UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS

FACULTAD DE DERECHO Y CIENCIA POLITICA

UNIDAD DE POSGRADO

Derecho de identidad digital en internet

TESIS

Para optar el Grado Académico de Doctor en Derecho y Ciencia Política

AUTOR

Julio Cesar Nuñez Ponce

ASESOR

Ulises Montoya Alberti

Lima – Perú

2016

I

SUMARIO

INTRODUCCION

La identidad digital en Internet es fundamental dentro del contexto de la Sociedad de la Información. Analizar el marco jurídico aplicable a Internet en nuestro ordenamiento jurídico, centrando la problemática en el derecho de identidad digital confluye dos temas jurídicos e informáticos de palpitante actualidad: la protección jurídica de los datos personales y la regulación de las firmas y certificados digitales.

Estos temas a su vez se interrelacionan con otros también de trascendencia y actualidad: comercio electrónico, negocios electrónicos, gobierno electrónico, aprendizaje electrónico y su normatividad propia del Derecho Informático en Internet.

El Problema formulado para la siguiente investigación es el siguiente:

- ¿Qué protección y regulación jurídica es necesario que tenga el derecho de identidad digital en Internet, para que la realidad jurídica y la respectiva política de Estado, sea adecuada y suficiente para que la persona realice en forma segura los procesos electrónicos, evitando el uso indebido de las múltiples identidades y la suplantación de identidad?

La hipótesis que se va a demostrar en esta tesis, es que este problema se va a resolver estableciendo un sistema funcional de identidad digital donde el documento credencial electrónico garantice la identidad digital formal por parte del Estado en Internet, para que el ciudadano pueda realizar en forma segura los procesos de gobierno electrónico, comercio electrónico, negocios electrónicos y aprendizaje digital.

Este sistema funcional de identidad digital que integre la protección de datos personales y el uso de las firmas y certificados digitales debe estar contenido en una Legislación sistemática en torno a la identidad digital que cohesione y sistematice en forma jerárquica las instituciones jurídicas relacionadas al derecho informático en internet.

La persona humana en internet tiene el derecho a la identidad digital. La Tesis va a delimitarse a la protección del derecho de la identidad de la persona natural en Internet. Interrelacionándolo con temas como el teletrabajo, los delitos informáticos, la autenticación biométrica, el proyecto de ley de identidad digital, entre otros. El tratamiento del derecho de la identidad digital de la persona jurídica es materia de otra investigación; sin embargo, se tratará temas relacionados con la identidad digital de la persona jurídica cuando estén directamente relacionados con la persona natural o con el uso de internet, que son los aspectos centrales de la identidad digital que vamos a desarrollar en esta tesis.

La identidad digital y el uso de los medios de identificación permiten verificar que soy la persona que digo ser en Internet, en forma indubitable. La identidad digital debe ser garantizada por el Estado, pero debe permitir que la persona natural sea identificada tanto en el ámbito público como en el ámbito privado.

“A partir de la introducción de la tecnología informática en la sociedad se han generado cuatro grandes procesos: el comercio electrónico, los negocios electrónicos, el aprendizaje electrónico y el gobierno

electrónico. Para participar en dichos procesos necesitamos tener una identidad digital adicional a nuestra identidad física"[1]. Es debido a esta realidad informática y jurídica que es necesario investigar sobre la protección y regulación del derecho de identidad digital que permitan que la persona pueda participar en forma segura en los procesos de comercio electrónico, negocios electrónicos, gobierno electrónico y aprendizaje electrónico, cuando se realizan estos procesos utilizando internet.

En el primer capítulo tratamos los fundamentos del Derecho a la Identidad Digital en Internet, iniciando con el Derecho Informático en Internet, se desarrolla luego el derecho la identidad, tanto en forma electrónica como digital. Luego se trata la protección y regulación del Derecho de Identidad en Internet. La Identidad Digital y la Identificación Digital o Numérica en Internet. Identificadores Numéricos o Digitales. Localizador Uniforme de Recursos (URL). Protocolo Internet, IP. Sistema de Nombre de Dominio. Correo electrónico-Email. El caso Vargas Llosa sobre Nombres de Dominio

En el segundo capítulo se analiza la Ley peruana de Protección de datos personales tratando el objeto de la ley, los principios, los derechos, el tratamiento de datos personales, los tipos de datos personales, la seguridad de información de ls banco de datos personales. Asimismo, se analiza la legislación de firmas y certificados digitales. Se trata la autenticación biométrica de la identidad y otra legislación relacionada.

En el tercer Capítulo se trata sobre la Necesidad de un Sistema Funcional de Identidad Digital que garantice la seguridad y confianza en los procesos electrónicos. Asimismo la Ubicación de una Ley de Identidad Digital dentro del Sistema Funcional Propuesto y contenido de Proyecto de Ley. Asimismo, se tratan Las Normas que complementan sistémicamente el sistema funcional propuesto: teletrabajo, delitos informáticos, votación electrónica. Se dan Lineamientos sobre el Ente Rector del Sistema Funcional propuesto.

[1] YRIVARREN LAZO, Jorge Luis: "Construyendo nuestra Identidad Digital". En Página de Opinión del Diario Oficial El Peruano. Lima, Jueves, 13 de Setiembre de 2012. Página 12.

Se explica los. Procesos Electrónicos donde el Sistema Funcional de Identidad Digital, Protección de Datos, Certificación y Registro Digital tiene incidencia.
En el cuarto Capítulo se plantea la problemática, las hipótesis, los instrumentos de campo, el análisis de resultados y contrastación de las hipótesis. Finalmente se incluyen las conclusiones y recomendaciones, anexos, bibliografía e Índice General.

En el anexo 6 adjuntamos el Proyecto de Ley de Identidad Digital propuesto por RENIEC y que actualmente está en la Comisión de Justicia del Congreso de la Republica. En el Anexo 7 presentamos el Proyecto de Ley que crea el Sistema funcional de Identidad Digital, Protección de Datos Personales y Certificación y Registro Digital, elaborado por el autor de esta Tesis.

Entre los objetivos de la presente investigación tenemos los siguientes: Delimitar la realidad jurídica e informática existente en torno al derecho de identidad digital en internet; Analizar la adecuación y suficiencia de la regulación y protección jurídica existente del derecho de identidad digital en internet; Validar en la realidad las normas jurídicas existentes de protección de datos personales y de firmas y certificados digitales evaluando su incidencia en el ejercicio de la persona de su derecho de identidad digital en internet. Analizar la incidencia de la regulación y protección existente en torno al derecho de identidad digital para que la persona realice en forma segura los procesos de comercio electrónico, negocios electrónicos, gobierno electrónico y aprendizaje electrónico.

En la Tesis, asimismo citamos jurisprudencia que consideramos está directamente relacionada con el tema de investigación. Entre las que podemos mencionar: el Caso Vargas Llosa sobre Nombres de Dominio; el Caso Mapfre sobre Nombres de Dominio; Caso sobre Spam; Jurisprudencia del Tribunal Constitucional sobre la Video Conferencia, entre otros.

Agradezco la acertada orientación y lineamientos dados por el *Dr. Ulises Montoya Alberti*, Asesor de la presente Tesis Doctoral y

Profesor Principal de la Facultad de Derecho y Ciencias Políticas de la Universidad Nacional Mayor de San Marcos. Asimismo, agradezco a *Thomas Smedinghoff*, experto estadounidense y representante en la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (UNICTRAL) en temas relacionados al Comercio Electrónico, Firma Electrónica e Identidad Digital, por concederme una entrevista sobre el tema de mi investigación. Agradecemos también al Dr. Alberto Stewart Balbuena por sus acertados comentarios y lineamientos para el desarrollo de la Tesis y asimismo al Dr. Gilmer Alarcón por su acertada orientación en el desarrollo de la tesis. Agradezco al Jefe Nacional de RENIEC, Dr. Jorge Yrivarren Lazo y a todo el personal de la institución, por permitir desde la experiencia y práctica diaria, profundizar en la protección y regulación de la identidad digital.

Asimismo, agradezco a mis maestros, Hermano Dr. Alberto Peinador Martin FSC[2] y al Dr. Carlos Torres y Torres Lara, por sus enseñanzas, ejemplo de vida y por la formación en principios y valores. Por otra parte, agradezco a mis alumnos de pregrado y postgrado de los cursos de Derecho Informático, Derecho de las Nuevas Tecnologías, Legislación y Ética Informática, Seminario de Tesis, que me han permitido sistematizar académicamente los temas tratados en la presente investigación y vivir mi vocación docente.

Lima, Febrero de 2016

[2] FSC: "Frater Scolarum Cristianarum". Hermano de la Escuelas Cristianas o Hermano de La Salle.

Capítulo 1

Fundamentos del Derecho de Identidad Digital en Internet.

1.1. El Derecho Informático en Internet.

"El Derecho Informático nace en el siglo XX al influjo creciente de la Informática en la vida social, …la actividad informática constituye el vínculo íntimo que otorga el fundamento teórico y la utilidad práctica que justifica concentrar en un mismo subsistema las regulaciones dispersas entre ramas tradicionales del Derecho, pues sólo así se podrá juzgar la conveniencia de apartarse de las soluciones previstas en cada una de ellas, es decir la aparición de un derecho especial frente al común, al que puede llamarse Derecho Informático o Derecho de la Informática"[3]

El Derecho Informático tiene por objeto de estudio la informática, buscando resolver los problemas jurídicos que plantea la informática, es la aplicación del derecho para resolver los problemas jurídicos que plantea la informática, incluido Internet; diferenciándose de la Informática Jurídica, en que ésta es la

[3] DELPIAZZO, Carlos E. y VIEGA, María José: "Lecciones de Derecho Telemático". Ed. Fundación de Cultura Universitaria. Montevideo, Uruguay. 2004. Página 13.

aplicación de la informática al Derecho, siendo "un instrumento al servicio del Derecho".

"El Derecho Informático o Derecho de la Informática es una materia inequívocamente jurídica; conformada por el sector normativo de los sistemas jurídicos contemporáneos integrado por el conjunto de disposiciones dirigidos a la regulación de las nuevas tecnologías de la información y comunicación, es decir la informática y la telemática"[4]

Las Tecnologías de Información y Comunicaciones (TICs) se han extendido a todos los ámbitos de la sociedad. El derecho ha tenido que adaptarse a este cambio tecnológico, que tiene y ha tenido influencia decisiva en la creación y fortalecimiento de la Sociedad de la Información. Actualmente, los distintos países incluido el Perù, buscan ampliar su infraestructura tecnológica, buscando ampliar su banda ancha y su red dorsal de fibra óptica, de forma tal que haya mayor interconectividad a nivel nacional. El uso de Internet se ha masificado y su influencia se hace latente en todas las actividades humanas.

"Los problemas jurídicos que originan Internet, el ciberespacio o la informática, las nuevas tecnologías de la información, son materia de estudio del derecho informático, uno de los conocimientos jurídicos de mayor actualidad y proyección, con incidencia en todas las actividades humanas en las que se utilizan dichas tecnologías; y su solución eficaz posibilita la mayor aceptación y confianza del ciudadano en los negocios electrónicos que se realizan en Internet"[5]

[4] PEREZ LUÑO, Antonio-Enrique: "Manual de Informática y Derecho". Ed. Ariel. Barcelona, España. 1996. Página 18.
[5] NUÑEZ PONCE, Julio: "Derecho de Negocios Electrónicos en Internet". En Libro Homenaje a los XXV años de la Facultad de Derecho. Ed. Fondo de Desarrollo Editorial de la Universidad de Lima. Lima, Perù. 2006. Página 424.

En los diversos eventos académicos en torno al Derecho y la Informática se evidenciado esta evolución de la tecnologías de la información. Por ejemplo, recientemente en el XVIII Congreso Iberoamericano de Derecho e Informática realizado en San Jose de Costa Rica, en Octubre de 2014, se planteó que la informática y las tecnologías de la información y comunicaciones (TICs) son un paradigma para el Derecho. Por tanto, frente a la clásica división que se hacía de Derecho Informático e Informática Jurídica plantean el IUSTICs como el Derecho de la Tecnologías de la Información y Comunicaciones y el TICSIUS como la Tecnologías de Información y comunicaciones aplicadas al Derecho[6].

Al respecto, consideramos que son atendibles estas propuestas, pero que debe mantenerse como base fundamental el Derecho Informático y la Informática Jurídica y entenderse las distintas evoluciones en la denominación como conceptos comprendidos en la denominación original. Por tanto, denominaciones como Derecho Electrónico, Derecho Telemático, Derecho de Internet, Derecho de Tecnologías de la Información y Comunicaciones son diversas manifestaciones contenidas en el concepto original. No obstante lo expresado, consideramos que independientemente de las nuevas denominaciones se mantiene el objeto de estudio que es la informática, en una amplia concepción que incluye el Derecho aplicable a Internet.

"A la hora de construir una [regulación y autorregulación] para el ciberespacio nos encontramos con las mismas cuestiones que en el espacio real…Ya estamos batallando con la sustancia: ¿el ciberespacio garantizará la privacidad o el acceso?, ¿preservará

[6] El XVIII Congreso Iberoamericano de Derecho e Informática, se realizó en San Josè de Costa Rica, del 13 al 17 de Octubre de 2014. En la sesión inaugural el Presidente del Comité Organizador Juan Diego Castro fundamentó esta posición. Pudimos virtualmente escuchar esta disertación a través de nuestro Smartphone, habiendo bajado la aplicación Livestream apps. Hubo nítida visión y audio.

un espacio para la libertad de expresión?, ¿facilitará un comercio verdaderamente libre y abierto?"[7]

Internet es una red de redes , es una biblioteca digital global de información y conocimientos. todas las computadoras concretadas a internet que utilizan el TCP/IP y que cumplen normas relativas a las direcciones IP y a los localizadores uniformes de dominio utilizan internet[8], adquieren derechos pero también obligaciones con respecto a los proveedores de servicio de internet y a los normas aplicables al sistema de nombres de dominio DNS, en lo que se denomina la Gobernanza en Internet.

"Internet es el tejido de nuestras vidas en este momento, No es futuro, es presente. Internet es un medio para todo, que interactúa con el conjunto de la sociedad… esta tecnología es más que una tecnología. Es un medio de comunicación, de interacción y de organización social,,, en lo esencial esto significa que Internet es ya y será aun más el medio de comunicación y relación esencial sobre la que se basa una nueva forma de sociedad que ya vivimos, la sociedad en red[9]".

"La Gobernanza en Internet es el desarrollo y la aplicación por los gobiernos, el sector privado y la sociedad civil, en las funciones que les competen respectivamente, de principios, reglas, procedimientos de adopción de decisiones y programas comunes que configuran la evolución y utilización de Internet[10]".

---

[7] LESSIG, Lawrence: "El Código y otras Leyes en el Ciberespacio". Ed. Taurus. Madrid, España. 2001. Pàgina 27.

[8] Vid. VALLEJOS, Oscar: "Introducción a Internet". En ing.unne.edu.ar/pub/internet.pdf. Fecha de consulta: 28 de agosto de 2015.

[9] CASTELLS, Manuel: "Internet y la Sociedad en Red". Lección Inaugural del programa de doctorado sobre la sociedad de la información y el conocimiento en 2001 en la Universidad Oberta de Cataluña (UOC). En http://tecnologiaedu.us.es/cuestionario/bibliovir/106.pdf Fecha de consulta 21 de noviembre de 2015.

[10] Esta definición ha sido propuesta por el Grupo de Trabajo de la Gobernanza en Internet (WGIG por sus siglas en ingles en Junio de 2005. Ha sido citada por PEREZ, Jorge y OLMOS, Ana: "Introducción a la Gobernanza de Internet". En Revista TELOS Julio-Setiembre 2009. Nº 80.
En: telos.fundaciontelefonica.com/telos/articulocuaderno.asp@idarticulo=1&rev=80.htm

La gobernanza en internet se basa en la colaboración de todas las partes interesadas que intervienen en los niveles o capas de Internet.

Hay tres niveles o capas en Internet: a) El nivel o capa de la infraestructura, que incluye los cables de fibra óptica, servicios portadores de internet, servidores. b) El nivel o capa de protocolos que incluye el protocolo TCP/IP. c) El Nivel o capa de información o contenidos donde empresas como Google o Facebook tienen una actividad preponderante.

Una característica importante de internet es su descentralización, “nadie gobierna internet porque gobiernan todos”, cada red conectada conserva su independencia. Sin embargo, para que semejante anarquía funcione es necesario la existencia de una serie de procedimientos y mecanismos de coordinación. La conexión a Internet se realiza por medio del proveedor de servicio de acceso a Internet. Los proveedores llegan a acuerdos de interconexión entre ellos. Existen proveedores con infraestructura de red de distintos tamaños y ámbitos geográficos, y esto implica cierta jerarquía de redes en cuyo vértice están las redes troncales que dan servicios a organizaciones finales. De la forma de funcionamiento de la Internet se desprende la necesidad de administrar una serie de recursos comunes. Esta especie de servicio público se denomina NIC (Network Information Center), que se encarga de asignación de direcciones y registros de nombres de dominio. Este trabajo esta descentralizado por áreas geográficas. La Autoridad mundial en esta materia (que es una asociación privada constituida en California) es ICANN (La Corporación de Internet para la Asignación de Nombres y Números) y en la que participan los multistakeholders (representantes del gobierno, empresas privadas, sector académico, sociedad civil).

La gobernanza en Internet requiere la participación de todos los multistakeholders[11] con la finalidad de establecer principios, normas, reglamentos que permitan un funcionamiento ordenado y regulado de internet a nivel global. El concepto de gobernanza a diferencia del de gobierno permite enfatizar el carácter participativo y descentralizado de la red de redes. El Derecho que regula la conducta humana y debe estar acorde con la realidad también es necesario que analice y delimite esta forma de organización que tiene alcance global.

Es este orden de ideas, consideramos que dentro del Derecho Informático se incluyen temas transversales como el derecho a la identidad digital en Internet que permitirá garantizar este derecho fundamental en Internet en los distintos procesos donde las personas se interrelacionan como son el comercio electrónico, los negocios electrónicos, el gobierno electrónico y el aprendizaje electrónico.

1.2. El Derecho de Identidad. La identidad Electrónica y la Identidad digital.

Identidad es el "conjunto de rasgos propios de un individuo o de una colectividad que los caracteriza frente a los demás"[12]. En la identidad podemos distinguir la identidad personal de la identidad de la colectividad.

Con respecto a la identidad de la persona humana, la Constitución Política del Perú, establece en el artículo 2º, que toda persona tiene derecho: "a la vida, a su identidad, a su integridad moral, psíquica y física y a su libre desarrollo y bienestar. El concebido es sujeto de

---

[11] El modelo multi-stakeholder o de múltiples partes interesadas se refiere a la participación y/o consideración de los enfoques de todos los actores que importan en un sistema. ICANN es un ejemplo de organización multistakeholder de múltiples partes interesadas**.**

[12] Diccionario de la Real Academia Española. Vigésima Segunda Edición. Tomo 6. Ed. Real Academia Española. Madrid, España. 2001. Página 843.

derecho en todo cuánto le favorece". La norma constitucional relaciona el derecho a la vida, con el derecho a la identidad y a su integridad. El derecho a la identidad es un derecho fundamental de la persona humana.

