentar la colaboración entre entidades. El **Marco de Arquitectura Empresarial** describe seis subdominios entre los que se destaca:

- Dominio de Estrategia
- Dominio de Negocio
- Dominio de Datos
- Dominio de Aplicaciones
- Dominio de Infraestructura
- Dominio de Seguridad

2. PROPUESTA NORMATIVA

2.1 DISPOSICIONES GENERALES

Conforme lo anterior, la propuesta normativa tiene como primer aspecto a relevar aquel referido a "Disposiciones Generales", el cual establece disposiciones sobre el "**OBJETO DE LA NORMA**", "**ÁMBITO DE APLICACIÓN**", "**DEFINICIONES**", "**FINALIDAD**" y "**PRINCIPIOS RECTORES**" que allana la comprensión e interpretación de las disposiciones sustantivas de la norma.

A. OBJETO DE LA NORMA

El objeto de la norma debe respetar, en primer lugar, lo señalado en la "Guía de Técnica Legislativa para elaboración de Proyectos Normativos de las Entidades del Poder Ejecutivo", la cual refiere que el *"objeto de la norma es la parte dispositiva de la norma en la que se identifica **la materia o asunto que se pretende regular**. Es real, fáctico, viable y único"*. Por otro lado, debe ser consistente con las facultades delegadas en el ítem d.3) del literal d) del numeral 5 del artículo 2 de la Ley N° 30823, la cual refiere que el Poder Ejecutivo tiene facultades para *establecer "**el marco normativo para promover el despliegue transversal de las tecnologías digitales** en las entidades del Estado; a fin de mejorar el alcance, condiciones, la prestación y el acceso de los ciudadanos a los servicios que presta el Estado"*; en ese sentido, tenemos lo siguiente:

La materia que se pretende regular tiene relación con las competencias de la Secretaría de Gobierno Digital:	**Facultades Delegadas**
Concordante con el artículo 47 y literal k) del artículo 48 del D.S. N° 022-2017-PCM, la Secretaría de Gobierno Digital - SEGDI tiene como función: Proponer y aprobar normas, lineamientos y estándares para promover el desarrollo e implementación de:	El marco normativo para promover el despliegue transversal de las tecnologías digitales en las entidades del Estado; a fin de mejorar el alcance, condiciones, la prestación y el acceso de los
Tecnologías Digitales	
Seguridad de la Información (Seguridad digital)	
Infraestructura de datos espaciales	

[34] Ver: https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/egov_docs/fea_v2.pdf

27

Datos abiertos	ciudadanos a los servicios que presta el Estado.
Interoperabilidad (Identidad digital)	
Portales del Estado	
Arquitectura Digital	

Tabla 2.- Competencias de la SEGDI

En línea con lo anterior, podemos indicar que ***"promover el despliegue transversal de las tecnologías digitales en las entidades de la administración pública"***, conlleva a "promover el despliegue transversal de la interoperabilidad, identidad digital, seguridad digital, datos y digitalización de servicios en las entidades de la administración pública", lo cual, obviamente, no sucede por meramente estar "definido en una norma", se requiere establecer *marcos de gobernanza* en cada uno de los ámbitos indicados y, conjuntamente en estos, el *régimen jurídico aplicable al uso transversal de tecnologías digitales en la administración pública, por ende el objeto de la norma es:*

La presente Ley tiene por objeto establecer 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.

B. ÁMBITO DE APLICACIÓN

En concordancia con el objeto de la norma y las recomendaciones realizadas por la Secretaría de Gestión Pública, la propuesta normativa es de aplicación a toda entidad que forma parte de la Administración Pública a que se refiere el artículo I del título Preliminar de la Ley N° 27444. Sus regulaciones también alcanzan a las personas jurídicas o naturales que por mandato legal, encargo o relación contractual ejercen potestades administrativas, y por tanto su accionar se encuentra sujeto a normas de derecho público, en los términos dispuestos por la Presidencia del Consejo de Ministros. En el caso de las empresas que conforman la actividad empresarial del Estado, su aplicación se da en todo aquello que le resulte aplicable.

C. DEFINICIONES

Dado que el uso transversal de las tecnologías digitales tiene como una serie de instrumentos y conceptos que provienen de ámbitos técnicos, es fundamental establecer definiciones desde un enfoque estratégico, que resalta el impacto de estos en materia de simplificación administrativa, modernización, gestión pública, innovación, eficiencia, eficacia, y generación de valor para los ciudadanos y personas en general.

Queda claro que, los principales conceptos en este ámbito nos servirán de "cimiento" para el entendimiento de la propia norma, su reglamento y proyectos que, en base a ella, realicen las entidades de la administración pública.

Cabe indicar que las definiciones se sustentan en normas aprobadas en nuestra legislación, estudios de organismos supranacionales (Foro Económico Mundial - FEM, Organización para la Cooperación y el Desarrollo Económicos, OCDE), buenas prácticas (COBIT 5), estándares (NTP ISO/IEC 27001:2014), experiencia internacional y normas técnicas ampliamente reconocidos a nivel internacional (NTP ISO/IEC 38500:2016).

1. **Gobierno Digital.-** Es el uso estratégico de las tecnologías digitales y datos en la Administración Pública para la creación de valor público. Se sustenta en un ecosistema compuesto por actores del sector público, ciudadanos y otros interesados, quienes apoyan en la implementación de iniciativas y acciones de diseño, creación de servicios digitales y contenidos, asegurando el pleno respeto de los derechos de los ciudadanos y personas en general en el entorno digital. Señalar que ésta definición se recoge en el numeral 6.1 de la propuesta normativa en razón que es el capítulo relacionado con la misma.

2. **Tecnologías Digitales.-** Se refieren a las Tecnologías de la Información y la Comunicación - TIC, incluidos Internet, las tecnologías y dispositivos móviles, así como la analítica de datos utilizados para mejorar la generación, recopilación, intercambio, agregación, combinación, análisis, acceso, búsqueda y presentación de contenido digital, incluido el desarrollo de servicios y aplicaciones aplicables a la materia de Gobierno Digital.
3. **Entorno Digital.-** Es el dominio o ámbito habilitado por las tecnologías y dispositivos digitales, generalmente interconectados a través de redes de datos o comunicación, incluyendo el Internet, que soportan los procesos, servicios, infraestructuras y la interacción entre personas.
4. **Servicio Digital.-** Es aquel provisto de forma total o parcial a través de Internet u otra red equivalente, que se caracteriza por ser automático, no presencial y utilizar de manera intensiva las tecnologías digitales, para la producción y acceso a datos y contenidos que generen valor público para los ciudadanos y personas en general.
5. **Arquitectura Digital.-** Es el conjunto de componentes, lineamientos y estándares, que desde una perspectiva integral de la organización permite alinear los sistemas de información, datos, seguridad e infraestructura tecnológica con la misión y objetivos estratégicos de la entidad, de tal manera que se promuevan la colaboración, interoperabilidad, escalabilidad, seguridad y el uso optimizado de las tecnologías digitales en un entorno de Gobierno Digital.
6. **Canal Digital.-** Es el medio de contacto digital que disponen las entidades de la Administración Pública a los ciudadanos y personas en general para facilitar el acceso a toda la información institucional y de trámites, realizar y hacer seguimiento a servicios digitales, entre otros. Este canal puede comprender páginas y sitios web, redes sociales, mensajería electrónica, aplicaciones móviles u otros.
7. **Ciudadano Digital.-** Es aquel que hace uso de las tecnologías digitales y ejerce sus deberes y derechos en un entorno digital seguro.
8. **Gobernanza Digital.-** Es el conjunto de procesos, estructuras, herramientas y normas que nos permiten dirigir, evaluar y supervisar el uso y adopción de las tecnologías digitales en la organización.

D. FINALIDAD

De acuerdo a lo señalado en la "Guía de Técnica Legislativa para elaboración de Proyectos Normativos de las Entidades del Poder Ejecutivo", la finalidad de la norma "***determina el porqué de la regulación que se propone. Expresa la voluntad del legislador u órgano decisor y sirve de guía para la interpretación de la norma***". Al respecto, y de acuerdo con el objeto de la propuesta legislativa, la finalidad debe ser consistente con las facultades delegadas en el ítem d.3) del literal d) del numeral 5 del artículo 2 de la Ley N° 30823. En ese sentido, la propuesta de finalidad para la presente propuesta legislativa comprende:

1. *Mejorar la prestación y acceso de servicios digitales en condiciones interoperables, seguras, disponibles, escalables, ágiles, accesibles, y que faciliten la transparencia para el ciudadano y personas en general.*
2. *Promover la colaboración entre las entidades de la Administración Pública, así como la participación de ciudadanos y otros interesados para el desarrollo del Gobierno Digital y sociedad del conocimiento.*

E. PRINCIPIOS RECTORES

Con miras a guiar la interpretación y aplicación de la propuesta normativa se han establecido una serie de principios guía, denominados "principios rectores", los cuales tienen como propósito fundamental que, a modo de columna vertebral, permitan brindar soporte y aporten un valor interpretativo a las disposiciones consignadas referida propuesta normativa, siendo básicamente su función orientar la "*...aplicación del Derecho mediante el señalamiento de unas guías o directrices*

29

ordenadoras que deben ser tomadas en consideración por el intérprete"[35]; los mismos que se sustentan en principios de la experiencia comparada establecidos en los documentos siguientes:

1. **Uruguay**[36].- Según indica la Agencia para el desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC) de Uruguay, el modelo de gobernanza en materia de gobierno digital contempla como aspecto fundamental el desarrollo de una educación básica que disponga de los recursos TIC necesarios para su alfabetización digital, así como su adecuada identificación digital; más aún URUGUAY (según la ONU se ubica en el 1er lugar en la región, 3ro en el mundo en participación electrónica y 14vo en servicios en línea) apuesta al desarrollo de un ***gobierno digital por defecto*** con metas claras plateadas en la Agenda Digital

2. **Colombia**[37].- En el documento "Revisión del Gobierno Digital en Colombia Hacia un Sector Público Impulsado por el ciudadano" la OCDE reitera que al momento de diseñar una Estrategia de Gobierno Digital resulta estratégico que se comprenda con claridad la importancia de ubicar la tecnología digital como núcleo de la modernización y reforma del sector público, en particular que se apliquen enfoques como "***digital por defecto***" o "***digital por diseño***" ***como principios que guíen la simplificación administrativa y racionalización; lo cual para el caso de Colombia no pareciera ser práctica actual.***

3. **Australia**[38], El Gobierno de Australia ha establecido la "Declaración digital por defecto" por la cual se reconoce que el uso y adopción de tecnologías digital es un aspecto crítico para la transformación digital y modernización de los servicios públicos, lo cual implica que los servicios estarán disponibles en línea y listo para usar en dispositivos móviles, diseñados de manera sencilla para uso de los ciudadanos.

4. **Reino Unido - United Kingdon**[39].- Las agencias de la administración pública entienden que los servicios públicos deben ser rediseñados de manera que se piensen en su prestación de manera digital primero o por defecto, lo cual conlleva a ahorros para la administración pública, nuevos enfoques de trabajo colaborativo.

5. **Perspectivas para Rusia - Gobierno Digital al 2020**[40]. Documento que establece cinco principios en materia de "Gobierno Digital".
   - *Digital por defecto, los servicios públicos deben ser diseñados y modelados para que sean digitales de extremo a extremo, ello con el fin de que puedan estar a disposición de los ciudadanos o administrados a través de canales digitales (dispositivos móviles, páginas web, etc.).*
   - *Agnóstico al dispositivo y centrado en los móviles, los servicios digitales deben ser accesibles a través de dispositivos móviles, teléfonos inteligentes, equipos portátiles u otros; esto sin lugar a duda representa una gran oportunidad para que las áreas de tecnologías de la información innoven los tradicionales procesos de negocio en las entidades pública y aprovechen las funcionalidades y capacidades de las tecnologías digitales.*
   - *Diseño de servicios centrados en el usuario, los servicios se diseñan buscando atender las demandas, problemas y necesidades de los ciudadanos o administrados, con ello aseguramos la generación de valor público.*
   - *Digital de extremo a extremo, repensar los procesos administrativos, portales institucionales, servicios digitales con el fin de que el flujo del trabajo sea completamente digital.*
   - *Gobierno como plataforma, promover que el gobierno proporcione información confiable, segura, precisa y disponible que pueda ser procesable por máquina (computadoras, aplicaciones, servicios digitales), con lo cual se fomenta además, la interoperabilidad, apertura de datos y la articulación con los infomediarios y usuarios en general.*

---

[35] En "*Comentario sistemático a la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos*", Gamero Casado – Valero Torrijos, Tercera Edición, noviembre 2010, p139.

[36] https://www.agesic.gub.uy/agesicweb/plantillas/imprimir.jsp?contentid=5416&channel=agesic&site=1

[37] https://books.google.com.pe/books?id=4jpbDwAAQBAJ&pg=PA39&lpg=PA39&dq=%22digital+por+defecto%22+-+ocde&source=bl&ots=8viggTN74Q&sig=awN76XLgrYahhola2899S-PgZG0&hl=es-419&sa=X&ved=2ahUKEwi4I_ip647dAhVIzlMKHTKDCAEQ6AEwBnoECAIQAQ#v=onepage&q=%22digital%20por%20defecto%22%20%20ocde&f=false

[38] https://digital.sa.gov.au/resources/topic/digital-government/digital-default-declaration

[39] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/296336/Government_Digital_Strategy_-_November_2012.pdf

[40] El documento puede ser consultado en: http://documents.worldbank.org/curated/en/562371467117654718/pdf/105318-WP-PUBLIC-Digital-Government-2020.pdf

30

6. **Recomendaciones de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) sobre la Gestión de Riesgos de Seguridad Digital para la Prosperidad Económica Social**[41]. Documento adoptado por el Grupo de Trabajo de la OCDE sobre Seguridad y Privacidad en la Economía Digital, el cual establece ocho (08) principios; cuatro (04) de los cuales son principios generales; mientras que los otros son principios operacionales.
   - *Conciencia, habilidades y empoderamiento.*
   - *Responsabilidad.*
   - *Derechos humanos y valores fundamentales.*
   - *Cooperación.*
   - *Evaluación de riesgos.*
   - *Medidas de Seguridad.*
   - *Innovación.*
   - *Preparación y continuidad.*

7. **Gobierno Digital - Construyendo una plataforma del siglo 21 para servir mejor a los americanos**[42]**.** Documento desarrollado por el gobierno de los Estados Unidos de América, en el cual se establecen cuatro principios:

   - *Centrado en la información, orienta la transición de una administración de "documentos" a la "gestión de datos y contenidos" con miras a que estos pueden clasificarse, eliminarse, analizarse y compartirse con los usuarios.*
   - *Plataforma compartida, se promueve el trabajo colaborativo, tanto dentro de las agencias como entre ellas, con la finalidad de reducir los costos, optimizar el uso de recursos, aplicar estándares consistentes y garantizar la coherencia en la forma en que creamos y entregamos la información.*
   - *Centrado en el cliente, se busca repensar el cómo creamos, administramos y presentamos los datos a través de sitios web, aplicaciones móviles, conjuntos de datos brutos y otros modos de entrega, y permite a los clientes configurar, compartir y consumir información cuando y como lo deseen.*
   - *Seguridad y privacidad, se asegura que esta innovación se realice de una manera que garantice la entrega y el uso seguros de los servicios digitales para proteger la información y la privacidad.*

8. **Carta Internacional de datos abiertos**[43]. Desarrollada por el Open Data Charter, establece una serie de principios por los cuales los datos deben ser:
   - *Abiertos por Defecto*
   - *Oportunos y Exhaustivos*
   - *Accesibles y Utilizables*
   - *Comparables e Interoperables*
   - *Para mejorar la Gobernanza y la Participación Ciudadana*
   - *Para el Desarrollo Incluyente y la Innovación*

9. **ISO/IEC 27000:2018 - Tecnología de la Información. Técnicas de Seguridad. Marco general y vocabulario del Sistema de Gestión de Seguridad de la Información.** Estándar internacional que establece un conjunto de principios fundamentales que contribuyen a una implementación exitosa de un Sistema de Gestión de seguridad de la Información, los cuales son:
   - *Conocimiento de la necesidad de seguridad de la información.*
   - *Asignación de responsabilidad para la seguridad de la información.*
   - *Incorporar el compromiso de gestión y los intereses de los interesados.*
   - *Mejorar los valores sociales.*
   - *Evaluaciones de riesgos que determinan controles apropiados para alcanzar niveles aceptables de riesgo.*
   - *La seguridad incorporada como un elemento esencial de las redes y sistemas de información.*
   - *Prevención activa y detección de incidentes de seguridad de la información.*
   - *Garantizar un enfoque integral para la gestión de la seguridad de la información.*
   - *Reevaluación continua de la seguridad de la información y realización de modificaciones según corresponda.*

---

[41] El documento puede ser consultado en: http://www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf
[42] El documento puede ser consultado en: https://obamawhitehouse.archives.gov/sites/default/files/omb/egov/digital-government/digital-government-strategy.pdf
[43] El documento puede ser consultado en: https://opendatacharter.net/principles-es/

31

10. **Identidad Digital - En el umbral de una revolución de la Identidad Digital (ENE2018)[44].** Documento técnico el cual refiere que la Identidad Digital habilita las transacciones en el mundo digital, ya sea con y entre personas, entidades públicas y empresas, en esa línea establece una serie de principios guía desde la perspectiva de la persona.

- ***Inclusión: cobertura universal y accesibilidad***
  - *Garantizar la cobertura universal para las personas desde el nacimiento hasta la muerte, sin discriminación.*
  - *Eliminar las barreras de acceso y uso, y las disparidades en la disponibilidad de información y tecnología.*
- ***Diseño: robusto, seguro, receptivo y sostenible***
  - *Establecer una identidad sólida, única, segura y precisa.*
  - *Crear una plataforma que sea interoperable y que responda a las necesidades de varios usuarios.*
  - *Usar estándares abiertos y garantizar la neutralidad de proveedores y tecnología.*
  - *Protección de la privacidad y el control del usuario a través del diseño del sistema.*
  - *Planificación de la sostenibilidad financiera y operativa sin comprometer accesibilidad.*
- ***Gobernanza: generar confianza mediante la protección de la privacidad y los derechos de los usuarios***
  - *Protección de la privacidad de los datos, la seguridad y los derechos de los usuarios a través de un marco legal y regulatorio integral.*
  - *Establecer mandatos institucionales claros y rendición de cuentas.*
  - *Hacer cumplir los marcos legales y de confianza a través de una supervisión y adjudicación independientes de las quejas.*

11. **Recomendaciones sobre Autenticación Electrónica y Lineamientos para la Autenticación Electrónica (2007)[45].** Refiere que la autenticación electrónica proporciona un nivel de seguridad en cuanto a si alguien o algo es quién o qué dice ser en un entorno digital; por lo tanto, la autenticación electrónica desempeña un papel clave en el establecimiento de relaciones de confianza para el comercio electrónico, el gobierno electrónico y muchas otras interacciones sociales; esta misma señala un conjunto de principios:

- *Enfoque de sistemas, el diseño, desarrollo e implementación de soluciones de autenticación debe verse como un proceso de desarrollo de sistemas coherente que involucra a todos los participantes relevantes. La selección de los niveles de seguridad y mecanismos para la autenticación debe ser basado en una evaluación de riesgos de los diversos componentes del sistema y del comportamiento del usuario.*
- *Proporcionalidad, el grado de responsabilidad y riesgo que asume cada participante en el proceso de autenticación debe ser proporcional al grado de conocimiento, control que razonablemente se pueda esperar que el participante tenga y al valor de la transacción o comunicación en sí.*
- *Seguridad y confianza, todos los participantes en un proceso de autenticación deben ser responsables y responsables de la seguridad, en proporción a sus roles en ese proceso.*
- *Roles y responsabilidades, todos los participantes deben actuar con prudencia y tomar medidas razonables para informarse sobre la naturaleza del proceso de autenticación, incluidos sus requisitos y limitaciones, para proteger la información asociada con el proceso y para gestionar los riesgos a los que están expuestos.*
- *Privacidad, cuando se diseñen e implementen procesos de autenticación deberían considerar cómo los sistemas pueden respetar adecuadamente la privacidad y la protección de datos en cada etapa del proceso.*
- *Gestión de riesgos, los riesgos asociados con los procesos de autenticación para las comunicaciones electrónicas deben identificarse, evaluarse y administrarse de manera razonable, justa y eficiente.*
- *Usabilidad, los procesos de autenticación deben ser efectivos, eficientes, confiables y fáciles de usar, y deben tener en cuenta los intereses y requisitos de las personas y las organizaciones.*
- *Estándares, el amplio despliegue de tecnologías de autenticación que pueden usarse en un contexto global depende en gran medida de las normas y estándares elaborados. Los organismos de estándares relevantes que emiten estándares importantes para la interoperabilidad global de los esquemas de autenticación incluyen: ISO, ITU, ETSI, CEN, ANSI, NIST, OASIS – Liberty Alliance, W3C, IETF and CC (Common Criteria) Multilateral Arrangement*

[44] El documento puede ser consultado en: http://www3.weforum.org/docs/White_Paper_Digital_Identity_Threshold_Digital_Identity_Revolution_report_2018.pdf
[45] El documento puede ser consultado en: http://www.oecd.org/sti/ieconomy/38921342.pdf

A partir de la revisión de los documentos señalados precedentemente, se han tomado como referencia los principios establecidos en cada uno de ellos para la formulación y definición de los principios rectores de la presente propuesta normativa:

- ***Principio de Especialidad,*** *según el cual la presente norma es aplicable a los servicios digitales prestados por las entidades de la Administración Pública en un entorno de Gobierno Digital, sin perjuicio de lo regulado para los procedimientos administrativos u otros que se rigen por su propia normatividad.*

- ***Principio de Equivalencia Funcional,*** *por el cual el ejercicio de la identidad digital para el uso y prestación de servicios digitales confiere y reconoce a las personas las mismas garantías que otorgan los modos tradicionales de relacionarse entre privados y/o en la relación con las entidades de la Administración Pública.*

- ***Principio de Privacidad desde el Diseño,*** *según el cual en el diseño y configuración de los servicios digitales se adoptan las medidas preventivas de tipo tecnológico, organizacional, humano y procedimental.*

- ***Principio de Igualdad de Responsabilidades,*** *las entidades de la Administración Pública responden por los actos realizados a través de canales digitales de la misma manera y con iguales responsabilidades que por los realizados a través de medios presenciales.*

- ***Principio de Usabilidad,*** *según el cual en el diseño y configuración de los servicios digitales se propenderá a que su uso resulte de fácil manejo para los ciudadanos y personas en general.*

- ***Principio de Cooperación Digital,*** *según el cual prima el intercambio de datos e información, la interoperabilidad de los sistemas y soluciones para la prestación conjunta de servicios digitales.*

- ***Principio Digital desde el Diseño,*** *según el cual los servicios, de manera preferente, progresiva y cuando corresponda, se diseñan y modelan para que sean digitales de principio a fin.*

- ***Principio de Proporcionalidad,*** *de modo que los requerimientos de seguridad y autenticación de los servicios digitales prestados por las entidades de la Administración Pública deben ser proporcionales al nivel de riesgo asumido en la prestación del mismo.*

- ***Principio de Abierto por Defecto****, de modo que los datos se encuentran abiertos y disponibles de manera inmediata, sin comprometer el derecho a la protección de los datos personales de los ciudadanos. Ante la duda corresponde a la Autoridad de Transparencia definirlo.*

- ***Principio de nivel de protección adecuado para los datos personales,*** *de modo que el tratamiento de los datos personales debe realizarse conforme a lo establecido en la Ley de Protección de Datos Personales y su Reglamento.*

Con los principios rectores finalizamos las disposiciones generales y damos inicio al otro gran componente de la propuesta legislativa en la cual se establecen marcos y garantías en materia de gobierno digital, que nos permita cumplir con lo dispuesto en el ítem d.3) del literal d) del numeral 5 del artículo 2 de la Ley N° 30823.

2.2 GOBIERNO DIGITAL

A. DE LA PRESIDENCIA DEL CONSEJO DE MINISTROS

Es oportuno mencionar que mediante la **Ley Nº 27658, Ley Marco de Modernización de la Gestión del Estado**, de 30ENE2002, se declara al Estado Peruano en proceso de modernización en sus

33

diferentes instancias, dependencias, entidades, organizaciones y procedimientos, teniendo como principal propósito el "*...mejorar la gestión pública y contribuir en el fortalecimiento de un Estado democrático, descentralizado y al servicio del ciudadano*"[46], y, en dicha línea, encierra como finalidad fundamental "*...la obtención de mayores niveles de eficiencia del aparato estatal, de manera que se logre una mejor atención a la ciudadanía, priorizando y optimizando el uso de los recursos públicos*"[47]. En consecuencia, interpretando de modo sistémico la legislación vigente y sus antecedentes, como alineando sus objetivos con la finalidad que persigue el proceso de Modernización del Estado, encontramos que lo establecido por la vigente *Política Nacional de Gobierno Electrónico 2013 – 2017*[48], en efecto, guarda estrecha relación con lo establecido por la *Política Nacional de Modernización de la Gestión Pública*[49] para cuya consecución tiene como uno de sus *ejes transversales* al *Gobierno Electrónico* (hoy denominado "*Gobierno Digital*").

Sin embargo, según estudio del año 2009 de la OCDE, se manifiesta que "*...durante muchos años el foco en la tecnología ha eclipsado la necesidad de cambios organizativos, estructurales y culturales en el sector público. Por lo tanto, los principales retos han quedado sin resolver (por ejemplo, las barreras legales y culturales para la colaboración y la cooperación dentro y entre niveles de gobierno como prerrequisitos para la construcción de servicios de gobierno electrónico llamativos, integrados y orientados al usuario). En la prestación de las funciones internas del gobierno y en hacer los procesos más eficientes y eficaces, a menudo se olvida los usuarios*"[50] (énfasis agregado), por tanto, se requiere fortalecer y desplegar acciones para el desarrollo del Gobierno Digital en nuestro país.

En esa línea, mediante la constitución del Sistema Nacional de Informática, a través del Decreto Legislativo N° 604; la creación de la Oficina de Gobierno Electrónico e Informática - ONGEI, mediante Decreto Supremo N° 063-2007-PCM, su reciente evolución a la categoría de Secretaría de Gobierno Digital - SEGDI, mediante Decreto Supremo N° 022-2017-PCM, la designación de esta como Líder Nacional de Gobierno Digital, mediante Decreto Supremo N° 033-2018-PCM, muestra por un lado, la clara visión del Gobierno por establecer los cimientos para la "**Transformación Digital**" del sector público, y por otro, los esfuerzos realizados en la transición del "**gobierno electrónico**[51]" al "**gobierno digital**[52]"

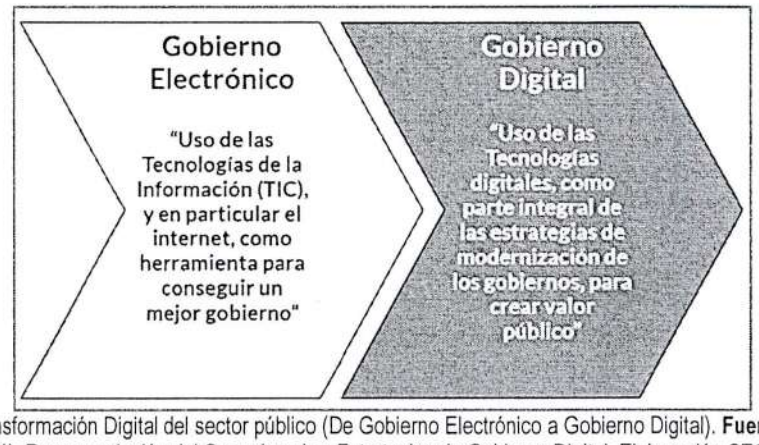

Gráfico 7.- Transformación Digital del sector público (De Gobierno Electrónico a Gobierno Digital). **Fuente:** Adaptado de OCDE (2014), Recomendación del Consejo sobre Estrategias de Gobierno Digital. Elaboración SEGDI julio 2018

En línea con lo anterior, mediante la Ley N° 30823, el Congreso de la República ha delegado en el Poder Ejecutivo la facultad de legislar para "***Establecer el marco normativo para promover el***

[46] Artículo 1° Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado.
[47] Artículo 4° Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado.
[48] Aprobada mediante el Decreto Supremo N° 081-2013-PCM (10JUL2013).
[49] Aprobada mediante el Decreto Supremo N° 004-2013-PCM (02ENE2013)
[50] En "Rethinking e-Government Services: user-centred approaches" (Repensando los servicios de Gobierno electrónico: enfoque centrado en el usuario), OECD e-Government Studies 2009, p13, traducción libre del texto en ingles "*For many years the focus on technology has overshadowed the need for organisational, structural, and cultural changes in the public sector. Key challenges (e.g. legal and cultural barriers for collaboration and co-operation within and across levels of government – the prerequisites for building attractive, integrated, user-focused e-government services) have hence been left unaddressed. In the process of rendering internal government functions and processes more efficient and effective, users were often forgotten*".
[51] Uso de las tecnologías de la información (TIC), y en particular el internet, como herramienta para conseguir un mejor gobierno.
[52] Uso de las tecnologías digitales, como parte integral de las estrategias de modernización de los gobiernos, para crear valor público.

34

despliegue transversal de las tecnologías digitales en las entidades del Estado; a fin de mejorar el alcance, condiciones, la prestación y el acceso de los ciudadanos a los servicios que presta el Estado"; lo cual requiere un profundo repensar sobre el rol estratégico de la Secretaría de Gobierno Digital - SEGDI y cómo ésta debe articular y apalancar el uso "transversal" de las tecnologías digitales en aras de un Estado más transparente, innovador, participativo, colaborativo e incluyente; entendiendo que la tecnología siempre es un medio y no el fin; el cual en esencia siempre ha de ser la persona.

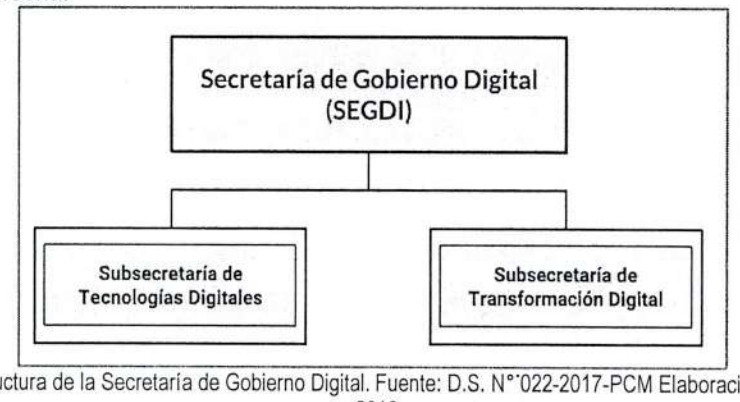

Gráfico 8.- Estructura de la Secretaría de Gobierno Digital. Fuente: D.S. N°022-2017-PCM Elaboración SEGDI agosto 2018

Ahora bien, lo anterior, ha sido ampliamente analizado por la OCDE en una serie de informes y estudios en varios países de nuestra región y el mundo, que hoy ostentan avances significativos en la materia, a saber:

1. Revisión del Gobierno Digital en Colombia - Hacia un sector público impulsado por el ciudadano (2018)[53].
2. Estudios de la OCDE sobre Gobernanza Pública Mejores servicios para un crecimiento inclusivo en la República Dominicana (2017)[54], en especial el capítulo 4 "Gobierno digital para mejores servicios y un crecimiento más incluyente en la República Dominicana".
3. Estudios de la OCDE sobre Reforma Regulatoria Política Regulatoria en Chile La Capacidad del Gobierno para Asegurar una Regulación de Alta Calidad (2016)[55], en especial el capítulo 11 "Gobierno digital y simplificación administrativa en Chile".
4. Comparación de estrategias de gobierno digital en países integrantes del Medio Oriente y Norte de África – MENA (2017)[56].
5. Gobierno Digital 2020 - Perspectivas para Rusia[57].
6. Experiencia del Reino Unido - Unidad de Servicio Digital del Gobierno.
7. Estudios de la OCDE sobre Gobernanza Pública "Perú Gobernanza Integrada para un crecimiento público inclusivo"[58].

Cada uno de los cuales plantea una serie de recomendaciones en materia de gobierno digital, que de manera resumida referimos a continuación:

1. **Revisión del Gobierno Digital en Colombia - Hacia un sector público impulsado por el ciudadano** (2018). El documento plantea recomendaciones para el Gobierno de Colombia, que se pueden organizar en tres ámbitos (gobernanza, datos y servicios digitales):

   Gobernanza

   a. *Considerar la creación de una agencia de digitalización a cargo de la coordinación de la implementación de la Política de Gobierno Digital a nivel nacional. Fortalecer la Dirección de Gobierno Digital en tanto que líder y supervisor y crear una alianza con el Centro de Innovación Pública Digital para promover los cambios organizacionales necesarios a lo largo y ancho del sector público.*

[53] OCDE (2018), Revisión del Gobierno Digital en Colombia: Hacia un Sector Público Impulsado por el Ciudadano, Éditions OCDE, Paris. http://dx.doi.org/10.1787/9789264292147-es

[54] OCDE (2017), Mejores servicios para un crecimiento inclusivo en la República Dominicana, Estudios de la OCDE sobre Gobernanza Pública, Éditions OCDE, Paris. http://dx.doi.org/10.1787/9789264277625-es

[55] OCDE (2016), Estudio de la OCDE sobre la Política Regulatoria en Chile: La Capacidad del Gobierno para Asegurar una Regulación de Alta Calidad, Ediciones OCDE, Paris. http://dx.doi.org/10.1787/9789264267060-es

[56] OECD (2017), Benchmarking Digital Government Strategies in MENA Countries, OECD Digital Government Studies, OECD Publishing, Paris. http://dx.doi.org/10.1787/9789264268012-en

[57] El documento puede ser consultado: http://documents.worldbank.org/curated/en/562371467117654718/Digital-government-2020-prospects-for-Russia

[58] El documento puede ser consultado en: https://bit.ly/2DHHlVJ

35

b. *Apoyar la definición de estrategias territoriales para el gobierno digital, como por ejemplo, la creación de grupos con representantes de los principales grupos de interés de cada región a fin de identificar las prioridades y necesidades específicas.*
c. *Desarrollar mecanismos que permitan asegurar el reconocimiento y adopción de la Política de Gobierno Digital a lo largo de todas las áreas y niveles (...).*
d. *Establecer mecanismos de coordinación estratégicos y operacionales dentro de los grupos de interés gubernamentales y no-gubernamentales para promover así la colaboración, la coordinación, la integración y el intercambio.*

Servicios Digitales

e. *Generar más oportunidades para que los ciudadanos y organizaciones de la sociedad civil puedan liderar procesos colaborativos a través del rediseño de plataformas centrales para la participación y oferta de servicios a fin de poder incorporar y reflejar sus necesidades.*

Datos

f. *Gestionar los datos del sector público de tal manera que se puedan utilizar tanto dentro como fuera del gobierno a fin de generar valor económico y mejorar el bienestar ciudadano. Esto implica la catalogación de los datos así como el desarrollo de directrices y pautas sobre el nivel de apertura e intercambio de datos, todo ello sustentado por una autoridad encargada de los datos y un marco regulatorio.*
g. *Ofrecer a los ciudadanos una mejor transparencia en lo relativo a datos personales almacenados y procesados por autoridades públicas y darles, asimismo, un papel más activo en la gestión de los mismos.*
h. *Alentar a los gerentes institucionales de datos a vincular los esfuerzos realizados en datos abiertos con la gestión y el intercambio global de datos a lo largo del sector público. Formar a los funcionarios públicos en el uso de datos para asegurar que existen las capacidades necesarias en el sector público.*
i. *Erigir la reutilización de los datos abiertos en el pilar principal de la política de datos abiertos e interactuar de manera activa con organizaciones de la sociedad civil, emprendedores, investigadores y periodistas para responder así a sus necesidades en términos de datos. Mejorar la medición del impacto de la colaboración digital entre el gobierno y los ciudadanos, y comunicar los resultados a fin de lograr un mayor compromiso ciudadano y fortalecer la confianza pública.*

2. **Estudios de la OCDE sobre Gobernanza Pública -Mejores servicios para un crecimiento inclusivo en la República Dominicana.** Establece una serie de recomendaciones que se pueden organizar en los tres ámbitos (gobernanza, datos y servicios digitales).

Gobernanza

a. *Fortalecer los marcos de gobernanza y coordinación para facilitar la puesta en marcha del gobierno digital, y asegurar la coherencia entre las distintas entidades haciendo lo siguiente:*
   i. *Aclarar la gobernanza de la política de gobierno digital. Esto debe tener por objeto aclarar las funciones y responsabilidades en el ámbito de la política de gobierno digital (...)*
   ii. *Aumentar la capacidad de la unidad coordinadora para hacer cumplir el marco normativo del gobierno digital. Esto debe basarse en una evaluación previa de la mezcla de instrumentos de política pública necesaria para producir el cambio, fortalecer la capacidad del órgano rector para hacer cumplir el marco normativo vigente para los proyectos de gobierno digital y TIC.*

Servicios digitales

b. *Asegurar que todos los factores clave del gobierno digital y la prestación de servicios digitales están en marcha, en particular haciendo lo siguiente:*
   i. *Ampliar el uso de la firma digital para permitir la prestación de servicios transaccionales por medios digitales*
   ii. *Crear una identidad digital común para los usuarios de servicios, que pueda usarse en todas las entidades de la administración pública.*
c. *Aumentar la accesibilidad y promover la creación participativa de servicios digitales para respaldar resultados más incluyentes haciendo lo siguiente:*
   i. *Crear ejercicios de capacitación y formación de capacidades para la prestación de servicios digitales.*
   ii. *Crear un enfoque de gobierno en conjunto de la prestación de servicios públicos, enmarcado en una estrategia de prestación de servicios.*

Datos

d. *Fortalecer la gobernanza de los datos para que la inteligencia del sector público promueva el crecimiento incluyente haciendo lo siguiente:*
   i. *Garantizar la interoperabilidad de los sistemas de información y datos del sector público.*

ii. *Crear una estrategia para fomentar una cultura motivada por los datos en el servicio público.*
iii. *Aclarar la gobernanza de los datos en el sector público. La gobernanza de los datos del sector público comprende una diversidad de funciones y responsabilidades, entre otras, la producción de estadísticas oficiales, la privacidad y seguridad de la información, la gestión de los sistemas informáticos, la gestión de los datos del sector público en sentido más amplio, y su inclusión en el ciclo de políticas públicas para garantizar sus efectos.*
iv. *Establecer en el gobierno central un equipo de gestión de datos que pueda hacer recomendaciones y tenga capacidades de análisis de datos masivos (big data analytics) para respaldar a las entidades públicas en la prestación de servicios digitales y en los esfuerzos de elaboración de políticas.*
v. *Elaborar una política integral de gestión de datos para el sector público dominicano.*

El referido estudio también cobra relevancia porque detalla un concepto muy importante "gobernanza pública" como "*el sistema de procesos y herramientas estratégicos, así como instituciones, reglas e interacciones para la elaboración eficaz de políticas públicas*", el que nos conlleva a inferir de manera "razonable" que cuando hablamos "De la materia de Gobierno Digital", tendremos que referirnos al conjunto de principios, políticas, normas, procedimientos, técnicas e instrumentos utilizados por las entidades de la Administración Pública en la gobernanza, gestión e implementación de tecnologías digitales para la digitalización de procesos, datos, contenidos y servicios públicos de valor para los ciudadanos.

3. **Estudios de la OCDE sobre Política Regulatoria en Chile, La Capacidad del Gobierno para Asegurar una Regulación de Alta Calidad**. El cual establece como recomendaciones:

a. *El gobierno de Chile debe tomar medidas para alinear mejor los programas de gobierno digital y de simplificación administrativa. Un mayor progreso en su evolución de gobierno electrónico a digital apoyaría la mejor alineación de estrategias fundamentales, alianzas sinérgicas entre los actores y una coordinación más afinada dentro y a través de todos los niveles del gobierno.*
   i. *Debe rediseñarse el marco de gobernanza del gobierno digital con el fin de mejorar la coordinación y la colaboración en el diseño e implementación de estrategias e iniciativas para el gobierno digital y la simplificación administrativa.*

b. *El gobierno de Chile debe aprovechar los instrumentos de política pública para alentar la alineación entre los objetivos de gobierno digital y los de simplificación administrativa.*
   i. *Se debe reflexionar detenidamente sobre los procesos empresariales dentro de la administración, empezando por dar prioridad al financiamiento de proyectos que apoyen la elaboración de normas para que las distintas plataformas de organismos/instituciones puedan vincularse y, por consiguiente, promuevan procesos administrativos más sencillos y una prestación de servicios integrada.*
   ii. *Se necesita utilizar el Programa de Mejoramiento de Gestión para incluir indicadores del desempeño en cuanto a los esfuerzos realizados en relación con la desmaterialización, la simplificación administrativa o la reducción de cargas mediante el proceso de digitalización de los servicios*

c. *Es importante fomentar una mejor integración entre los programas de simplificación administrativa y de gobierno digital mediante la implementación de las iniciativas y los proyectos individuales.*
   i. *Detectar la necesidad de fortalecer las capacidades para utilizar las TIC a fin de avanzar en la simplificación administrativa y no solo en meras habilidades tecnológicas.*
   ii. *Identificar a un defensor político en el uso de las TIC para apoyar el programa de simplificación y empezar a cambiar las conductas dentro de los organismos.*
   iii. *Crear redes de personas en el seno de los ministerios que apoyan el cambio*

d. *El gobierno de Chile debe involucrar a las partes interesadas y adoptar un enfoque impulsado por los usuarios para acercar la administración a ellos y recibir su retroalimentación, a fin de que mejore el impacto.*
   i. *Hay buenas prácticas respecto a los usuarios de los servicios de consulta que por el momento no se han optimizado, pero es necesario coordinar la recopilación de datos y la información. Además, un mayor intercambio de esos datos aunado a un uso más estratégico, sería también una buena oportunidad para involucrar mejor a los usuarios.*

37

4. **Marco de referencia y coordinación efectivos para el gobierno digital en países integrantes del Medio Oriente y Norte de África – MENA.**, Proporciona un análisis realizado por la OCDE sobre la visión general del estado actual del liderazgo y apoyo político en pro de los esfuerzos de digitalización en el sector público en las economías que conforman el MENA, para lo cual considera importante el establecimiento de marcos de gobernanza y coordinación efectivos, para lo cual recomienda:

   a. *Identificar los roles y responsabilidades en el marco de Gobernanza.*
   b. *Establecer una unidad en el centro de gobierno a cargo de coordinar la política en materia de gobierno digital a nivel nacional.*
   c. *Establecer mecanismos de coordinación dentro y entre los niveles de gobierno:*
      i. *Desde una perspectiva estratégica, dichos mecanismos deben apoyar la toma de decisiones estratégica a nivel político y de alta dirección.*
      ii. *Desde una perspectiva operativa: dichos mecanismos deben apoyar la implementación de los objetivos establecidos por la parte estratégica u órgano de gobierno.*

5. **Digital Government 2020 – Prospects for Russia.** Sostiene que, si bien cada país tiene y define un modelo de gobernanza para el desarrollo de Gobierno Electrónico, aquellos que han tenido un mayor éxito son aquellos que han tenido una mayor centralización y alto nivel de desempeño en sus actividades de gobernanza; lo cual no limita a aquellos países con un alto nivel de colaboración y articulación a avanzar en este tema.

6. **Reino Unido (United Kingdom).** Definió que para la gobernanza de la entrega de servicios digitales se constituya y ubique en el centro del gobierno, el Servicio Digital del Gobierno (Government Digital Service - GDS[59], en inglés) como unidad adscrita a la Oficina del Gabinete del Reino Unido cuya responsabilidad y misión es la de hacer que los servicios públicos sean más simples, más rápidos, claros y digitales de principio a fin. El GDS lidera la transformación digital con el enfoque de repensar los servicios gubernamentales para hacer que el gobierno sea más ágil y rentable, y para cambiar profundamente las interacciones entre la sociedad y el gobierno a través del adecuado entendimiento de las demandas y necesidades de los ciudadanos con miras a que se encuentren adecuadamente integradas la reforma del sector público y diseño de servicios digitales. No menos importante es la Red de Líderes Digitales y Tecnología creado por el Reino Unido a principios del 2012, con miras a promover una Agenda Digital en dicho Gobierno.

7. **Estudios de la OCDE sobre Gobernanza Pública "Perú Gobernanza Integrada para un crecimiento público inclusivo".** El cual establece como recomendaciones:

   a. ***Establecer el gobierno digital en el corazón de la reforma del sector público.***
      i. *Adoptar un concepto más amplio de gobierno digital que el simple gobierno electrónico e implementarlo reformulando la estrategia actual de gobierno electrónico para que integre el uso del gobierno digital como herramienta estratégica clave o facilitadora para el objetivo que persigue el gobierno en cuanto a su agenda general de reforma del sector público. Esto podría implicar la identificación de complementariedades y el aseguramiento y refuerzo mutuo entre la estrategia de gobierno digital y otras estrategias relevantes para el sector a nivel de gobierno central y local.*
   b. ***Asegurar el liderazgo para una gobernanza, gestión y planificación más sólidas***
      i. *Revisar el marco de gobernanza para asegurar un alto nivel de compromiso y apoyo a la estrategia digital. Para ello, el Estado podría crear un marco institucional estable con un alto cargo que se encargue formalmente de la dirección estratégica para el gobierno digital (como por ejemplo, un CIO), basándose en la Oficina Nacional de Gobierno Electrónico e Informática actual de la PCM, y establecer roles y responsabilidades claras para la coordinación del gobierno digital*
   c. ***Construir una estructura organizacional y financiera efectiva para que el gobierno digital difunda la estrategia digital dentro de los principales planes de modernización y desarrollo multianuales del gobierno, (...).***
   d. ***Lograr la digitalización usando un enfoque coherente e integrado a nivel de todo el país.***

[59] Se puede encontrar más detalle sobre el Servicio Digital del Gobierno en: https://www.gov.uk/government/organisations/government-digital-service

38

i. *Apoyar la implementación de cambios legales y hacer uso efectivo de los habililtadores horizontales clave (por ejemplo interoperabilidad) para poder asegurar un impacto real en la vida de los ciudadanos a través de una administración más integrada y accesible.*

e. ***Allanar el camino hacia un sector público movido por datos.***

i. *Desarrollar y asegurar el compromiso del liderazgo político para implementar una estrategia de cambio a una cultura movida por datos en el sector público y promover datos de gobierno abierto, basándose en el establecimiento reciente del portal de datos abiertos (desarrollado por la ONGEI en coordinación con la SGP).*

ii. *Desarrollar más el portal de datos del gobierno nacional con la idea de convertirlo en una plataforma abierta a los aportes de los ciudadanos y para facilitar el acceso, uso y reúso de los datos.*

iii. *Planificar y ejecutar un marco de datos abiertos, con orientación que permita la recopilación y publicación de datos de calidad en formatos abiertos.*

iv. *Permitir y promover la producción, uso y reúso de datos abiertos entre los actores gubernamentales y no gubernamentales, con el fin de maximizar la entrega de beneficios de buena gobernanza y perspectivas de valor económico y social.*

De lo anterior, claro está que cuando nos referimos a Gobierno Digital estamos hablando de un concepto que, como aspecto fundamental, busca evolucionar el ya referido gobierno electrónico, enfocándose en el "**valor público**" que pueden generar para los ciudadanos y la sociedad en general; lo cual se obtiene cuando el gobierno usa estratégicamente las tecnologías digitales en la prestación de servicios públicos; no obstante, como se vio en los párrafos anteriores, materializar la referida "evolución" implica establecer adecuados "marcos de articulación" en temas como: Tecnologías Digitales, Identidad digital, Servicios Digitales, Arquitectura Digital, Gobernanza de Datos, Interoperabilidad y Seguridad digital.

En línea con ello, es importante entonces definir con claridad ¿Qué es Gobierno Digital para el Estado Peruano?, ante lo cual la presente propuesta normativa señala que:

"Gobierno Digital es el uso estratégico de las tecnologías digitales y datos en la Administración Pública para la creación de valor público. Se sustenta en un ecosistema compuesto por actores del sector público, ciudadanos y otros interesados, quienes apoyan en la implementación de iniciativas y acciones de diseño, creación de servicios digitales y contenidos, asegurando el pleno respeto de los derechos de los ciudadanos y personas en general en el entorno digital."[60].

Y, tendrá como ámbitos de acción: tecnologías digitales, Identidad digital, Servicios Digitales, Datos, Interoperabilidad, Seguridad digital y Arquitectura Digital.

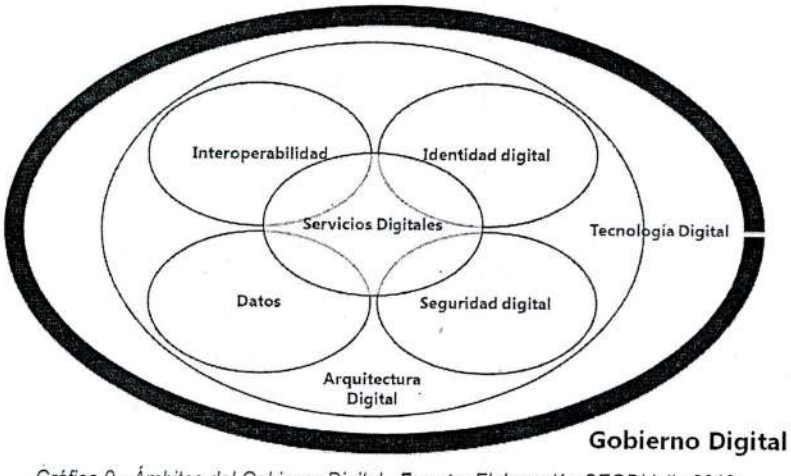

*Gráfico 9. -Ámbitos del Gobierno Digital - **Fuente:** Elaboración SEGDI julio 2018*

Entendiendo lo anterior, podemos decir que la materia de Gobierno Digital comprende el conjunto de principios, políticas, normas, procedimientos, técnicas e instrumentos utilizados por las entidades

[60] Adaptado en base a lo indicado por la OCDE en OCDE (2014), Recommendation of the Council on Digital Government Strategies, París, http://www.oecd.org/gov/digital-government/recommendation-on-digital-government-strategies.htm, Decreto Supremo N° 050-2018-PCM, que aprueba la definición de seguridad digital en el ámbito nacional.