Tal como afirma el Dr. Carlos Fernández Sessarego: "Entendemos como identidad personal el conjunto de atributos y características que permiten individualizar a la persona en sociedad. Identidad personal es todo aquello que hace que cada cual sea "uno mismo" y no "otro". Este plexo de características de la personalidad de "cada cual" se proyecta hacia el mundo exterior, se fenomenaliza, y permite a los demás, y permite conocer a la persona, a cierta persona, en su "mismidad", en lo que ella es en cuánto específico ser humano[13].

Estos atributos permiten individualizar a la persona en la sociedad de la información. Es necesario en un entorno digital que cada cual sea "uno mismo" y no "otro". Más aún en el contexto de la globalización y de Internet las características de la personalidad de cada cual se proyecta en la red de redes pudiendo en corto tiempo ser identificado por sus atributos utilizando las herramientas de las tecnologías de la información y comunicaciones (TICs). Tal es así que una persona puede ser fotografiada desde un teléfono móvil, ser subida su imagen a una red social tipo facebook, linkedin u otros y vista en cuestión de segundos por distintas personas en tiempo real.

Conforme el artículo 1º de la Constitución Política del Perú: "la defensa de la persona humana y el respeto a su dignidad son el fin supremo de la sociedad y del estado". En un entorno digital, la identidad de la persona humana debe ser defendida para garantizar el respeto de su dignidad y su privacidad. El vertiginoso desarrollo tecnológico permite a las personas de todo el mundo utilizar las tecnologías de la información y las comunicaciones y, al mismo tiempo a través de herramientas tecnológicas como la minería de datos o "data minning" se aumenta la capacidad de realizarse en forma indiscriminada

[13] FERNANDEZ SESSAREGO, Carlos: "Derecho a la Identidad Personal". Ed. Astrea. Buenos Aires, Argentina. 1992. Página 113.

actividades de vigilancia, interceptación y recopilación de datos que pueden vulnerar derechos de la persona. Por tanto, protegiendo el derecho de identidad en un entorno digital también podemos proteger su dignidad y privacidad.

La identificación permite verificar la identidad y ejercer el derecho de la identidad en la "sociedad digital actual". Para analizar esta problemática, es necesario tener en cuenta que "..la noción del Derecho a la Identidad , si bien ha conocido algunas variaciones con el correr del tiempo, continua siendo en su esencia aquello que De Cupis estableció por primera vez, a saber, el derecho de cada uno a ser sí mismo y de ser reconocido y representado de acuerdo a sus características verdaderas, vale decir, sin imputaciones ni omisiones falaces que lo tergiversen ante los demás"[14]

Esta protección a sus características verdaderas es importante y esencial en un entrono digital. Los distintos procesos en que la persona interviene como son el comercio electrónico, los negocios electrónicos, el gobierno electrónico y el aprendizaje electrónico requieren en sociedad actual que la persona humana sea adecuadamente identificada sin imputaciones ni omisiones falaces que influyen en su reputación en línea ni que se divulgue información inexacta, falsa o desactualizada que tergiversa su imagen virtual ante los demás.

"El Derecho a la Identidad es una situación jurídica en la que se tutela la identificación de los sujetos de derecho (identidad estática), en la que se encuentran datos como el nombre, el domicilio, las generales de ley entre otros, así como la proyección social (Identidad Dinámica), vale decir el conglomerado ideológico de una persona, sus experiencias sus vivencia, tanto su ser como su quehacer"[15]

La identidad estática en un entorno digital es necesaria que sea actualizada de forma tal que sea veraz y exacta y de una visión

[14] RENIEC: "Enciclopedia del Sistema Registral" Ed. Registro Nacional de Identificación y Estado Civil. Lima, Perú. 2010. Página 139.
[15] ESPINOZA, Juan: "Derecho de Personas." Ed. Gaceta Jurídica. Lima, Perú. 2004. Páginas 253 y 254.

completa y confiable de su identidad. En el documento nacional de identidad los datos que conforman la identidad estática son consignados, sistematizados y procesados en un registro público que distingue los datos de acceso público de los datos reservados.

La identidad dinámica en un entorno digital es necesaria que sea controlada y protegida por el estado, las instituciones y personas jurídicas que realizan tratamiento de datos y por la propia persona. La identidad dinámica incluye los hábitos, pensamientos y aspectos del proyecto de vida de cada persona, lo que hace necesario su protección y regulación adecuada.

En la "sociedad digital" la identidad estática y la identidad dinámica se interrelacionan en las base de datos, en las redes sociales y en los distintos sistemas de información la identidad de la personas es esencial para que las personas puedan acceder a servicios y realizar distintas actividades con relevancia jurídica como son: el comercio electrónico, los negocios electrónicos, el gobierno electrónico, la educación digital y el desenvolvimiento de la persona humana en la "sociedad digital".

En este orden de ideas, la identidad dinámica, "se configura por lo que constituye el patrimonio ideológico cultural de la personalidad. Es la suma de los pensamientos, opiniones, creencias, actitudes, comportamientos de cada persona que se explayan en el mundo de la intersubjetividad… Es aquello que define la personalidad proyectada hacia el exterior. Es en síntesis el bagaje de características y atributos que definen la "verdad personal" en que cada cual consiste"[16]

Esta identidad dinámica en la red conjuntamente con la estática, están relacionadas con la "reputación en línea" que las personas tienen en las redes y sistemas de información, así como con las leyes, reglamentos y distintas normas jurídicas que forman parte del Derecho Informático.

[16] FERNANDEZ SESSAREGO, Carlos: "Derecho a la Identidad Personal" Ed. Astrea. Buenos Aires, Argentina. 1992. Página 114.

El artículo 2º inciso 19 de la Constitución, establece que “toda persona tiene derecho a su identidad étnica y cultural. El Estado reconoce y protege la pluralidad étnica y cultural de la Nación”. En un entorno digital la identidad étnica y cultural debe ser protegida, tanto en sus características estáticas como dinámicas. Tal es asì que sus nombres y sus costumbres e idioma en la red también deben ser protegidos.

Las personas jurídicas tienen existencia distinta a sus miembros, sin embargo en un entorno digital su identidad puede estar relacionada con la de sus miembros en cuánto al prestigio y reputación en lìnea. La existencia de la persona jurídica de derecho privado comienza el dìa de su inscripción en el registro respectivo. Con los sistemas de constitución en línea de determinadas personas jurídicas, incluso el procedimiento de constitución de algunas de ellas, puede darse en un entorno digital. La persona jurídica de derecho público interno se rige por la ley de su creación y su identidad también puede estar relacionada con la de sus miembros. En este orden de ideas, cuando se trata sobre la identidad digital frecuentemente se incluye a las personas naturales y a las personas jurídicas, teniendo en cuenta que la identidad es personal y es de la colectividad.

Definimos a la Identificación Electrónica como el procedimiento que mediante elementos externos, permite asignar una identidad con determinados atributos a una persona concreta, esto es a la comprobación de datos que acreditan que un individuo es efectivamente la persona que dice ser, sujeto de derecho con determinados atributos**.**

Entendemos que la Autenticación Electrónica es el proceso de verificación de la autenticidad de las identificaciones realizadas o solicitadas por una persona física o entidad, sobre datos tales como un mensaje u otros medios de transmisión electrónica. El proceso de autenticación es la segunda de dos etapas que comprenden: 1) La presentación de un medio que acredita la identificación ante el sistema y 2) la presentación o generación de información que corrobora la relación entre el medio presentado y la persona o entidad identificada.

El Sistema Biométrico es un sistema informático de reconocimiento con base en uno o varios patrones, que opera requiriendo datos biométricos a un individuo, extractando un patrón de estos datos adquiridos y comparando el ejemplo contra una plantilla previamente registrada. Dependiendo la aplicación, esta plantilla puede estar almacenada en una base de datos centralizada o en un dispositivo individual, como un token o una tarjeta inteligente.

Puede entenderse la identidad digital de las personas naturales y jurídicas a aquella identidad electrónica basada en un documento credencial electrónico, emitido en el marco de la Infraestructura Oficial de Firma Electrónica (IOFE), y conforme a las disposiciones legales vigentes. Esta definición parte de la premisa que un documento credencial electrónico como el documento nacional de identidad electrónico garantiza la identidad en un entorno digital en forma segura y confiable.

Sin embargo, hay que tener en cuenta otros puntos de vista, por cuánto "bajo la expresión "identidad digital" se han venido agrupando de forma reciente las técnicas que permiten a las personas y a las organizaciones identificarse y actuar en las redes, mediante mecanismos de autenticación de mayor o menor robustez. Se entendería esta identidad como el conjunto de datos (a menudo denominados "atributos") que nos diferencian suficientemente del resto de personas o entidades"[17]

En este orden de ideas se señala que la identidad digital es aquella que distingue a las persona en la red, pudiéndose distinguir distintas clases como son la identidad electrónica personal, la corporativa y la del cliente[18]. Tal como señalamos a continuación:

[17] CHAVEZ VALDIVIA, Ana Karin: "Identidad Virtual: Implicancias en el Derecho a la Intimidad". Ponencia presentada en el XVIII Congreso Iberoamericano de Derecho e Informática. San José de Costa Rica, el jueves 16 de Octubre de 2014. Página 184. En http://www.juandiegocastro.com Fecha de consulta: 17 de Noviembre de 2014.

[18] Cfr. ALAMILLO DOMINGO, Ignacio : "La Identidad en la Red". Investigación y Ciencia. ISSN-0210-136X. Nº 386, 2008. Pàginas 54 a 61. ALAMILLO DOMINGO, Ignacio y HENAO HOYOS, Erika: "La Gestiòn electrónica de la Identidad y de la firma electrónica en el intercambio electrónico de Datos entre Administraciones Pùblicas" En Revista de Derecho Informàtico, ISSN-e 1681 – 5726 , Nº 121, 2008.

a) La identidad digital personal es aquella regulada por el Estado, válida dentro de su territorio, especialmente basada en procesos robustos de identificación física. En algunos países se acredita con el DNI electrónico.
b) La identidad digital corporativa es aquella que nos vincula con una organización pública o privada mediante una relación jurídica de pertenencia o vinculación y frecuentemente se construye sobre el documento de acreditación de la identidad física personal como sucede en el fotochek de un trabajador o un funcionario.
c) La identidad digital del cliente que es aquella que nos vincula con una organización pública o privada con la que se establece una relación de negocio con vocación de permanencia, como sucede con la identidad financiera, programas de fidelización, entre otros.

Más aún algunos autores, van más allá diferenciado además de la identidad digital, la identidad virtual. Se afirma que: "La identidad virtual propiamente dicha es aquella que sin estar necesariamente vinculada con alguna institución u organismo (como seria la identidad electrónica corporativa o de cliente) y además sin necesidad de contar con el respaldo del estado (el caso de la identidad electrónica personal) es creada en la red como un tipo de identidad parcial, convirtiéndose en un nuevo paradigma en la gestión de la identidad debido a que se basa en una gestión realizada únicamente por el propio usuario de todo el ciclo de vida de su identidad, con mayor control sobre la divulgación de sus datos personales"[19]. Incluso autores como Philipe Mouron[20] afirman: "La identidad virtual recubre tres acepciones diferentes: la identidad numérica, la identidad virtualizada y la identidad inmaterial". Diferenciando la identidad virtual de la identidad real y su uso en el ciberespacio

No obstante lo señalado, insistimos en la importancia de la identidad digital. Al respecto, Jorge Yrrivaren[21] afirma lo siguiente: "La identidad digital es la posibilidad de verificar que soy la persona que digo ser en internet, de manera indubitable. Para eso es necesaria la autenticación

[19] CHAVEZ VALDIVIA, Ana Karin: Ob. Cit. Página 187.
[20] MOURON PHILIPE: "Internet et Identité virtuelle des persones". En: http:// junon-u-3mrs.fr/u3ired01/Main%20docu/internet/chronp-identitevirtuelle.pdf Fecha de Consulta: 05 de Octubre de 2015.
[21] YRIVARREN, Jorge: "Identidad, Identificacion y Persona Humana: Por la institucionalidad de lo diverso". En : RENIEC: "Identidad Digital: La identificación desde los registros parroquiales al DNI Electronico". Primera Edicion, diciembre 2015. Pagina 41.

a partir de lo que tengo, lo que se y lo que soy: tengo un dispositivo informático como una tarjeta inteligente que cuenta con un chip o con una memoria flash o usb que almacenan o procesan datos; sé un código o PIN que puede ser validado con la información almacenada en el chip o la memoria; soy (aunque de manera un tanto restrictiva) una o varias características biométricas, como huellas dactilares, rasgos faciales, configuraciones vasculares o una cadena genética (ADN). Estos tres elementos en conjunto garantizan la autenticidad de mi identidad ante el sistema, empresa o institución que atiende mi tramite o transacción".

En la presente tesis, delimitaremos el concepto del derecho de identidad digital, teniendo presente los criterios anteriormente expuestos y otros que a lo largo de la investigación iremos tratando en forma sistemática. Al respecto, cabe tener en cuenta que: "la identidad digital es la expresión electrónica del conjunto de rasgos con los que una persona se individualiza frente a los demás. Los cimientos de la identidad digital se hallan tanto en la creación como en la recopilación de los atributos identificativos por su titular o por terceros"[22]. Lo que posibilita la identidad digital como una identidad formal protegida, reconocida y garantizada por el derecho es autenticar, identificar a la persona de manera segura y confiable en el mundo del ciberespacio o internet.

1.3. La protección y regulación del Derecho de Identidad en Internet.

"Recientemente en Iberoamérica, con la aprobación del marco para la identificación electrónica social, se están dando los primeros pasos para la construcción de una política de identidad digital en la región, resultando interesante su estudio desde la experiencia de países europeos con un mayor desarrollo como España, caracterizado por ser pionero a nivel mundial en la difusión del DNIe[23]".

[22] FERNANDEZ BURGUEÑO, Pablo: "La Identidad Digital de la Persona Fisica en la Sociedad del Conocimiento. Ponencia XIX Congreso Iberoamericano de Derecho e Informática. 26, 27 y 28 de Agosto de 2015. Medellin, Colombia

[23] ARTEAGA, Sor: "DNI en Iberoamérica : Hacia la construcción de una política de identificación electrónica en la Región. Libro de Memorias del XVI Congreso Iberoamericano de Derecho e Informática". Quito, Ecuador, del 10 al 14 de Setiembre de 2012. Ed. Ministerio de Justicia. Páginas 262 a 279.

En Europa el 23 de Julio de 2014, el Parlamento Europeo y el Consejo han aprobado el Reglamento (UE) Nº 910/14, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior. Este Reglamento deroga la Directiva 1999/93/CE que establecía un marco comunitario para la firma electrónica.

En este orden de ideas, tanto en Iberoamérica como en Europa se han dado "pasos concretos" para la protección y regulación del Derecho de Identidad en Internet. La finalidad es proporcionar un marco coherente con vistas a garantizar un elevado nivel de seguridad y de certidumbre jurídica del derecho identidad en internet para generar confianza en la red.

"Sin identificación no existen derechos. El ejercicio de los derechos requiere necesariamente la identificación plena de las personas, función que corresponde al Estado. El Estado es el responsable de la identificación de las personas, y de garantizar la identidad a cada uno. En un mundo cada vez más informatizado, los gobiernos utilizan las TIC‟s para la implementación de las políticas públicas sustantivas. Cómo lograr la plena identificación de las personas, cómo reconocer entre países dichas identificaciones, cómo facilitar el acceso remoto a los servicios que brinda la Administración, son cuestiones que tienen que ver con una adecuada identificación electrónica de las personas"[24].

La identidad digital, garantizada por el Estado permite desarrollar los procesos de comercio, electrónico, negocios electrónicos, gobierno electrónico y aprendizaje electrónico, dentro de un contexto de seguridad y confianza. La confianza en los servicios en línea, en la identificación electrónica, que incluye la digital y la seguridad de la plataforma tecnológica, son fundamentales para que los usuarios aprovechen estos procesos en forma plena.

[24] Marco para Identificación Electrónica Social Iberoamericana" **Aprobado por la XIII Conferencia Iberoamericana de Ministros y Ministras de Administración Pública y Reforma del Estado** Asunción, Paraguay, 30 de junio - 1° de julio de 2011. Página 3.

"Esta identificación electrónica es necesaria para el acceso a sistemas informáticos, a las aplicaciones de gobierno electrónico, de comercio electrónico, pero también para la ejecución de políticas sociales. Además de este uso, los modernos documentos de identidad, básicamente los pasaportes y los documentos nacionales, están utilizando elementos de identificación electrónica, lo cual lleva a considerar que aún en los supuestos de identificación presencial, las tecnologías de la información y las comunicaciones cobran un rol relevante"[25].

Las políticas sociales permiten acercar el Estado al ciudadano, donde más lo necesita; pero además permiten garantizar la identidad de las personas tanto estática como dinámica y proteger su identidad étnica y cultural. Más aún se garantiza la seguridad de la gestión de los servicios de apoyo y asistencia social del estado, con la finalidad que el apoyo gubernamental llegue a las personas que realmente lo necesitan tanto en la niñez, juventud y tercera edad.

"La identificación de las personas constituye un requisito esencial para el pleno ejercicio de sus derechos. Como una obligación ineludible de los Estados iberoamericanos, se tiene que garantizar la correcta identificación de las personas, así como salvaguardar y proteger el derecho a la identidad de cada uno de los habitantes de su suelo[26]"

Es en este sentido, que el derecho de identidad digital y la identificación debe ser garantizada por la legislación de cada país, de forma tal de que los derechos de cada persona sean respetado en forma coherente e integral.

1.3.1. La Identidad Digital y la Identificación Digital o Numérica en Internet

"Los identificadores digitales o numéricos pueden ser definidos como signos que caracterizan a un individuo con una perspectiva que es en parte a manera temporal y en parte definitiva, en el contexto

[25] Ibidem

[26] Marco para Identificación Electrónica Social Iberoamericana" **Aprobado por la XIII Conferencia Iberoamericana de Ministros y Ministras de Administración Pública y Reforma del Estado** Asunción, Paraguay, 30 de junio - 1° de julio de 2011. Página 20.

electrónico. Estas señales se crean y gestionan en línea. Estos identificadores numéricos son la dirección de correo electrónico, o correo electrónico, nombre de dominio de Internet , URL y direcciones IP"[27].

1.3.1.1. Identificadores Numéricos o Digitales

a) Localizador Uniforme de Recursos (URL)

El Localizador Uniforme de Recursos o URL, es un formato de asignación de nombres universal, utilizado para indicar y dirigir recursos en Internet y el método para acceder a ellos: sitios de Internet, imágenes, documentos html, casillas electrónicas, foros, etc.