39

de la Administración Pública en la gobernanza, gestión e implementación de tecnologías digitales para la digitalización de procesos, datos, contenidos y servicios públicos de valor para los ciudadanos. Constituyéndose la Presidencia del Consejo de Ministros como la autoridad técnico-normativa a nivel nacional en materia de gobierno digital y tecnologías digitales. Dicta las normas y establece los procedimientos en materia de gobierno digital y, es responsable de su operación y correcto funcionamiento.

Asimismo, los objetivos del Gobierno Digital son:

- *Normar las actividades en materia de gobernanza, gestión e implementación de tecnologías digitales, identidad digital, servicios digitales, arquitectura digital, interoperabilidad, seguridad digital y datos.*
- *Coordinar, integrar y promover la colaboración entre las entidades de la Administración Pública.*
- *Promover la investigación y desarrollo en la implementación de tecnologías digitales, identidad digital, servicios digitales, interoperabilidad, seguridad digital y datos.*
- *Promover y orientar la formación y capacitación en materia de Gobierno Digital y tecnologías digitales en todos los niveles de gobierno.*

Adicionalmente, se establece La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, es el ente rector en materia de gobierno digital que comprende tecnologías digitales, identidad digital, interoperabilidad, servicio digital, datos, seguridad digital y arquitectura digital. Dicta, establece, coordina, desarrolla e implementa la política de Gobierno Digital, sus normas y procedimientos, así como su operación y correcto funcionamiento, para lo cual se establece como sus funciones:

- *Programar, dirigir, coordinar, supervisar y evaluar la aplicación de la materia de Gobierno Digital.*
- *Elaborar y proponer normas reglamentarias y complementarias que regulan el Gobierno Digital.*
- *Emitir opinión vinculante sobre el alcance, interpretación e integración de normas que regulan la aplicación del Gobierno Digital de manera transversal en la Administración Pública.*
- *Emitir opinión previa a fin de validar técnicamente proyectos de tecnologías digitales de carácter transversal en materia de interoperabilidad, seguridad digital, identidad digital, datos, arquitectura digital o aquellos destinados a mejorar la prestación de servicios digitales.*
- *Elaborar lineamientos, procedimientos, metodologías, modelos, directivas u otros estándares de obligatorio cumplimiento para la implementación de las materias de gobierno digital.*
- *Brindar apoyo técnico a las entidades públicas en la gestión e implementación de tecnologías digitales.*
- *Definir los alcances del marco normativo de la materia de Gobierno Digital.*
- *Supervisar y fiscalizar, cuando corresponda, el cumplimiento del marco normativo de Gobierno Digital.*
- *Promover mecanismos que aseguren la identidad digital como pilar fundamental para la inclusión digital y la ciudadanía digital.*
- *Promover y gestionar la implementación de proyectos de implementación de tecnologías digitales u otros mecanismos destinados a mejorar la prestación de servicios digitales, en coordinación con las entidades públicas, según corresponda.*
- *Promover la digitalización de los procesos y servicios a partir del uso e implementación de tecnologías digitales.*
- *Realizar acciones de coordinación y articulación con representantes de la administración pública, ciudadanos u otros interesados con la finalidad de optimizar el uso de tecnologías digitales para el desarrollo del Gobierno Digital y tecnologías digitales.*

B. IDENTIDAD DIGITAL

El Perú reconoce el derecho a la identidad de la persona en el inciso 1), del Artículo 2º de la vigente Constitución Política del Perú de 1993[61], la misma que se acredita a través del Documento Nacional de Identidad, conforme al artículo 26 de la Ley N° 26497[62], Ley Orgánica del Registro Nacional de Identificación y Estado Civil - RENIEC.

---

[61] Artículo 2º.- Toda persona tiene derecho:
1. "A la vida, a su identidad, a su integridad moral, psíquica y física y a su libre desarrollo y bienestar... (...)".
[62] Ver: http://www.reniec.gob.pe/Transparencia/TransparenciaAdministrativaInfoGnral.jsp?idInformacion=41

Ahora bien, a nivel de las interacciones ciudadano y administración pública, sobre todo para la identificación de estos en "entornos presenciales", se ha sustentado en el empleo del **Documento Nacional de Identidad (DNI)**, permitiendo con ello establecer relaciones de **CONFIANZA**, dado que por un lado, la entidad se asegura que un ciudadano es quien dice ser; mientras que por el otro un ciudadano ejercer sus plenos derechos de acceso a información y servicios, lo cual es razón de ser de la entidad.

Dicho enfoque se ha mantenido durante mucho tiempo invariable e inmutable hasta el surgimiento del internet y las computadoras, las cuales han permitido digitalizar los procesos y servicios públicos, traduciéndose ello en relaciones ciudadano-administración pública de naturaleza no presencial, los llamados servicios digitales.

Según la OCDE, dicho cambio de paradigma hacia el enfoque ciudadano en la prestación de servicios digitales tiene un principal desafío para los Estados, entre otros, generar "*...confianza de los usuarios en sus gobiernos y la gestión de la información personal y sus **identidades digitales**: garantizando que la información, los datos y las **identidades digitales** se utilizan de modo confiable y respetando la integridad, la autenticidad y la privacidad como requisitos básicos para una mayor aceptación*"[63] (énfasis agregado).

En el mismo sentido, la Comisión Económica para América Latina y el Caribe (CEPAL)[64] manifiesta que el Gobierno Electrónico es un "*...concepto de gestión que fusiona la utilización intensiva de las TIC, con modalidades de gestión, planificación y administración, como una nueva forma de gobierno*" implicando un "*...**cambio de paradigma** en la gestión gubernamental*", siendo uno sus objetivos primordiales "*...acercar el Estado a los ciudadanos y de fomentar su participación en las decisiones públicas*"[65].

En dicha línea, la CEPAL indica que los gobiernos tienen la capacidad de establecer un "*...marco regulatorio que respalde y sustente el diseño, implementación, uso y evaluación de tecnologías de información y comunicación al interior del propio gobierno y en sus relaciones con otros actores sociales*"[66], de modo que permita incorporar "*...un **principio de confianza** para los procedimientos administrativos y la simplificación de la vida cotidiana de los ciudadanos, siendo ello un problema frecuente e influye en el interés de los funcionarios públicos que desempeñan funciones en los órganos administrativos del Estado*", para lo cual el "*...Gobierno digital es un instrumento clave para la implementación exitosa de los respectivos programas simplificación administrativa*" (énfasis agregado)[67].

En el caso de Internet y canales digitales, la adecuada identificación del ciudadano que interactúa con la administración, ***no se ajusta a las prácticas establecidas para los medios presenciales***, en razón que en tal medio se requiere formas adecuadamente seguras en cada caso, en base a los riesgos en la prestación de un determinado servicio digital, permita la función de "autenticar" (confirmar) la identidad, lo cual en la actualidad es inviable en razón que la forma por la cual se "identifican" las personas en dicho medio se basa en "identidades" creadas y controladas por ellas mismas, lo cual no permite brindar la certeza que logre, en efecto, asegurar que una persona determinada es quien dice ser.

---

[63] En "Rethinking e-Government Services: user-centred approaches" (Repensando los servicios de Gobierno electrónico: enfoque centrado en el usuario), op. cit, p15 y 16, traducción libre del texto en ingles "The paradigm shift towards citizen centricity has helped to focus governments attention on why user take-up of e-government services is lagging. To understand the reasons why users utilise e-government services, one must understand the different prerequisites for using those services. One way to get an overview of these different prerequisites is to look at the existing experiences in OECD countries whose e-government programmes have been peer reviewed by the OECD. The main challenges for increased user take-up among those countries are:... Trust by users in governments and their management of often sensitive personal information, data and digital identities: ensuring that information, data and digital identities are stored and used in a trusted and secured way respecting their integrity, authenticity, and privacy is among the basic prerequisite for higher uptake".

[64] CEPAL es un organismo dependiente de Naciones Unidas fundándose para contribuir al desarrollo económico de América Latina, coordinar las acciones encaminadas a su promoción y reforzar las relaciones económicas de los paises entre si y con las demás naciones del mundo. Posteriormente, amplió su labor a los paises del Caribe incorporándose el objetivo de promover el desarrollo social; Perú es miembro desde 25FEB1948 en: http://www.cepal.org/.

[65] El gobierno electrónico en la gestión pública", elaborado por el Instituto Latinoamericano y del Caribe de Planificación Económica y Social (ILPES), publicado por las Naciones Unidas en Abril 2011, p 5 y 8.

[66] "*El gobierno electrónico en la gestión pública*", op. cit., p20.

[67] En "Simplification of public administration through use of ICT and other tools" (La simplificación de la administración pública a través del uso de las TIC y otras herramientas), en estudio de Dra, Mirlinda Batalli, profesor de la Facultad de Derecho de la Universidad de Pristina, Kosovo, publicado por European Journal of ePractice Nº 12, March/April 2011 · ISSN: 1988-625X, p1, traducción libre del texto en inglés.

41

Sobre el particular, la doctrina empieza a orientarse por la necesidad de una ***identidad digital*** a ser empleada en medios "*no presenciales*" que posea como características que sea "*...segura y universal que todo el mundo reconozca*", para lo cual se requiere que como mínimo al menos "*...un tercero de confianza acredite estas identidades expidiendo un tipo de documento acreditativo digital que el usuario pueda presentar en Internet cuando sea necesario*"[68].

En consonancia con ello, es oportuno mencionar que en el marco de la XIII Conferencia Iberoamericana de Ministros de Administración Pública y Reforma del Estado[69], se emite el Consenso de Asunción a través del cual, entre otros, se declara continuar con la adopción de la Carta Iberoamericana de Gobierno Electrónico[70] siendo para ello necesario "*...incentivar la inclusión digital de todos los habitantes de la región*" para lo cual se debe "***...impulsar políticas de identificación electrónica social y convertir a la Sociedad de la Información y el Conocimiento en una oportunidad para todos y todas, especialmente de aquellos en peligro de quedar rezagados***" (énfasis agregado); para dicho fin, "*...los Ministros y las Ministras, los Jefes y Jefas de Delegación se comprometen a impulsar e implantar estrategias de cambio necesarias para hacer posible la transformación de los Estados iberoamericanos para el desarrollo, como condición indispensable para promover el desarrollo sostenible, integral, inclusivo y armónico de las sociedades iberoamericanas*"[71].

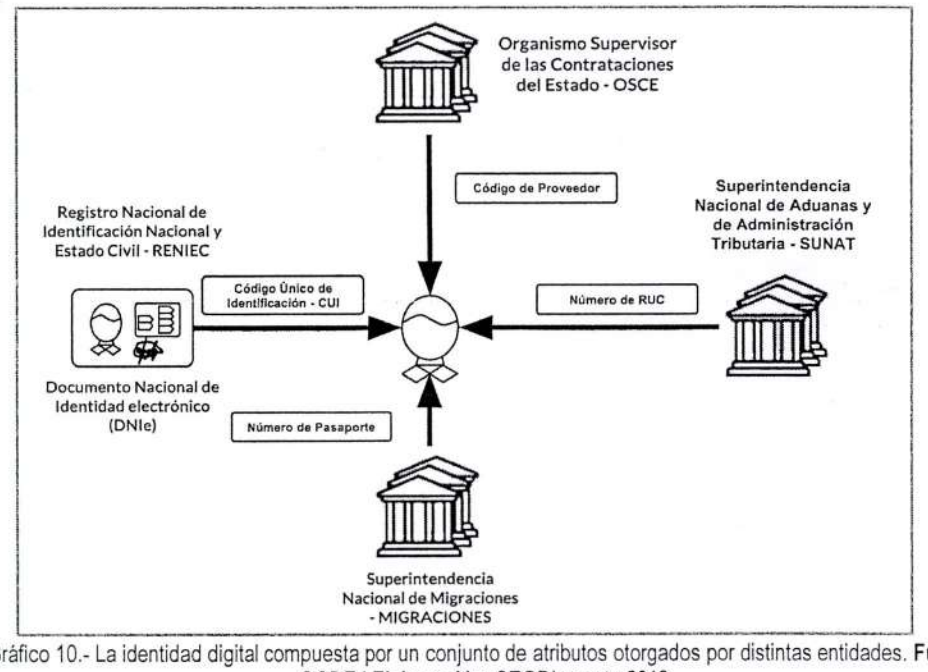

Gráfico 10.- La identidad digital compuesta por un conjunto de atributos otorgados por distintas entidades. **Fuente**: OCDE | **Elaboración**: SEGDI agosto 2018

➢ **Gestión de la Identidad Digital para las Personas Naturales**

En línea con lo anterior, en la presente propuesta legislativa en materia de "Identidad Digital", se toma como referencia el Documento Técnico N° 186[72] OCDE "Gestión de la Identidad Digital para personas naturales - Facilitar la innovación y la confianza en la economía de internet - Orientación para los formuladores de Políticas Públicas"; el mismo que tiene como sustento el resultado del análisis llevado a cabo por el Grupo de Trabajo sobre Seguridad de la Información y Privacidad del referido organismo internacional (WPISP) durante cuatro años sobre estrategias

[68] "El Manual Práctico de Supervivencia en la Administración Electrónic@"; LÓPEZ TALLÓN, Alberto López; Primera Edición – Septiembre 2010 (edición revisada), en Blog del autor del libro: http://www.microlopez.org.

[69] Realizada del 30 de Junio y 1° de julio de 2011, organizada por el Centro Latinoamericano de Administración para el Desarrollo (CLAD)

[70] Aprobada por la IX Conferencia Iberoamericana de Ministros de Administración Pública y Reforma del Estado, llevada a cabo entre el 31 de mayo y 1° de junio de 2007, documento adoptado por la XVII Cumbre Iberoamericana de Jefes de Estado y de Gobierno con fecha 10 de noviembre de 2007, eventos organizados por el Centro Latinoamericano de Administración para el Desarrollo (CLAD), el texto integro del citado documento puede ser consultado a través del enlace: http://www.clad.org/documentos/declaraciones/cartagobelec.pdf.

[71] "Consenso de Asunción", CLAD 2011, p.3; el texto integro del citado documento puede ser consultado a través del enlace: http://www.clad.org/documentos/declaraciones/consenso-de-asuncion

[72] OECD (2011), "Digital Identity Management for Natural Persons: Enabling Innovation and Trust in the Internet Economy - Guidance for Government Policy Makers", OECD Digital Economy Papers, No. 186, OECD Publishing, Paris. http://dx.doi.org/10.1787/5kg1zqsm3pns-en

nacionales para la gestión de identidad digital en los países de la OCDE. El referido estudio se centra, exclusivamente, en la gestión de la identidad de una persona natural ("Persona") que interactúa con los sistemas de información (Servicios Digital) de organizaciones públicas o privadas (denominados, en el documento técnico, como "Proveedores de Servicios").

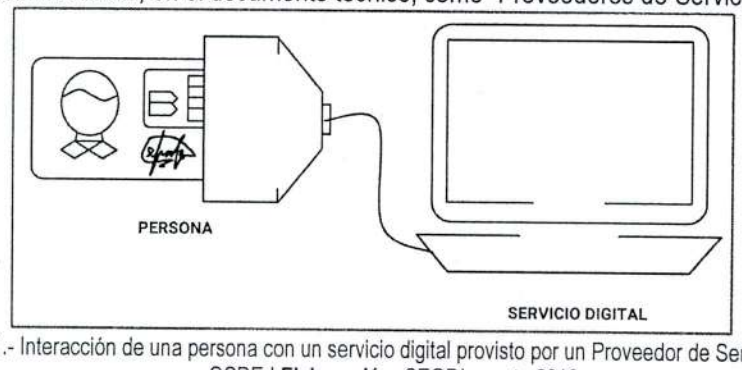

Gráfico 11.- Interacción de una persona con un servicio digital provisto por un Proveedor de Servicios. **Fuente**: OCDE | **Elaboración:** SEGDI agosto 2018

El documento técnico señala que es sumamente importante entender que la gestión de la Identidad Digital tiene un "**Ciclo de Vida**", la cual comprende los siguientes procesos básicos:

1. ***Registro o Inscripción:*** *Para que una "Persona" pueda interactuar con un "Sistema de Información" primero debe registrarse, segundo, las "condiciones" relacionadas con su identidad o atributos de identidad deben ser verificadas para poder proporcionar un conjunto de credenciales.*
2. ***Autorización****: Se asignan a la "Persona" los permisos y privilegios apropiados para acceder a los recursos de la organización.*
3. ***Autenticación:*** *Cuando la "Persona" requiere un recurso, inicia sesión en el sistema con las credenciales proporcionadas durante el proceso de Registro o Inscripción.*
4. ***Control de Accesos:*** *El resultado del proceso de autenticación se utiliza en el proceso de Control de Acceso, mediante el cual el sistema verifica que el individuo tenga la autorización apropiada para acceder al recurso.*
5. ***Revocación:*** *Cuando la "Persona" ya no está asociada con el sistema debe producirse un proceso por el cual se rescinden sus credenciales.*

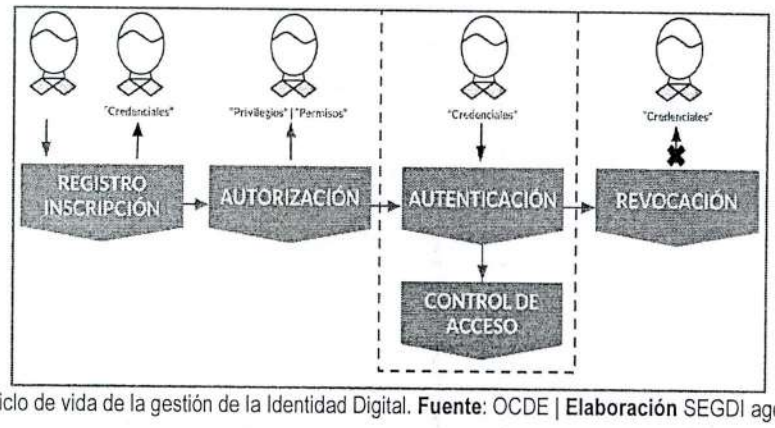

Gráfico 12.- Ciclo de vida de la gestión de la Identidad Digital. **Fuente**: OCDE | **Elaboración** SEGDI agosto 2018

Claro está que dichos procesos ya existen, se ejecutan y se realizan en nuestro mundo físico, presencial o no digital; sin embargo, no nos damos cuenta de ello, en la mayoría de los casos, por ejemplo:

a. Cuando queremos realizar un préstamo o aperturar una cuenta bancaria en una entidad financiera nos piden el DNI.
b. Cuando queremos tramitar un certificado, licencia, entre otros en las mesas de partes de entidades públicas, muchas veces nos piden el DNI.
c. Cuando queremos ingresar a una entidad pública, nos solicitan nuestro DNI o FOTOCHECK.
d. Cuando votamos en alguna elección, nos solicitan nuestro DNI.

43

La gestión de identidades en el mundo físico, no presencial, nos ayuda a abordar los riesgos asociados con las interacciones humanas y aumenta la **CONFIANZA** entre las partes que interactúan. De similar manera en el entorno digital, en la interacción Persona – Sistemas de Información o en la interacción Persona - Servicio Digital necesitamos generar **CONFIANZA** mediante mecanismos válidos, que nos permitan gestionar adecuadamente el vínculo entre una "Persona" y una "Identidad digital", lo cual dotaría de mayor certeza a las interacciones que en este ámbito se desarrollen. Sin embargo, es necesario tener en cuenta que dichos mecanismos deben proteger la privacidad de las personas en el entorno digital. Implementar lo anterior implica que los gobiernos tienen por lo menos tres desafíos identificados:

a) Promover una oferta adecuada de organizaciones que presten servicios de identidad digital, los cuales en la mayoría de casos serán responsables de: registrar o inscribir a la persona, establecer su identidad (cara-cara | *face to face*) y entregar las credenciales; entendiendo que estas implementaran prácticas mucho más seguras y fiables que las que tienen las propias entidades públicas.

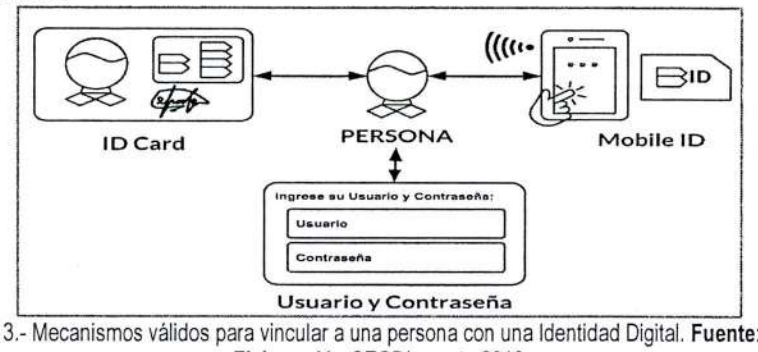

Gráfico 13.- Mecanismos válidos para vincular a una persona con una Identidad Digital. **Fuente**: OCDE | **Elaboración** SEGDI agosto 2018

b) Muchas credenciales, conforme las personas se registran a servicios digitales, se vuelve un poco más complejo gestionar cada una de las credenciales otorgadas.

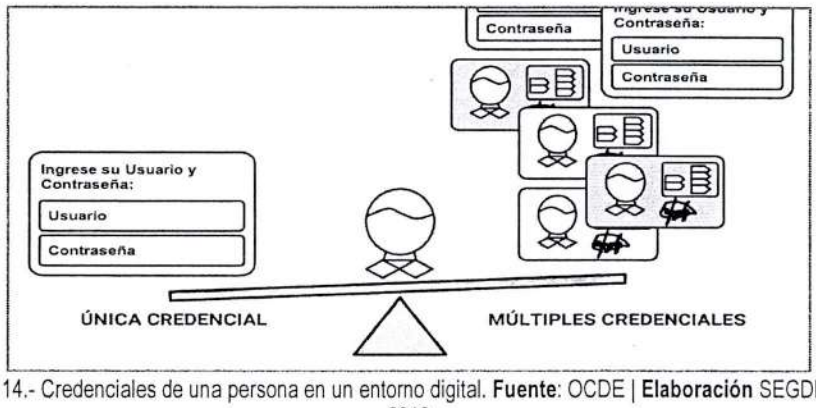

Gráfico 14.- Credenciales de una persona en un entorno digital. **Fuente**: OCDE | **Elaboración** SEGDI agosto 2018

c) Romper con el círculo nada virtuoso, por el cual, por un lado, entidades públicas o del sector privado no prestan servicios hasta que un gran porcentaje de personas dispongan de credenciales de autenticación sólidas; y por otro lado, las personas esperan una oferta considerable de servicios que requieran un mecanismo de autenticación fuerte.

En atención a los desafíos indicados anteriormente, el estudio de la OCDE refiere que los gobiernos deberían:

1. *Adoptar una estrategia nacional para la gestión de identidad digital, la misma que promovería la migración de servicios públicos y privados de un mundo, tradicionalmente, presencial a uno digital de principio a fin ("No presencial").*
2. *Definir una política de credenciales digitales adecuadamente balanceada, la estrategia anteriormente indicada debe tener como uno de sus objetivos reducir o limitar el número de credenciales digitales que los individuos deben usar en los servicios del sector público y privado.*

44

3. *Balancear el número de credenciales digitales.*
4. *Los niveles de seguridad de la identidad digital deben ser acordes con el nivel de riesgo del servicio o transacción desarrollada.*
5. *Los gobiernos deberían trabajar juntos para permitir la gestión de identidad digital transfronteriza, más aún cuando se quiere promover el desarrollo del gobierno electrónico y comercio electrónico entre las economías.*

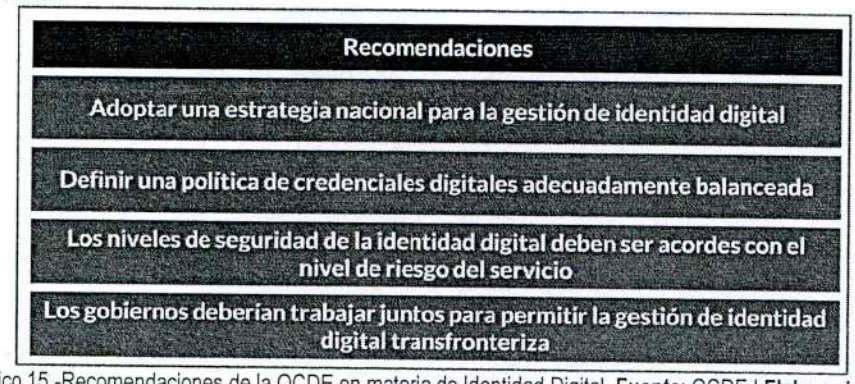

Gráfico 15.-Recomendaciones de la OCDE en materia de Identidad Digital. **Fuente**: OCDE | **Elaboración** SEGDI agosto 2018

Conforme lo anterior, la presente propuesta normativa entiende como **Identidad Digital** a aquel conjunto de atributos que individualiza y permite distinguir a una persona en entornos digitales. En el Estado los atributos de la identidad digital son otorgados por distintas entidades de la Administración Pública que, en su conjunto, caracterizan al individuo.

Más aún para su adecuado desarrollo y gestión a nivel nacional y, sobre todo, con miras a promover el despliegue transversal de las ***tecnologías digitales en la administración pública***, se precisa establecer un ***Marco de identidad digital a nivel del Estado Peruano***, el cual comprenda lineamientos, especificaciones, guías, directivas, estándares e infraestructura de tecnologías digitales, que permiten de manera efectiva la identificación y autenticación de los ciudadanos y personas en general cuando acceden a los servicios digitales.

Ahora bien, conforme las ***buenas prácticas y estándares internacionales revisados, el referido marco deberá comprender*** como aspectos fundamentales para su adecuada implementación la gestión de *Credenciales de Identidad Digital*, la misma que la presente propuesta define como: ***"Aquella representación de una identidad digital que comprende los atributos inherentes a la persona definidos en el Marco de Identidad Digital del Estado Peruano, a fin de facilitar la autenticación digital".***

Por otro lado, es de suma importancia la especificación de procedimientos de identificación digital y su correspondiente materialización en mecanismos de autenticación digital, los cuales para la presente norma:

- ***Identificación Digital.-*** *La identificación digital es el procedimiento de reconocimiento de una persona como distinta de otras, en el entorno digital. Las entidades de la Administración Pública deben establecer los procedimientos para identificar a las personas que accedan a los servicios digitales.*
- ***Autenticación Digital.-*** *La autenticación digital es el procedimiento de verificación de la identidad digital de una persona, mediante el cual se puede afirmar que es quien dice ser. Para el acceso a un servicio digital las entidades de la Administración Pública deben adoptar los mecanismos o procedimientos de autenticación digital, considerando los niveles de seguridad a establecerse en la norma reglamentaria.*

Cabe recordar que a la fecha los ciudadanos peruanos disponemos, a través del Documento Nacional de Identidad electrónico (DNIe), emitido por el RENIEC, una credencial digital, que contiene atributos básicos de su identidad digital, la misma que en materia de esta propuesta normativa se constituirá un tipo de credencial oficial de **Identidad Digital Nacional** del Estado Peruano.

45

En esa línea, y acorde a las recomendaciones de la OCDE, el DNIe se constituye como uno de los medios por el cual la propuesta normativa prevé que se accedan, desarrollen e implementen servicios digitales y con el que podamos materializar la transición de un *"...paradigma centrado en el gobierno a un paradigma centrado en el ciudadano, poniendo más atención en el contexto (por ejemplo, los factores sociales, organizacionales e institucionales)"*[73] como lo propugna el referido organismo internacional.

De lo anterior, y conforme los estándares internacionales[74], debemos dejar en claro que la **Identidad Digital** está conformada por un conjunto de atributos que representan características o propiedades de una persona para describirla, por lo que la gestión de las identidades digitales debe encontrarse a cargo de "**entidades**" que puedan pronunciarse o efectuar afirmaciones verificables sobre la validez y/o corrección de uno o más valores de tales atributos. En suma, **cualquier entidad de la Administración Pública puede hacer uso de mecanismos existentes para la autenticación de las personas en entornos digitales dentro de un contexto determinado, conforme a los lineamientos y plazos a establecerse en el reglamento de la propuesta legislativa.**

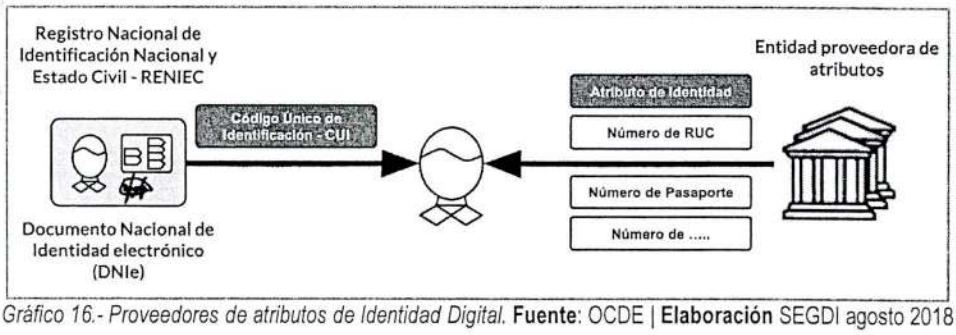

Gráfico 16.- Proveedores de atributos de Identidad Digital. **Fuente**: OCDE | **Elaboración** SEGDI agosto 2018

Bajo este contexto, el RENIEC, ente constitucionalmente autónomo a cargo del Registro Único de Identificación de las Personas Naturales (RUIPN), y en el marco de sus competencias y funciones con cargo a su presupuesto, podrá desarrollar y proveer diferentes mecanismos de identificación basados en credenciales de identidad digital conforme a las necesidades que se presenten o a la evolución tecnológica en las que se incorporen los valores de los atributos que gestiona, incluso contemplándose otros nuevos atributos que las circunstancias así lo justifiquen. Cabe señalar que las facultades del RENIEC, no excluyen el que otras entidades puedan gestionar identidades digitales, en particular con atributos que sean de su competencia, respetando los valores de los atributos inherentes a la persona que componen la Identidad Digital Nacional.

Para ello, haciendo un análisis de legislación comparada, las nuevas tecnologías brindan a muchos países la oportunidad de superar los sistemas basados en mecanismos tradicionales y establecer sólidas infraestructuras. Como resultado, los países adoptan cada vez más programas de identificación digital (ID) a nivel nacional y los aprovechan en otros sectores.

Partiendo de los criterios precedentes y haciendo un análisis económico del derecho, la presente propuesta legislativa no pretende cerrar el mercado ni que los disruptores tecnológicos lo vean como una zona sobre-regulada. Por el contrario, se busca una sólida economía de pares desde la gestión de sistemas de identidad digital que garanticen seguridad, confidencialidad, privacidad y grados de responsabilidad cada vez que las personas sean tratadas en entornos digitales. Con dicho cambio de enfoque basado en la **Identidad Digital** se facilitará la implementación de servicios digitales de principio a fin.

Es fundamental señalar que los mecanismos contenidos en el DNIe que posibilitan la manifestación de voluntad, sólo otorgan garantía sobre la identificación de la persona natural, más no el cargo, rol, atribuciones o facultades que ostenta el funcionario o servidor de una entidad de la Administración

[73] En "Rethinking e-Government Services: user-centred approaches" (Repensando los servicios de Gobierno electrónico: con enfoque centrado en el usuario), p14.
[74] Estándar ISO / IEC 24760-1: 2011. Tecnología de la información - Técnicas de seguridad - Un marco para la gestión de identidad - Parte 1: Terminología y conceptos. Este estándar fue revisado y confirmado por última vez en 2017. Por lo tanto, esta versión se mantiene actualizada, el mismo que puede ser consultado en: https://www.iso.org/obp/ui/#iso:std:iso-iec:24760:-1:ed-1:v1:en.

Pública. Dicho funcionario o servidor público es el responsable de gestionar en su entidad las autorizaciones de acceso y asignación de roles, atribuciones o facultades para hacer uso del indicado DNIe en los sistemas de información que hagan uso del mismo; para efectos de regulación del uso de las credenciales en el ejercicio de cualquier rol o función, esta debe ser normada por cada entidad de la entidad de Administración Pública a fin de garantizar que corresponda a un determinado perfil.

Cabe indicar que el RENIEC en el ámbito de sus funciones y competencias emitirá las normas que resulten pertinentes para el registro y acreditación de la identidad digital nacional y otorgamiento del domicilio digital nacional. Más aun, el RENIEC puede desarrollar diferentes mecanismos de identificación determinando sus características técnicas, contenidos, procedimientos de emisión, de revocación, entre otros.

Al respecto, y sobre el señalado "domicilio digital" es de indicar que en nuestro ordenamiento jurídico puede hablarse de diversas clases de domicilio. Entre ellos, y en cuanto interesa a los fines de esta propuesta legislativa, hallamos al domicilio real, al legal y al procesal. Sin ánimo de brindar una acabada definición, podemos señalar que tradicionalmente se ha entendido al domicilio como un lugar dentro del ámbito geográfico territorial, que la ley atribuye como asiento jurídico de la persona para la producción de determinados efectos jurídicos.

Esa imposición legal es necesaria a fin de que las personas puedan ser localizadas para el cumplimiento de sus obligaciones y el ejercicio de sus derechos tratados preliminarmente en el presente documento, por lo que puede afirmarse que toda persona tiene el deber y el derecho de tener un domicilio, para así garantizar el derecho a la información y cualquier decisión que el Estado prevea.

Para la aplicación de tecnologías al sistema jurídico tradicionalista se debe extraer la concepción de territorialidad para efectos de notificación y darse preponderancia a otros derechos conexos de mayor jerarquía; como el de ejercer el derecho de defensa, materializado al estar informado, más aún cuando está de por medio la cuestión del apercibimiento; la posibilidad de caducidad que nos ofrece el tiempo, hace inevitablemente caducar este derecho.

Así, el "domicilio digital nacional" sustrae el elemento 'domicilio' tradicional (conceptual) de la territorialidad y de la norma sustantiva (electoral, tributaria, etc.), y aquí es que yace la supresión de la concepción del domicilio tradicionalista para dejar sentada estrictamente la interpretación material a una interpretación subjetiva de derecho.

Ahora bien, la implementación de las nuevas tecnologías en el ámbito tradicionalista dio lugar a la irrupción y este tipo de domicilio (Domicilio Digital Nacional), el que puede definirse en el ámbito de la justicia innovadora como lugar-espacio que el Registro Nacional de Identificación y Estado Civil - RENIEC prevé, desde el cual sus titulares se encuentran habilitados para hacer verificaciones sobre la certeza del acto de comunicaciones o notificaciones electrónicas.

De esta manera, al tradicional concepto de domicilio se le incorpora el factor informático: el "domicilio digital nacional" es un lugar-espacio que la parte involucrada en un proceso o procedimiento constituye a fin de recibir las comunicaciones o notificaciones electrónicas que allí se cursen, pero con la característica de que es intangible y no físico.

En suma, el domicilio digital tiene validez y eficacia jurídica, produciendo los mismos efectos que el domicilio habitual constituido, siendo legales y vinculantes todas las notificaciones y comunicaciones que en el mismo se practiquen.

Finalmente, conforme la entidad pública haga uso de "Identidad Digital" de las personas, estas deberán implementar progresivamente, en función a sus recursos y capacidades, espacios o centros de acceso público, previstos en la Ley de Promoción de Banda Ancha y Construcción de la Red

47

Dorsal Nacional de Fibra Óptica, con miras a fortalecer capacidades y facilitar el proceso de inclusión digital de los ciudadanos y personas en general el acceso a los servicios digitales, con especial atención en los niños, adultos mayores y personas con discapacidad, contribuyendo a la Inclusión Digital, la cual se entiende en la presente norma como ***"el acceso y uso de los servicios digitales por parte de los ciudadanos a través de su Identidad Digital, promoviendo la ciudadanía digital. Para tal fin las entidades de la Administración Pública adoptan las disposiciones que emite el ente rector para la prestación de dichos servicios".***

Gráfico 17.- Propuesta de Modelo de Centro de Acceso Público. **Fuente: SEGDI | Elaboración:** SEGDI agosto 2018

En línea con lo anterior, la presente propuesta establece que dichas entidades comuniquen a la Secretaría de Gobierno Digital dicha implementación para llevar un Registro de Centros de Acceso Público a nivel nacional. Más aun, para no generar confusión sobre los centros de acceso ciudadano establecido en el Reglamento de la Ley de Firmas y Certificados Digitales, se entenderá a partir de la presente al Centro de Acceso Público a los Centros de Acceso Ciudadano"

C. PRESTACIÓN DE SERVICIOS DIGITALES

En el ámbito de la Administración Pública, si bien los actos como los procedimientos administrativos, y servicios públicos prestados a los ciudadanos y personas en general cuentan con el marco legal del actual Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General – LPAG, dicha regulación precisa de un marco normativo complementario que acompañe la prestación de servicios digitales y brinde confianza en el uso y despliegue transversal de las tecnologías digitales en la Administración Pública que, a su vez, facilite la evolución hacia un "Gobierno Digital" en el Perú, ello sin perjuicio de lo regulado para los procedimientos administrativos previstos en el señado TUO de la Ley 27444 u otros que se rigen por su propia normatividad.

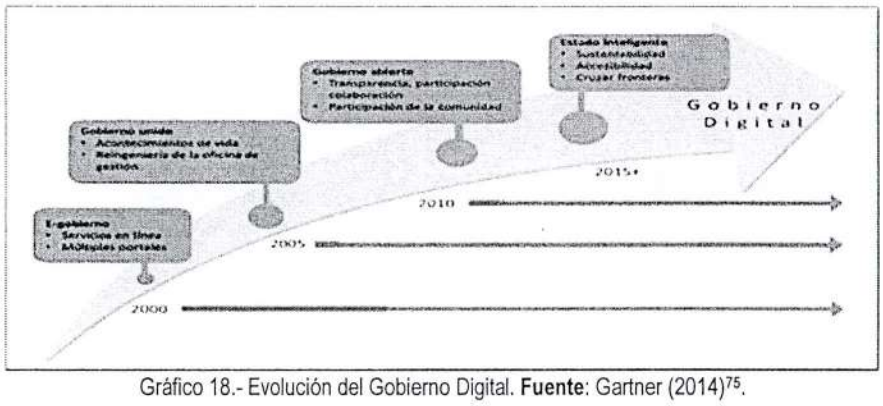

Gráfico 18.- Evolución del Gobierno Digital. **Fuente**: Gartner (2014)[75].

[75] Rick Howard. (2014), Agenda Overview for Government, 2014. © 2014 Gartner, Inc. and/or its affiliates. All rights reserved.

48

En efecto, en su momento y por la época en la cual se desarrolló la LPAG (año 2001) ésta reguló muy básicamente algunos aspectos que en aquel momento eran adoptados de manera muy general como la "notificación por medios electrónicos" así como el empleo, opcional, de "microformas" para los expedientes administrativos; al respecto, el vigente artículo 30 del actual TUO de la LPAG regula la posibilidad de contar con procedimientos electrónicos el cual se encuentra sujeto a la aprobación de lineamientos por parte de la Presidencia del Consejo de Ministros respecto de las condiciones y uso de las tecnologías y medios electrónicos en los procedimientos administrativos al que se refiere el numeral 30.4 del TUO de la Ley 27444, empero incluso con la aprobación de los mismos y, en el estado actual del avance de la tecnología, de emitirse "lineamientos" resultan insuficientes y, sobre todo, no tendrán el nivel normativo, para lograr una plena digitalización de la Administración Pública y, menos aún, cumplir con la Estrategia de Modernización del Estado y Política de Gobierno Electrónico que han sido emitidas en los últimos años[76].

Así las cosas, según el documento "*El fin del Trámite Eterno: Ciudadanos, Burocracia y Gobierno Digital*[77]", elaborado por el Banco Interamericano de Desarrollo (BID) se sabe que a nivel de América Latina, el 89% de trámites[78] se realiza de manera presencial, más aún, refiere que "*Los trámites no solo son difíciles de realizar, pues demandan mucho tiempo y varias interacciones para hacerlos, sino que son muchos, lo cual genera pérdidas para los ciudadanos y las empresas. Por otra parte, pueden ser un foco de corrupción, minando la confianza de los ciudadanos en el Estado. Además, los problemas con los trámites tienen un carácter regresivo, al afectar más a las personas de menores ingresos. En resumen, ante trámites difíciles, los ciudadanos tienen tres opciones: aguantarse, pagar un soborno, o tirar la toalla. Por último, los trámites difíciles le generan costos al gobierno.*"
Asimismo, el referido documento del BID señala que en América Latina los trámites son:

- **Difíciles de hacer y generan costos de transacción.** Según los datos de Latinobarómetro (2017) en promedio los ciudadanos gastan 5.4 horas[79] en realizar un trámite; y de manera detallada el 59% requiere más de 2 horas, el 28% más de 5 horas, y el 13% más de 10 horas[80]. Algunos factores que influyen para ellos son los desplazamientos que realizan los ciudadanos para llegar a la entidad a realizar el trámite, las múltiples veces que se tiene que ir a la entidad para completar el trámite, entre otros[81]. En el Perú para completar un trámite se requiere 8.6 horas, solo el 29% de ciudadanos completa su trámite en una sola visita, y solo el 17% de trámites son catalogados como fáciles, es decir, se realizan en una sola interacción y en menos de 02 horas"[82].

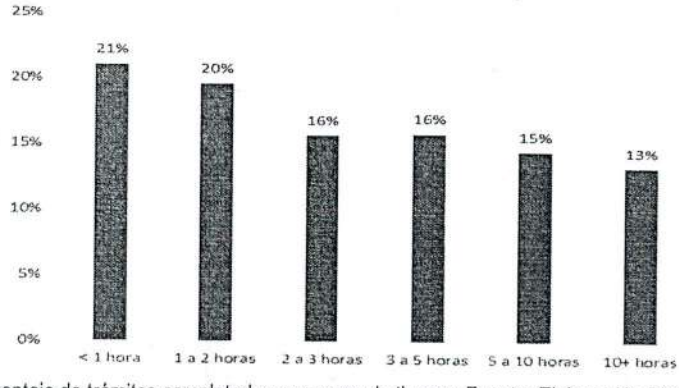

Gráfico 19.- Porcentaje de trámites completados por rango de tiempo. Fuente: Elaboración BID en base a los datos de Latinobarómetro (2017)

[76] Las cuales no pudieron cumplirse integralmente al no contar con un marco legal ordenado, sino que al contrario encontramos diversidad de normas, de distinto rango y naturaleza, sobre diferentes aspectos de la Administración y el Procedimiento Administrativo Digital que debido a su dispersión no han permitido su desarrollo y ha generado descoordinación.
[77] BID. 2018. El fin del trámite eterno: ciudadanos, burocracia y gobierno digital / Benjamin Roseth, Angela Reyes, Carlos Santiso, editores. Ver: https://bit.ly/2MOZDss
[78] Según el documento se entiende como Trámite "...al conjunto de requisitos, pasos o acciones a través de los cuales los individuos o las empresas piden o entregan información a una entidad pública, con el fin de obtener un derecho –generación de un registro, acceso a un servicio, obtención de un permiso– o para cumplir con una obligación"
[79] Op.Cit P.19
[80] Op.Cit P.47
[81] Op.Cit P.53
[82] Op.Cit P.58

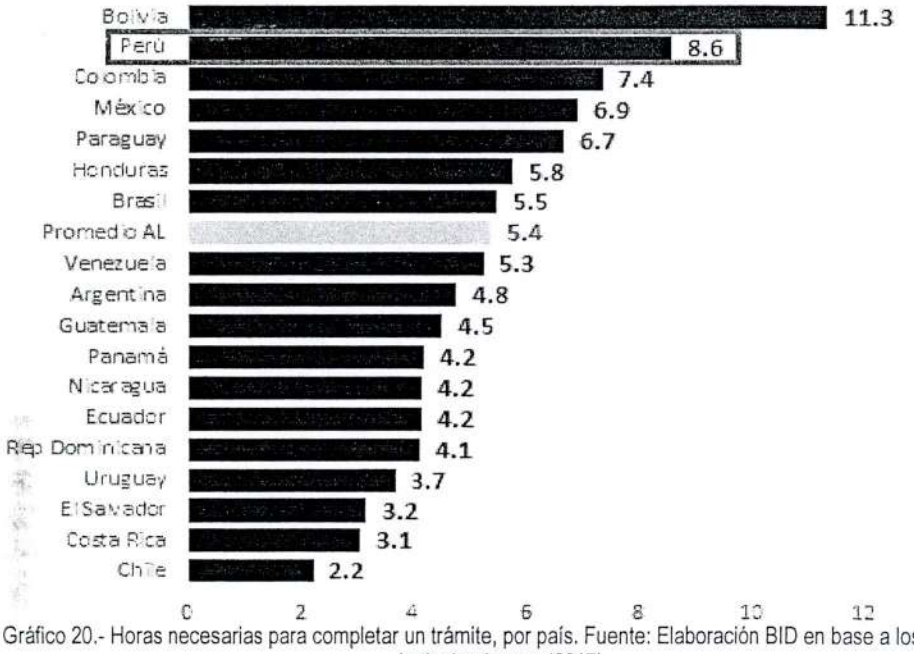

Gráfico 20.- Horas necesarias para completar un trámite, por país. Fuente: Elaboración BID en base a los datos de Latinobarómetro (2017)

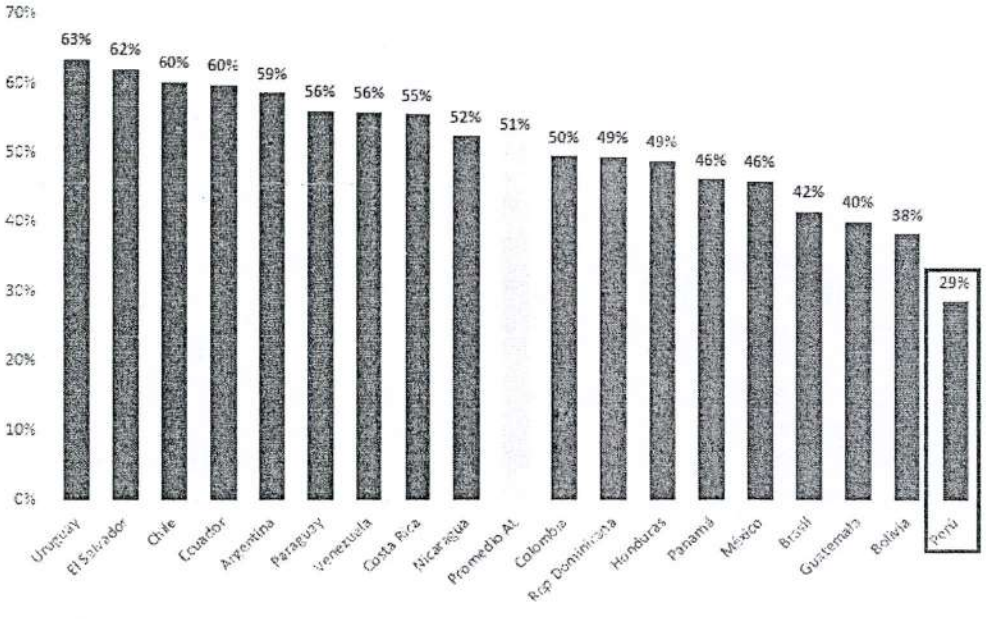

Gráfico 21.- Porcentaje de trámites resueltos en una sola interacción. Fuente: Elaboración BID en base a los datos de Latinobarómetro (2017)

- **Un foco de corrupción que afecta la confianza en el gobierno.** El 29% de los latinoamericanos reportó haber pagado un soborno en el contexto de un servicio público en el 2017, y con respecto al Perú el 39% de personas indicó haber pagado un soborno[83]. Así señala que *"La existencia de corrupción en los servicios públicos afecta negativamente a los ciudadanos y al gobierno. En el caso de los ciudadanos, no solo tiene un impacto negativo en términos monetarios (...). La corrupción resulta en un efecto negativo para el gobierno, por varias razones. Por una parte, tiene un impacto en la efectividad de las políticas públicas si existen individuos que pagan sobornos para acceder a servicios a los que no tienen derecho".*[84]

[83] Op.Cit P.64
[84] Op.Cit P.65

50

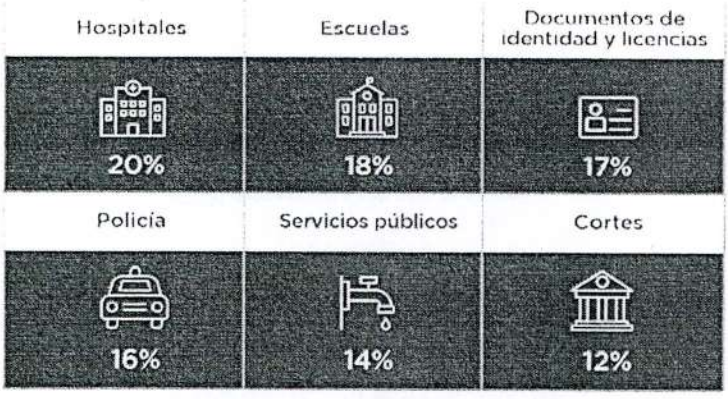

Gráfico 22.- Ciudadanos que pagaron un soborno, por tipo de servicio. Fuente: Elaboración BID en base a los datos de Transparencia Internacional (2017)

Desafortunadamente, menciona el documento, que los costos, así como la dificultad de los trámites afectan más a las personas de bajos ingresos; mientras que por otro lado, los trámites ineficientes le generan costos al gobierno (costos monetarios, de imagen reduciendo la confianza, de efectividad).

Asimismo, el referido documento señala que las razones para dicha dificultad se explican por cuatro (04) razones[85]:

1. *Falta de conocimiento de la verdadera experiencia ciudadana de parte del gobierno;*
2. *Alta complejidad regulatoria*
3. *Poca coordinación y colaboración interinstitucional.*
4. *Desconfianza del gobierno hacia los ciudadanos.*

Adicionalmente, el documento señala que *"El uso del canal digital puede ayudar a solucionar los problemas con los trámites: en general, son más rápidos, son más baratos de prestar y son menos vulnerables a la corrupción"*, así indica que la digitalización de trámites tiene como mayor beneficio para el ciudadano el ahorro de tiempo *"Los trámites completamente digitales –los que no requieren ninguna interacción física– que están funcionando actualmente en América Latina y el Caribe (ALC) se demoran en promedio un 74% menos que los trámites presenciales"*[86]. El costo operativo de prestación de un trámite digital oscila entre el 1,5% y el 5% de lo que cuesta prestar un trámite por el canal presencial[87].