La URL se organiza en cinco secciones: i) Protocolo comunicación, que el lenguaje utilizado para comunicarse en la red, por ejemplo el http[28] ii) Inicio de sesión y contraseña, que permite especificar los parámetros de acceso de un servidor seguro. iii) Nombre del servidor, es un nombre de dominio del equipo que aloja el recurso solicitado. Iv) Numero de puerto, es un numero relacionado con un servicio que le permite al servidor conocer el tipo de recurso solicitado v) Ruta de acceso al recurso.

Cada vínculo hipertexto de la web se construye con la URL del recurso señalado.

b) Protocolo Internet, IP

La dirección IP (Internet Protocol) es el numero que identifica los distintos recursos informáticos (computador, teléfono IP, ruteador, etc) conectado a una red que utiliza el protocolo de internet.

"El numero que constituye la dirección IP implica, en la versión 4 del protocolo Internet (IPv4), cuatro números incluidos entre 0 y 255,

[27] ITEANU, Olivier: L´identité numerique en question. 10 scenarios pour la amitrise juridique de son identite sur internet"Ed. EYROLLES. Paris, Francia. Abril 2008. Paginas 5 y 6. En ir.nmu.org.ua/bitstream/handie/123456789/1c5018659518F67372c0bf9687170a9d.pdf?sequence=1.

[28] Hyper Text Transfer Protocol (protocol de transferencia de hipertexto) que posibilita el intercambio de paginas web en formato html. Otros protocolos utilizados el FTP (File transfer Protocol) y el Gopher (que permite acceso de información a través de menus.

separados por puntos como 212.134.19.159. El rápido desarrollo de internet ha saturado las direcciones IPv4 disponibles. En su versión 6, el IPv6 ha sido desarrollado en respuesta a la necesidad creciente de direcciones IP. Una dirección IPv6 implica 8 números, incluidos entre 0 y 65,535 (en anotación hexadecimal) separados por dos puntos, como IFFF:O: A88 : 85 A 3:O: O:ACIF:8OO1[29]".

Existen dos tipos de direcciones IP: las fijas y las dinámicas. Las fijas están relacionadas con una conexión permanente o estable con un proveedor de acceso a internet; en cambio, la dirección IP dinámica se renueva a cada conexión a la red de internet, principalmente con dispositivos móviles que dan un acceso temporal o por tiempo limitado.

c) Sistema de Nombres de Dominios, DNS

El sistema de nombres de dominio es un componente esencial de la infraestructura operativa de Internet que permite localizar los computadores conectados a la red.

Cada equipo conectado a internet tiene al menos una dirección IP específica, sin embargo los usuarios no desean trabajar con direcciones IP como 196.159.206.28 sino con nombres de dominio, por ejemplo: www.unmsm.edu.pe. Es posible asociar nombres que son de mas fácil uso y recuerdo que las direcciones IP.

En el ejemplo señalado www significa world wide web , el nombre de dominio propiamente se cuenta de atrás para adelante; el primer nivel en el ejemplo es .pe que es el nivel territorial de Perú o ccTLD (country coude top level domain); otros ejemplos de nivel territorial tenemos: ar de Argentina; mx de México; es de España; br de Brasil. Por otra parte, el segundo nivel en el ejemplo es .com de comercio ; otros ejemplos de nivel genérico tenemos .edu (educación) , gob (gobierno), org (organización), mil (militar), etc. El tercer nivel en el

[29] ITEANU, Olivier: ob.cit. Página 15

ejemplo es unmsm es el acrónimo o abreviatura de la Universidad Nacional Mayor de San Marcos.

En el Perú el administrador delegado de nombres de dominio de nivel territorial .pe es la Red Científica Peruana (RCP). Actualmente se puede registrar un nombres de dominio por vía electrónica aplicando el principio de "que el primero que llega es el primero en ser atendido". Asimismo, se puede registrar directamente dominios con nivel territorial .pe sin que en su estructura tengan un dominio genérico. Con respeto a la solución de conflictos o controversias por inscripción de nombres de dominio con marcas, nombres comerciales, derechos de autor, otros nombres de dominio u otros casos, se opta por el arbitraje por internet estableciendo como órganos de resolución de conflictos a la Organización Mundial de la Propiedad Intelectual y al Cibertribunal Peruano.

Conforme las normas y procedimientos de registro del nivel .pe: Los caracteres que podrán ser utilizados para conformar un nombre de dominio serán las letras del alfabeto inglés ("a"-"z"). De igual modo se podrán utilizar los dígitos ("0"-"9") y el guión ("-"). Asimismo, se podrán utilizar los caracteres "á", "é", "í", "ó", "ú" y "ñ".

En el caso del guión ("-"), el mismo no puede ir al inicio ni al final de la combinación de caracteres que se solicite, ni podrá utilizarse en la tercera y cuarta posición simultáneamente. No hay una longitud mínima requerida, sin embargo se establece 63 caracteres como máximo posible.

Asimismo, conforme las normas y procedimientos del registro .pe[30] : "La Política de Resolución de Controversias de Nombres de Dominio bajo el Punto.pe se establece como instrumento para dilucidar las disputas que pudieran aparecer una vez registrados un nombre de dominio bajo el Punto.pe. La solicitud de registro representa una aceptación por parte del solicitante de las condiciones establecidas en las presentes políticas, así como en las Políticas de Resolución de Controversias establecidas dentro del sistema Peruano de nombres de dominio bajo el Punto.pe. La delegación de un nombre de dominio

[30] https://punto.pe/rules_and_procedures.php

implica el mantenimiento en la Tabla de Zona del Punto.pe de dicho nombre, relacionado o no, a determinado número IP, por parte de Punto.pe".

d) Correo Electrónico- email.

La Dirección de correo electrónico es el conjunto de palabras o caracteres que identifican a una persona que puede enviar y recibir correo. Cada dirección es única y pertenece siempre a la misma persona.

"El correo electrónico es uno de los servicios mas populares de Internet. Es un servicio de transferencia de mensajes entre interlocutores, que permite a sus usuarios escribir, enviar y recibir mensajes y archivos rápidamente mediante sistemas de comunicación electrónica"[31]

La Ley 28493 regula el envío de comunicaciones comerciales publicitarias o promocionales no solicitadas, realizadas por correo electrónico, sin perjuicio de la aplicación de las disposiciones vigentes en materia comercial sobre publicidad y protección al consumidor.

Son derechos de los usuarios de correo electrónico: i) Rechazar o no la recepción de correos electrónicos comerciales. ii) Revocar la autorización de recepción, salvo cuando dicha autorización sea una condición esencial para la provisión del servicio de correo electrónico. iii) Que su proveedor de servicio de correo electrónico cuente con sistemas o programas que filtren los correos electrónicos no solicitados. d) El reenvío del correo electrónico al emisor del correo electrónico comercial no solicitado, con la copia respectiva a la cuenta implementada por INDECOPI.

Todo correo electrónico comercial, promocional o publicitario no solicitado, originado en el país, debe contener: a) La palabra "publicidad", en el campo del "asunto" (o subject) del mensaje. b) Nombre o denominación social, domicilio completo y dirección de

[31] ITEANU, Olivier: ob.cit. Página 12.

correo electrónico de la persona natural o jurídica que emite el mensaje. c) La inclusión de una dirección de correo electrónico válido y activo de respuesta para que el receptor pueda enviar un mensaje para notificar su voluntad de no recibir más correos no solicitados o la inclusión de otros mecanismos basados en internet que permita al receptor manifestar su voluntad de no recibir mensajes adicionales.

1.3.1.2. Relevancia Jurídica de la identificación numérica y los Nombres de Dominio en Internet.

"Todo identificador generalmente se lleva a cabo dentro de un sistema que será llamado " sistema de identidad" Este sistema se compone generalmente de cuatro elementos que interactúan entre sí . a) Los identificadores propios b) Por ser única la identificación de un individuo, esta debe ser registrada en un registro o una base de datos mantenida y vigilada por un tercero neutral y confiable. c) Los identificadores proporcionan información sobre la persona individualizada a que se refieren. Esta información se registra en los soportes que les permitan la autenticación de número de identidad válido. d) Los identificadores otorgan derechos, pero también deberes para las partes a las que se refieren"[32].

Con respecto a la identidad digital, cabe destacar dos casos de laudos arbitrales por Internet resueltos por la Organización Mundial de la Propiedad Intelectual (OMPI) que son los siguientes: c.1) El caso Vargas Llosa y c.2) El caso Mapfre.

1.3.1.2.1. **El caso Vargas Llosa sobre Nombres de Dominio**[33]. El Centro de Arbitraje y Mediación de la OMPI recibe la demanda por correo electrónico del Doctor Jorge Mario Pedro Vargas Llosa, quien es mejor conocido en el mundo de la cultura como Mario Vargas Llosa, solicitando la transferencia del nombre de dominio mariovargasllosa.org, con los siguientes argumentos:

[32] ITEANU, Olivier; "L`identitè numérique en question. 10 scénarios pour la maitrise juridique de son identité sur Internet". Ob.cit. Pàgina 18.

[33] Caso Nº D2004-0956. Decisión del Panel Administrativo de la OMPI. Demandante: Jorge Mario Pedro Vargas Llosa versus Demandado: Instituto Cultural "Mario Vargas Llosa. Demanda iniciada el 12 de noviembre de 2004 y resuelta el 16 de febrero de 2005. En: http://www.wipo.int/amc/en/domains/decisions/html/2004/d2004-0956.html

i) Que Mario Vargas Llosa goza de un gran prestigio nacional e internacional. Su fama se debe al fruto de una vida dedicada a la creatividad y al desarrollo profesional como autor de obras literarias. Como consecuencia, cuenta con una vasta lista de galardones y premios que han sido otorgados a su persona y a su obra por varia instituciones de renombre tanto en el Perú como en el ámbito internacional.

ii) La actividad profesional en el campo de la literatura y las letras del demandante no solo se pone al público a través de sus obras escritas, sino también cuenta con presencia en Internet a través del sitio vargasllosa.com , por lo que el nombre de dominio mariovargasllosa.org (registrado y utilizado por la parte demandada) causa confusión no solo con el nombre propio del autor (Doctor Mario Vargas Llosa) sino también con el sitio del Demandante www.vargasllosa.com , pues los visitantes del sitio objeto del presente litigio creen que el origen, la administración y los contenidos del mismo están a cargo personalmente del Doctor Mario Vargas Llosa.

iii) Que el nombre civil del demandante Mario Vargas Llosa no ha sido registrado como marca. No obstante lo anterior, el Demandante aclara que los nombres propios o civiles de los autores y de distintas personalidades del mundo artístico, de la política, de la cultura y de otras esferas han sido reconocido como "marca de hecho" por lo que les ha sido aplicable la Política. El Demandante apunta varios casos que han sido resueltos por Expertos ante el Centro de Arbitraje y Mediación de la OMPI[34] en los que el nombre propio o civil de una persona ha obtenido esta especial protección y argumenta que debido a la especial fama y mundialmente conocida obra del autor, el nombre "Mario Vargas Llosa" también debería tener la misma protección de marca de hecho.

iv) El Demandado no tiene derechos ni intereses legítimos en el nombre de dominio mariovargasllosa.org ya que el Doctor Mario

[34] Caso OMPI Nº D2000-1649:Montero Gallo versus Galileo Asesores S.L.. Caso OMPI Nº D2000-0210: Julia Fiona Roberts versus Russell Boyd. Caso OMPI Nº D2000-0235 Jeanette Winterson versus Mark Hogarth.

Vargas Llosa no tiene relación alguna con el demandado, más que las varias solicitudes que ha efectuado para recuperar el nombre de dominio mariovargasllosa.org e incluye en su demanda las comunicaciones en las que el Demandante solicita al Demandado que se abstenga de usar el dominio antes señalado.

v) Que el demandado ha venido obteniendo ingresos con el uso del dominio materia del presente procedimiento mediante la venta de banners, publicidad y uso comercial que hace en el sitio www.vargasllosa.org . Por tanto, afirma que el registro de nombre de dominio y su utilización por parte del Demandado, ha sido y está siendo de mala fe. Según lo expuesto por el propio demandante en su demanda "el demandado, utilizando el dominio, ha venido atrayendo con ánimo de lucro a los usuarios de internet".

vi) Que el registro y uso del nombre dominio y su utilización, por parte del Demandado no solo es de mala fe por parte del Demandado, sino que causa un serio perjuicio a la imagen y prestigio del Demandante, quien es ajeno a las actividades que se llevan a cabo en el sitio.

En apoyo a su demanda, la parte demandante aportó las pruebas documentales con la que se fundamenta los hechos expuestos. El Demandado contesto la Demanda[35] afirmando que el Instituto Cultural Iberoamericano Mario Vargas llosa es una entidad sin fines de lucro, que tiene autorización directa, verbal e implícita del escritor Mario Vargas Llosa para utilizar su nombre y por ende para registrar y utilizar el nombre de dominio mariovragasllosa.org. El Panel aplica al caso la Política[36] y afirma: "el tratamiento jurídico de marca que se le han atribuido a los nombres propios de las personalidades o personajes del mundo de las artes, la cultura, la música, la política" y establece

[35] Se incluye como anexo en la presente tesis el Caso Nº D2004-0956, donde puede observarse que el demandado se defiende afirmando que el Instituto Cultural Mario Vargas Llosa inicio sus actividades en febrero de 1997 y que sus actividades de carácter cultural han sido reconocidas por universidades e instituciones de carácter intelectual en diferentes países de América Latina y Europa.

[36] Política de solución de conflictos por medios electrónicos, párrafo 4, literalmente establece: a) Controversias aplicables: usted estará obligado a someterse a un procedimiento administrativo obligatorio en caso que un tercero (un demandante) sostenga ante el proveedor competente, en cumplimiento del reglamento que:"..hay identidad o similitud del nombre de dominio hasta el punto de causar confusión con respecto a una marca de productos o servicios sobre que el demandante tiene derechos.

que si es aplicable a Mario Vargas Llosa ese tipo de protección por su prestigio y actividad literaria.

Asimismo, el Panel para resolver el caso afirma: "el nombre propio del demandante es a su vez el nombre que lo identifica como autor de obras literarias en el ejercicio del derecho de autor", concretamente del derecho moral de paternidad de la obra de Mario Vargas Llosa que cumple las siguientes funciones: Identificador del origen de la obra literaria[37] ; nombre del autor como medio de identificación comercial[38]; nombre del autor como elemento de distinción[39]. Debido a estas consideraciones y probar que el Demandante utilizo y registro el nombre de dominio de mala fe, el Panel decide: "que el nombre de dominio mariovargasllosa.org es idéntico al nombre del Demandante, el que es ampliamente conocido como Mario Vargas Llosa, que este nombre constituye una marca de hecho de la que es titular el Demandante, que el Demandado no probó tener un interés legitimo en el nombre de dominio y que el registro y uso del mismo se ha llevado a cabo de mala fe".

1.3.1.2.2. **El caso Mapfre sobre Nombre de Dominio**[40]. El Centro de Arbitraje y Mediación de la OMPI recibe la demanda por correo electrónico de Mapfre Familiar, Compañía de Seguros y Reaseguros S.A, con domicilio en Madrid, España. El registro del nombre de

[37] El Panel al resolver el caso afirma: "El derecho a la paternidad de la obra consiste en la facultad que tiene todo autor de que se reconozca su condición de creador de la obra. El derecho a la paternidad de la obra artística protege la intima relación existente entre el autor y el fruto de su creatividad intelectual, y puede ser ejercido mediante el uso del nombre propio del autor (como es el caso de Mario Vargas Llosa) o mediante el uso de seudónimo".

[38] El nombre del autor, en forma similar a una marca, puesto en su obra (producto) permite facilitar su comercialización a través de los distintos medios publicitarios. Son innumerables los factores que llevan a una obra de arte, musical o literaria al éxito comercial. El Panel al resolver el caso afirma: "Uno de esos factores es sin lugar a dudas, el nombre del autor o del artista que crea la obra o que está involucrada en la misma. En el presente caso, al tratarse de un autor de fama y prestigio internacional su nombre es valioso y el mismo es un identificador que sin lugar a dudas permite que su obra puesta en el mercado sea más atractiva al publico que otras obras de otros autores del mismo género".

[39] El Panel al resolver el caso afirma: "El nombre del autor Mario Vargas Llosa, por si mismo y en forma similar a una marca es suficientemente especial y notorio que estar impreso en un libro, revista o cualquier escrito, indudablemente el lector asocie directamente al autor con su obra"

[40] Caso Nº D2013-0548. Decisión del Panel Administrativo de la OMPI. Demandante: Mapfre Familiar, Compañía de Seguros y Reaseguros S.A. con domicilio en Madrid, España versus Demandada: PRQ Inet KB con domicilio en Estocolmo, Suecia. Demanda presentada el 20 de marzo de 2013 y resuelta por el Panel Administrativo el 29 de mayo de 2013. El texto del Caso es incluido como Anexo en la presente Tesis.

dominio en disputa es: Mapfre-teestafamos.com y fue realizado el 31 de diciembre de 2012, de cual la demandante solicita la transferencia por los siguientes argumentos:

i) Mapfre Familiar es titular de toda una familia de marcas en torno al signo distintivo MAPFRE tanto en España como a nivel comunitario e internacional.
ii) El nombre de dominio en disputa está formado de dos elementos unidos por un guión: El primer elemento está compuesto por el término "mapfre", lo cual supone una reproducción literal de la denominación de la marca renombrada MAPFRE. El segundo elemento está compuesto por la expresión descriptiva "te estafamos", que evidentemente juega con la denominación del programa de fidelizacion de "Mapfre Te Cuidamos".
iii) El registro de un nombre de dominio que coincide con la marca de un tercero implica una infracción de los derechos de exclusiva el titular de la marca. La infracción es aun mas grave si la marca que ha sido incorporada como nombre de dominio es notoria, como es el caso del registro de MAPFRE de la actora.
iv) La Demandada PRQ Inet KB no es comúnmente conocida por el nombre de dominio en disputa y carece de registros de marca en torno al elemento de MAFPRE. Mafpre familiar en ningún momento ha autorizado el registro del nombre de dominio similar a sus marcas.
v) El derecho a la libertad de expresión no legitima a PRQ Inet KB el registro de un nombre de dominio idéntico o similar hasta el punto de crear confusión con la marca MAPFRE.
vi) PRQ Inet KB tenía que conocer con anterioridad al registro al nombre de dominio la marca MAFPRE por ser un signo renombrado y aparecer los logotipos en la propia página web. PRQ Inet KB puede ejercer su

derecho a la libertad de expresión haciendo uso de otro nombre de dominio que no sea idéntico o confundible con la marca MAFPRE. PRQ Inet KB hacen uso de la expresión "te estafamos" junto a la marca MAPFPRE con el manifiesto objeto de menoscabar el lema de la Demandante "te cuidamos" y su actividad a través del nombre de dominio mapfretecuidamos.com.

vii) En definitiva, son muchas las circunstancias que revelan como la demandada no sólo no ostenta derechos e intereses legítimos sobre el nombre de dominio en disputa, sino que ponen de manifiesto el registro y uso del mismo de mala fe.