Sin embargo, a pesar de su potencial el uso de los trámites a través de canales digitales aún es bajo por parte de la población, lo cual puede deberse a algunos factores como la disponibilidad de los trámites en línea, capacidades (brechas de identificación legal y digital, la conectividad, la alfabetización digital, entre otros), la experiencia en el uso de los trámites digitales, entre otros.

Por ejemplo, en nuestro país solo el 15.15% de trámites puede iniciarse en línea, y en mucho menor porcentaje puede completarse a través de ese canal, según el BID ello se podría explicar en el nivel de complejidad, ya que se requiere cumplir todos los pasos de los trámites presenciales a través del canal digital, como 1) verificación de la identidad, 2) presentación de información de otras entidades, 3) firma del solicitante, 4) procesar pagos, entre otros.

[85] Op.Cit Sección II ¿Por qué son los trámites tan difíciles de hacer?
[86] Op.Cit P.100
[87] Op.Cit P.103

51

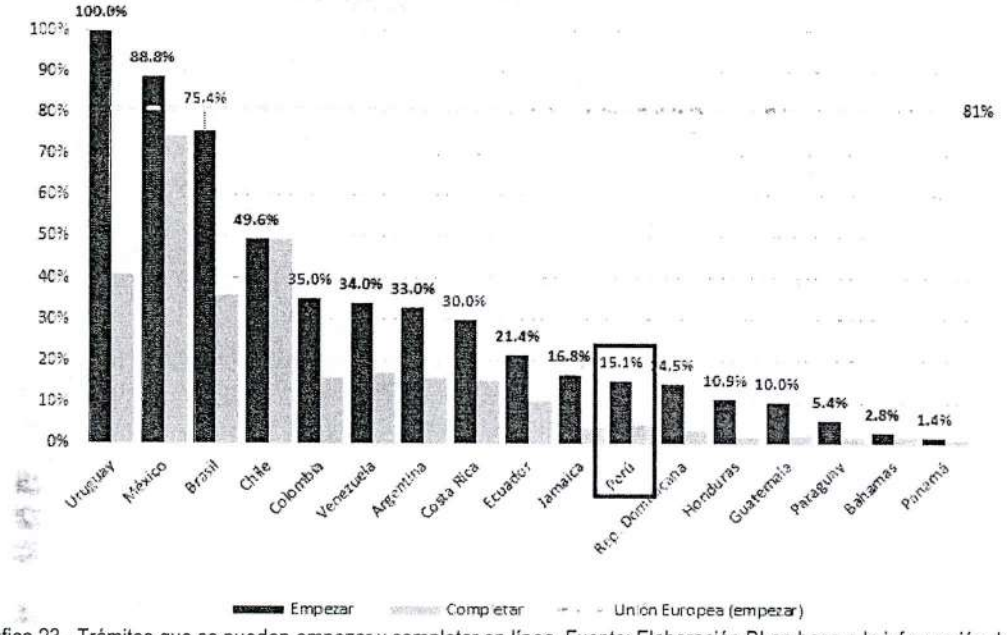

Gráfico 23.- Trámites que se pueden empezar y completar en línea. Fuente: Elaboración BI en base a la información de la Encuesta BID-GEALC (2017)

En tal sentido, atendiendo a los resultados del estudio y, sobre todo, a la necesidad de establecer un marco normativo que nos permita dotar de coherencia y unidad sistemática a la normativa peruana para promover el uso transversal de las tecnologías digitales en la administración pública, así como impulsar la adecuada "colaboración entre entidades" (Interoperabilidad) y, al mismo tiempo, minimizar riesgos asociados con la "seguridad digital", de cara a generar "confianza" en el proceso de "Transformación Digital" del Estado Peruano, la presente norma tiene como encuadre jurídico la de ser una norma de carácter "**especial**" respecto de aquella que regula de modo "general" el actuar de la Administración Pública, esto es, la indicada Ley N° 27444, y, que por la naturaleza misma de la materia a normarse con la presente Ley posibilite la adopción ordenada e integral de las denominadas tecnologías digitales en dicho ámbito, viabilizando el tránsito hacia "Servicios Digitales" interoperables, seguros, escalables, ágiles, confiables y que faciliten la transparencia en un entorno de Gobierno Digital. El anotado carácter "especial" del presente dispositivo permitirá al menos dos efectos, a saber:

1. En caso de discrepancia entre el dispositivo "especial" y "general", prevalezca el primero facilitando su aplicación en caso de conflicto normativo; y
2. Las normas que regulan el ámbito administrativo son de carácter "general" y supletorias de la disposición especial, siendo ésta aplicable al ámbito material del "Uso transversal de las tecnologías digitales en la Administración Pública" coexistiendo ambas normas al no ser excluyentes sino complementarias.

En este punto la presente propuesta normativa sienta las bases para la prestación de servicios digitales considerando, sin perjuicio de los tópicos a desarrollar en el Reglamento respectivo, los siguientes aspectos "Garantías para la prestación de servicios digitales", especificaciones para la "Conservación de documentos electrónicos firmados digitalmente", "Sede Digital", "Registro Digital" y "Domicilio Digital"

Para el caso de las **garantías** en la prestación de servicios digitales, estas se implementan de manera progresiva y cuando corresponda, las mismas que están orientadas a facilitar la interacción de los ciudadanos y personas en general en un entorno de gobierno digital, empero sin descuidar que cada entidad de la Administración Pública fortalezca las capacidades de sus servidores y funcionarios en materia de firmas electrónicas, firmas y certificados digitales, protección de datos personales, interoperabilidad, seguridad digital, datos abiertos y Gobierno Digital. Lo cual se realizará de forma progresiva y analizando cada caso en concreto.

- Reconocer y aceptar el uso de la identidad digital de todas las personas según lo regulado en la presente Ley.
- Garantizar la disponibilidad, integridad y confidencialidad de la información de los servicios digitales con la aplicación de los controles de seguridad que correspondan en la prestación de dichos servicios conforme a las disposiciones contenidas en la presente Ley y en la normatividad vigente sobre la materia.
- Capacitar en temas en materia de firmas electrónicas, firmas y certificados digitales, protección de datos personales, interoperabilidad, arquitectura digital, seguridad digital, datos abiertos y Gobierno Digital.
- Facilitar el acceso a la información requerida por otra entidad de la Administración Pública, sobre los datos de las personas que obren en su poder y se encuentren en soporte electrónico, únicamente para el ejercicio de sus funciones en el ámbito de sus competencias. Queda excluida del intercambio la información que pueda afectar la seguridad nacional o aquella relacionada con la legislación sobre Transparencia y Acceso a la Información Pública, o la que expresamente sea excluida por Ley.
- Implementar servicios digitales haciendo un análisis de la arquitectura digital y rediseño funcional.
- Considerar la implementación de pagos a través de canales digitales.
- Facilitar a las personas información detallada, concisa y entendible sobre las condiciones de tratamiento de sus datos personales.
- Garantizar la conservación de las comunicaciones y documentos generados a través de canales digitales en las mismas o mejores condiciones que aquellas utilizadas por los medios tradicionales.
- Garantizar que en el diseño y configuración de los servicios digitales se adoptan las medidas técnicas, organizativas y legales para la debida protección de datos personales y la confidencialidad de las comunicaciones.

En materia de ***conservación de documentos electrónicos firmados digitalmente***, la propuesta normativa precisa que se emplearán sellos de tiempo y mecanismos basados en estándares internacionalmente aceptados que permitan verificar el estado del certificado digital asociado. Cuando dicho tipo de documentos electrónicos, y sus respectivos formatos que aseguran la característica de perdurabilidad de la firma digital, deban ser conservados de modo permanente, éstos se archivarán observando las disposiciones legales sobre la materia Decreto Legislativo N° 681, Normas Técnicas Peruanas (NTP 392.030-2 2015), Resolución de Secretaria de Gobierno Digital N° 001-2017-PCM/SEGDI u otros aplicables.

Por otro lado, cuando se aborde el tema de "sede digital", "registro digital" y "domicilio digital" la presente propuesta legislativa entiende que:

- *La sede digital es un tipo de canal digital, a través del cual pueden acceder los ciudadanos y personas en general a un catálogo de servicios digitales, realizar trámites, hacer seguimiento de los mismos, recepcionar y enviar documentos electrónicos, y cuya titularidad, gestión y administración corresponde a cada entidad de la Administración Pública en los tres niveles de gobierno, el mismo que debe ser accesible para las personas a través de internet.*

- *Las sedes digitales de las entidades de la Administración Pública cuentan con un registro digital para recibir documentos, solicitudes, escritos y comunicaciones electrónicas dirigidas a dicha entidad.*

- *Es uno de los atributos de la identidad digital que se constituye en el domicilio habitual de un ciudadano en el entorno digital, el cual es utilizado por las entidades de la Administración Pública para efectuar comunicaciones o notificaciones.*

53

De otro lado, se ha previsto que las entidades de la Administración Pública que a la fecha de entrada en vigencia de la propuesta legislativa hayan implementado y brinden servicios digitales adoptan y adecuan las disposiciones de los mismos de manera progresiva conforme a sus recursos, capacidades, lineamientos y plazos a establecerse en el reglamento de la referida propuesta, sin perjuicio de lo establecido en el numeral 5.1 de la propuesta normativa.

D. GOBERNANZA DE DATOS

La norma entiende como dato a la representación descifrable de hechos, información o concepto, expresado en cualquier forma apropiada para su procesamiento, almacenamiento, comunicación e interpretación; y se considera como "Elemento Estructural", en razón que es el elemento esencial para la transparencia, gobierno abierto, interoperabilidad, digitalización y lucha anticorrupción, reconocido así por distintos marcos y estándares internacionales, tales como:

a) Gobierno Digital - Construyendo una plataforma del siglo 21 para servir mejor a los americanos[88].
b) Carta Internacional de datos abiertos[89].
c) ISO/IEC 38505-1:2017 - Gobernanza de datos[90].
d) Perspectivas para Rusia - Gobierno Digital al 2020[91].

En esa línea, las entidades de la Administración Pública deben administrar sus datos como un activo estratégico, garantizando que estos se capturen, creen, almacenen, procesen y pongan a disposición durante el tiempo que sea necesario y cuando sea apropiado considerando las necesidades de información, riesgos y la normatividad vigente en materia de Gobierno Digital, seguridad digital, transparencia, protección de datos personales y cualquier otra vinculante.

De igual manera, resulta conveniente revisar algunos estándares sobre la gestión y gobernanza de datos, entre ellos tenemos:

a) **ISO / IEC 38505-1: 2017 Gobernanza de datos**[92]
Estándar que proporciona "principios rectores" para los miembros de los órganos de gobierno de las organizaciones (propietarios, directores, socios, gerentes ejecutivos o similares) sobre el uso eficaz, eficiente y aceptable de los datos dentro de sus organizaciones.
b) **ISO / IEC 38505-2: 2017 Gobernanza de datos**[93]
Estándar que proporciona orientación a los miembros de los órganos de gobierno de las organizaciones y sus gerentes ejecutivos sobre las implicaciones de ISO / IEC 38505-1 para la gestión de datos. Este documento permite un diálogo informado entre el órgano de gobierno y el equipo directivo superior / ejecutivo de una organización para garantizar que el uso de datos en toda la organización se alinee con la dirección estratégica establecida por el órgano rector.
c) **Data Management Body Of Knowledge (DAMA-BOK)** - Cuerpo de Conocimiento para la Gestión de Datos – DAMA 2.0[94]
Marco de referencia que profundiza las áreas vinculadas con la gestión de datos, el mismo que tiene como aspecto central "La gobernanza de datos"; componente requerido para aspectos vinculados con la consistencia de los datos, así como para el balance entre las funciones de negocios.

De lo anterior, podemos ver que a nivel del Estado se requiere constituir una Infraestructura Nacional de Datos, la cual se define como conjunto articulado de políticas, normas, medidas, procesos, tecnologías digitales, repositorios y bases de datos destinadas a promover la adecuada recopilación, procesamiento, publicación, almacenamiento y puesta a disposición de los datos que gestionan las entidades de la Administración Pública, a fin de asegurar la eficacia y eficiencia en su uso y la digitalización de procesos, apoyar la oportuna toma de decisiones, promover el desarrollo socio-económico, competitividad, transparencia e innovación en todos los sectores y niveles.

---

[88] Ver en: https://obamawhitehouse.archives.gov/sites/default/files/omb/egov/digital-government/digital-government-strategy.pdf
[89] Ver en: https://opendatacharter.net/principles-es/
[90] Puede ser consultado en : https://www.iso.org/standard/56639.html
[91] Ver en: http://pubdocs.worldbank.org/en/840921460040867072/Digital-Government-Russia-2020-ENG.pdf
[92] Op. cit. 82
[93] El documento puede ser consultado en: https://www.iso.org/obp/ui/#iso:std:iso-iec:tr:38505:-2:ed-1:v1:en
[94] El documento puede ser consultado en: https://dama.org/content/body-knowledge

54

Ahora bien, de manera complementaria a la Infraestructura Nacional de Datos, a nivel del Estado y de las entidades públicas se requiere establecer con claridad los procesos de gobernanza y gestión de datos; es decir, definir un Marco de Gobernanza y Gestión de Datos del Estado Peruano, el mismo que está constituido por instrumentos técnicos y normativos que establecen los requisitos mínimos que las entidades de la Administración Pública deben implementar conforme a su contexto legal, tecnológico y estratégico para asegurar un nivel básico y aceptable para la recopilación, procesamiento, publicación, almacenamiento y apertura de los datos que administre.

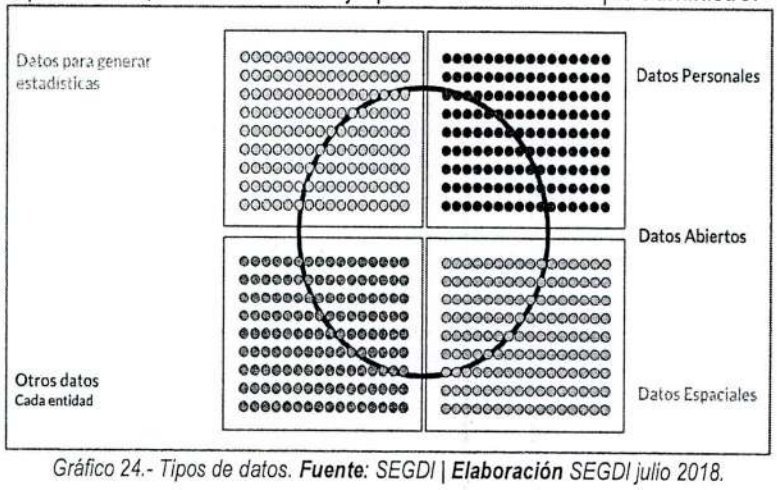

Gráfico 24.- Tipos de datos. ***Fuente:*** *SEGDI |* ***Elaboración*** *SEGDI julio 2018.*

Cabe indicar que conforme a lo indicado en el Decreto Supremo N° 022-2017-PCM, la materia de datos abiertos, así como su despliegue e implementación es responsabilidad de la Secretaría de Gobierno Digital; mientras que el Gobierno Abierto está a cargo de la Secretaría de Gestión Pública, ambos ámbitos se complementan y coordinan sus acciones.

E. INTEROPERABILIDAD

La propuesta normativa entiende como Interoperabilidad a la capacidad de interacción de organizaciones diversas y dispares para alcanzar objetivos que hayan sido acordados conjuntamente, recurriendo a la puesta en común de información y conocimientos, a través de los procesos y el intercambio de datos e información entre sus respectivos sistemas de información.

La misma que toma como referencia lo expresado, en su oportunidad por la Carta Iberoamericana de Gobierno Electrónico de 2007[95], la cual ampliando significación del uso de las tecnologías digitales, entendió que el empleo de las mismas en el ámbito público tiene por objeto "*...mejorar la información y los servicios ofrecidos a los ciudadanos, orientar la eficacia y eficiencia de la gestión pública... (e)...incrementar sustantivamente la transparencia del sector público y la participación de los ciudadanos...*", manifestando que la adopción de tecnologías en la gestión pública de los Estados tienen como propósito la "*...satisfacción de las necesidades así como contribuir al desarrollo de la sociedad*" lo cual no puede fundarse "*...en una simple respuesta a las ofertas tecnológicas que provienen del mercado*"[96].

La citada Carta Iberoamericana de Gobierno Electrónico, recogiendo prácticas de la legislación comparada[97], impulsa el reconocimiento por parte de los Estados Iberoamericanos del derecho al acceso electrónico a la Administración, el mismo que, a su vez, amplía a fin que no sólo comprenda la relación de los ciudadanos con la Administración Pública, sino que lo incardina en un concepto

[95] Aprobada por la IX Conferencia Iberoamericana de Ministros de Administración Pública y Reforma del Estado, llevada a cabo entre el 31 de mayo y 1° de junio de 2007, documento adoptado por la XVII Cumbre Iberoamericana de Jefes de Estado y de Gobierno con fecha 10 de noviembre de 2007, eventos organizados por el Centro Latinoamericano de Administración para el Desarrollo (CLAD), el texto integro del citado documento puede ser consultado a través del enlace: http://www.clad.org/documentos/declaraciones/cartagobelec.pdf.

[96] "Carta Iberoamericana de Gobierno Electrónico", Centro Latinoamericano de Administración para el Desarrollo (CLAD), 2007, Op. Cit., p.7 y 8.

[97] Como por ejemplo la regulación española contenida en la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, el texto integro de la norma puede ser consultado en: http://www.boe.es/boe/dias/2007/06/23/pdfs/A27150-27166.pdf.

mayor como es "*el derecho al Gobierno Electrónico*", lo cual, adicionalmente, importa la necesidad que las entidades públicas se encuentren "*...interrelacionadas entre sí de modo que se simplifiquen procedimientos*"[98], implicando la "*interoperabilidad*"[99] como un "...pre-requisito a la puesta en funcionamiento de servicios públicos electrónicos inter-administrativos y de alto valor añadido para el ciudadano"[100], siendo dicho fundamento la razón para que la "interoperabilidad" sea considerado en la presente ley como otro de sus elementos estructurales (énfasis agregado).

Entre las recomendaciones que realiza el CLAD, en los documentos antes reseñados, destacan a la "interoperabilidad" como un medio por el cual se logra la integración interadministrativa y la prestación conjunta de servicios públicos electrónicos orientados a los ciudadanos y personas en general, para lo cual la presente propuesta legislativa regula la interoperabilidad a fin de permitir una efectiva gestión de la colaboración entre las distintas entidades de la Administración Pública completándose el desarrollo del nivel jurídico[101] que integra a los niveles organizativos[102], semánticos[103] y técnicos[104] desde una perspectiva sistémica, facilitando que dicha colaboración entre entidades propicie igualmente el desarrollo y la consolidación del Gobierno Digital en el país.

Gráfico 25.- Niveles de la Interoperabilidad. **Fuente**: Elaboración SEGDI julio 2018[105].

Con relación al indicado "nivel jurídico" de la Interoperabilidad, consideramos lo indicado por el CLAD en el documento "Bases para una Estrategia Iberoamericana de Interoperabilidad" de 2010[106], que constituye una "adenda" a la antes reseñada Carta de Gobierno Electrónico de 2007, donde se expresa que la "*...interoperabilidad organizativa también debe contar con el componente jurídico, en la medida que los servicios se encuentran ligados a una normativa que regula su funcionamiento y condiciona su prestación, singularmente, en entornos intergubernamentales*", indicando que una normativa sobre "*...identidad digital es uno de los aspectos básicos para desarrollar servicios*" precisando que "*...la puesta en marcha y desarrollo de proyectos de interoperabilidad en el Gobierno electrónico requiere una actuación conjunta en materia de certificación e identidad digital*"[107](énfasis agregado).

---

[98] Numeral 7 de la "Carta Iberoamericana de Gobierno Electrónico", Centro Latinoamericano de Administración para el Desarrollo (CLAD), 2007, Op. Cit., p.10.

[99] "...entendida al menos como la propiedad mediante la cual sistemas heterogéneos pueden intercambiar información y procesos técnicos o datos", enForo Iberoamericano sobre Estrategias para la Implantación de la Carta Iberoamericana de Gobierno Electrónico, En "Foro Iberoamericano sobre Estrategias para la Implantación de la Carta Iberoamericana de Gobierno Electrónico", de 16 y 17 de abril de 2009, Isla de Margarita, Venezuela; organizado por el Centro Latinoamericano de Administración para el Desarrollo (CLAD), documento en línea: http://www.clad.org/documentos/otros-documentos/foro-iberoamericano-sobre-estrategias-para-implementar-la-carta-iberoamericana-de-gobierno-electronico-interoperabilidad, p. 2.

[100] En "Foro Iberoamericano sobre Estrategias para la Implantación de la Carta Iberoamericana de Gobierno Electrónico", (CLAD), 2009, Op. Cit., p 4.

[101] Alude a la "...sincronización adecuada de la legislación de un determinado ámbito político para que los datos electrónicos originarios del mismo sean conformes al Derecho aplicable en otros, y se reconozcan recíprocamente cuando ello sea necesario para su utilización en ámbitos distintos del originario. Esta dimensión de la interoperabilidad se preocupa, por ejemplo, de que un certificado electrónico (o una firma electrónica) válido en España también lo sea en Holanda...", por GAMERO CASADO, Op. Cit, p297.

[102] "En la dimensión organizativa de la interoperabilidad hacemos referencia a los diferentes universos de sujetos y usuarios, públicos o privados, que pueden verse implicados en la necesidad de ser interoperables. La interoperabilidad es, de hecho, un objetivo a escala mundial, y su implantación no debe limitarse a grupos cerrados de sujetos o a entidades de un mismo sector", por GAMERO CASADO, Eduardo en: "INTEROPERABILIDAD Y ADMINISTRACIÓN ELECTRÓNICA: CONÉCTENSE, POR FAVOR", en Revista de Administración Pública ISSN: 0034-7639, núm. 179, Madrid, mayo-agosto (2009), p296.

[103] "...hace referencia a que la información intercambiada pueda ser interpretable de forma automática y reutilizable por aplicaciones que no intervinieron en su aplicación", por GAMERO CASADO, Op. Cit, p296.

[104] Determinados "...por la relación entre sistemas y servicios de tecnologías de la información, incluyendo aspectos tales como los interfaces, la presentación de la información, la interconexión, la integración de datos y servicios, la presentación de la información, la accesibilidad y la seguridad", por GAMERO CASADO, Op. Cit, p297.

[105] En base a "El carácter poliédrico de la interoperabilidad", en "Comentario sistemático a la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos", GAMERO CASADO y VALERO TORRIJOS (coordinadores), Editorial Aranzadi, Tercera Edición 2010, p763.

[106] Elaborado por el Centro Latinoamericano de Administración para el Desarrollo (CLAD), para la consideración de la XII Conferencia Iberoamericana de Ministros de Administración Pública y Reforma del Estado, llevada a cabo en Buenos Aires, Argentina, 1-2 de julio de 2010, cuyo contenido íntegro puede ser consultado en: http://www.clad.org/siare_isis/innotend/gobelec/BasesEstrategialberoamericanaInteroperabilidad.pdf.

[107] En "Bases para una Estrategia Iberoamericana de Interoperabilidad", Op. Cit., p31 y 39.

56

Similar referencia podemos hallar en el documento "*Nuevo Marco Europeo de Interoperabilidad en la promoción de servicios y flujos de datos sin interrupciones para las administraciones públicas europeas*"[108], el cual señala que existen dimensiones cuando nos referimos a interoperabilidad, las cuales son:

- ***Interoperabilidad Legal,*** *la cual consiste en garantizar que las organizaciones que operan bajo diferentes marcos legales, políticas y estrategias puedan trabajar juntas.*
- ***Interoperabilidad Organizacional,*** *se refiere a la forma en que las administraciones públicas alinean sus procesos de negocios, responsabilidades y expectativas para lograr objetivos comúnmente acordados y mutuamente beneficiosos. En la práctica, la interoperabilidad organizacional significa documentar e integrar o alinear procesos e información relevante intercambiada.*
- ***Interoperabilidad Semántica****: garantiza que el formato y el significado precisos de los datos y la información intercambiados se conserven y se comprendan a lo largo de los intercambios entre las partes, en otras palabras, "lo que se envía es lo que se entiende".*
- ***Interoperabilidad Técnica****: Comprende las aplicaciones y las infraestructuras que interconectan sistemas y servicios. Los aspectos de la interoperabilidad técnica incluyen especificaciones de interfaz, servicios de interconexión, servicios de integración de datos, presentación de datos y intercambio y protocolos de comunicación segura.*

Gráfico 26.- Tipos de Interoperabilidad. ***Fuente****: Marco Europeo de Interoperabilidad |* ***Elaboración****: SEGDI agosto 2018*[109]

Asimismo, a nivel nacional podemos referir el trabajo realizado por el Consejo Nacional de Política Criminal, la cual en su sesión de fecha 16MAY2017, acordó la elaboración del Plan Nacional de Interoperabilidad del Sistema de Administración de Justicia Penal (SAJ – PENAL), esto en respuesta a la ausencia de un modelo de gobernanza, acciones institucionales por modernizarse aisladas y desarticuladas, pocos esfuerzos por implementar estándares técnicos internacionales, ausencia de servicios web que permitan el intercambio de información con otra entidad del SAJ, la disparidad de los sistemas informáticos, falta de estandarización de datos e información en los procesos vinculados con: (1). la investigación, (2). el proceso judicial y (3). Ejecución de penas de una presunta comisión de conductas tipificadas como faltas o delitos. Concordante con lo anterior, el Grupo de Trabajo Interinstitucional de Naturaleza Temporal, conformado por veintiséis (26) representantes de siete (07) entidades públicas elaboró el Plan Nacional de Interoperabilidad del Sistema de Administración de Justicia.