La demandada no contesto las alegaciones de la Demandante. El Panel basa su decisión en la Política[41] , y afirma que: "la inclusión en su totalidad de una marca notoriamente conocida en un nombre de dominio, independientemente de los elementos adicionales que la acompañan, no elimina la evidente identidad entre la una y la otra".

Asimismo, afirma que: "la demandada no tiene derechos o intereses legítimos sobre el nombre de dominio en disputa" y que la "demandada ha registrado y usado el nombre de dominio de mala fe"[42] . Debido a estas consideraciones y probar que el Demandante utilizo y registro el nombre de dominio de mala fe, el Panel decide: "que el nombre de dominio Mapfre-testafamos.com sea transferido al demandante".

[41] Política Uniforme de Solución de Conflictos. Apartado 4 a): "Que el nombre de dominio registrada por la demandada sea idéntico, u ofrezca semejanza que produzca la confusión con una marca de productos o servicios sobre la que el Demandante tenga derechos". "Que la demandada carezca de derecho o interés legitimo en relación con el nombre de dominio en disputa". "Que el nombre de dominio en disputa haya sido registrado y usado de mala fe".

[42] El Panel para resolver el caso afirma: "no equivale a actuar de buena fe registrar un nombre de dominio cuya parte dominante es la marca de un tercero para criticar a ese tercero".

1.3.1.2.3. **Caso sobre Correo Electrónico No solicitado (SPAM)**[43]: El Denunciante es Alfredo San Martin el Denunciado es Escuela de Empresa SAC. El Señor Alfredo San Martin denuncio a Escuela de Empresa SAC (en adelante, La Comisión) por enviar a su cuenta de correo electrónico publicidad comercial no solicitada, sin cumplir con las disposiciones de la Ley 28493- Ley que regula el uso del Correo Electrónico Comercial No Solicitado (SPAM)- puesto que: (i) los correos electrónicos remitidos no incluirían la palabra "publicidad" en el asunto; (ii) se habría variado el nombre de la empresa y agregado un espacio en el dominio para evitar su bloqueo; y (iii) la dirección desde la que abrían sido enviados los correos electrónicos no existirían.

La Comisión de Protección al Consumidor[44] declaró fundada la denuncia presentada por el Señor San Martin contra la Escuela de Empresa por infracción de la Ley 28493 y del artículo 8º de la Ley de Protección al Consumidor y sancionarla con una multa de 5 Unidades Impositivas tributarias, por haber remitido publicidad no solicitada mediante un correo electrónico que no cumplía con las formalidades previstas en la primera norma. Asimismo, ordena a la denunciada como medida correctiva que cumpla con abstenerse de enviar correos electrónicos comerciales a la dirección del denunciante y con adecuar el envío de los mismos a lo dispuesto en las normas en materia de correos electrónicos no solicitados.
La denunciada apeló la resolución indicando que no había quedado acreditado que su empresa hubiera sido la emisora de los correos electrónicos objeto de la controversia. En tal sentido, señalo que era probable que los mensajes fueran enviados por un tercero que deseaba generarle un perjuicio. Asimismo, afirmó que el denunciante debió ejercer su derecho de solicitar que no

[43] Tribunal de Defensa de la Competencia y de la Propiedad Intelectual. Sala de Defensa de la Competencia Nº 2. Resolución 0774-2009/SC2-INDECOPI. Expediente 0415-2007/CPC
[44] Resolución 1380-2008/CPC del 16 de Julio de 2008.

se le continúen enviando correos electrónicos no deseados, situación que no habría sido probada por éste. Finalmente, manifestó que la multa resultaba excesiva y desproporcionada.

El Tribunal afirma: La denunciada ha manifestado que los correos electrónicos podrían haber sido enviados por un tercero con la finalidad de generarle perjuicio. Sin embargo, no ha incorporado al expediente material probatorio que sustente tal afirmación. Lo anterior, pese a lo previsto en el artículo 196º del Código Procesal Civil- de aplicación supletoria al presente procedimiento[45]-, el cual dispone que la carga de la prueba corresponde a quien afirma los hechos que configuran su pretensión o a quien los contradice alegando nuevos hechos. En este extremo, es necesario señalar que si bien en procedimientos sancionadores, al Administración debe probar la comisión efectiva de una infracción, la ley es expresa al establecer como responsables por los correos electrónicos que incumplan sus disposiciones a los beneficiarios del mismo, situación que justifica que en tales caso, estos deben probar en vía de defensa que no guardan vinculación alguna con las personas que habrían remitido los referidos correos".

1.3.2. La Construcción de la Identidad Moderna en un entorno Digital

"Para formular la cuestión en términos de identidad es menester la pre-condición de un cierto desarrollo en nuestra comprensión de nosotros mismos… eso significa también que nuestra identidad, definida de la manera que nos proporcione nuestra orientación fundamental, es de hecho muy compleja y multilateral. Estamos enmarcados por lo que percibimos como compromisos universalmente validos…y también por lo que consideramos como identificadores particulares… el hecho es

[45] Código Procesal Civil. Disposiciones Finales. Primera. Las disposiciones de este Código se aplican supletoriamente a los demás ordenamientos procesales, siempre que sean compatibles con su naturaleza.

que nuestra identidad es más profunda y multilateral que cualquier posible articulación que hagamos con ella"[46].

Charles Taylor[47] explora varias facetas de la identidad moderna. Afirma que la identidad personal (selfhood) o individualidad y el bien o moralidad son temas que van inextricablemente entretejidos. Nuestras nociones sobre justicia, respeto a la vida ajena, bienestar y dignidad están directamente relacionados con la identidad y dignidad de las personas. Las cuestiones morales tienen una fuerte valoración en torno a la identidad personal.

Asimismo, Charles Taylor incide sobre la necesidad de coherencia en lo que respecta nuestras reacciones morales. La cuestión de coherencia se plantea cuando la reacción va relacionada con un objeto idóneo, como es la identidad digital que permite asignar atributos y características morales a una persona por sus relaciones en internet.

En el caso citado[48] de nombres de Dominio de Mario Vargas Llosa observamos como la identidad digital en internet es fundamental para que haya coherencia entre el atributo moral de escritor mundialmente conocido, identificado en su nombre de dominio vargasllosa.com con los atributos asignados a su identidad digital atribuida por el nombre de dominio mariovargasllosa.org de la persona jurídica Instituto Cultural iberoamericano Mario Vargas Llosa. La coherencia en la identificación de las características esenciales de su identidad digital son fundamentales para el ejercicio de sus derechos.

"La unidad de la persona se manifiesta en la coherencia de su proyecto, basándose esta unidad en el deseo de orden superior

[46] TAYLOR, Charles: "Fuentes del yo : La construcción de la identidad moderna". Ed. Paidos. Barcelona, España. 2006. Páginas 53, 54.
[47] Vid, TAYLOR, Charles: ob.cit. páginas 19 a 27.
[48] Ver el 1.3.1 de la presente tesis, donde reseñamos el casode Nombres de Dominio Mario Vargas Llosa. Asimismo, en los anexos transcribimos el caso completo.

que ha de seguirse, en formas congruentes con su sentido del derecho y de la justicia, principios de la elección racional. Naturalmente, una persona no configura sus objetivos de súbito, sino solo de manera gradual; pero, dentro de los modos permitidos por la justicia, puede formular y seguir un proyecto de vida, construyendo así su propia unidad. El rasgo distintivo de una concepción de fin dominante es la forma que se supone se realiza la unidad del yo"[49].

Como dice John Rawls[50] la coherencia de su proyecto de vida, se manifiesta en a la unidad de la persona; aplicado, al ámbito de internet, esta coherencia de la persona se atribuye a la unidad del yo que es expresado en el entorno digital. La identidad digital con participación de un tercero de confianza, como puede ser el Estado, garantiza esta unidad del yo y esta coherencia en su proyecto de vida.

Asimismo, John Rawls precisa que la personalidad moral se caracteriza por la concepción del bien y el sentido de la justicia. El propósito de las personas consiste en establecer condiciones justas y favorables para que cada construya su propia unidad, que sea coherente con su proyecto de vida y que sea protegido y garantizado por la justicia y la ley. En un entorno digital la identidad digital contiene esta unidad de la persona y su correspondiente proyecto de vida, de ahí la importancia de su regulación adecuada de acuerdo a un sistema funcional y coherente que proteja a la persona contra el uso indebido de las múltiples identidades y de la suplantación de identidad.

"Internet es la sociedad, expresa los procesos sociales, los intereses sociales, los valores sociales, las instituciones sociales. ¿Cuál pues, es la especificidad de Internet, si es la sociedad?.

[49] RAWLS, Jhon: "Teoria de la Justicia" Ed. The Belknap Press of Harvard University, Cmabirdge, Massachussets. Segunda Edicion en Español, sexta reimpresion. 2006. Pagina 507.
[50] Vid. RAWLS, Jhon Rawls: ob.cit. paginas 506 a 512.

La especificidad es que se constituye en la base material y tecnológica de la sociedad red, es la infraestructura tecnológica y el medio organizativo que permite el desarrollo de una serie de nuevas formas de relación social que no tienen su origen en internet, que son fruto de una serie de cambios históricos, pero no podrían desarrollarse sin internet..Lo que hace Internet es procesar la virtualidad y transformarla en nuestra realidad, constituyendo la sociedad red, que es la sociedad en que vivimos"[51].

Como afirma Manuel Castells[52] Internet es el tejido de nuestras vidas en este momento. La utilización de Internet para desarrollar nuestras tareas e intereses concretos, es lo que genera niveles de interaccion mas fuertes en internet. Es decir, la reafirmación de la unidad del yo en el ámbito digital, la búsqueda de coherencia entre lo que aparece publicado de cada persona en internet con lo que es en realidad la propia persona, construyendo su "reputación on line", es lo que en la sociedad da valor e importancia a la identidad digital en el proceso de construir nuestra identidad moderna en un entorno digital. La persona necesita de una identidad segura que impida la suplantación de identidad. Por lo cual, cada persona requiere que su identificación digital sea garantizado debidamente por la justicia y el derecho.

1.3.3. Importancia de la Identificación Digital para el Pleno Ejercicio de los Derechos

"Desde una perspectiva jurídica, la identidad de la persona es la base sobre la que se construye el andamiaje de derechos y obligaciones. Si bien los derechos están establecidos *erga omnes*, vale decir, para todos en general, la apropiación de una situación particular amparada por el marco normativo con sus respectivos derechos y obligaciones, surge a partir de la identidad específica de cada persona[53]"

[51] CASTELLS, Manuel: ob.cit. Pagina 13.
[52] Vid. CASTELLS, Manuel: ob.cit. Páginas 1 al 13.
[53] Marco para Identificación Electrónica Social Iberoamericana" Ob. Cit.

En un entorno digital, en el ejercicio de los derechos y obligaciones de la persona en internet, la protección y regulación de la identidad digital permiten que la regulación en torno al comercio electrónico, con la compraventa de bienes y servicios se efectúen con seguridad jurídica y los derechos contenidos en los contratos y la legislación puedan cumplirse a cabalidad; con respecto a los negocios electrónicos, que los servicios de contabilidad, medicina, arquitectura en línea se realicen en forma confiable y segura; con respecto al gobierno electrónico que el Estado esté digitalmente donde el ciudadano necesite y pueda identificar a quienes y con qué periodicidad realiza su apoyo; con respecto al aprendizaje electrónico, se identifica el cumplimiento en cada persona en un entorno digital, del proceso de enseñanza – aprendizaje.

La identificación comprobando los datos que acreditan la identidad permite evitar la suplantación de las personas en los distintos procesos digitales que realizan. Para el fortalecimiento del derecho informático una adecuada regulación y protección del derecho de identidad en internet, garantiza mecanismos de seguridad y confianza que permita a las personas realizar actividades económicas y sociales concretas en la red.

En una relación entre dos personas o más, con efectos jurídicos, es necesario acreditar la identidad de las partes que intervienen en ella. Un contrato, una demanda, un matrimonio, una adquisición, una venta, en fin, cada operación con efectos jurídicos requiere la identificación de las personas que participan de ella como paso previo a su celebración. En la administración pública, ocurre algo similar. Los trámites que se realizan ante la Administración requieren la identificación de la persona que lo inicia y de los funcionarios que intervienen.

Los casos de suplantación de identidad en compra venta de inmuebles, en bigamia, fraudes y engaños diversos en la red, pueden disminuir con una adecuada identificación; asimismo, el expediente electrónico judicial y administrativo, la notificación electrónica, la historia clínica electrónica, van a funcionar en forma màs segura y confiable con una adecuada regulación y protección del derecho de identidad digital en Internet.

La implementación de políticas públicas de alcance social requiere también la identificación de sus beneficiarios utilizando tecnologías de la información y comunicaciones (TICs). Las políticas educativas, las de salud, las de inclusión digital, todas se apoyan en una correcta identificación de las personas que son beneficiarias utilizando base de datos, sistemas de información, internet. Para acceder a estas políticas sociales, las personas deben identificarse , muchas veces en un entorno digital ante los órganos administrativos mediante mecanismos de autenticación virtual, que en algunos casos incluye el dni electrónico, a fin de acceder a los beneficios y ejercer plenamente sus derechos.

La identificación de las personas, conforme nuestro ordenamiento jurídico, es un elemento esencial de los actos jurídicos, ya que el error o inexactitud sobre la identidad de una persona, acarrea la nulidad del acto jurídico, al constituirse un vicio del consentimiento que invalida la relación jurídica. Los actos jurídicos pueden realizarse, también por medios electrónicos, por tanto en un entorno digital, también es importante la identificación para que el desarrollo de las personas se realice en forma segura; para lo cual es necesario contar con una adecuada regulación y protección del derecho de identidad digital en Internet.

"La identidad y la identificación de las personas, son materia del derecho sustantivo y del derecho procesal. La identificación hace referencia tanto a los datos de identidad de una persona (nombre, apellidos, naturaleza, edad, sexo, domicilio y nacionalidad), como al acto y procedimiento de comprobación y acreditación de la identidad. La identificación de la persona supone su individualización dentro del colectivo social. El nombre es uno de los criterios principales de identificación, al referirse a la filiación de la persona. Lo identifican otros datos, como se verá más adelante, que son los datos objeto de la biometría. Rasgos personales, únicos, que sirven para identificar indubitablemente a la persona[54]".

El nombre es una expresión más de la identidad personal que consiste en el empleo de varias palabras o fonemas para designar a una persona. En el caso, de la persona natural su nombre en el entorno

[54] Ibidem

digital es esencial que sea debidamente identificado para evitar las consecuencias jurídicas en los casos de requerimiento penal de personas que tienen homonimia.

En la legislación peruana en materia informática está vigente la Ley 28119 modificada por la Ley 29139, que prohíbe el acceso de menores de edad a páginas web de contenido pornográfico y cualquier otra forma de comunicación en red de igual contenido, en las Cabinas Públicas en Internet, contiene disposiciones relacionadas con la identificación e identidad digital.

El Reglamento[55] tiene por objeto regular la aplicación de la prohibición del acceso a menores de edad a páginas web de contenido pornográfico y cualquier otra forma de comunicación en red (chat, redes sociales, etc). La norma se aplica a los propietarios, conductores, encargados de turno y aquellas personas que tienen a su cargo la administración de las cabinas públicas, quienes están obligados entre otras acciones a las siguientes: i) Instalar, en todos los equipos de computo, un software especial de filtro de contenido; que tenga como efecto impedir a menores de edad, la visualización de páginas web de contenido y/o información pornográfica. ii) Solicitar a toda persona, que ingresa al establecimiento, su Documento Nacional de Identidad-DNI para identificar si se trata de un menor de edad; sin perjuicio de solicitarles también su DNI siendo mayor de edad; para el registro escrito de usuarios. Iii) El administrador o responsable de turno tiene la obligación de tener disponible el registro escrito de usuarios y exhibirlo cada vez que sea requerido por la autoridad competente. Incumplir esta obligación constituye una infracción a la exhibición del registro escrito de los usuarios.

[55] Decreto Supremo Nº 025-2010-ED, publicado en el Diario Oficial El Peruano, el miércoles 01 de diciembre de 2010.

1.3.4. Los Instrumentos, Declaraciones, Convenios Internacionales y el Derecho de Identidad Digital.

1.3.4.1. Declaraciones y Documentos sobre Sociedad de la Información e Identidad Electrónica.

En la Cumbre Mundial de la Sociedad de la Información, en la declaración de principios[56] se afirma lo siguiente:"declaramos nuestro deseo y compromiso comunes de construir una Sociedad de la Información centrada en la persona, integradora y orientada al desarrollo".. "cada persona debería tener la posibilidad de adquirir las competencias y los conocimientos necesarios para comprender la Sociedad de la Información y la economía del conocimiento, participar activamente en ellas y aprovechar plenamente sus beneficios"…"el fomento de un clima de confianza, incluso en la seguridad de la información y la seguridad de redes, la autenticación, la privacidad, es requisito previo para que se desarrollo la Sociedad de la Informacion"
Según la Declaración de Bàvaro[57], definimos la Sociedad de la Información como "un sistema económico y social donde el conocimiento y la información constituyen fuentes fundamentales de bienestar y progreso, que representa una oportunidad para nuestros países y sociedades, si entendemos que el desarrollo de ella en un contexto tanto global como local requiere profundizar principios fundamentales tales como el respeto a los derechos humanos dentro del contexto más amplio de derechos fundamentales, la democracia, la protección del medio ambiente, el fomento a la paz, el derecho al desarrollo, las libertades fundamentales, el progreso económico y la equidad social".

Durante el año 2010, se desarrolló una intensa agenda de reuniones de la Cumbre Iberoamericana de Jefes de Estado y de Gobierno. Se realizaron reuniones ministeriales sectoriales que convocaron a los responsables de las áreas de Agricultura, Salud, Trabajo, Administración Pública y Reforma del Estado, Turismo, Educación, Infancia y Adolescencia, Justicia, Presidencia, Vivienda y Urbanismo. Dichas actividades concluyeron en la XX Cumbre Iberoamericana, que

[56] Cumbre Mundial sobre la Sociedad de la Información, Ginebra 2003-Tunez 2005. Declaración de Principios. Construir la Sociedad de la Información: Un desafío global para el nuevo milenio. En www.itu.int/wsis
[57] En el Marco de la Conferencia Ministerial Regional Preparatoria de América Latina y el Caribe para la Cumbre Mundial de la Sociedad de la Información.

emitió la Declaración de Mar del Plata “Educación para la Inclusión Social”.

En todas las reuniones ministeriales sectoriales, de una u otra manera, se abordó el tema de la inclusión social como eje de las políticas públicas de la región. Especialmente, en la XIII Reunión de la Red Iberoamericana de Ministros de La Presidencia y Equivalentes (RIMPE), celebrada en Lisboa, Portugal, se abordó el tema de la Participación de los Ciudadanos en la era del Gobierno electrónico. En dicho encuentro, los países acordaron que “los objetivos del gobierno electrónico deben trascender la mera eficacia y eficiencia de los procesos de administración, hacia formas que permitan cambios sociales, políticos, económicos en pro del desarrollo humano, la igualdad de oportunidades y la justicia social.”

La XIII Reunión de la Red Iberoamericana de Ministros de La Presidencia y Equivalentes (RIMPE), giró en torno a la Participación de los Ciudadanos en la era del Gobierno Electrónico: Educación para la Ciudadanía e Inclusión Digital. Los ministros acordaron reforzar la cooperación, información y coordinación en el área del Gobierno Electrónico en el espacio iberoamericano. Asimismo, se acordó la recogida de información sobre programas, acciones y buenas prácticas en el área de la simplificación, la modernización administrativa y la inclusión digital llevados a cabo en diversos países iberoamericanos, con el fin de desarrollar proyectos de cooperación de interés común.

Entre otras, la Declaración de Lisboa, contiene recomendaciones a los Gobiernos relativas a lograr “un modelo de Administración más abierto, transparente y colaborativo, que permita responder eficazmente a los desafíos económicos, sociales, culturales y ambientales que se plantean a nivel mundial”. Para ello, la Declaración contempla el uso de las TIC‟s para transformar la Administración. En ese sentido, los países signatarios consideran que “las políticas de administración electrónica y simplificación administrativa deben contribuir, de manera articulada, al desarrollo de servicios públicos con mayor calidad”.

Los niveles de seguridad deben caracterizar el grado desconfianza de un medio de identificación electrónica para establecer la identidad de una persona. La Administración pública debe organizarse con el respaldo seguro de identificar en forma indubitable con la personas que se relaciona en la red.

"En la sociedad de la red el uso de nuestros derechos se efectúa cada vez más en internet y en el entorno digital. Desde el punto de vista del bienestar jurídico este hecho presupone un minucioso diseño jurídico de los sistemas y redes de datos. La cultura informática y jurídica así como la competencia profesional deberían sincronizarse. La realización de la sincronización suficiente presupone, además de la estrecha colaboración entre las profesiones, estándares diseñados desde el punto de vista jurídico. El desarrollo de los estándares,
donde la protección de los datos personales sea uno de los puntos de partida, sigue estando en sus comienzos. y por el rápido desarrollo de la informática, implican un elevado número de problemas. El diseño de los estándares está haciéndose una modalidad de la destreza jurídica"[58].
Por otra parte, cabe señalar, que en el Consejo de Derechos Humanos de las Naciones Unidas en su 20º periodo de Sesiones, del 29 de Junio de 2012, se afirma: "que los derechos de las personas también deben estar protegidos en Internet" y se reconoce "la naturaleza mundial y abierta de Internet como fuerza impulsora de la aceleración de los progresos hacia el desarrollo en sus distintas formas". Por tanto, el derecho de identidad, como derecho humano también debe estar protegido en internet.

En la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI o UNCITRAL), se ha emitido un documento sobre la posible labor futura en materia de comercio electrónico: cuestiones jurídicas relacionadas con la gestión de identidad y los servicios de confianza, en Mayo de 2015, donde se afirma que: "Habida cuenta de la creciente importancia de la comprobación de la identidad de la otra parte en las operaciones comerciales electrónicas de todos los tipos y del uso cada vez mayor por las partes de los

[58] Saarenpää **,** Ahti : "Legal Welfare And Legal Planning In The Network Society" . En Memorias del XVI Congreso Iberoamericano de Derecho e Informática . Ed. Ministerio de Justicia, Derechos Humanos y Culto. Imprenta Moreno. Quito, Ecuador. Septiembre 2012. Página 41.

servicios de confianza en ciertos tipos de operaciones electrónicas, parece conveniente comenzar a trabajar en cuestiones jurídica conexas en el marco de la CNUDMI"[59].

1.3.4.2 Reglamento del Parlamento Europeo sobre Identificación Electrónica y los Servicios de Confianza en el Mercado Interior.

El Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo de Europa del 23 de Julio de 2014, relativo a la identificación electrónica y los servicios de confianza en el mercado interior y por la que se deroga la Directiva 1999/93/CE, es de importancia y actualidad para el tema investigado.
En los numerales 1, 2, 3, 4, 5 y 6 de los Considerandos de dicho Reglamento[60], se afirma lo siguiente:

a) "La creación de un clima de confianza en el entorno en línea es esencial para el desarrollo económico y social. La desconfianza en particular debida a la inseguridad jurídica percibida, hace que los consumidores, las empresas y las administraciones públicas duden a la hora de realizar transacciones por via electrónica y adoptar nuevos servicios".

b) "El presente Reglamento se propone reforzar la confianza en las transacciones electrónicas en el mercado interior proporcionando una base común para lograr interacciones electrónicas seguras entre los ciudadanos, las empresas y las administraciones públicas".

c) "La Directiva 1999/93/CE del Parlamento Europeo y del Consejo se refiere a las firmas electrónicas, sin ofrecer un marco global transfronterizo e intersectorial para garantizar unas transacciones seguras, fiables y de fácil uso. El presente reglamento refuerza y amplía el acervo que representa dicha Directiva".

---

[59] COMISION DE NACIONES UNIDAS PARA EL DERECHO MERCANTIL INTERNACIONAL (CNUDMI): "Posible Labor Futura en materia de comercio electrónico: cuestiones jurídicas relacionadas con la gestión de identidad y los servicios de Confianza". Propuesta de Austria, Bèlgica, Francia, Italia y Polonia. A/CN.9/854. 5 de Mayo de 2015. Documentación para el 48º periodo de sesiones en Viena, Austria, de 29 de Junio al 16 de Julio de 2015. Página 5. En: http://www.uncitral.org

[60] Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo de 23 de Julio de 2014. Diario Oficial de la Unión Europea del 28.8.2014. L 257/73 .

d) "La Comunicación de la Comisión de 26 de Agosto de 2010 titulada "Una Agenda Digital para Europa" señalaba que la fragmentación del mercado digital, la falta de interoperabilidad y el incremento de la ciberdelincuencia constituían obstáculos importantes para el ciclo virtuoso de la economía digital. En su informe sobre la ciudadanía de 2010, titulado "La eliminación de los obstáculos a los derechos ciudadanos de la UE", la Comisión subrayó asimismo la necesidad de resolver los principales problemas que impiden a los ciudadanos de la Unión disfrutar de los beneficios de un mercado único digital y unos servicios digitales transfronterizos".

e) "En sus conclusiones de 4 de febrero de 2011 y del 23 de Octubre de 2011, el Consejo Europeo invitó a la Comisión a crear un mercado único digital para 2015 a fin de progresar rápidamente en ámbitos clave de la economía digital y promover un mercado único digital plenamente integrado facilitando el uso transfronterizo de los servicios en línea, con especial atención a la identificación y autenticación electrónicas seguras".

f) "En sus conclusiones del 27 de mayo de 2011 el Consejo invitó a la Comisión a contribuir al mercado único digital creando condiciones apropiadas para el reconocimiento mutuo a través de las fronteras de instrumentos clave tales como la identificación electrónica, los documentos electrónicos, las firmas electrónicas y los servicios de entrega electrónicos, así como para unos servicios de administración electrónica interoperables en toda la Unión Europea.

Capítulo 2

Relación de la Protección de Datos Personales y las Firmas y Certificados Digitales con el Derecho de Identidad Digital en Internet.

2.1. Análisis de la Ley 29733, Ley de Protección de Datos Personales y su relación con el derecho de identidad digital.

La Ley 29733, Ley de Protección de Datos Personales fue publicada el 03 de Julio de 2011. El Reglamento de la Ley de Protección de Datos Personales D.S. 003-2013-JUS fue publicado el 22 de Marzo de 2013. Tanto la totalidad de la ley como el Reglamento entraron en vigencia en el plazo de treinta días hábiles desde la publicación del reglamento, es decir desde el miércoles 08 de Mayo de 2013

La Resolución Directoral N° 019-2013-JUS/DGDP que aprueba la Directiva de Seguridad de la Información administrada por los Banco de Datos Personales fue emitida el 11 de Octubre de 2013 y publicada en el Portal Institucional del Ministerio de Justicia.

Por Resolución Directoral Nº 060-2014/DGPDP, publicada el 01 de Agosto de 2014 en el Diario Oficial El Peruano, se aprueba la Directiva Nº 001-2014-JUS/DGPDP sobre protección de datos personales en el marco de los procedimientos para la construcción, administración, sistematización y actualización de base de datos personales

vinculados con programas sociales y subsidios que administra el Estado.

La Primera Disposición Complementaria Transitoria del Reglamento de la Ley de Protección de Datos Personales establece: "En el plazo de dos (2) años de la entrada en vigencia del presente reglamento, los banco de datos personales existentes, deben adecuarse a lo establecido por la Ley y el presente reglamento". Es decir, el plazo de adecuación para los banco de datos personales existentes la 08 de Mayo de 2013, es hasta el 08 de Mayo del 2015.

La Segunda Disposición Complementaria Transitoria del Reglamento establece: "la facultad sancionadora de la Dirección General de los banco de datos personales existentes a la fecha de entrada en vigencia del reglamento (es decir el 08 de mayo de 2013), queda suspendida hasta el vencimiento del plazo de adecuación (es decir el 08 de mayo de 2015).

"El objetivo de la protección de datos personales es tutelar a las personas cuyos datos son objeto de tratamiento. Normalmente, dicho objetivo se logra combinando los derechos del interesado y las obligaciones de quienes tratan los datos o controlan dicho tratamiento"[61]. En el Perú la Ley de Protección de Datos Personales tiene por objeto "garantizar el derecho fundamental a la protección de datos personales, previsto en el artículo 2º inciso 6 de la Constitución Política del Perú, en un marco de respeto de los demás derechos fundamentales que en ella se reconocen".

Una de las principales prioridades con la dación de la Nueva Ley Peruana de Datos Personales, debe ser extender y consolidar en la sociedad una auténtica cultura de la protección de datos personales en el contexto de la sociedad de la información y un uso intensivo de internet y las tecnologías de comunicaciones digitales e informática.

[61] FERNANDEZ LOPEZ, Juan Manuel: "Flujo Internacional de Datos". En Revista Iberoamericana de Derecho Informático Nºs 30, 31,32. 1999. Ed. Universidad Nacional de Educación A Distancia. Centro Regional de Extremadura- Mérida, España. Página 189.

2.1.1. Objeto y aplicación de la ley de protección de datos personales y el derecho de identidad digital.

"Es pertinente preguntarse cómo nació el derecho a la privacidad. Podemos identificar dos nacimientos: uno en los Estados Unidos, con los trabajos de Warren y Brandeis en la década de 1890.. A su turno, la privacidad también nace en Europa, esta vez bajo la forma de la protección de datos personales. El motivo subyacente es un hecho histórico: el exterminio de judíos, gitanos y otros grupos determinados de personas que emprendieron los nazis en Alemania, utilizando los datos del censo para identificarlos. De allí aprendieron los alemanes que la única protección de los ciudadanos en el futuro, ante nuevas concentraciones de poder, era evitar desde raíz la acumulación de datos personales. Esta percepción de la protección de datos personales como un derecho fundamental se extiende por toda Europa"[62]

La Nueva Ley de Protección de datos Personales tiene la siguiente estructura: Título I: Disposiciones Generales. Título II: Principios Rectores. Título III: Tratamiento de Datos Personales. Título IV: Derechos del Titular de Datos Personales: Título V: Obligaciones del titular y del encargado del banco de datos personales. Título VI: Banco de Datos Personales. Título VII: Autoridad Nacional de Protección de Datos Personales, Título VIII: Infracciones y Sanciones administrativas. Disposiciones Complementarias Finales.

"En su estructura normativa puede distinguirse una parte general dedicada a la proclamación del derecho de la protección de datos personales y sus manifestaciones, integrada por los Títulos I al V; y una parte especial, en la que se establecen los mecanismos

[62] DE GRACIA, Carlos Gregorio: "¿Está muerta la Privacidad? Algunas Reflexiones a Modo de Respuesta". En "Habilitando la apertura: el futuro de la sociedad de la información en América Latina y el Caribe". Ed. Fundación Comunica, Montevideo, Uruguay y Coedición: International Development Research Center, Otawa, Canadá. 2013. Páginas 147 y 148.

organizativos e institucionales para el adecuado funcionamiento de los bancos de datos personales, formada por los Títulos VI al VIII… El derecho a la protección de datos personales es un derecho fundamental de tercera generación estrechamente vinculado a otros derechos de la misma nauraleza, pero de primera generación, como son el derecho al honor, buena reputación, intimidad, voz e imagen propias. Sin duda, por ser además un derecho relacional, su tratamiento inadecuado podría afectar el ejercicio de otros derechos fundamentales.."[63]

Por tratamiento de datos personales se entiende en la nueva ley peruana de protección de datos personales: "Cualquier operación o procedimiento técnico, automatizado o no, que permite la recopilación, registro, organización, almacenamiento, conservación, elaboración, modificación, extracción, consulta, utilización, bloqueo, supresión, comunicación por transferencia o por difusión o cualquier otra forma de procesamiento que facilite el acceso, correlación o intreconexión de los datos personales".

En el ámbito de aplicación, se precisa que esta Ley es de aplicación a los datos personales contenidos o destinados a ser contenidos en banco de datos personales de administración pública y de administración privada, cuyo tratamiento se realice en territorio nacional. Son objeto de protección especial los datos sensibles.

Por banco de datos personales se entiende: "Conjunto organizado de datos personales automatizados o no, independientemente del soporte, sea éste físico, magnético, digital, óptico u otros que se creen, cualquiera fuera la forma o modalidad de su creación, formación, almacenamiento, organización y acceso".

[63] Exposición de Motivos del Proyecto de Ley 4079/2009-PE sobre Protección de Datos Personales, página 33. Publicada en la Página Web: http://www.minjus.gob.pe. Fecha de Consulta: 28 de Junio de 2010.

El Banco de datos personales de administración privada es aquel “cuya titularidad corresponde a una persona natural o a una persona jurídica de derecho privado, en cuánto el banco no se encuentre estrictamente vinculado al ejercicio de potestades de derecho público”. En cambio, el banco de datos personales de administración pública es aquel “cuya titularidad corresponde a una entidad pública”.

Los datos sensibles, que deben objeto de protección especial por parte del Estado, están constituidos por los biométricos que por sí mismo pueden identificar al titular, datos referidos al origen racial y étnico; opiniones o convicciones políticas, religiosas, filosóficas o morales; hábitos personales; información sindical; e información relacionada a la salud o a la vida sexual.

Por otra parte, cabe señalar que las disposiciones de esta ley, no serán de aplicación a los siguientes datos personales:

a) A los contenidos o destinados a ser contenidos en banco de datos personales creados por personas naturales para fines exclusivamente relacionados con su vida privada o familiar.

b) A los contenidos o destinados a ser contenidos en banco de datos de la administración pública, sólo en tanto su tratamiento resulte necesario para el estricto cumplimiento de las competencias asignadas por ley a las respectivas entidades públicas: - para la defensa nacional, -seguridad pública, -el desarrollo de actividades en materia penal para la investigación y represión del delito.

Adicionalmente, debe tenerse en cuenta que la dación de la ley peruana de protección de datos personales permite al Estado peruano cumplir la vigésimo novena política de Estado del Acuerdo Nacional denominada "acceso a la información, libertad de expresión y prensa" y ejercer su potestad como estado parte en el Tratado de Libre Comercio celebrado con Estados Unidos , así como cumplir los mejores esfuerzos para la protección de los datos personales en el marco de los Tratados de Libre Comercio suscrito con Canadá y con la Unión Europea, respectivamente. También es el cumplimiento de un compromiso asumido en el marco de Privacidad de la APEC y del Plan de Acción del eLAC 2007 a través de su meta 25 y del Plan de Acción del eLAC 2010 a través de su meta 78, además de responder a la estrategia 3.3 del objetivo 3 del Plan de Desarrollo de la Sociedad de la Información en el Perú, la Agenda Digital.

Las disposiciones de la Ley y el Reglamento son de aplicación al tratamiento de datos personales cuando[64]:

i) Sea efectuado en un establecimiento del titular del banco de datos o de quien resulte responsable del tratamiento, ubicado en territorio peruano.
ii) Sea efectuado por un encargado del tratamiento con independencia de su ubicación, a nombre de un titular de banco de datos o de quien sea el responsable del tratamiento establecido en territorio peruano.
iii) El titular del banco de datos o quien resulte responsable del tratamiento no esté establecido en territorio peruano pero le resulte aplicable la legislación peruana, por disposición contractual o del derecho internacional.
iv) El titular del banco de datos o quien resulte responsable no esté establecido en territorio peruano pero utilice medios situados en dicho territorio, slavo que tales medios se utilicen únicamente con fines de tránsito que no impliquen un tratamiento.

[64] Reglamento de la Ley de Protección de Datos Personales. D.S. 003-2013-JUS, publicado el 22 de Marzo de 2013.

2.1.2. Conceptos y definiciones de protección de datos personales y el derecho de identidad digital.

2.1.2.1. El derecho a la autodeterminación informativa

"En la visión europea la protección de datos es uno de los derechos comprendidos por la libertad de expresión. Esta libertad incluye en primer lugar el derecho a expresarse. Pero también el derecho a no expresarse (también llamado autodeterminación informativa, que es equivalente al derecho de protección de datos personales), así como el derecho de audiencia… Cuando se analizan los riesgos actuales resulta obvio que la privacidad y la protección de datos personales están siendo atacadas, pero no pueden morir, porque sin estos derechos seríamos mucho más vulnerables a ser discriminados (en el empleo, en el acceso al crédito, a los seguros o a la salud) sin ningún tipo de protección"[65]

"La autodeterminación informativa..gira sobre el concepto que el ciudadano es el único que decide cuándo, dónde y por quién se conocen sus datos y, en su caso, se someten a tratamiento" [66]

La Constitución Peruana de 1993, reconoce la institución de la protección de datos personales (o derecho de autodeterminación informativa) como el derecho fundamental de toda persona a que los servicios informaticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar.

Seguidamente se incluye la tutela del hábeas data como garantía constitucional contra el hecho u omisión, por parte de cualquier autoridad, funcionario o persona, que lo vulnere o amenace.

[65] DE GRACIA, Carlos Gregorio: Ob. Cit. Páginas 149 y 150.
[66] DAVARA RODRIGUEZ, Miguel Angel: "La Protección de Datos en las Instituciones Sanitarias". En Anuario de Derecho de Tecnologías de la Información y Comunicaciones (TICs) 2006. Ed. Davara &Davara Asesores Jurídicos. Fundación Vodafone España. Madrid, España 2006. Páginas 3 a 69.

La Ley 29733 de Protección de Datos Personales, en su sexta disposición complementaria final establece: "las normas establecidas en el Código Procesal Constitucional sobre el proceso de hábeas data se aplican en el ámbito constitucional, independientemente del ámbito administrativo , materia de la presente ley. El Procedmiento Administrativo establecido en la presente ley no constituye via previa para el ejercicio del derecho via proceso constitucional".