Así las cosas, mediante acta de acuerdos del 15MAY2018, el Consejo Nacional de Política Criminal acordó aprobar el Plan Nacional de Interoperabilidad del Sistema de Administración de Justicia Penal[110].

El referido Plan se sustenta en experiencias de la Unión Europea ("Justicia en Línea", "e-Justicia"), Reino Unido ("Access to Justice", "Justicia Rápida"), España ("Punto Neutro Judicial - PNJ", "Ley 18/2011 Reguladora del Uso de Tecnologías de la Información y la Comunicación en la Administración de Justicia"), Corea del Sur ("Sistema de Información Coreano de Servicios de Justicia Criminal – KICS") y Brasil ("Ley del Proceso Electrónico N° 11.419"), entrevistas a profundidad, talleres de trabajo, análisis documental y revisión de tendencias internacionales. Y, en base a ello, define la interoperabilidad como *"La capacidad de que las organizaciones diversas y*

[108] El documento puede ser consultado: https://ec.europa.eu/isa2/sites/isa/files/eif_brochure_final.pdf
[109] En base al "Nuevo Marco Europeo de Interoperabilidad en la promoción de servicios y flujos de datos sin interrupciones para las administraciones públicas europeas" y "Bases para una Estrategia Iberoamericana de Interoperabilidad (CLAD)", Op. Cit.
[110] El documento puede ser consultado en: https://asuntoscriminologicos.minjus.gob.pe/wp-content/uploads/2018/06/ACTA-13%C2%B0-SESION-DEL-CONAPOC_13.pdf

57

dispares interactúen con vistas a alcanzar objetivos comunes que sean mutuamente beneficiosos y hayan sido acordados conjuntamente, recurriendo a la puesta en común de información y conocimientos entre las organizaciones, a través de los procesos empresariales a los que apoyan, mediante el intercambio de datos entre sus respectivos sistemas TIC", y la entiende como un conjunto de dimensiones que permiten comprenderla de manera integral:

- ***Dimensión Técnica:*** *Cubre las cuestiones técnicas (hardware, software y telecomunicaciones), necesarias para interconectar sistemas computacionales y servicios, incluyendo aspectos clave como interfaces abiertas, servicios de interconexión, integración de datos y middleware, presentación e intercambio de datos, accesibilidad y servicios de seguridad.*
- ***Dimensión Semántica****: Se ocupa de asegurar que el significado preciso de la información intercambiada sea entendible sin ambigüedad por todas las aplicaciones que intervengan en una determinada transacción y habilita a los sistemas para combinar información recibida con otros recursos de información y así procesarlos de forma adecuada.*
- ***Dimensión Organizacional****: Se ocupa de definir los objetivos de negocios, modelar procesos y facilitar la colaboración de administraciones que desean intercambiar información y pueden tener diferentes estructuras organizacionales y procesos internos. Además de eso, busca orientar, con base en los requerimientos de la comunidad usuaria, los servicios que deben estar disponibles, fácilmente identificables, accesibles y orientados al usuario.*
- ***Dimensión Político – Legal:*** *considera los instrumentos legales que facilitan el intercambio de información, así como los temas concernientes a la responsabilidad legal y el tratamiento de la información que se intercambia.*
- ***Dimensión Cultural:*** *Considera la divulgación de los compromisos de intercambio de información, el desarrollo de las habilidades y competencias para la prestación y consumo de información; así como el fomento de la colaboración para facilitar la gestión del conocimiento entre las entidades.*

Conforme lo anterior, la presente propuesta normativa contempla que se debe establecer un Marco de Interoperabilidad del Estado Peruano, *el cual está constituido por políticas, lineamientos, especificaciones, estándares e infraestructura de tecnologías digitales, que permiten de manera efectiva la colaboración entre entidades de la Administración Pública para el intercambio de información y conocimiento, para el ejercicio de sus funciones en el ámbito de sus competencias, en la prestación de servicios digitales inter-administrativos de valor para el ciudadano provisto a través de canales digitales.*

El mismo que se gestionará en los siguientes niveles:

- ***Interoperabilidad a nivel organizacional:*** *Se ocupa del alineamiento de objetivos, procesos, responsabilidades y relaciones entre las entidades de la Administración Pública para intercambiar datos e información para el ejercicio de sus funciones en el ámbito de sus competencias*

- ***Interoperabilidad a nivel semántico:*** *Se ocupa del uso de los datos y la información de una entidad garantizando que el formato y significado preciso de dichos datos e información a ser intercambiada pueda ser entendido por cualquier aplicación de otra entidad de la Administración Pública. Dichas entidades deben adoptar los estándares definidos por el ente rector para el intercambio de datos e información.*
- ***Interoperabilidad a nivel técnico:*** *Se ocupa de los aspectos técnicos relacionados con las interfaces, la interconexión, integración, intercambio y presentación de datos e información, así como definir los protocolos de comunicación y seguridad.*
- ***Interoperabilidad a nivel legal:*** *Se ocupa de la adecuada observancia de la legislación y lineamientos técnicos con la finalidad de facilitar el intercambio de datos e información entre las diferentes entidades de la Administración Pública, así como el cumplimiento de los temas concernientes con el tratamiento de la información que se intercambia.*

Adicionalmente, la propuesta normativa busca promover la reutilización de software o programas de ordenador de titularidad de las entidades de la Administración Pública, desarrollados para implementar sus procesos o servicios, ya sea mediante la contratación de proveedores o desarrollados por personal de la entidad, debiendo ponerlas a disposición de cualquier otra entidad de la Administración Pública sin contraprestación y sin necesidad de convenio, teniendo en cuenta que el fin perseguido es su aprovechamiento y reutilización. En esa línea, mediante Decreto Supremo

N° 051-2018-PCM[111], se crea el Portal de software Público Peruano y se establecen disposiciones adicionales sobre el software Público Peruano, el cual señala en su artículo 5 "Obligatoriedad de compartir Software Público Peruano" que "Todas las entidades comprendidas en el artículo 2 del presente Decreto Supremo deben compartir, a través del Portal de Software Público Peruano, con cualquier otra entidad que lo solicite todo Software Público Peruano que cumpla con los requisitos técnicos y legales que establezca la SEGDI, incluidas las versiones mejoradas y validadas de dicho software, con su correspondiente control de versiones. Lo dispuesto en el presente Decreto Supremo no será de aplicación para el caso de software propietario o cuando la entidad pública sea sólo licenciataria del software, ni comprenderá los componentes licenciados para el funcionamiento del Software Público Peruano".

Consistente con ello, la presente propuesta legislativa establece que *"Las entidades de la Administración Pública titulares de Software Público Peruano, desarrollado mediante la contratación de terceros o por personal de la entidad para soportar sus procesos o servicios, adoptan las medidas necesarias a fin de obtener la titularidad exclusiva sobre los derechos patrimoniales del referido Software Público Peruano. Todas las entidades de la Administración Pública deben compartir Software Público Peruano bajo licencias libres o abiertas que permitan (i) usarlo o ejecutarlo, (ii) copiarlo o reproducirlo, (iii) acceder al código fuente, código objeto, documentación técnica y manuales de uso, (iv) modificarlo o transformarlo en forma colaborativa, y (v) distribuirlo, en beneficio del Estado Peruano".*

F. SEGURIDAD DIGITAL

Mediante Decreto Supremo N° 050-2018-PCM[112], de fecha 15MAY2018, se aprueba la definición de Seguridad Digital en el ámbito nacional, señalando que ésta "... *es el estado de confianza en el entorno digital que resulta de la gestión y aplicación de un conjunto de medidas proactivas y reactivas frente a los riesgos que afectan la seguridad de las personas, la prosperidad económica y social, la seguridad nacional y los objetivos nacionales en dicho entorno. Se sustenta en la articulación con actores del sector público, sector privado y otros quienes apoyan en la implementación de controles, acciones y medidas; debiéndose tener presente para estos efectos los aspectos siguientes:*

a) *Nota 1: La confianza en el entorno digital o también denominada confianza digital emerge como resultado de cuán veraz, predecible, seguro y confiable son las interacciones digitales que se generan entre empresas, individuos o cosas.*
b) *Nota 2: Las medidas proactivas y reactivas comprenden tecnología, políticas, controles, programas de capacitación y sensibilización que tienen por finalidad preservar la confidencialidad, integridad y disponibilidad de la información contenida en el entorno digital.*
c) *Nota 3: Los riesgos en el entorno digital o riesgo de seguridad digital es resultado de una combinación de amenazas y vulnerabilidades en el entorno digital. La gestión del riesgo de seguridad digital comprende los procesos que garantizan que las acciones o medidas son apropiadas con los riesgos y objetivos económicos y sociales en juego.*
d) *Nota 4: La prosperidad económica y social comprende la creación de riqueza, la innovación, la competitividad, entre otros, así como aspectos vinculados con las libertades individuales, salud, educación, cultura, participación democrática, ciencia, ocio y otras dimensiones del bienestar en las que el entorno digital está impulsando el progreso."*

Ahora bien, la "Seguridad Digital" como elemento estructural responde a que asegura el proceso para encaminar la "Transformación Digital" del Estado Peruano, preservando la integridad, disponibilidad y confidencialidad de la información que fluye en los sistemas y redes de información de las entidades de la Administración Pública, así como la interacción de las personas en el entorno digital, procurando mediante una adecuada gestión de riesgos, establecer controles o acciones que reduzcan las vulnerabilidades y exposición al riesgo, durante el tránsito hacia la digitalización de procesos y servicios, e interacción en el entorno digital.
En dicha línea, desde el 2002 la OCDE en su documento "Guías de la OCDE para la seguridad de sistemas de información y redes: Hacia una cultura de seguridad", menciona que "...*como resultado*

[111] Ver: https://bit.ly/2oEvQVQ
[112] El documento puede ser consultado en:
https://busquedas.elperuano.pe/download/url/aprueban-la-definicion-de-seguridad-digital-en-el-ambito-nac-decreto-supremo-n-050-2018-pcm-1647865-1

59

de la creciente conectividad, los sistemas de información y las redes son más vulnerables ya que están expuestos a un número creciente así como un rango de variedad mayor de amenazas y vulnerabilidades", por lo que se requiere contar con mecanismos adecuados para su gestión en dicho entorno.

Con fecha 17SEP2015, la OCDE emitió un documento denominado "Recomendaciones sobre gestión de riesgos de seguridad digital para la prosperidad económica y social[113]", el cual busca guiar a los países miembros y no miembros en la formulación de estrategias en materia de gestión de riesgos de seguridad digital, considerando los ámbitos económicos y sociales. Asimismo, el referido documento señala que *"Los problemas de seguridad digital a menudo se capturan a través del conveniente término "ciberseguridad", que abarca todas las dimensiones de seguridad digital, desde tecnología, hasta aspectos económicos y sociales, legales, de aplicación de la ley, derechos humanos, seguridad nacional, guerra, estabilidad internacional, inteligencia y otros aspectos. El uso generalizado de este término a menudo enmascara la naturaleza amplia y compleja del tema".*

Por otro lado, en el apartado denominado "De la seguridad de los sistemas de la información a la gestión de riesgos de seguridad digital (2002-2015)" se indica que *"La Recomendación de 2015 representa tanto una continuación como un cambio importante con respecto a las Directrices de seguridad de 2002; (...) El principal cambio es que el enfoque de los Principios se ha reorientado desde "Seguridad de los sistemas y redes de información" al riesgo de seguridad de las actividades económicas y sociales que dependen del entorno digital. No obstante, la Recomendación subraya la necesidad de cooperación con los expertos encargados de diseñar y mantener el entorno digital (es decir, los profesionales de las TIC) que probablemente entiendan mejor los factores de riesgo de la seguridad digital y las posibles medidas de seguridad relacionadas." (Énfasis añadido)*

Claro está que cuando abordamos el tema de Seguridad Digital nos articulamos y sustentamos con lo establecido a nivel de normas, procesos, roles y mecanismos regulados e implementados a nivel nacional en materia de Seguridad de la Información (Ley N° 30618, D.S. N° 022-2017-PCM, R.M. N° 166-2017-PCM y R.M. N° 004-2016-PCM). Conviene precisar que la Seguridad de la Información se enfoca en la información, de manera independiente de su formato y soporte. La Seguridad Digital se ocupa de las medidas de seguridad de la información procesada, transmitida, almacenada o contenida en el entorno digital, procurando generar confianza, gestionando los riesgos que afecten la seguridad de las personas y la prosperidad económica y social en dicho entorno.

Consistente con lo anterior, es bueno referir algunas experiencias internacionales en dicha materia, sobre todo en lo referido al nivel de gestión y articulación con actores de defensa, inteligencia y operadores de justicia.

- **Experiencia de Estonia**[114], conforme lo indicado en el documento "Organización de la Ciberseguridad - Estonia", dicho país articula acciones para responder las amenazas a la seguridad en el ciberespacio o entorno digital como sigue:
  - *Gobernanza de la seguridad en el entorno digital, la Autoridad de Sistemas de Información de Estonia es responsable de coordinar la implementación de políticas, estrategias y estándares en materia de seguridad en el entorno digital.*
  - *Inteligencia en el ciberespacio, es responsabilidad del Servicio de Seguridad Interno de Estonia (Estonian Internal Security Service - KAPO)[115], quien debe detectar y prevenir las amenazas en el ciberespacio o entorno digital, vinculado a terrorismo y atentados.*
  - *Defensa en el Ciberespacio, responsabilidad del Ministerio de Defensa de Estonia (MOD[116]), quien es la autoridad coordinadora para la defensa en el entorno digital o ciberespacio.*

[113] OECD (2015), Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document, OECD Publishing, Paris. DOI: http://dx.doi.org/10.1787/9789264245471-en

[114] El documento puede ser consultado en: https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_ESTONIA_032015_1.pdf

[115] Información adicional puede ser obtenida en: https://www.kapo.ee/

[116] Información adicional puede ser obtenida en: http://www.kaitseministeerium.ee/en

60

- **Experiencia de Reino Unido**[117], conforme lo indicado en el documento "Organización Nacional de la Ciberseguridad - Reino Unido", el Reino Unido articula las acciones para responder las amenazas a la seguridad en el ciberespacio o entorno digital como sigue:
  - *Gobernanza de la seguridad en el entorno digital, la Oficina de Seguridad Cibernética y Aseguramiento de la Información (Office of Cyber Security & Information Assurance - OCSIA), apoya al Ministro de la Oficina del Gabinete y al Consejo de Seguridad Nacional para determinar las prioridades para asegurar el ciberespacio.*
  - *Inteligencia en el ciberespacio, la Secretaría de Seguridad Nacional (Government Communications Headquarters - GCHQ) es la responsable de coordinar cuestiones de inteligencia de importancia estratégica para el gobierno, entre las que se encuentra las acciones de inteligencia en el ciberespacio.*
  - *Defensa en el ciberespacio, el Ministerio de Defensa del Reino Unido es el responsable de dirigir la política de defensa en el ciberespacio.*

De manera concordante con las experiencias revisadas la presente propuesta normativa considera necesario que se establezca con claridad las responsabilidades en relación a la Seguridad Digital a nivel nacional, por ello plantea contar con un Marco de Seguridad Digital del Estado Peruano que se constituye en el conjunto de principios, modelos, políticas, normas, procesos, roles, tecnología y estándares mínimos que permitan preservar la confidencialidad, integridad, disponibilidad de la información en el entorno digital administrado por las entidades de la Administración Pública.

Asimismo, dicho Marco es gestionado por la Presidencia del Consejo de Ministros a través de la Secretaría de Gobierno Digital, encargado de dirigir la política en materia de seguridad digital a nivel nacional, supervisar su cumplimiento, evaluar las necesidades de las entidades en dicha materia y comunicar al Presidente del Consejo de Ministros los resultados y avances del mismo; adicionalmente, promueve la cooperación con otras organizaciones de similar naturaleza a nivel internacional, a través de acuerdos, convenios u otros mecanismos.

El Marco de Seguridad Digital del Estado Peruano tiene los siguientes ámbitos:

a. ***Defensa**: El Ministerio de Defensa (MINDEF) en el marco de sus funciones y competencias dirige, supervisa y evalúa las normas en materia de ciberdefensa.*
b. ***Inteligencia**: La Dirección Nacional de Inteligencia (DINI) como autoridad técnica normativa en el marco de sus funciones emite, supervisa y evalúa las normas en materia de inteligencia, contrainteligencia y seguridad digital en el ámbito de ésta competencia.*
c. ***Justicia**: El Ministerio de Justicia y Derechos Humanos (MINJUS), el Ministerio del Interior (MININTER), la Policía Nacional del Perú (PNP), el Ministerio Público y el Poder Judicial (PJ) en el marco de sus funciones y competencias dirigen, supervisan y evalúan las normas en materia de ciberdelincuencia.*
d. ***Institucional:** Las entidades de la Administración Pública deben establecer, mantener y documentar un Sistema de Gestión de la Seguridad de la Información (SGSI).*

Para lo antes indicado, la OCDE señala que se hace necesario "*...tener una mayor consciencia y entendimiento de los aspectos de seguridad, así como de desarrollar una cultura de seguridad*"[118], razón por la cual se ha puesto "*...el acento en la naturaleza cooperativa de las respuestas a incidentes de seguridad y en la necesidad de cooperación internacional en determinados supuestos*" conforme lo remarca en su documento de 2015 "Perspectiva de la OCDE sobre economía digital de 2015"[119].

Es pertinente mencionar que el proyecto normativo que aprueba la Ley de Gobierno Digital mantiene la concordancia la Ley Nº 27658, Ley Marco de Modernización de la Gestión del Estado, así como con la vigente Política Nacional de Modernización de la Gestión Pública 2013-2016, aprobada mediante Decreto Supremo Nº 004-2013-PCM, alineada con la Política Nacional de Gobierno Electrónico 2013-2017, aprobada mediante Decreto Supremo N° 081-2013-PCM.

---

[117] Información adicional puede ser obtenida en: https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_UK_032015_0.pdf

[118] En "Guías de la OCDE para la seguridad de los sistemas de información y redes: Hacia una cultura de seguridad", p3 y ss., OCDE 2002, documento puede consultarse en: http://www.anacom.pt/streaming/1946922.pdf?categoryId=45842&contentId=132698&field=ATTACHED_FILE.

[119] En "Perspectiva de la OCDE sobre economía digital de 2015", p256. OCDE 2015. documento puede consultarse en: http://www.ccoo.es/7ca5782b36b4c532407d13dc6f4c4762000001.pdf

61

Adicionalmente, se ha previsto que los artículos 11, 12, 14, 15, 19, 20, 21, 22, 25, 27, 31 y numerales 18.1, 18.5, 18.6 y 18.8 del artículo 18 entrarán en vigor con la norma reglamentaria correspondiente, ya que estos necesitan de su reglamentación para poder ser implementados.

Finalmente, la propuesta normativa debe interpretarse de acuerdo con la finalidad que expresamente anuncia y hacerlo de otro modo resultaría perverso. En ese sentido, este marco normativo permite ampliar los preceptos desde todo punto de vista del derecho de modo que la progresión tecnológica avanza y el derecho no debe ser ajeno a estas realidades, teniendo como fin último la creación de valor público y transparencia para el ciudadano.

III. ANÁLISIS COSTO BENEFICIO

Se ha considerado que la implementación y financiamiento de las acciones que se derivan de la aplicación de la propuesta normativa, que involucran a los servicios digitales, arquitectura digital, interoperabilidad, seguridad digital y datos, entre otras, es progresivo y se sujeta a la disponibilidad presupuestal de las entidades involucradas, en el marco del Presupuesto del Sector Público para cada año fiscal, debiéndose priorizar los recursos para tales fines, sin demandar recursos adicionales al Tesoro Público.

No obstante, es necesario señalar cuales son los beneficios esperados de su implementación:

a. Se fortalece el marco de Gobernanza en materia de Gobierno Digital en el Estado Peruano

De manera consistente con las recomendaciones de la Organización para la Cooperación y el Desarrollo Económicos (**OCDE**), **Banco Mundial** y las experiencias revisadas de distintas economías, en materia de Gobierno Digital, podemos indicar que la determinación de una definición de gobierno digital en el ámbito nacional, la creación de la Secretaría de Gobierno Digital como ente rector del Sistema Nacional de Informática, se alinea a lo dispuesto en el Decreto Supremo N° 086-2015-PCM, mediante la cual se "Declaran de interés nacional las acciones, actividades e iniciativas desarrolladas en el marco del proceso de vinculación del Perú con la Organización para la Cooperación y Desarrollo Económico (OCDE) (...)", segundo, fortalece los marcos de gobernanza y coordinación para facilitar el despliegue del gobierno digital a nivel nacional en los tres niveles de gobierno y tercero, se evidencia la voluntad del gobierno por articular de manera adecuada los esfuerzos y acciones en materia de gobierno digital y modernización.

b. Se establece un régimen jurídico aplicable al uso de tecnologías digitales en las entidades de la Administración Pública

La propuesta normativa establece el **régimen jurídico,** de carácter especial, que, por un lado, complementa al régimen del procedimiento administrativo general (**norma de carácter general**), y por otro, encuadra el disperso conjunto de normas en materia de digitalización y gobierno digital. Como resultado de esto, se habilita a las entidades, desde una perspectiva legal, viabilizar iniciativas y acciones en pro de eficiencias en los diferentes entes y niveles que la comprenden, en particular como resultado de adoptar progresivamente las tecnologías digitales en sus procesos operativos y servicios, en el marco del proceso de Transformación Digital del Estado Peruano; con lo cual se espera puedan desarrollar servicios digitales de valor para los ciudadanos, en condiciones interoperables, seguras, confiables y facilitando la transparencia en un entorno de Gobierno Digital.

c. Se establece el marco legal para el reconocimiento de la Identidad Digital ante trámites, procedimientos y servicios digitales

La promulgación de la propuesta normativa establece el marco legal que permite el reconocimiento y la formalización de la identidad digital, sino que, además, permita brindar un

62

contexto legal apropiado para que la Administración pueda prestar sus servicios digitales en torno a la identidad digital bajo un "enfoque centrado en las personas"; lo cual reviste importancia, toda vez que el proceso de "identificación" participa al inicio de todo trámite, procedimiento o servicio digital.

Más aún, podemos encontrar entre los beneficios y usos de la Identidad Digital, lo siguiente:

- **Desde una perspectiva del ciudadano:**
  - Habilitar la Identificación fehaciente (autenticación de la identidad) ante la administración pública como ante organizaciones privadas;
  - Promover la confianza en el entorno digital, habilitando el acceso seguro a servicios públicos digitales y, aquellos prestados por el sector privado.
  - Optimizar el tiempo usado para la realización de trámites públicos o privados.

- **Desde la perspectiva de la Administración Pública y de los privados:**
  - Habilitar la Identificación fehaciente como funcionario público en atención del ciudadano y del sector privado;
  - Generar mejoras de la gestión al reducir tiempos y trámites presenciales propiciando la eficacia en la prestación de servicios.
  - Generar eficiencia en la gestión documental al desarrollar esquemas de documentación electrónicos válidos (cero papel), generando de una parte ahorros propios del uso del papel y, de otra, mitigando riesgos como la "suplantación de identidad", "alteración de documentos", "pérdida de confidencialidad en los documentos y expedientes", "rechazo o repudio", "negación de recepción" y "conflictos en la fecha y hora".
  - Habilita mejoras en la gestión de los programas sociales al disponerse de un mecanismo digital confiable para la adecuada identificación de los beneficiarios.

d. Promueve iniciativas para reducir la brecha digital y ampliar el alcance de los servicios públicos a nivel nacional

Sobre este punto, es preciso indicar que según estudios realizados por "**Oficina del Gabinete del Reino Unido**", se ha determinado que los servicios digitales tienen el potencial de ser accedidos y usados por más ciudadanos, lo cual cobra mayor relevancia en un contexto en el cual cerca de 82% de su población usa frecuentemente internet. En esa línea, según cifras del Instituto Nacional de Estadística e Informática - INEI[120], para el caso peruano a marzo del 2017, tenemos que cerca del **40.7%** del total de **hogares** tiene acceso a una computadora, mientras que **34%** de ellas tiene acceso a internet; por otro lado, al 2016, cerca del 45.5% de la población de seis años a más hace uso de internet, lo cual genera una oportunidad enorme para promover un mayor acercamiento al ciudadano y reducción de la brecha digital, mediante la provisión de servicios digitales.