Con respecto al derecho de autodeterminación informativa se afirma que: "el legislador…siguió la línea de la Unión Europea tutelándolo como un derecho autónomo e independizado del derecho a la intimidad, lo que resulta altamente positivo. En efecto, si bien ambos derechos se funden en la búsqueda proteccionista de la vida privada personal y familiar, su diferencia radica en que el derecho a la protección de datos busca el amparo, no [sólo] ya de aspectos privados o íntimos, sino de cualquier tipo de datos, en tanto estos puedan identificar o hacer identificable a una persona y servir para la confección de un verdadero perfil ideológico, sexual, económico, o de cualquier otra naturaleza"[67]

El Tribunal Constitucional del Perú se ha pronunciado sobre el derecho de autodeterminación informativa, distinguiéndolo del derecho de la intimidad[68]. Reconociendo que es un derecho de tercera generación que a su vez permite una protección adecuada del los derechos de primera generación como son el derecho de intimidad, al honor, a la voz, a la imagen, a la reputación, a la identidad, y demás derechos fundamentales reconocidos en la Constitución.

En el ordenamiento jurídico peruano hay que distinguir distintos ámbitos de protección: El ámbito constitucional, con el proceso constitucional de hábeas data. El ámbito penal con el delito de

[67] RODRIGUEZ TADEO, María Jose: "Impacto de la Protección de Datos Personales en Uruguay". En Memorias del XIV Congreso Iberoamericano de Derecho e Informática. Nuevo León, México del 25 al 30 de Octubre de 2010. Versión Digital. Páginas 725 y 726.
[68] Sentencia del Tribunal Constitucional de fecha 29.01.2003, recaída en el Expediente Nº 1797-2002-HD/TC. Disponible en: http://www.tc.gob.pe

violación a la intimidad. El ámbito civil con la indemnización por daño a la persona. El ámbito administrativo con la ley de protección de datos personales.

2.1.2.2. La Teoría de la Drittwirkung y el Derecho a la Identidad Digital

Ahora, hay otros ámbitos que desde un punto de vista jurídico e informático podría considerarse, como el ámbito laboral, el ámbito de protección al consumidor, entre otros. Para estos efectos cabe referirse a algunas instituciones jurídicas existentes en el derecho comparado, como por ejemplo la doctrina alemana. "La Teoría de la Drittwirkung pretende garantizar el ejercicio de los derechos fundamentales no sólo frente al Estado, sino en las situaciones más diversas entre los sujetos particulares. Por ello se llama en ocasiones eficacia horizontal de los derechos fundamentales…En la doctrina y jurisprudencia alemana pueden encontrarse diferentes construcciones del efecto de los derechos fundamentales en la relación de los particulares…"[69]

Lo cual, implica que los derechos fundamentales, incluyendo el derecho de autodeterminación informática pueden ser tutelados, incluso entre particulares, tanto en actividades que realizan como el cloud computing o medios en que se comunican como las redes sociales. Debe tenerse en cuenta que "para algunos autores la Drittwirkung es sólo indirecta, mientras que para otros es inmediata o directa… Los partidarios de la Drittwirkung indirecta… postulan la necesidad de una mediación del legislador y del juez…En cambio, la corriente doctrinal que defiende la eficacia directa de los derechos fundamentales en las relaciones privadas… sostiene que en ausencia de norma aplicable, la Constitución se aplicará directamente.."[70].

Las posturas doctrinarles más representativas sobre el efecto horizontal de los derechos fundamentales (Drittwirkung der

[69] ROIG, Antonio: "El uso de Internet en la Empresa: Aspectos Constitucionales". En Libro "El uso laboral y sindical del Correo Electrónico e Internet en la empresa". Ed. Tirant Lo Blanch. Valencia, España 2007. Páginas 24 y 25.
[70] ROIG, Antonio: Ob.cit. Páginas 26, 27, 28.

Grundechte) son las de eficacia inmediata o directa y la eficacia mediata o indirecta.

a) La Eficacia inmediata o directa de los derechos fundamentales
La Teoria[71] del efecto directo sostiene, que los derechos fundamentales "modifican las normas de derecho privado que existen (no interesa que se trate de derecho vinculante o dispositivo, clausulas generales o ciertas normas jurídicas); crean normas nuevas (que pueden ser prohibiciones, mandatos, derechos subjetivos, leyes de protección, razones de justificación)"[72]
Tratandose del derecho de identidad digital con esta teoría como derecho fundamental su efecto seria directo modificando las normas de derecho privado que existen como clausulas generales en páginas web y otros dispositivos de internet.

b) La Eficacia mediata o indirecta de los derechos fundamentales
Esta Teoría del efecto mediato o indirecto[73] sostiene que "los derechos fundamentales al ser desarrollados por ley, deben interpretarse en la forma que el legislador ha deparado su contenido, alcances y limites. Pero, además los derechos fundamentales serian necesario puntos de partida para la interpretación de la legalidad ordinaria, tendrían una eficacia interpretativa. Vale decir, la legalidad debe ser interpretada conforme el sentido de aquellos"[74]. Tratándose de la identidad digital con una ley específica sobre la materia estaría constituiría punto de partida para la interpretación de otras normas jurídicas relativas a la identidad en internet.

2.1.2.3. Otras consideraciones.

[71] Representada por Hans Carl Nipperdey, quien desde 1950, sostuvo que los derechos fundamentales vinculan las relaciones jurídicas entre particulares de modo directo.
[72] MENDOZA ESCALANTE, Mijail: "La Eficacia de los Derechos Fundamentales en las relaciones entre particulares". Pagina 3. En http://www.consultoriaconstitucional.com . Fecha de Consulta: 28 de Noviembre de 2015.
[73] Esta representada por Gunter Düring y sostiene que los derechos fundamentales tienen una eficacia mediata o indirecta.
[74] MENDOZA ESCALANTE, Mijail: Ob.cit. Pagina 4.

Por otra, parte, tenemos que tener en cuenta que, en el ordenamiento jurídico peruano tenemos la ley de protección de datos personales, pero también la ley que protege contra el correo electrónico no autorizado, spam. También tenemos iniciativas para precisar la regulación de la protección de datos personales en el ámbito laboral.

Con respecto, al ámbito laboral debe considerarse que, "la problemática del uso de las nuevas tecnologías en los lugares de trabajo se presenta en relación con la extensión, o si se prefiere los límites contractuales que se imponen en el uso de las nuevas tecnologías. El correo electrónico, Internet o el ordenador no dejan de ser herramientas de trabajo. Ahora bien, las referidas tecnologías no son sólo meras herramientas de trabajo… lo que se discute es..la existencia o no de un derecho del trabajador a usar con fines personales las TICs en la empresa y, en consonancia con ello, la sanción de las indicadas conductas"[75]

Por otro lado, en las relaciones contractuales en Internet con respecto a la protección del derecho de autodeterminación informativa,"el carácter adecuado del nivel de protección que ofrece un país u organismo internacional se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos"[76]: también debe considerarse la protección del derecho autodeterminación informativa en el comercio electrónico y el comercio internacional, para lo cual habrá que tener presente el marco de privacidad de APEC, así como las obligaciones específicas incluidas en los diversos instrumentos internacionales comerciales suscritos por Perú.

[75] MARTINEZ FONS, Daniel: "El Uso y Control del Correo Electrónico e Internet en la Empresa: Aspectos Laborales. En Libro "El uso laboral y sindical del Correo Electrónico e Internet en la empresa". Ed. Tirant Lo Blanch. Valencia, España 2007. Página 179.

[76] BRENNA, Ramón Gerónimo: "Internet y Privacidad. Reflexiones sobre la Sociedad de la Información y la Recolección de Datos on Line". En Informática y Derecho. Aportes de Doctrina Internacional, Volúmen 8. Ed. Depalma. Buenos Aires, Argentina, 2002. Página 9.

Las autopistas de la información facilitan todas las comunicaciones. El papel de la tecnología es proporcionar más flexibilidad y eficacia. La autopista de la información simplifica y estandariza el comercio y ahorra tiempo. Los datos personales se comunican, recopilan, registran, almacenan, se elaboran, se difunden, se intercambian y se transfieren en las autopistas de la información. El derecho de autodeterminación informativa, permite a través de la autorización y consentimiento controlar y proteger los datos personales dentro de la sociedad de la información.

2..1..3. Principios rectores de protección de datos personales y el derecho de identidad digital.

Los principios rectores contenidos en la ley peruana de protección de datos personales son los siguientes: legalidad: consentimiento; finalidad; proporcionalidad; calidad; seguridad; disposición de recurso; nivel de protección adecuado.

La actuación de los titulares y encargados de los bancos de datos personales y en general, de todos los que intervengan en relación a datos personales, deberán ajustarse a los principios rectores señalados. Esta relación de principios rectores es enunciativa más no limitativa.

Los principios rectores servirán de criterio interpretativo para resolver cuestiones que puedan suscitarse en la aplicación de esta ley, así como parámetro para la elaboración de otras disposiciones y para suplir vacíos en la legislación sobre la materia.

Conforme el artículo 12 de la Ley: “La actuación de los titulares y encargados de los banco de datos personales, y, en general, de todos los que intervengan con relación a datos personales, deben ajustarse a los principios rectores”. Dentro de los principios, tenemos el de consentimiento que tiene limitaciones establecidas en la ley y el reglamento. Por otra parte, la Ley establece los siguientes derechos del titular de datos personales: derecho de información; derecho de acceso; derecho de actualización, inclusión, rectificación y supresión; derecho de impedir el suministro; derecho de oposición; derecho al

tratamiento objetivo; derecho a la tutela; derecho a ser indemnizado. Conforme el principio de disposición de recurso: "Todo titular de datos personales debe contar con las vías administrativas o jurisdiccionales necesarias para reclamar y hacer valer sus derechos, cuando estos sean vulnerados por el tratamiento de sus datos personales.

El artículo 11. del Reglamento establece: "el titular de banco de datos o quien resulte responsable del tratamiento, deberá obtener el consentimiento para el tratamiento de los datos personales, de conformidad con lo establecido en la Ley y en el presente reglamento, salvo los supuestos establecidos en el artículo 14 de la Ley". El artículo 14 de la Ley 29733, dispone lo siguiente: "No se requiere el consentimiento del titular de datos personales, para efectos de su tratamiento, en los siguientes casos: 1. "Cuando los datos personales se recopilen o transfieran para el ejercicio de las funciones de las entidades públicas en el ámbito de su competencia". 2. "Cuando se trate de datos personales contenidos o destinados a ser contenidos en fuentes accesibles al público".

"El Tribunal Supremo de Justicia de España[77] ha rechazado la pretensión de la asociación Productores de Música de España (Promusicae) de recopilar sin consentimiento de los afectados los datos de los usuarios de redes P2P (peer to peer) -mediante las cuales se comparten archivos musicales- con el fin de ejercer la defensa de los derechos de propiedad intelectual de los productores y editores de fonogramas y videos musicales.
El alto tribunal, que confirma la sentencia dictada en el caso por la Audiencia Nacional en septiembre de 2011[78], establece que Promusicae no está eximida del deber de informar a los usuarios de redes P2P sobre el tratamiento de sus datos que establece la Ley Orgánica de Protección de Datos.
La asociación de productores reclamaba, entre otros datos, poder tratar las direcciones IP (Internet Protocols) sin informar a los

[77] http://www.poderjudicial.es/cgpj/es/Poder-Judicial/Sala-de-Prensa/Notas-de-prensa/El-TS-prohibe-a-Promusicae-usar-los-datos-de-los-usuarios-de-redes-de-intercambio-de-archivos-sin-su-consentimiento. Miércoles 22 de Octubre de 2014.
[78] Id. Cendoj: 28079130062014100516. Órgano: Tribunal Supremo. Sala de lo Contencioso Sede: Madrid Sección: 6. Tipo de Resolución: Sentencia. Fecha de resolución: 03/10/2014 Nº Recurso: 6153/2011. Ponente: JOSE MARIA DEL RIEGO VALLEDOR. Procedimiento: CONTENCIOSO. Idioma: Español

afectados, al considerar que con ese dato era incapaz de llegar a conocer la identidad del usuario.
El Supremo, en una sentencia de la que ha sido ponente el magistrado José María del Riego, señala que "las direcciones IP son datos personales", ya que contienen información concerniente a personas físicas "identificadas o identificables". Para rechazar otro de los argumentos de Promusicae, el TS destaca que "no puede equipararse el conocimiento por el titular de que su dirección IP es visible en las redes P2P, con su consentimiento para su tratamiento automatizado junto con otros datos de su tráfico".
La sentencia no comparte tampoco la alegación de los productores de que para poder concretar las conductas ilícitas de los usuarios de redes P2P no tenían más remedio que tratar las direcciones IP. El Supremo indica que el recurrente no ha justificado de forma suficiente esa necesidad por inexistencia de medidas protectoras alternativas en el ordenamiento jurídico, bien en el orden civil, en particular en la Ley de Propiedad Intelectual, bien en el orden penal, que fuesen más respetuosas con el derecho a la protección de los datos personales.
La sentencia estima que en este caso, por sus características de extensión y falta de acreditación de su estricta necesidad para la finalidad legítima perseguida, no está justificado limitar el contenido esencial del derecho fundamental a la protección de datos de un número desconocido de personas"[79].

Entre los fundamentos contenidos en esta Sentencia del Tribunal Supremo Español, señalamos las siguientes:

a) Cuando una norma jurídica establece excepciones a las prohibiciones de tratamiento de datos sin consentimiento del interesado, es exigible que los realice en forma precisa.
b) Que una habilitación legal tácita o implícita para tratar datos personales sin consentimiento del titular, en los términos que pretende la parte recurrente, no es conforme con el contenido del derecho de protección de datos como derecho fundamental.
c) El Tribunal Constitucional Español, en la Sentencia 292/2000 (fj16) sobre cuestiones relacionadas sobre el derecho

[79] http://www.poderjudicial.es/cgpj/es/Poder-Judicial/Sala-de-Prensa/Notas-de-prensa/El-TS-prohibe-a-Promusicae-usar-los-datos-de-los-usuarios-de-redes-de-intercambio-de-archivos-sin-su-consentimiento. Miércoles 22 de Octubre de 2014.

fundamental de protección de datos ha señalado no sólo la necesidad de que las limitaciones a un derecho fundamental estén fundadas en una previsión legal que tenga justificación constitucional y sean proporcionadas, sino además, "que la Ley que restrinja este derecho de expresar con precisión todos y cada uno de los presupuestos materiales de la medida limitadora", y tal requisito de precisión y certeza no es compatible con la limitación normativa implícita del derecho fundamental a la protección de datos que alega el recurrente.

d) La ley establece en los casos de tratamiento de datos de carácter personal, el deber de informar previamente a los titulares de los datos, y si los datos de carácter personal no han sido recabados del interesado, como sucede en este caso, se impone al responsable del fichero el deber de informar al interesado dentro de los tres meses siguientes al registro de los datos.

2..1.4. El Tratamiento de Datos Personales y el Derecho de Identidad Digital.

"Las posibilidades de recolectar datos personales se expanden en gran medida a partir de la masificación de nuestra vida en línea. La invalorable posibilidad abierta por las tecnologías digitales y el acceso a Internet para comunicarnos, interactuar, organizarnos, aprender, leer, visitar sitios lejanos, tomar decisiones de compra…tiene como contrapartida directa una transacción en términos de privacidad. El anonimato en la red está en vías de extinción. Los sistemas que utilizamos regularmente van dejando huellas trazables de cada actividad en línea: Navegación por sitios web, cookies, envío de correos electrónicos, participación en plataformas de redes sociales, descarga de diversos contenidos. Las personas que desean mantener su anonimato deben tomar medidas deliberadas: rasgos propios e identificables como las direcciones IP desde las cuales nos conectamos, los inicios de sesiones autenticados y los cookies están incluidos en infinidad de aplicaciones de uso cotidiano, y la recolección de estos datos pasa prácticamente inadvertida. Como si esto no fuera

suficiente, nos encontramos ante una tendencia generalizada a promover la identificación personal en el uso de diversos servicios , en particular las redes sociales"[80]

El tratamiento de datos personales debe realizarse con pleno respeto de los derechos fundamentales de la persona y de los derechos del titular de datos personales. El tratamiento de datos personales incluye cualquier forma de procesamiento que facilite el acceso, correlación o interconexión de los datos personales. La transferencia de datos personales, implica la comunicación de datos personales dentro o fuera del territorio nacional realizado a persona distinta del titular de los datos personales. Para el tratamiento de los datos personales de un menor de edad, se requerirá el consentimiento de los titulares de la patria potestad o tutores, según corresponda.

Tanto el tratamiento de datos personales como la transferencia de datos personales esta relacionados con el derecho de la identidad digital en internet, por cuanto se procesan los datos personales debieran realizarse basándose en una única identidad digital de la persona natural que cohesione las múltiples identidades digitales de la persona. En tal sentido, la trazabilidad, las direcciones IP y el rastreo de información deben lograr dar seguridad que la identidad de la persona no va a ser suplantada en internet o va a ser indebidamente utilizada. Los datos personales relacionados directamente con la identidad digital de la persona deben ser veraces, exactos y actualizados, de forma tal que haya correspondencia entre la identidad real y la identidad digital.

También tratándose de niños y adolescentes su identidad digital y sus datos personales deben ser debidamente protegidos. Hay avances relacionados con el internet de las cosas[81] que permiten que niños y

[80] BUSANICHE, Beatriz: "La Vida de los Otros". En "Habilitando la apertura: el futuro de la sociedad de la información en América Latina y el Caribe". Ed. Fundación Comunica, Montevideo, Uruguay y Coedición: International Development Research Center, Otawa, Canadá. 2013. Páginas 171 y 172.

[81] El anuncio de Hello Barbie de Matell de constesar preguntas de niñas a través de internet ha originado el debate de la vulneración de los datos personales, la intimidad y el derecho de identidad digital de los menores de edad. Fuente: Diario El País, Lunes 30 de Marzo de 2015. Página 25. Sección Sociedad. Año XL. Numero 13783. Edición América.

niñas hablen con sus "juguetes" y que estas conversaciones sean grabadas en internet y revelen sus datos personales sin consentimiento de sus padres. Es en este contexto, tanto de adultos como de niños, que el tratamiento de datos personales, su transferencia y flujo de dato transfronterizo debe respetar los derechos del titular, la existencia de la persona, su consentimiento adecuado y el derecho de identidad digital en internet.

2.1.5. Los derechos del titular , la existencia de la persona y el derecho de identidad digital.

"En el caso de los derechos vinculados a la vida privada, la masificación de las Tecnologías de la Información y Comunicaciones (TICs) ha supuesto la renovación de antiguas preguntas y la aparición de otra nuevas, vinculadas básicamente a las nuevas posibilidades relativas al tratamiento de la información personal de los ciudadanos a través de estas plataformas. Mientras que los derechos relacionados con la privacidad parecían verse agotados con asegurar el derecho a estar solo o el derecho a la no intrusión del Estado, la extensión del uso de las TICS parece enfrentarnos a antiguas preguntas sobre el alcance de la privacidad y lo privado, pero también a otras nuevas relativas al consentimiento para el procesamiento de información personal por terceros"[82]

El tratamiento de datos personales se realiza en pleno respeto de los derechos fundamentales de sus titulares.

Tiene derecho a ser informado el titular de datos personales, en forma detallada, sencilla, expresa, inequívoca y de manera previa a su recopilación, entre otros temas, los siguientes:

a) Sobre la finalidad para la que sus datos serán tratados.
b) Quienes serán o podrán ser sus destinatarios.

[82] RUIZ, Claudio: "¿Está muerta la pivacidad? Propuestas para una reflexión crítica sobre la protección de la privacidad en la era de internet". En "Habilitando la apertura: el futuro de la sociedad de la información en América Latina y el Caribe". Ed. Fundación Comunica, Montevideo, Uruguay y Coedición: International Development Research Center, Otawa, Canadá. 2013. Páginas 143 y 144.

c) El carácter obligatorio o facultativo de sus respuestas al cuestionario que se le proponga.
d) Las consecuencias de proporcionar sus datos personales y de su negativa a hacerlo.
e) El tiempo durante el cual se conservarán sus datos personales.

Si los datos personales son recogidos en línea a través de redes de comunicaciones electrónicas, el derecho a ser informado, podrá satisfacerse mediante la publicación de políticas de privacidad, las que deberán ser fácilmente accesibles e identificables. Las políticas de privacidad deberán contener la forma que los derechos de la persona, los datos personales y el derecho de identidad digital en internet de la persona va a ser protegido, así como disposiciones que aseguren un uso adecuado de sus datos personales durante la existencia de la persona, tanto en el ámbito real como el digital. .

Por el derecho de acceso, el titular de datos personales tiene derecho a obtener la información que sobre sí mismo sea objeto de tratamiento en banco de datos de la administración pública o privada, la forma en que sus datos fueron recopilados, las razones que motivaron su recopilación y a solicitud de quien se realizó la recopilación, así como las transferencias realizadas o que se prevén hacer de ellos. Esta información es importante, porque la puede controlar la forma y fondo del tratamiento de datos personales en Internet, teniendo incidencia directa en su reputación en línea y en el ejercicio del derecho de identidad digital en internet.

El derecho de cancelación, supresión o "derecho al olvido tiene incidencia en el ejercicio de la identidad digital Hay que tener en cuenta que "en los últimos años se está configurando un conjunto de nuevas vías de ejecución de derechos ya existentes denominados "derecho al olvido" para su mejor comprensión. Este derecho permite a las personas gozar en la red del mismo perdón y olvido que se les otorga en la vida offline"[83]

[83] FERNANDEZ BURGUEÑO, Pablo: Ob. Cit. Páginas 10 y 11..

El Derecho a la identidad Digital es el derecho a existir en Internet y tener una reputación online respetando su privacidad. "La privacidad es el poder de controlar lo que los demás pueden llegar a saber de ti"[84], La existencia de la persona en Internet, debe guardar relación con la existencia de la persona en la vida real. La persona humana es sujeto de derecho desde su nacimiento. La muerte pone fin a la persona natural. En consecuencia, la identidad digital debe estar relacionada con el nacimiento y la muerte de la persona.

Los registros civiles de nacimiento y defunción es necesario que tengan su correlato en el "mundo digital". En el Perú, el Acta Registral electrónica es un producto digital que registra las inscripciones de nacimientos, matrimonios y defunciones. Al respecto, cabe señalar que el Registro de Identificación y Estado Civil (RENIEC) conjuntamente con las Oficinas de Registros Civiles de las Municipalidades ha realizado acciones y regulado[85] el "registro en línea" de hechos vitales y actos modificatorios del estado civil de las personas y demás procedimientos registrales, utilizando el Sistema de Registros Civiles y Microformas del RENIEC.

La información digital de la persona que está relacionada con su identidad digital en las redes sociales y sistemas de información es necesario que tengan un término o final, de forma tal que el precepto de que la muerte pone fin a la persona natural también se dé en el mundo digital. Se han dado casos de personas que han fallecido pero siguen presentes en redes sociales como facebook y linkedin. Hay un procedimiento de cancelar una página en facebook pero requiere el nombre del usuario y la contraseña. Será necesario prever procedimientos para que los herederos puedan ejercer este derecho. Para lo cual la identidad digital y su actualización por una entidad pública oficial va a dar confianza, certeza y seguridad para esta

[84] LESSIG, Lawrence: "El Código y otras Leyes del Ciberespacio". Ed. Taurus Digital. Madrid, España. 2001. Página 266.

[85] Mediante Resolución Jefatural Nº 116-2013-JNAC-RENIEC del 05 de Abril del 2013, se delegaron a las Oficinas de Registros Civiles (OREC) que funcionan en las municipalidades o centros poblados el registro en línea de hechos vitales y actos modificatorios del estado civil de las personas y demás procedimientos registrales.

finalidad. Los contratos y términos y condiciones están en constante revisión, por lo que recomendamos que se incluyan estos procedimientos que permitan que haya un correlato entre la existencia real y la existencia digital de la persona natural.

Por otra parte, la protección de datos personales debe garantizar los derechos de información, acceso y los otros derechos como un mecanismo de control que asegure la privacidad y otros derechos fundamentales consagrados en la constitución. La información y el acceso están relacionados también con la existencia de la persona humana en el "mundo real" y en el "mundo digital".

Puede darse el caso, que la identidad de la persona se desenvuelva en el mundo real pero que por razones justificadas se decida que su identidad digital ya no se realice en forma continuada en internet. En estos casos, el derecho de cancelación o supresión posibilitará que se materialice esta decisión.

En este orden de ideas, hay que tener en cuenta que el ejercicio del derecho de cancelación, supresión o derecho al olvido implica ejercer la protección de los datos personales en internet, la protección de la identidad digital y su contextualización de la información[86]. Al respecto, cabe mencionar el caso europeo de Mario Costeja y la Agencia Española de Proteccion de Datos Personales, según la Sentencia del Tribunal de Justicia Europeo del 13 de Mayo del 2014[87], con respecto al derecho de cancelación, o también llamado derecho al olvido:

a) El Señor. Costeja González[88], presentó ante la Agencia Española de Protección de Datos Personales (AEPD) contra el

[86] Vid. FINOCCHIARIO, Giusella: "Identità Personalle su Internet: Il diritto alla contestualizzazione dellínformazione". Rivista "Il Diritto dell'informazione e dell ìnformatica . Anno XXVII. Fasc.3. 2012. Milano. Giufrè Editore. Italia.

[87] Sentencia del Tribunal de justicia Europero del 13 de Mayo de 2014. Google Spain SL y Google Inc vs Agencia de Proteccion de Datos Peronales Española (AEPD) y Mario Costeja Gonzales. En: http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=ES

[88] El 5 de marzo de 2010 presento la reclamación, El Sr. Costejas que es de nacionalidad española y domiciliado en España. La Vanguardia Ediciones, S.L., publica un periódico de gran difusión, concretamente en Cataluña (en lo sucesivo, «La Vanguardia»). La fecha de publicación de la Vanguardia de los avisos materia de la reclamación son del 19 de enero y del 9 de marzo de 1998, respectivamente. En: http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=ES

Diario La Vanguardia y contra Google Spain y Google Inc. Esta reclamación se basaba en que, cuando se introducía el nombre del Sr. Costeja González en el motor de búsqueda de Google (en lo sucesivo, «Google Search»), obtenía como resultado vínculos hacia dos páginas del periódico La Vanguardia en las que figuraba un anuncio de una subasta de inmuebles relacionada con un embargo por deudas a la Seguridad Social, que mencionaba el nombre del Sr. Costeja González, que ya no tenían relevancia..

b) Mediante esta reclamación, el Sr. Costeja González solicitaba, que se exigiese a Google Spain o a Google Inc. que eliminaran u ocultaran sus datos personales para que dejaran de incluirse en sus resultados de búsqueda y dejaran de estar ligados a los enlaces de La Vanguardia
c) Se aceptó la reclamación en la medida en que se dirigía contra Google Spain y Google Inc. A este respecto, la AEPD consideró que: "quienes gestionan motores de búsqueda están sometidos a la normativa en materia de protección de datos, dado que llevan a cabo un tratamiento de datos del que son responsables y actúan como intermediarios de la sociedad de la información"[89].
d) La Agencia Española de Protección de Datos Personales (AEPD) consideró que: "estaba facultada para ordenar la retirada e imposibilitar el acceso a determinados datos por parte de los gestores de motores de búsqueda cuando considere que su localización y difusión puede lesionar el derecho fundamental a la protección de datos y a la dignidad de la persona entendida en un sentido amplio, lo que incluye la mera voluntad del particular afectado cuando quiere que tales datos no sean conocidos por terceros"[90].

Este caso sobre el llamado derecho al olvido en internet o derecho de cancelación de datos personales, está relacionado con el derecho a la identidad digital en internet porque permite que una persona natural pueda solicitar la cancelación de sus datos personales relacionados

[89] Sentencia del Tribunal de justicia Europero del 13 de Mayo de 2014. Google Spain SL y Google Inc vs Agencia de Proteccion de Datos Peronales Española (AEPD) y Mario Costeja Gonzales. En: http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=ES
[90] Ibidem.

con identidad digital de forma global, de forma tal que cada vez que se busque su nombre en los buscadores no se relacione su nombre con los datos personales cancelados. El Tribunal Europeo respaldo esta posición y constituye una jurisprudencia que ha tenido difusión e influencia a nivel internacional.

Otros de los principios fundamentales, que tienen relación con el derecho de identidad digital en internet es la autorización o consentimiento. Con respecto al principio de consentimiento, la obtención del consentimiento deberá ser:

i) Libre: Sin que medie error, mala fe, violencia o dolo que puedan afectar la manifestación de voluntad del titular de los datos. Esta libertad es fundamental en el consentimiento, que implica efectuarlo sin coacción ni medida de fuerza que afecte la manifestación de voluntad. El otorgamiento de beneficios no afectan la condición de libertad. En cambio, el condicionamiento o amenaza de denegar el servicio si afecta la libertad del consentimiento.

ii) Previo: anterior a la recopilación de los datos, o, en su caso, anterior al tratamiento distinto a aquel por el cual ya se recopilaron. Implica que el consentimiento debe ser anterior al hecho que se está consintiendo. El conocimiento y manifestación de voluntad en Internet coadyuva a que se cumpla esta condición de que sea previa.

iii) Expreso e inequívoco: de forma que el consentimiento haya sido manifestado en condiciones que no admitan dudas de su otorgamiento.

iv) Informado: al titular del dato personal se le debe comunicar clara, expresa e inequívocamente, la identidad y domicilio o dirección del titular del banco de datos personales o del responsable del tratamiento al que pueda dirigirse para revocar el consentimiento o ejercer sus derechos; la finalidad o finalidades del tratamiento a la que sus datos serán

sometidos; la identidad de los que son o pueden ser sus destinatarios; las consecuencia y si habrá transferencia o no.

Un caso, donde se desarrolla las características del consentimiento es el procedimiento sancionador con el expediente Nº 40-2015/JUS/DGPDP-PS de la Autoridad Nacional de Protección de Datos Personales Peruana, donde la Clínica fiscalizada[91] tiene una página web , donde con el título de Políticas Protección de Datos Personales se afirma lo siguiente: "La navegación en la página web de la clínica, la participación de promociones comerciales y cualquier otra interacción web implica el consentimiento libre, expreso e inequívoco del usuario para la Cesión de Datos Personales a la Clínica..". Se afirma:

a) Que estas no son políticas de protección de datos personales, sino que pretenden ser clausulas de consentimiento.
b) Que en el presente caso el consentimiento no es libre, en la medida que no se da al titular del dato personal la oportunidad de manifestar su consentimiento y menos de denegarlo, habida cuenta que, como lo señalan dichas políticas, cualquier interacción web, en sí misma, implica que la Clínica de por otorgado su consentimiento.
c) En el caso bajo análisis no se verifica ninguna manifestación de voluntad de titular del dato personal, toda vez que la Clínica, en buena cuenta, presumía el consentimiento.
d) En el presente caso, se evidencia que este carece de la indicación expresa respecto de a quien tiene que dirigirse la solicitud de revocatoria de consentimiento, la finalidad específica del tratamiento al que serán sometidos los datos personales, empleando por ende formulas generales que en ningún caso hace referencia específica a la información que mínimamente debe ser proporcionada al titular del dato personal.

[91] Resolución Nº 43-2015-JUS/DGPDP-DS, del 31 de Julio de 2015. Procedimiento Administrativo Sancionador a la Clínica San Felipe S.A por la Dirección de Sanciones del Ministerio de Justicia del Perú. En . http://www.minjus.gob.pe/wp-content/uploads/2015/10/RD-43-primera-instancia-Clinica-San-Felipe.pdf . Esta resolución quedo firme porque el recurso de apelación fue declarado extemporáneo por Resolución Directoral Nº 028-2015-JUS/DGPDP del 21 de setiembre de 2015.

Asimismo, con respecto al consentimiento[92], debe tenerse en cuenta que el Reglamento de la Ley de Protección de Datos Personales, establece lo siguiente:

- Se considera que el consentimiento expreso se otorga verbalmente cuando el titular lo expresa oralmente de manera presencial o mediante el uso de cualquier tecnología que permita la interlocución oral, como la videoconferencia y el skype.

- Se considera consentimiento escrito a aquél que otorga el titular mediante un documento con su firma autógrafa, huella dactilar o cualquier otro mecanismo autorizado por el ordenamiento jurídico que queda o puede ser impreso en una superficie de papel o similar, como el código de barras, sistemas de codificación gráficas u otros.

- Tratándose del entorno digital, también se considera expresa la manifestación consistente en "hacer click", "clickear", "pinchar", "dar un toque", "touch" o "pad". En este contexto el consentimiento escrito podrá otorgarse mediante firma electrónica, mediante escritura que quede grabada de forma que pueda ser leída e impresa o cualquier mecanismo o procedimiento establecido que permita identificar al titular y recabar su consentimiento, a través de texto escrito. También podrá otorgarse mediante texto preestablecido, fácilmente visible, legible y en lenguaje sencillo, que el titular pueda hacer suyo, o no, mediante una respuesta gráfica o mediante click, pinchado o toque.

2.1.6. Tipos de datos personales sometidos a tratamiento y el derecho a la identidad digital.

a) Datos de carácter identificativo

[92] Reglamento de la Ley de Protección de Datos Personales. D.S. 003-203-JUS, publicado el 22 de Marzo de 2013.

Los datos de carácter identificativo son: Nombres y Apellidos. Número de Documento Nacional de Identidad (DNI). Número de Registro Único de Contribuyente (RUC). Numero de Pasaporte. Dirección de domicilio. Teléfono. Dirección de correo electrónico. Imagen. Voz. Firma.

Los nombres y apellidos. Toda persona tiene derecho y el deber de llevar un nombre, este incluye los apellidos. En el mundo digital el nombre es un dato personal que identifica la persona y garantiza su identidad.

El Número del Documento Nacional de Identidad. Tiene ocho dígitos y constituye un código único de identificación. Existe la propuesta por parte de RENIEC que este número esté relacionado con la cadena de ADN de cada ciudadano que a través de análisis de sangre pueda identificarse y con procedimientos matemáticos se conviertan en números de ocho dígitos, en lo que se ha denominado DNI genético.

Número de Registro Único de Contribuyente que identifica al contribuyente en los sistemas tributarios que administra la Superintendencia Nacional de Administración Tributaria (SUNAT).

Numero de Pasaporte que identifica a la persona natural en la Dirección General de Migraciones. Está en proceso el pasaporte con circuito integrado o chip para facilitar en forma segura el viaje de los ciudadanos a otros países.

Dirección de domicilio que es necesario que sea actual y realmente corresponda a la residencia habitual de la persona. El domicilio es una dato personal que el ámbito digital permite ubicar a la persona a través de la geo-referenciación. RENIEC de manera permanente realiza acciones de verificación de la dirección domiciliaria declarada. Para estos efectos, RENIEC puede solicitar a las instituciones públicas los

informes y registros que correspondan, a fin de verificar la autenticidad de los datos consignados[93] en el documento nacional de identidad.

Teléfono, que incluye tanto el teléfono fijo como el teléfono celular. Dado el uso de los "smartphones" o teléfonos inteligentes este dato personal tiene especial relevancia para la identificación de la persona en internet.

Dirección de correo electrónico que permite identificar y comunicarse con la persona en internet. Este dato constituye un identificador numérico o digital que tiene gran importancia en la identificación digital. Es importante señal la necesidad que a cada ciudadano que obtenga su DNI electrónico RENIEC le otorgue una dirección de correo electrónico que constituya su domicilio electrónico oficial.

Imagen, que incluye la fotografía de la persona. Con la utilización de la biometría facial permite identificar a la persona natural.

Voz, es otro dato personal de especial relevancia porque existen sistemas informáticos de reconocimiento de voz. Por otra parte, existen sistemas de identificación biométrica de voz que complementan a los otros sistemas existentes.

Firma que incluye la firma manuscrita que tiene por finalidad identificar, asegurar o autenticar la identidad de una persona. La firma también es la firma electrónica que incluye la firma digital. La identidad digital se fortalece en forma segura con el uso de la firma digital.

b) Datos de características personales

Los datos personales de características personales son: Estado civil. Fecha de nacimiento. Nacionalidad. Sexo. Profesión, Edad.

Estado civil, que precisa si la persona natural es soltero, casado, viudo o divorciado. Conforme la ley[94] la falta de actualización de datos del

[93] Artículo 37.4 de la Ley 26497. Ley Orgánica de RENIEC, modificada por Ley Nº 30338, publicada en el Diario Oficial El Peruano, el 27 de Agosto de 2015.
[94] Artículo 37.3 de la Ley 26497, modificada por Ley Nº 30338, publicada en el Diario Oficial El Peruano, el 27 de Agosto de 2015.

estado civil del titular, dentro de los treinta días de producidos, no genera la invalidez del documento nacional de identidad sino el pago de una multa equivalente al 0.3 por ciento de la Unidad Impositiva Tributaria.

Fecha de nacimiento, es la fecha consignada en la partida de nacimiento como tal y como dato personal tiene relevancia en el ejercicio del derecho de la identidad digital en internet, porque permite individualizar y diferenciar a la persona, entre otros casos, cuando se trata de homonimia. En la ley que regula el procedimiento en los casos de homonimia[95] se incluye el dato personal de fecha y lugar de nacimiento para identificar a la persona ante un mandato de detención.

La nacionalidad es un dato personal que tiene relevancia en la identidad digital. En la Ley de Nacionalidad[96] se regula la nacionalidad por nacimiento y por naturalización. Se establece, asimismo que los peruanos de nacimiento que adoptan la nacionalidad de otro país, no pierden su nacionalidad, salvo que hagan renuncia expresa de ella. Las personas que gozan de doble nacionalidad, ejercitan los derechos y obligaciones de la nacionalidad del país donde domicilian.