Asimismo, entendiendo que por temas de capacidades, habilidades o acceso existirá un porcentaje de la población que no acceda a servicios digitales se ha establecido el deber de las entidades de la administración pública la provisión de espacios o centros de acceso para el fortalecimiento de capacidades o acceso a servicios digitales.

e. Uso eficiente de los recursos públicos, mediante ahorros generados por el uso de canales digitales

Según estudios[121] realizados por el Banco Mundial para el documento "**Digital Government 2020 – Prospects for Russia**", se ha establecido que es mucho más económico utilizar los canales digitales que los canales presenciales, tal como se muestra en la siguiente tabla:

[120] El documento puede ser consultado en: https://www.inei.gob.pe/estadisticas/indice-tematico/tecnologias-de-la-informacion-y-telecomunicaciones/
[121] El documento puede ser consultado en: **http://www.iis.ru/en/docs/2016-05-05_hohlov.pdf**

63

Canal	Costo Relativo
Digital	1
Telefónico	20
Correo	30
Presencial	50

Tabla 3.- **Fuente**: Elaboración SEGDI, en base a investigación del Instituto para el Desarrollo de la Sociedad de la Información (IIS) de Rusia, el mismo que puede ser consultado en: https://bit.ly/2mBhK6B

Lo anterior implicaría, por ejemplo, que por cada por cada sol que cueste la prestación de un servicio digital en Rusia, su equivalente en el mundo presencial varía entre veinte (20) a cincuenta (50) soles, estamos hablando de una proporción en ahorros de recursos de **alto impacto en nuestras arcas.**

Para la presente propuesta normativa podemos citar los "**beneficios**", **entiéndase ahorros y uso eficiente de recursos**, generados por la Plataforma de Interoperabilidad del Estado Peruano - PIDE, la cual provee a las entidades de la administración pública acceso de manera gratuita, a través de la interoperabilidad información actualizada que administre, recabe, sistematice, creen o posean respecto de usuarios o administrados, que las demás entidades requieran para la tramitación de sus **procedimientos administrativos** o para sus **actos de administración interna**, en pleno respeto y cumplimiento de las leyes, normas y disposiciones en materia de **Protección de datos Personales, Transparencia, etc.** Así, podemos mencionar, por ejemplo los ahorros generados por la PIDE durante el semestre **ENE-JUN 2018**, solo provenientes de cinco (05) servicios de información, proporcionados por cinco (05) entidades, las cuales han sido consumidas en promedio por 47 entidades a nivel nacional, generando ahorros aproximados de **81 millones de soles.**

Estadisticas de Transacciones que las entidades utilizan por servicios PIDE (5 servicios)

Primer Semestre (ENE-JUN 2018)

Item	Entidad Proveedora	Nombre del Servicio	Ope. Enero	Ope. Febrero	Ope. Marzo	Ope. Abril	Ope. Mayo	Ope. Junio	Total Ope.	Costo por Ope. Canal Digital (Cd)	Costo por Tramite Canal Presencial (CP)	Costo Total por usar Canal Digital (Cd)	Costo Total por usar Tramite Canal Presencial (CP)	Ahorros Generados
1	PODER JUDICIAL	Validación de Antecedentes Penales	34383	38489	38489	34125	34923	34200	212609	S/. 1.60	S/. 52.80	S/. 340,174.40	S/. 11,225,755.20	S/. 10,885,580.80
2	INPE	Consulta de Antecedentes Judiciales	919	8253	12480	13525	15163	18520	68840	S/. 1.60	S/. 37.00	S/. 110,144.00	S/. 2,547,080.00	S/. 2,436,936.00
3	MININTER	Antecedentes Policiales	1169	3580	5310	7801	7950	8359	34169	S/. 1.60	S/. 17.00	S/. 54,670.40	S/. 580,873.00	S/. 526,202.60
4	SUNARP	Titularidad de Dominio / Vigencia de Poder	167978	230325	220325	23996	240325	274404	1157353	S/. 1.60	S/. 60.00	S/. 1,851,764.80	S/. 69,441,180.00	S/. 67,589,415.20
5	SUNEDU	Consulta de Grados	2038	2210	3200	3901	4100	5200	20649	S/. 1.60	S/. 9.00	S/. 33,038.40	S/. 185,841.00	S/. 152,802.60
Ahorros Generados														S/. 81,590,937.20

*Tabla 4.- **Fuente**: Elaboración SEGDI, en base a información de la SSTED julio 2018*

Es importante mencionar que para los cálculos de los ahorros generados se tomó como referencia la tarifa establecida por **RENIEC** empresas privadas sobre la consulta en línea vía internet para consultar información sobre: número de DNI, primer apellido, segundo apellido, prenombre, lugar de nacimiento, fecha de nacimiento, estatura, sexo, estado civil, grado de instrucción, fecha de emisión de documento, restricciones y constancia de votación, la misma que varía entre S/. 1.60 a S/. 2.50 por consulta.

*f. **Demuestra el compromiso y voluntad política por el desarrollo del Gobierno Digital***

Cada dos años, el Departamento de Asuntos Económicos y Sociales de la ONU elabora el Estudio de Gobierno Electrónico de sus Estados miembros (193 aproximadamente). Para dicho estudio la ONU define un indicador conocido «**Índice de Desarrollo de Gobierno Electrónico (IDGE)**», el cual es el promedio ponderado de tres (3) sub índices normalizados, los cuales corresponden a tres dimensiones: 1. **Servicios en Línea**[122] (**Online Service - Servicios Digitales**), 2. Infraestructura de Telecomunicaciones (Telecommunication Infrastructure) y 3. Capital Humano (Human Capital).

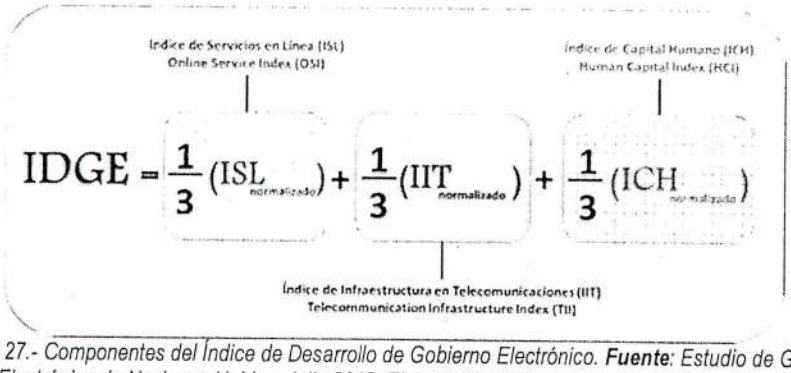

*Gráfico 27.- Componentes del Índice de Desarrollo de Gobierno Electrónico. **Fuente**: Estudio de Gobierno Electrónico de Naciones Unidas. Julio 2018. Elaboración SEGDI en base al referido Estudio*

Ahora bien, cuanto más el IDGE se acerque al valor de uno, el país muestra un mayor nivel de desarrollo en gobierno electrónico; mientras que cuando el valor está más cerca a cero, el país muestra un menor compromiso por desarrollar el gobierno electrónico.

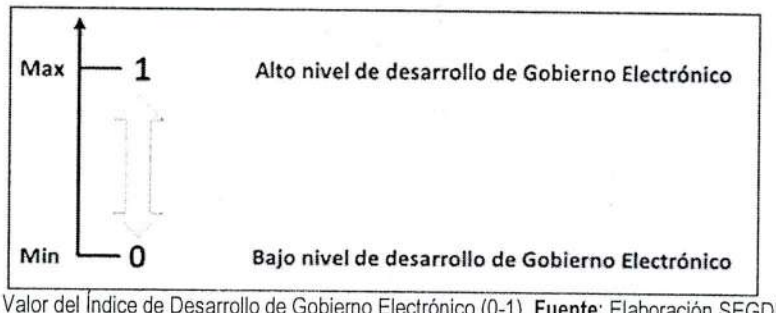

Gráfico 28.- Valor del Índice de Desarrollo de Gobierno Electrónico (0-1). **Fuente**: Elaboración SEGDI en base a información del Estudio de Gobierno Electrónico julio 2018

En línea con lo anterior, es importante referir que el estudio evalúa entre muchas otras si contamos con un portal nacional de ventanilla única, información sobre funcionarios del gobierno responsables de la provisión de servicios o consultas en línea; y por otro lado, **si es que nuestros servicios digitales** tienen formularios en línea, permiten el uso de certificados digitales para poder firmar digitalmente, son accesibles para personas con discapacidad, permiten el pago en línea (mediante tarjeta de crédito o débito); y no menos importante si contamos con una **política de participación electrónica que permita a los ciudadanos expresar su opinión sobre servicios públicos, política o estrategias.**

Consistente con lo anterior, la presente propuesta normativa denota la voluntad política por obtener mayores niveles de eficiencia, eficacia, y productividad de los procesos de las entidades, organizaciones, empresas públicas; así como también promover la prestación de servicios digitales seguros, confiables, accesibles a los ciudadanos; procurando además, establecer canales para promover la participación ciudadana por medios digitales.

[122] En el contexto del Estudio de la ONU, servicio electrónico, servicio en línea o servicio público digita, se refiere a aquellos servicios públicos que son ofrecidos de forma total o parcial a través de plataformas TICs.

65

Visto lo anterior, la presente propuesta normativa **es de alto impacto y sumamente beneficiosa para los ciudadanos y sociedad en general, toda vez, que permitirá establecer el régimen jurídico aplicable al uso de tecnologías digitales en las entidades de la Administración Pública**, mediante la cual la prestación y el acceso de la ciudadanía a los servicios digitales en condiciones interoperables, seguras, confiables y facilitando la transparencia tendrá un sustento jurídico y una sólida base legal que permita el despliegue de iniciativas en materia de simplificación administrativa, digitalización de procesos, documentos e información. Más aun, nos permitirá mejorar en los indicadores internacionales tales como el de la Organización de las Naciones Unidas - ONU, Foro Económico Mundial - WEF, Banco Mundial - BM, Organización para la Cooperación y el Desarrollo Económicos (OCDE), entre otros.

Asimismo, y a propósito del estado actual de los avances tecnológicos, la *Identidad Digital* puede acreditarse mediante diferentes credenciales dependiendo del entorno o contexto bajo el que nos encontremos; no obstante, el RENIEC otorga a los peruanos el DNI electrónico como credencial OFICIAL basada en certificados digitales emitidos bajo las exigencias de la Infraestructura Oficial de Firma Electrónica, brindándole así en el mundo virtual (*no presencial*) la seguridad jurídica que hoy dicha entidad brinda en el ámbito presencial, posibilitando la autenticación de la identidad y, en su caso, la manifestación de la voluntad en medios electrónicos, de manera confiable y segura.

En tal orden de cosas, cabe mencionar que el RENIEC ha dado inicio a la masificación del DNIe dentro de lo que significa el proceso evolutivo del documento de identidad y, a la vez, a la prestación de servicios de certificación digital que permitan el soporte para los servicios digitales en una administración y gobierno digital.

Asimismo, la Ley busca mitigar el impacto económico y el impacto en la confianza de los ciudadanos que suponen los riesgos asociados con la adopción de las TIC en las comunicaciones electrónicas, riesgos tales como la "*suplantación*", "*alteración*", "*pérdida de confidencialidad*", "*rechazo o repudio*", "*negación de recepción*" y "*conflictos en la fecha y hora*", así como su repercusión sobre la incidencia probatoria y validez jurídica. Por ello, el beneficio esperado es mitigar dichos riesgos y propiciar el empleo de las tecnologías digitales en el ámbito administrativo fomentando la confianza en los servicios digitales prestados por la administración pública "*...que la información, los datos y las identidades digitales se utilizan de modo confiable y respetando la integridad, la autenticidad y la privacidad como requisitos básicos para una mayor aceptación*" en el país, y a su vez en terceros países o bloques de estos.

Sin embargo, implementar la identidad digital y sus temas asociados como garantizar la seguridad de la información y generar servicios digitales, tiene unos costos que se diluyen y entremezclan dentro de implementaciones de servicios digitales tanto por su complejidad, como por su alcance e impacto variados, donde además el mercado local de proveedores de tecnologías para la identidad digital es incipiente aún, por lo que sus costos son variables y sus tasas de variación indeterminadas, empero donde, a su vez, existen costos ya realizados (hundidos) tanto por el RENIEC como por la Autoridad Administrativa Competente de la IOFE a cargo del Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual - INDECOPI en componentes de infraestructura que son de uso común para la firma digital y la identidad digital, especialmente para el ámbito público.

Así, una estimación de los costos resulta bastante difícil y compleja, y la estimación cuantitativa del total de beneficios de la identidad digital sería imposible en la práctica toda vez que los beneficios alcanzan tanto al Estado como a la ciudadanía y al sector privado y que dichos beneficios se diluyen y entremezclan dentro de implementaciones de servicios digitales de complejidad, alcance e impacto variados. Sin embargo, los beneficios se presentan en una espiral creciente de nuevos beneficios que surgen de las ventajas y ahorros que se derivan de los primeros, ello en razón que los nuevos usos y aplicaciones de la identidad digital aparecen cada día, al igual que la implementación de nuevas soluciones basadas en ésta, siendo que la identidad digital ofrece beneficios intangibles de alto impacto como el acceso a derechos, el incremento de la seguridad (jurídica y de otros tipos) y de la confianza, los que no se pueden cuantificar.

En tal sentido, con la propuesta normativa se materializa no sólo el acceso de las personas a los servicios digitales haciendo uso de su identidad digital, sino también acercar el Estado a las personas como parte de la estrategia del país en su transformación digital y de una efectiva instauración del Gobierno Digital.

De otro lado, con el Decreto Supremo N° 181-2018-EF se aprobó la operación de Endeudamiento Externo con el BID por la suma de US$ 50 000 000,00 (CINCUENTA MILLONES Y 00/100 DOLARES AMERICANOS), los cuales serán destinados a financiar parcialmente el Proyecto "Mejoramiento y Ampliación de los Servicios de Soporte para la Provisión de los Servicios a los Ciudadanos y las Empresas, a Nivel Nacional", siendo la Unidad Ejecutora de dicho proyecto la Presidencia del Consejo de Ministros.

En efecto, el objetivo general del proyecto es mejorar y ampliar los servicios de soporte para la prestación de servicios a ciudadanos y empresas, reduciendo los costos de transacción. Esto contribuirá a la mejora del grado de satisfacción de los ciudadanos y la mejora del clima de negocios. Los objetivos específicos son: (i) simplificación, estandarización y mejora regulatoria; (ii) mejora y ampliación de las capacidades de interoperabilidad de las entidades del Estado; (iii) mejora de la gestión en la atención a ciudadanos y empresas; y (iv) mejora de las condiciones para la planificación y coordinación de los servicios.

En particular, el Componente (ii): Mejora y ampliación de las capacidades de interoperabilidad de las entidades del Estado (US$14,5 millones), el mismo que tiene como objetivo promover la interoperabilidad efectiva entre bases de datos del Estado para apoyar una mejora y ampliación de la oferta de servicios digitales a ciudadanos y empresas. Con este fin, se financiarán actividades en las siguientes líneas de acción: (i) mejoramiento y ampliación de las capacidades de interoperabilidad técnica, a través del fortalecimiento de la PIDE, actualizando el hardware, software y mecanismos de seguridad; (ii) ampliación de las capacidades de interoperabilidad organizacional de la PIDE; desarrollando herramientas para su gestión, promoviendo la integración de servicios complejos; (iii) integración de bases de datos de ciudadanos; a través de la implementación de la Carpeta Ciudadana y la integración de información de los canales de atención al ciudadano; (iv) digitalización de documentación institucional prioritaria, incluyendo su organización, descripción y selección previa, así como, el diseño de un sistema gestor de archivos; y (v) mejoramiento de la seguridad de la información, mediante equipamiento para la PIDE y el desarrollo de procedimientos y estándares.

Asimismo, el Componente (iii) Mejora de la gestión en la atención a ciudadanos y empresas (US$ 24,4 millones), tienen por objetivo mejorar la calidad en la atención de los servicios públicos. Con este fin, se financiarán actividades, entre otros, (iii) mejora de la atención a los ciudadanos a través de los portales del Estado; incluyendo la mejora de la infraestructura tecnológica de los portales del Estado y la implementación del portal Gob.pe, de asistencia técnica en la digitalización de servicios priorizados.

De otra parte, el Componente (iv) Mejora de las condiciones para la planificación y coordinación de los servicios (US$ 8,7millones), tiene como objetivo mejorar las condiciones para la planificación de los servicios públicos, a través de: (a) la mejor articulación multisectorial e intergubernamental, (b) la mejor capacidad de gestión de conflictos y (c) la disponibilidad de mejores instrumentos para la gestión territorial, con este fin, se financiarán las siguientes líneas de acción: en los que respecta al literal (a) se financiarán actividades para: i) gestionar adecuadamente el cumplimiento de las políticas prioritarias del gobierno; ii) contar con mecanismos de coordinación de políticas multisectoriales; y iii) contar con agencias de desarrollo regional; en lo que respecta al literal (b) se financiará actividades para: iv) crear un sistema de información para prevención y gestión de factores de riesgos de conflictos, diseñar herramientas para prevención de conflictos y desarrollar talleres de capacitación para implementación de herramientas. Al respecto, en lo que relacionado con el literal (c) se financiará actividades para v) contar con información geoespacial y registros administrativos y estadísticos de infraestructura de servicios básicos estandarizados (Infraestructura de Datos Espaciales del Perú-

67

IDEP y Sayhuite), aspectos estos últimos que son administrados por la SEGDI y que se verán mejorados y potenciados.

El impacto del proyecto será un aumento del nivel de satisfacción de los usuarios con los servicios públicos, siendo la meta que el nivel de percepción sobre la burocracia gubernamental, como factor problemático, se reduzca y que el nivel de satisfacción de los usuarios del interior del país se incremente.

Adicionalmente, la Presidencia del Consejo de Ministros suscribió con el Ministerio del Interior de la República de Corea del Sur un Memorándum de Entendimiento 2017 (MOU), para promover la cooperación y el intercambio de experiencias en el ámbito del Gobierno Electrónico mediante el establecimiento y funcionamiento del Centro de Cooperación de Gobierno Electrónico Corea – Perú, el cual viene funcionando en las instalaciones de la PCM, y se estableen los compromisos y proyectos a ejecutarse en dicho centro hasta el año 2020. La implementación de lo anterior se viene realizando a través de la cooperación no reembolsable de la República de Corea del Sur por un monto de US$ 1 000 000 (UN MILLÓN DE DÓLARES AMERICANOS) hasta el año 2020.

Finalmente, hay que señalar que la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, viene desarrollando acciones para el despliegue del Gobierno Digital y transformación digital en la Administración Pública.

IV. ANÁLISIS DE IMPACTO DE LA VIGENCIA DE LA NORMA EN LA LEGISLACIÓN NACIONAL

La norma propuesta no deroga ni modifica norma con rango legal vigente de nuestro ordenamiento jurídico puesto que, como ya se ha indicado, por un lado, mediante Decreto Legislativo N° 604 ya se ha creado el Sistema Nacional de Informática, mientras que a través del Decreto Supremo N° 022-2017-PCM y Decreto Supremo N° 033-2018-PCM se ha establecido que la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, es el Líder Nacional de Gobierno Digital encargado de dirigir, evaluar y supervisar el proceso de transformación digital y dirección estratégica del Gobierno Digital, para lo cual en el ejercicio de sus funciones promueve espacios de coordinación con representantes de la administración pública, sector privado, academia, sociedad civil organizada y ciudadanos con la finalidad de optimizar el uso de las tecnologías digitales aplicadas a la modernización de la gestión del Estado.

Más aún, el impacto de la presente propuesta es claramente positivo porque damos cumplimiento a lo indicado en el ítem d.3) del literal d) del numeral 5 del artículo 2 de la Ley N° 30823.

PODER EJECUTIVO

DECRETOS LEGISLATIVOS

DECRETO LEGISLATIVO Nº 1412

EL PRESIDENTE DE LA REPÚBLICA

POR CUANTO:

Que, mediante Ley N° 30823, el Congreso de la República ha delegado en el Poder Ejecutivo la facultad de legislar en materia de gestión económica y competitividad, de integridad y lucha contra la corrupción, de prevención y protección de personas en situación de violencia y vulnerabilidad y de modernización de la gestión del Estado, por el plazo de sesenta (60) días calendario;

Que, el literal d) numeral 5 del artículo 2, de la citada Ley faculta al Poder Ejecutivo para legislar en materia de modernización del Estado, a fin de implementar servicios y espacios compartidos por parte de las entidades públicas, así como establecer disposiciones para el gobierno digital y las plataformas multiservicios y de trámites que faculten a las entidades públicas para delegar la gestión y resolución de actos administrativos a otras entidades públicas bajo criterios que prioricen eficiencia, productividad, oportunidad y mejora de servicios para el ciudadano y la empresa; o a terceros, en las etapas previas a la emisión de la resolución que contenga la decisión final de la entidad;

Que, el ítem d.3) del literal d) del numeral 5 del artículo 2 de la citada norma establece la facultad de legislar para establecer el marco normativo para promover el despliegue transversal de las tecnologías digitales en las entidades del Estado; a fin de mejorar el alcance, condiciones, la prestación y el acceso de los ciudadanos a los servicios que presta el Estado;

Que, la Política 35 del Acuerdo Nacional, sobre Sociedad de la Información y Sociedad del Conocimiento, señala en el literal e) que el Estado fomentará la modernización del Estado, mediante el uso de las Tecnologías de la Información y la Comunicación (TIC), con un enfoque descentralista, planificador e integral;

Que, mediante el Decreto Supremo N° 086-2015-PCM, se declara de interés nacional las acciones, actividades e iniciativas desarrolladas en el marco del proceso de vinculación del Perú con la Organización para la Cooperación y el Desarrollo Económicos (OCDE) e implementación del Programa País, y crea la Comisión Multisectorial de naturaleza permanente para promover las acciones de seguimiento del referido proceso, y comprende la participación del Estado peruano en las actividades previstas en el Acuerdo y Memorando de Entendimiento suscritos entre la OCDE y el Gobierno del Perú, así como todas las demás actividades relacionadas con la organización, promoción, impulso y apoyo al referido proceso;

Que, las tecnologías digitales y el gobierno digital son conceptos integrados en las actividades, lenguaje y estructuras de la sociedad actual, y hacen parte del proceso de vinculación del Perú con la Organización para la Cooperación y el Desarrollo Económicos (OCDE), organización que entiende su uso estratégico como parte integral del diseño de políticas y estrategias de modernización del gobierno, con la finalidad de crear servicios digitales de valor, seguros, confiables y accesibles para los ciudadanos y sociedad en general, lo cual se sustenta en un ecosistema compuesto por actores del sector público, sector privado, academia y otros interesados, quienes apoyan en la implementación de iniciativas y acciones para diseño, creación, producción de datos, servicios y contenidos, asegurando el pleno respeto los derechos de las personas en el entorno digital;

Que mediante Decreto Legislativo N° 604, se aprueba la Ley de Organización y Funciones del Instituto Nacional de Estadística e Informática - INEI, que crea el Sistema Nacional de Informática el cual tiene como objetivos normar las actividades de informática; coordinar, integrar y racionalizar las actividades de informática; y promover la capacitación, investigación y desarrollo de las actividades de informática;

Que, conforme lo establecido en el artículo 47 del Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros, aprobado mediante Decreto Supremo N° 022-2017-PCM, la Secretaría de Gobierno Digital - SEGDI 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. Asimismo, es el órgano rector del Sistema Nacional de Informática;

Que, dentro de este contexto, es necesario adecuar la gobernanza y gestión del gobierno digital en el Estado Peruano y mejorar la articulación en los tres niveles de gobierno, para lo cual resulta indispensable establecer el marco normativo que regule y habilite a las entidades del Estado integrar de manera intensiva las tecnologías digitales para la prestación de servicios digitales en condiciones seguras, confiables, transparentes, interoperables en un entorno de gobierno digital;

De conformidad con lo establecido en el literal d) del numeral 5 del artículo 2 de la Ley N° 30823 y el artículo 104 de la Constitución Política del Perú;

Con el voto aprobatorio del Consejo de Ministros; y,

Con cargo de dar cuenta al Congreso de la República;

Ha dado el Decreto Legislativo siguiente:

DECRETO LEGISLATIVO QUE APRUEBA LA LEY DE GOBIERNO DIGITAL

TÍTULO I

DISPOSICIONES GENERALES

Artículo 1.- Objeto

La presente Ley tiene por objeto establecer 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.

Artículo 2.- Ámbito de aplicación

2.1. La presente Ley es de aplicación a toda entidad que forma parte de la Administración Pública a que se refiere el artículo I del Título Preliminar del Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General. Sus regulaciones también alcanzan a las personas jurídicas o naturales que, por mandato legal, encargo o relación contractual ejercen potestades administrativas, y por tanto su accionar se encuentra sujeto a normas de derecho público, en los términos dispuestos por la Presidencia del Consejo de Ministros.

2.2. En el caso de las empresas que conforman la actividad empresarial del Estado, su aplicación se da en todo aquello que le resulte aplicable.

Artículo 3.- Definiciones

Para efectos de la presente Ley, se adoptan las siguientes definiciones:

1. **Tecnologías Digitales.-** Se refieren a las Tecnologías de la Información y la Comunicación - TIC, incluidos Internet, las tecnologías y dispositivos móviles, así como la analítica de datos utilizados para mejorar la generación, recopilación, intercambio, agregación, combinación, análisis, acceso, búsqueda y presentación de contenido digital, incluido el desarrollo de servicios y aplicaciones aplicables a la materia de gobierno digital.

2. **Entorno Digital.-** Es el dominio o ámbito habilitado por las tecnologías y dispositivos digitales,

generalmente interconectados a través de redes de datos o comunicación, incluyendo el Internet, que soportan los procesos, servicios, infraestructuras y la interacción entre personas.

3. **Servicio Digital.-** Es aquel provisto de forma total o parcial a través de Internet u otra red equivalente, que se caracteriza por ser automático, no presencial y utilizar de manera intensiva las tecnologías digitales, para la producción y acceso a datos y contenidos que generen valor público para los ciudadanos y personas en general.

4. **Canal Digital.-** Es el medio de contacto digital que disponen las entidades de la Administración Pública a los ciudadanos y personas en general para facilitar el acceso a toda la información institucional y de trámites, realizar y hacer seguimiento a servicios digitales, entre otros. Este canal puede comprender páginas y sitios web, redes sociales, mensajería electrónica, aplicaciones móviles u otros.

5. **Ciudadano Digital.-** Es aquel que hace uso de las tecnologías digitales y ejerce sus deberes y derechos en un entorno digital seguro.

6. **Gobernanza Digital.-** Es el conjunto de procesos, estructuras, herramientas y normas que nos permiten dirigir, evaluar y supervisar el uso y adopción de las tecnologías digitales en la organización.

7. **Arquitectura Digital.-** Es el conjunto de componentes, lineamientos y estándares, que desde una perspectiva integral de la organización permiten alinear los sistemas de información, datos, seguridad e infraestructura tecnológica con la misión y objetivos estratégicos de la entidad, de tal manera que se promuevan la colaboración, interoperabilidad, escalabilidad, seguridad y el uso optimizado de las tecnologías digitales en un entorno de gobierno digital.

Artículo 4.- Finalidad

La presente Ley tiene por finalidad:

4.1 Mejorar la prestación y acceso de servicios digitales en condiciones interoperables, seguras, disponibles, escalables, ágiles, accesibles, y que faciliten la transparencia para el ciudadano y personas en general.

4.2 Promover la colaboración entre las entidades de la Administración Pública, así como la participación de ciudadanos y otros interesados para el desarrollo del gobierno digital y sociedad del conocimiento.

Artículo 5.- Principios rectores

Las disposiciones contenidas en la presente Ley, así como su aplicación se rigen por los siguientes principios rectores:

5.1 **Especialidad.-** La presente norma es aplicable a los servicios digitales prestados por las entidades de la Administración Pública en un entorno de gobierno digital, sin perjuicio de lo regulado para los procedimientos administrativos u otros que se rigen por su propia normatividad.

5.2 **Equivalencia Funcional.-** El ejercicio de la identidad digital para el uso y prestación de servicios digitales confiere y reconoce a las personas las mismas garantías que otorgan los modos tradicionales de relacionarse entre privados y/o en la relación con las entidades de la Administración Pública.

5.3 **Privacidad desde el Diseño.-** En el diseño y configuración de los servicios digitales se adoptan las medidas preventivas de tipo tecnológico, organizacional, humano y procedimental.

5.4 **Igualdad de Responsabilidades.-** Las entidades de la Administración Pública responden por los actos realizados a través de canales digitales de la misma manera y con iguales responsabilidades que por los realizados a través de medios presenciales.

5.5 **Usabilidad.-** En el diseño y configuración de los servicios digitales se propenderá a que su uso resulte de fácil manejo para los ciudadanos y personas en general.

5.6 **Cooperación Digital.-** Prima el intercambio de datos e información, la interoperabilidad de los sistemas y soluciones para la prestación conjunta de servicios digitales.

5.7 **Digital desde el Diseño.-** Los servicios, de manera preferente, progresiva y cuando corresponda, se diseñan y modelan para que sean digitales de principio a fin.

5.8 **Proporcionalidad.-** Los requerimientos de seguridad y autenticación de los servicios digitales prestados por las entidades de la Administración Pública deben ser proporcionales al nivel de riesgo asumido en la prestación del mismo.

5.9 **Datos Abiertos por Defecto.-** Los datos se encuentran abiertos y disponibles de manera inmediata, sin comprometer el derecho a la protección de los datos personales de los ciudadanos. Ante la duda corresponde a la Autoridad de Transparencia definirlo.

5.10 **Nivel de protección adecuado para los datos personales.-** El tratamiento de los datos personales debe realizarse conforme a lo establecido en la Ley de Protección de Datos Personales y su Reglamento.

TÍTULO II

GOBIERNO DIGITAL

CAPÍTULO I

GOBIERNO DIGITAL

Artículo 6.- Gobierno Digital

6.1. El gobierno digital es el uso estratégico de las tecnologías digitales y datos en la Administración Pública para la creación de valor público. Se sustenta en un ecosistema compuesto por actores del sector público, ciudadanos y otros interesados, quienes apoyan en la implementación de iniciativas y acciones de diseño, creación de servicios digitales y contenidos, asegurando el pleno respeto de los derechos de los ciudadanos y personas en general en el entorno digital.

6.2. Comprende el conjunto de principios, políticas, normas, procedimientos, técnicas e instrumentos utilizados por las entidades de la Administración Pública en la gobernanza, gestión e implementación de tecnologías digitales para la digitalización de procesos, datos, contenidos y servicios digitales de valor para los ciudadanos.

Artículo 7.- Objetivos del Gobierno Digital

Los objetivos del gobierno digital son:

7.1 Normar las actividades de gobernanza, gestión e implementación en materia de tecnologías digitales, identidad digital, servicios digitales, arquitectura digital, interoperabilidad, seguridad digital y datos.

7.2 Coordinar, integrar y promover la colaboración entre las entidades de la Administración Pública.

7.3 Promover la investigación y desarrollo en la implementación de tecnologías digitales, identidad digital, servicios digitales, interoperabilidad, seguridad digital y datos.

7.4 Promover y orientar la formación y capacitación en materia de gobierno digital y tecnologías digitales en todos los niveles de gobierno.

Artículo 8.- Ente Rector en materia de Gobierno Digital

La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, es el ente rector en materia de gobierno digital que comprende tecnologías digitales, identidad digital, interoperabilidad, servicio digital, datos, seguridad digital y arquitectura digital. Dicta las normas y establece los procedimientos en materia de gobierno digital y, es responsable de su operación y correcto funcionamiento.

Artículo 9.- Funciones del ente rector en materia de gobierno digital

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

9.1 Programar, dirigir, coordinar, supervisar y evaluar la aplicación de la materia de gobierno digital.

9.2 Elaborar y proponer normas reglamentarias y complementarias que regulan la materia de gobierno digital.

70

9.3 Elaborar lineamientos, procedimientos, metodologías, modelos, directivas u otros estándares de obligatorio cumplimiento para la implementación de las materias de gobierno digital.

9.4 Emitir opinión vinculante sobre el alcance, interpretación e integración de normas que regulan la materia de gobierno digital.

9.5 Emitir opinión previa a fin de validar técnicamente proyectos de tecnologías digitales de carácter transversal en materia de interoperabilidad, seguridad digital, identidad digital, datos, arquitectura digital o aquellos destinados a mejorar la prestación de servicios digitales.

9.6 Brindar apoyo técnico a las entidades públicas en la gestión e implementación de tecnologías digitales.

9.7 Definir los alcances del marco normativo en materia de gobierno digital.

9.8 Supervisar y fiscalizar, cuando corresponda, el cumplimiento del marco normativo en materia de gobierno digital.

9.9 Promover mecanismos que aseguren la identidad digital como pilar fundamental para la inclusión digital y la ciudadanía digital.

9.10 Promover y gestionar la implementación de proyectos de implementación de tecnologías digitales u otros mecanismos destinados a mejorar la prestación de servicios digitales, en coordinación con las entidades públicas, según corresponda.

9.11 Promover la digitalización de los procesos y servicios a partir del uso e implementación de tecnologías digitales.

9.12 Realizar acciones de coordinación y articulación con representantes de la administración pública, ciudadanos u otros interesados con la finalidad de optimizar el uso de tecnologías digitales para el desarrollo del gobierno digital y tecnologías digitales.

CAPÍTULO II

IDENTIDAD DIGITAL

Artículo 10.- De la Identidad Digital

10.1 La identidad digital es aquel conjunto de atributos que individualiza y permite identificar a una persona en entornos digitales.

10.2 Los atributos de la identidad digital son otorgados por distintas entidades de la Administración Pública que, en su conjunto, caracterizan al individuo.

Artículo 11.- Marco de Identidad Digital del Estado Peruano

El Marco de Identidad Digital del Estado Peruano está constituido por lineamientos, especificaciones, guías, directivas, estándares e infraestructura de tecnologías digitales, que permiten de manera efectiva la identificación y autenticación de los ciudadanos y personas en general cuando acceden a los servicios digitales.

Artículo 12.- Credencial de Identidad Digital

Es la representación de una identidad digital que comprende los atributos inherentes a la persona definidos en el Marco de Identidad Digital del Estado Peruano, a fin de facilitar la autenticación digital.

Artículo 13.- Identificación Digital

La identificación digital es el procedimiento de reconocimiento de una persona como distinta de otras, en el entorno digital. Las entidades de la Administración Pública deben establecer los procedimientos para identificar a las personas que accedan a los servicios digitales.

Artículo 14.- Autenticación Digital

La autenticación digital es el procedimiento de verificación de la identidad digital de una persona, mediante el cual se puede afirmar que es quien dice ser.

Para el acceso a un servicio digital las entidades de la Administración Pública deben adoptar los mecanismos o procedimientos de autenticación digital, considerando los niveles de seguridad a establecerse en la norma reglamentaria.

Artículo 15.- Inclusión digital

La inclusión digital es el acceso y uso de los servicios digitales por parte de los ciudadanos a través de su identidad digital, promoviendo la ciudadanía digital. Para tal fin las entidades de la Administración Pública adoptan las disposiciones que emite el ente rector para la prestación de dichos servicios.

Artículo 16.- Documento Nacional de Identidad electrónico (DNIe)

El Documento Nacional de Identidad Electrónico (DNIe) es una credencial de identidad digital, emitida por el Registro Nacional de Identificación y Estado Civil - RENIEC, que acredita presencial y no presencialmente la identidad de las personas.

Artículo 17.- Uso del Documento Nacional de Identidad electrónico

Los funcionarios y servidores públicos al servicio de las entidades de la Administración Pública pueden hacer uso del Documento Nacional de Identidad Electrónico (DNIe) para el ejercicio de sus funciones en los actos de administración, actos administrativos, procedimientos administrativos y servicios digitales.

El DNIe sólo otorga garantía sobre la identificación de la persona natural, mas no en el cargo, rol, atribuciones o facultades que ostenta un funcionario o servidor de una entidad de la Administración Pública; dicho funcionario o servidor público es el responsable de gestionar en su entidad las autorizaciones de acceso y asignación de roles, atribuciones o facultades para hacer uso del indicado DNIe en los sistemas de información que hagan uso del mismo.

CAPÍTULO III

PRESTACIÓN DE SERVICIOS DIGITALES

Artículo 18.- Garantías para la prestación de servicios digitales

Las entidades de la Administración Pública, de manera progresiva y cuando corresponda, deben garantizar a las personas el establecimiento y la prestación de los servicios digitales, comprendidos en el ámbito de aplicación de la presente Ley, debiendo para tal efecto:

18.1 Reconocer y aceptar el uso de la identidad digital de todas las personas según lo regulado en la presente Ley.

18.2 Garantizar la disponibilidad, integridad y confidencialidad de la información de los servicios digitales con la aplicación de los controles de seguridad que correspondan en la prestación de dichos servicios conforme a las disposiciones contenidas en la presente Ley y en la normatividad vigente sobre la materia.

18.3 Capacitar en temas en materia de firmas electrónicas, firmas y certificados digitales, protección de datos personales, interoperabilidad, arquitectura digital, seguridad digital, datos abiertos y gobierno digital.

18.4 Facilitar el acceso a la información requerida por otra entidad de la Administración Pública, sobre los datos de las personas que obren en su poder y se encuentren en soporte electrónico, únicamente para el ejercicio de sus funciones en el ámbito de sus competencias. Queda excluida del intercambio la información que pueda afectar la seguridad nacional o aquella relacionada con la legislación sobre Transparencia y Acceso a la Información Pública, o la que expresamente sea excluida por Ley.

18.5 Implementar servicios digitales haciendo un análisis de la arquitectura digital y rediseño funcional.

18.6 Considerar la implementación de pagos a través de canales digitales.

18.7 Facilitar a las personas información detallada, concisa y entendible sobre las condiciones de tratamiento de sus datos personales.

18.8 Garantizar la conservación de las comunicaciones y documentos generados a través de canales digitales en las mismas o mejores condiciones que aquellas utilizadas por los medios tradicionales.

18.9 Garantizar que en el diseño y configuración de los servicios digitales se adoptan las medidas técnicas,

organizativas y legales para la debida protección de datos personales y la confidencialidad de las comunicaciones.

Artículo 19.- Conservación de los documentos electrónicos firmados digitalmente

Para conservar documentos electrónicos y garantizar la perdurabilidad en el tiempo de la firma digital incorporada en aquellos se emplean sellos de tiempo y mecanismos basados en estándares internacionalmente aceptados que permitan verificar el estado del certificado digital asociado.

Cuando dicho tipo de documentos electrónicos, y sus respectivos formatos que aseguran la característica de perdurabilidad de la firma digital, deban ser conservados de modo permanente, éstos se archivarán observando las disposiciones legales sobre la materia.

Artículo 20.- Sede Digital

La sede digital es un tipo de canal digital, a través del cual pueden acceder los ciudadanos y personas en general a un catálogo de servicios digitales, realizar trámites, hacer seguimiento de los mismos, recepcionar y enviar documentos electrónicos, y cuya titularidad, gestión y administración corresponde a cada entidad de la Administración Pública en los tres niveles de gobierno.

Artículo 21.- Registro Digital

Las sedes digitales de las entidades de la Administración Pública cuentan con un registro digital para recibir documentos, solicitudes, escritos y comunicaciones electrónicas dirigidas a dicha entidad.

Artículo 22.- Domicilio Digital

Es uno de los atributos de la identidad digital que se constituye en el domicilio habitual de un ciudadano en el entorno digital, el cual es utilizado por las entidades de la Administración Pública para efectuar comunicaciones o notificaciones.

CAPÍTULO IV

GOBERNANZA DE DATOS

Artículo 23.- Datos

23.1 Los datos son la representación dimensionada y descifrable de hechos, información o concepto, expresada en cualquier forma apropiada para su procesamiento, almacenamiento, comunicación e interpretación.

23.2 Las entidades de la Administración Pública administran sus datos como un activo estratégico, garantizando que estos se recopilen, procesen, publiquen, almacenen y pongan a disposición durante el tiempo que sea necesario y cuando sea apropiado, considerando las necesidades de información, riesgos y la normatividad vigente en materia de gobierno digital, seguridad digital, transparencia, protección de datos personales y cualquier otra vinculante.

Artículo 24.- Infraestructura Nacional de Datos

La Infraestructura Nacional de Datos se define como el conjunto articulado de políticas, normas, medidas, procesos, tecnologías digitales, repositorios y bases de datos destinadas a promover la adecuada recopilación, procesamiento, publicación, almacenamiento y puesta a disposición de los datos que gestionan las entidades de la Administración Pública.

Artículo 25.- Marco de Gobernanza y Gestión de Datos del Estado Peruano

El Marco de Gobernanza y Gestión de Datos del Estado Peruano está constituido por instrumentos técnicos y normativos que establecen los requisitos mínimos que las entidades de la Administración Pública deben implementar conforme a su contexto legal, tecnológico y estratégico para asegurar un nivel básico y aceptable para la recopilación, procesamiento, publicación, almacenamiento y apertura de los datos que administre.

CAPÍTULO V

INTEROPERABILIDAD

Artículo 26.- Interoperabilidad

La Interoperabilidad es la capacidad de interactuar que tienen las organizaciones diversas y dispares para alcanzar objetivos que hayan acordado conjuntamente, recurriendo a la puesta en común de información y conocimientos, a través de los procesos y el intercambio de datos entre sus respectivos sistemas de información.

Artículo 27.- Marco de Interoperabilidad del Estado Peruano

El Marco de Interoperabilidad del Estado Peruano está constituido por políticas, lineamientos, especificaciones, estándares e infraestructura de tecnologías digitales, que permiten de manera efectiva la colaboración entre entidades de la Administración Pública para el intercambio de información y conocimiento, para el ejercicio de sus funciones en el ámbito de sus competencias, en la prestación de servicios digitales inter-administrativos de valor para el ciudadano provisto a través de canales digitales.

Artículo 28.- Gestión del Marco de Interoperabilidad del Estado Peruano

El Marco de Interoperabilidad del Estado Peruano se gestiona a través de los siguientes niveles:

28.1. **Interoperabilidad a nivel organizacional:** Se ocupa del alineamiento de objetivos, procesos, responsabilidades y relaciones entre las entidades de la Administración Pública para intercambiar datos e información para el ejercicio de sus funciones en el ámbito de sus competencias.

28.2 **Interoperabilidad a nivel semántico:** Se ocupa del uso de los datos y la información de una entidad garantizando que el formato y significado preciso de dichos datos e información a ser intercambiada pueda ser entendido por cualquier aplicación de otra entidad de la Administración Pública. Dichas entidades deben adoptar los estándares definidos por el ente rector para el intercambio de datos e información.

28.3. **Interoperabilidad a nivel técnico:** Se ocupa de los aspectos técnicos relacionados con las interfaces, la interconexión, integración, intercambio y presentación de datos e información, así como definir los protocolos de comunicación y seguridad. Es ejecutado por personal de las Oficinas de Informática o las que hagan sus veces de las entidades de la Administración Pública, de acuerdo con los estándares definidos por el ente rector.

28.4. **Interoperabilidad a nivel legal:** Se ocupa de la adecuada observancia de la legislación y lineamientos técnicos con la finalidad de facilitar el intercambio de datos e información entre las diferentes entidades de la Administración Pública, así como el cumplimiento de los temas concernientes con el tratamiento de la información que se intercambia.

Artículo 29.- Reutilización de Software

Las entidades de la Administración Pública titulares de Software Público Peruano, desarrollado mediante la contratación de terceros o por personal de la entidad para soportar sus procesos o servicios, adoptan las medidas necesarias a fin de obtener la titularidad exclusiva sobre los derechos patrimoniales del referido Software Público Peruano.

Todas las entidades de la Administración Pública deben compartir Software Público Peruano bajo licencias libres o abiertas que permitan (i) usarlo o ejecutarlo, (ii) copiarlo o reproducirlo, (iii) acceder al código fuente, código objeto, documentación técnica y manuales de uso, (iv) modificarlo o transformarlo en forma colaborativa, y (v) distribuirlo, en beneficio del Estado Peruano.

CAPÍTULO VI

SEGURIDAD DIGITAL

Artículo 30.- De la Seguridad Digital

La seguridad digital es el estado de confianza en el entorno digital que resulta de la gestión y aplicación de

un conjunto de medidas proactivas y reactivas frente a los riesgos que afectan la seguridad de las personas, la prosperidad económica y social, la seguridad nacional y los objetivos nacionales en dicho entorno. Se sustenta en la articulación con actores del sector público, sector privado y otros quienes apoyan en la implementación de controles, acciones y medidas.

Artículo 31.- Marco de Seguridad Digital del Estado Peruano

El Marco de Seguridad Digital del Estado Peruano se constituye en el conjunto de principios, modelos, políticas, normas, procesos, roles, tecnología y estándares mínimos que permitan preservar la confidencialidad, integridad, disponibilidad de la información en el entorno digital administrado por las entidades de la Administración Pública.

Artículo 32.- Gestión del Marco de Seguridad Digital del Estado Peruano

El Marco de Seguridad Digital del Estado Peruano tiene los siguientes ámbitos:

a. Defensa: El Ministerio de Defensa (MINDEF) en el marco de sus funciones y competencias dirige, supervisa y evalúa las normas en materia de ciberdefensa.

b. Inteligencia: La Dirección Nacional de Inteligencia (DINI) como autoridad técnica normativa en el marco de sus funciones emite, supervisa y evalúa las normas en materia de inteligencia, contrainteligencia y seguridad digital en el ámbito de esta competencia.

c. Justicia: El Ministerio de Justicia y Derechos Humanos (MINJUS), el Ministerio del Interior (MININTER), la Policía Nacional del Perú (PNP), el Ministerio Público y el Poder Judicial (PJ) en el marco de sus funciones y competencias dirigen, supervisan y evalúan las normas en materia de ciberdelincuencia.

d. Institucional: Las entidades de la Administración Pública deben establecer, mantener y documentar un Sistema de Gestión de la Seguridad de la Información (SGSI).

Artículo 33.- Articulación de la Seguridad Digital con la Seguridad de la Información

El Marco de Seguridad Digital del Estado Peruano 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 de la Información se enfoca en la información, de manera independiente de su formato y soporte. La seguridad digital se ocupa de las medidas de la seguridad de la información procesada, transmitida, almacenada o contenida en el entorno digital, procurando generar confianza, gestionando los riesgos que afecten la seguridad de las personas y la prosperidad económica y social en dicho entorno.

Artículo 34.- Financiamiento

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

Artículo 35.- Refrendo

El presente Decreto Legislativo es refrendado por el Presidente del Consejo de Ministros y el Ministro de Justicia y Derechos Humanos.

DISPOSICIONES COMPLEMENTARIAS FINALES

Primera.- Reglamentación

La Presidencia del Consejo de Ministros, mediante Decreto Supremo, aprueba el Reglamento del presente Decreto Legislativo en un plazo máximo de ciento ochenta (180) días, contados a partir del día siguiente de su publicación en el Diario Oficial El Peruano.

Segunda.- Normas sobre Identidad Digital Nacional

El Registro Nacional de Identificación y Estado Civil (RENIEC) en el ámbito de sus funciones y competencias emitirá las normas que resulten pertinentes para el otorgamiento, registro y acreditación de la identidad digital nacional. La Identidad Digital Nacional proporciona el mismo valor legal que el Documento Nacional de Identidad.

Tercera.- Fortalecimiento de capacidades

La Autoridad Nacional del Servicio Civil (SERVIR) en el ámbito de sus funciones y competencias, en coordinación con la Secretaría de Gobierno Digital, promueve el fortalecimiento de capacidades en materia de gobierno digital y tecnologías digitales a los funcionarios y servidores de las entidades de la Administración Pública.

Cuarta.- Registro de Centros de Acceso Público

Las entidades de la Administración Pública que implementan progresivamente, en función a sus recursos y capacidades, espacios o centros de acceso público, previstos en la Ley de Promoción de Banda Ancha y Construcción de la Red Dorsal Nacional de Fibra Óptica, con miras a fortalecer capacidades y facilitar el proceso de inclusión digital de los ciudadanos y personas en general el acceso a los servicios digitales deben comunicarlo a la Secretaría de Gobierno Digital para el registro respectivo.

Entiéndase que toda referencia a los Centros de Acceso Ciudadano previstos en el Reglamento de la Ley de Firmas y Certificados Digitales se entenderá hecha al Centro de Acceso Público previsto en la presente norma.

Quinta.- Vigencia

El presente Decreto Legislativo entra en vigencia a partir del día siguiente de su publicación, con excepción de lo previsto en los artículos 11, 12, 14, 15, 19, 20, 21, 22, 25, 27, 31 y numerales 18.1, 18.5, 18.6 y 18.8 del artículo 18, que entrarán en vigor con la norma reglamentaria correspondiente.

DISPOSICIONES COMPLEMENTARIAS TRANSITORIAS

Primera.- Credencial de Identidad Digital

Las entidades de la Administración Pública pueden hacer uso de los mecanismos existentes para la autenticación de las personas en entornos digitales dentro de un contexto determinado, conforme a los lineamientos, progresividad y plazos a establecerse en el reglamento del presente Decreto Legislativo.

Segunda.- Servicios Digitales

Las entidades de la Administración Pública que a la fecha de entrada en vigencia del presente Decreto Legislativo hayan implementado y brinden servicios digitales adoptan y adecuan las disposiciones de los mismos de manera progresiva conforme a sus recursos, capacidades, lineamientos y plazos a establecerse en el reglamento de la presente Ley, sin perjuicio de lo establecido en el numeral 5.1 del artículo 5 del presente Decreto Legislativo.

POR TANTO:

Mando se publique y cumpla, dando cuenta al Congreso de la República.

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

MARTÍN ALBERTO VIZCARRA CORNEJO
Presidente de la República

CÉSAR VILLANUEVA ARÉVALO
Presidente del Consejo de Ministros

VICENTE ANTONIO ZEBALLOS SALINAS
Ministro de Justicia y Derechos Humanos

1691026-1

"Decenio de la Igualdad de oportunidades para mujeres y hombres"
"Año del Diálogo y la Reconciliación Nacional"

Lima, 13 de setiembre de 2018

OFICIO Nº 243 -2018 -PR

Señor
DANIEL SALAVERRY VILLA
Presidente del Congreso de la República
Presente. -

Tenemos el agrado de dirigirnos a usted señor Presidente del Congreso de la República, de conformidad con lo dispuesto por el artículo 104° de la Constitución Política, con la finalidad de comunicarle que, al amparo de las facultades legislativas delegadas al Poder Ejecutivo mediante Ley N° 30823, y con el voto aprobatorio del Consejo de Ministros, se ha promulgado el Decreto Legislativo N° 1412 , Decreto Legislativo que aprueba la Ley de Gobierno Digital.

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

Atentamente,

MARTIN ALBERTO VIZCARRA CORNEJO
Presidente de la República

CÉSAR VILLANUEVA ARÉVALO
Presidente del Consejo de Ministros

196244-ATD

CONGRESO DE LA REPÚBLICA

Lima, 18 de Setiembre de 20 18

En aplicación de lo dispuesto en el inc. b) del artículo 90° del Reglamento del Congreso de la República: para su estudio PASE el expediente del Decreto Legislativo N° 1412,

a la Comisión de Constitución y Reglamento

.....

JOSÉ ABANTO VALDIVIESO
Oficial Mayor (e)
CONGRESO DE LA REPÚBLICA

2

75