Sexo, es un dato personal de importancia vinculado a la identidad de la persona. "El sexo (femenino o masculino) asignado a la persona desde su nacimiento, es uno de aquellos rasgos distintivos de carácter objetivo, viniendo tal característica de una realidad biológica indisponible, necesaria para que la persona pueda ser individualizada como corresponde a su derecho a la identidad y al correlativo deber de respetar los derechos e intereses de terceros. Asimismo, tal realidad genética resulta determinante para las distintas consecuencias que se derivan de la condición de mujer y de hombre en el ordenamiento jurídico (por ejemplo, en lo que respecta al derecho o capacidad para contraer matrimonio)[97]".

[95] Ley 27411, Ley que establece el procedimiento en caso de homonimia, modificada por Ley Nº 28121, de noviembre del 2003.
[96] Ley 26574, Ley de Nacionalidad, de Enero de 1996.
[97] Sentencia del Tribunal Constitucional. Exp. Nº 00139-2013-PA/TC del 18 de Marzo de 2014. En http://www.tc.gob.pe . Fecha de consulta: 27 de agosto de 2015.

Profesión u ocupación, es un dato personal que tiene relación con el derecho de identidad en cuanto que describe la actividad laboral que realiza la persona humana. Este datos personal cuando se trata se trata de profesionales está relacionada a los datos de colegiación y de habilidad para el ejercicio de la profesión. Por ejemplo, la ley[98] establece que todo ingeniero para ejercer como tal en el Perú tiene que estar titulado, colegiado y habilitado. En otras profesiones también se exigen requisitos y obligaciones equivalentes.

c) Datos económicos financieros

Los datos personales económicos financieros[99], son: Créditos, préstamos, avales. Datos bancarios. Historial de créditos, Información tributaria. Seguros. Hipotecas. Deudas, Tarjetas de crédito. Bienes patrimoniales. Planes de pensión y jubilación. Beneficios recibidos de programas sociales.

Créditos, préstamos, avales. Estos datos personales forman parte de la información sobre la solvencia patrimonial y la situación económica de la persona. Los datos bancarios, historial de crédito, deudas, seguros, hipotecas, tarjetas de crédito tienen esta finalidad y están relacionadas con la información de riesgos. Al respecto la ley[100] establece que la información de riesgos es: "la información relacionada con obligaciones o antecedentes, financieros, comerciales, tributarios, laborales, de seguros de una persona que permita evaluar su solvencia económica vinculada principalmente a su capacidad y trayectoria de endeudamiento y pago" y se establece que "se puede recolectar información de riesgo de fuentes pública y de fuentes privadas".

[98] Ley 28858, que establece que todo ingeniero para ejercer la profesión requiere estar titulado, colegiado y habilitado.
[99] En los formularios de inscripción de banco de datos personales, aprobados por la DireccionGeneral de Proteccion de Datos personales se establece esta clasificación.
[100] Ley Nº 27489, Ley que regula las Centrales Privadas de información de riesgos y de protección al titular de la información y su Ley modificatoria 27863.

La información de riesgos que incluyan datos personales económicos y financieros que deben ser lícitos, veraces y exactos, de forma tal que responda a la situación real del titular de la información en determinado momento.

d) Datos de carácter social

Pertenencia a clubes o asociaciones. Aficiones y hábitos personales. Características de vivienda.

Los datos personales de carácter social precisan y dan información sobre el estilo de vida e interacción social de la persona, que incluyen características del alojamiento, vivienda, situación familiar, aficiones, hábitos personales, pertenencia a clubes o asociaciones, licencias, permisos, autorizaciones. Determinan muchas veces información sobre la identidad dinámica de las personas y en un entorno digital pueden establecer características singulares y distintivas de cada persona. Esta información personal idéntica y hace identificables a la persona dentro de un entorno social que refleja el status económico y nivel de vida de la persona. En base de estos datos personales, que muchas veces se comparten en redes sociales puede delimitarse los hábitos y perfil detallado de la persona.

e) Datos sensibles

Origen étnico. Características físicas. Información relativa a la salud física o mental. Vida sexual. Vida afectiva o familiar. Convicciones religiosas. Convicciones políticas. Convicciones filosóficas o morales. Ingresos económicos. Afiliación sindical. Huella digital y otros datos biométricos.

Los Datos sensibles son datos especialmente protegidos porque afectan la intimidad del titular y su uso indebido puede dar lugar a discriminación. Estos datos están en la esfera privada e intima de la persona como son los datos biométricos que por sí mismos pueden identificar al titular; los datos que revelan la ideología, afiliación sindical, religión y creencias; los datos relativos al origen racial, a la salud y a la vida sexual.

Los ingresos económicos son considerados por la ley de protección de datos personales como datos sensibles y por tanto son objeto de especial protección y su tratamiento y transferencia requiere el consentimiento expreso del titular de los datos personales por escrito. Sin embargo, en la legislación peruana "hay la obligación de presentar la Declaración jurada de bienes y rentas de los funcionarios y servidores públicos del Estado"[101], asimismo se establece, que la Declaración jurada debe contener todos los ingresos, bienes y rentas, debidamente especificados y valorados, tanto en el país como el extranjero.

Con respecto, a la dicotomía existente entre lo regulado por la ley de protección de datos personales de que los ingresos económicos son datos sensibles y la existencia de la ley sobre la obligación de declarar estos ingresos económicos por parte de los servidores y funcionarios públicos, cabe señalar que "la existencia de normas o regímenes particulares o especiales, aun cuando incluyan regulaciones sobre datos personales, no excluye a las entidades públicas o privadas a las que dicho régimen se aplica del ámbito de aplicación de la ley de protección de datos personales.. lo cual no implica la derogatoria o inaplicación de las normas particulares, en tanto su aplicación no genere la afectación del derecho a la protección de datos personales"[102]. Por tanto, debe primar la protección de datos personales, más aun cuando estos ingresos económicos son publicados en los portales web de las instituciones publica; esta información económica forma parte de los datos personales que inciden directamente en el ejercicio del derecho a la identidad digital en internet, porque información que siendo sensible es publicada en forma abierta en los portales de transparencia por mandato legal, afectando el derecho a la protección de datos personales.

[101] Ley Nº 27482, Ley que regula la publicación de la declaración jurada de ingresos y de bienes y rentas de los funcionarios y servidores del Estado.
[102] D.S. 003-2013-JUS, Reglamento de la Ley de Protección de Datos Personales, articulo 3º.

2.1.7. La Autoridad Nacional de Protección de Datos y el derecho de identidad digital.

La Autoridad Nacional de Protección de Datos Personales es la Dirección Nacional de Justicia del Ministerio de Justicia quien por ley cuenta con la asesoría y apoyo técnico de la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) de la Presidencia del Consejo de Ministros que es el órgano rector del Sistema Nacional de Informática.

El Registro Nacional de Identificación y Estado Civil (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. Entre las funciones del RENIEC, tenemos: velar por el irrestricto respeto del derecho a la intimidad e identidad de la persona y los demás derechos fundamentales inherentes a ella derivadas de su inscripción en el registro; garantizar la privacidad de los datos relativos a las personas que son materia de inscripción; implementar, organizar, mantener y supervisar el funcionamiento de los registros dactiloscópico y pelmatoscópico de las personas.

El Reglamento precisa que la Autoridad Nacional de Protección de Datos Personales es la entidad a que se refiere la ley o el reglamento, es decir el Ministerio de Justicia, que en concordancia con las nomenclaturas y estructuras de la respectiva ley de organización y funciones, puede constituir una Dirección General u otro órgano administrativo de competencia nacional, "sin que la nomenclatura o ubicación orgánica afecten sus funciones o competencias ni requieran modificación de la denominación, la misma que podrá ser usada indistintamente con la que se establece o establezca en las normas.."[103]

[103] Reglamento de la Ley de Protección de Datos Personales, Artículo 2, numeral 1. D.S. 003-2013-JUS. Publicado el 22 de Marzo de 2013.

Si bien el legislador ha optado por designar al Ministerio de Justicia como Autoridad Nacional de Proteccion de Datos. Es necesario determinar en materia de Protección de Datos Personales un sistema que incluya entidades como ONGEI y RENIEC para coadyuvar en el fortalecimiento de una cultura de protección de datos personales y la consolidación de un sistema eficaz de protección. Este es un camino progresivo donde la difusión de la problemática, su implementación y discusión en una ámbito académico universitario va a contribuir a que se lleguen a soluciones integrales acordes a la realidad. El proceso de aplicación en la realidad de la normativa va a contribuir a que se lleguen a estas soluciones. Lo fundamental es que tenemos norma vigente y que ésta debe implementarse, los demás aspectos se solucionarán paulatinamente.

Las funciones de la Autoridad Nacional de Protección de Datos Personales establecidas en la Ley 29733, son: administrativas, orientadoras, normativas, resolutivas, fiscalizadoras y sancionadoras y pueden observarse esquemáticamente en el siguiente cuadro:

Funciones	*Base Legal*	*Descripción o detalle*
Administrativa	Art. 33 inc. 1, 2,3,7, 14 de Ley 29733	- Representar al país. - Celebrar convenios. - Administrar y actualizar registro. - Coordinar inclusión información.
Orientadora	Art. 33 inc. 4, inc 5, inc. 6, 11, 13 de Ley 29733	-Publicitar en Páginas Web Banco de Datos Personales. - Promover Campañas de

		Difusión. - Promover Cultura de Protección de Datos. - Absolver Consultas.
Normativa	Art. 33 inc. 12 de la Ley 29733	- Emitir Directivas que correspondan.
Resolutiva	Art. 33 inc. 9, inc. 16, inc. 17, inc. 18 de la Ley 29733	- Emitir autorizaciones. - Resolver Reclamaciones
Fiscalizadora	Art. 33 inc. 8, inc. 11 de la Ley 29733	- Supervisar exigencia flujo transfronterizo de datos personales. - Supervisar Tratamiento de Datos.
Sancionatoria	Art. 32 inc. 20	- Aplicar sanciones administrativas correspondientes.

En el Registro Nacional de Protección de Datos Personales, se incluye la categoría de datos, que es proporcionada en el formulario de inscripción por el titular del banco de datos personales, de acuerdo a cada caso concreto. Esta categoría de datos puede incluir, dependiendo cada caso concreto: I Datos de carácter identificativo: Nombres y Apellidos, N° de DNI, N° de RUC, N° de Pasaporte, Dirección del Domicilio; Teléfono, Dirección del Correo Electrónico, firma, firma electrónica. II. Datos de características personales: estado civil, fecha de nacimiento, nacionalidad, sexo, profesión, edad, ocupación, cargo y giro del negocio. III. Datos económicos, financieros y de

seguros: créditos, préstamos, avales; datos bancarios; historial de créditos; información tributaria; seguros; hipotecas; deudas; tarjeta de crédito; bienes patrimoniales; planes de pensión o jubilación, beneficios recibidos de programas sociales, otros. IV. Datos de carácter social: pertenencia a clubes o asociaciones; Aficiones y Hábitos personales; características de vivienda V. datos sensibles: Origen étnico; características físicas; Información relativa a la salud física o mental; vida sexual; vida afectiva o familiar; convicciones religiosas; convicciones políticas; convicciones filosóficas o morales; ingresos económicos; afiliación sindical; huella; otros datos de carácter biométrico.

2.1.8. La Seguridad de la Información y la Protección de Datos Personales

"Los sistemas informáticos que manejen banco de datos personales o impliquen el tratamiento de datos personales, deberán incluir en su funcionamiento registros que guarden todo tipo de interacción con los datos lógicos, de tal manera que se identifiquen a los usuarios, cambios, consultas, horas de inicio y cierre de cesión y otras acciones realizadas. Estos registros sólo admitirán el acceso de personal competente, autorizado e identificado. Asimismo, se deben establecer las medidas de seguridad relacionadas con los accesos autorizados a los datos mediante procedimientos de identificación y autenticación que garanticen la confidencialidad e integridad de los datos"[104]

Los ambientes en los que se procese datos personales, almacene o transmita información privada, deberán ser implementados teniendo en cuenta los controles, políticas, estándares y recomendaciones de seguridad física y ambiental establecidos en:

a) Norma Técnica Peruana "NTP-ISO/IEC 17799: 2007 EDI. Tecnología de Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2º Edición".

[104] Reglamento de la Ley Peruana de Protección de Datos Personales. D.S. 003-2013-JUS publicado el 22 de Marzo de 2013.

b) "NTP-ISO/IEC 27001: 2008 EDI. Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad. Sistemas de gestión de seguridad de la información. Requisitos".

La Seguridad Informática en el contexto de la Protección de Datos Personales debe garantizar la accesibilidad, la continuidad, productividad, colaboración y uso adecuado de los datos personales.

En cuanto a la accesibilidad debe garantizarse el acceso a la información personal que se necesita evitando el acceso indebido y la modificación no autorizada de datos.

Con respecto a la continuidad del negocio, debe garantizarse que cualquier ataque a la seguridad de los datos no impida que estos sigan siendo utilizados en los ámbitos necesarios para que el negocio o actividad informática continúe . Hay que prevenir incidentes y retomar, recuperar y restauras las operaciones afectadas.

Los sistemas de información deben garantizar que la productividad se mantenga y se responda rápida y adecuadamente a los requerimientos diversos de los usuarios o clientes.

La colaboración garantiza que los usuarios de los sistemas personales, en el contexto de la protección de datos personales, puedan comunicarse en forma segura e íntegra desde cualquier parte del mundo.

El uso adecuado de los datos debe darse en el marco de la ley de protección de datos personales, la observancia de los principios rectores y la defensa de los derechos del titular de los datos personales, cuyo ejercicio tiene carácter personalísimo.

La Directiva de Seguridad de la Información administrada por los banco de datos personales establece cinco categorías en el tratamiento de datos personales: básico, simple, intermedio, complejo, crítico. Con respecto a la categoría de crítico, establece que

corresponde a la categoría de mayor nivel e incluye a banco de datos personales que: - sirven para el tratamiento de datos personales cuya finalidad está respaldada por una norma legal. –Sirven para el tratamiento de datos cuya finalidad se cumple en un plazo indeterminado o superior a un (01) año. – Sirven para el tratamiento de datos personales que es realizado en múltiples localizaciones (Oficinas o dependencias diferentes en la misma ciudad o ciudades diferentes, servicios tercerizados o similares). – Pueden incluir datos sensibles. – Tiene como titular a una persona jurídica o entidad pública. Por tanto, RENIEC clasifica en la categoría de crítico.

La Directiva de Seguridad de Información administrada por los banco de datos personales, establece: "Las entidades públicas pertenecientes al Sistema Nacional de Informática tienen la obligatoriedad de implementar la NTP-ISO/IEC 27001 según la resolución Ministerial 129-2012-PCM. Por lo que, al incorporar los banco de datos personales dentro del alcance del SGSI, el sistema de gestión ayudará al cumplimiento de la mayor parte de los requisitos y medidas señaladas en la directiva de seguridad de la información administrada por los banco de datos personales, incluso a mayor nivel del definido en la directiva. Siendo necesario identificar cuáles son los aspectos que el SGSI no cubre y que la Directiva señala". Además precisa que: "Las instituciones pueden utilizar el ISO 31000 o ISO/IEC 27005 como referencias de gestión de riesgo y utilizar el enfoque de "Privacidad por Diseño".

La Directiva de Seguridad de la Información administrada por los banco de Datos Personales es aplicable a RENIEC en la categoría Crítico, que implica además de cumplir los lineamientos organizativos, legales, técnicos y de seguridad que establece la Directiva e implementar la NTP-ISO/IEC 27001, aplicar como recomendación el Enfoque de Privacidad de Diseño, que incluye los siguientes principios: i) Proactivo, no reactivo; Preventivo no correctivo. ii) Privacidad como la configuración Predeterminada. iii) Privacidad incrustada en el Diseño. iv) Funcionalidad Total- "Todos ganan", no "Si alguien gana otro pierde. v) Seguridad Extremo-a-Extremo- Protección de Ciclo de vida completo. vi) Visibilidad y Transparencia- mantenerlo abierto. vii) Respeto por la Privacidad de los usuarios – Mantener un Enfoque Centrado al Usuario.

La incorporación de mecanismos que garanticen la seguridad del tratamiento de datos personales deben ser demostrables en aplicación de la trazabilidad. La trazabilidad es la cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o una entidad, dejando rastro del respectivo acceso.

2.1.9. La Ley de Historias Clínicas Electrónicas y la Identidad Digital

El día miércoles 22 de Mayo de 2013 se ha publicado la Ley 30024 que crea el Registro Nacional de Historias Clínicas Electrónicas. El objeto de la ley es "crear el Registro Nacional de Historias Clínicas Electrónicas y establecer sus objetivos, administración, organización, implementación, confidencialidad y accesibilidad".

Se define al Registro Nacional de Historias Clínicas Electrónicas como "la infraestructura tecnológica especializada en salud que permite al paciente o su representante legal y a los profesionales de la salud que son previamente autorizados por aquellos, el acceso a la información clínica contenida en las historias clínicas electrónicas dentro de los términos estrictamente necesarios para garantizar la calidad de la atención en los establecimientos de salud y en los servicios de la atención en los establecimientos de salud y en los servicios médicos de apoyo públicos, privados o mixtos, en el ámbito de la Ley 26842, Ley General de Salud".

El Registro Nacional de Historias Clínicas contiene una base de datos de filiación de cada persona con la relación de los establecimientos de salud y de los servicios médicos de apoyo que le han brindado atención de salud y generado una historia clínica electrónica. El Ministerio de salud es el titular de dicha base de datos.

El Registro Nacional de Historias Clínicas Electrónicas utiliza la Plataforma de Interoperabilidad del Estado (PIDE) para el acceso a la información clínica solicitada o autorizada por el paciente o su representante legal.

La ley define autenticar como "controlar el acceso a un sistema mediante la validación de la identidad de un usuario, otro sistema o dispositivo antes de autorizar el acceso". Asimismo, define a historia clínica electrónica como "la historia clínica cuyo registro unificado y personal se encuentra contenido en una base de datos electrónica, registrada mediante programas de computación y refrendada con firma digital del profesional tratante. Su almacenamiento, actualización y uso se efectúa en estrictas condiciones de seguridad…".

El Ministerio de Salud administra el Registro Nacional de Historias Clínicas Electrónicas y emite las normas complementarias para el establecimiento de los procedimientos técnicos y administrativos necesarios para su implementación y sostenibilidad, a fin de garantizar la interoperabilidad, procesamiento, interpretación y seguridad de la información contenida en las historias clínicas electrónica.

Se declara de interés nacional la implementación del Registro Nacional de Historias Clínicas Electrónicas. Todo establecimiento de salud o servicio médico de apoyo que cuente con historias clínicas electrónicas debe acreditar obligatoriamente su sistema de información para acceder al Registro Nacional de Historias Clínicas Electrónicas (RENHICE).

El sistema de información de historias clínicas electrónicas de cada establecimiento de salud o servicio médico de apoyo, permite que cada paciente pueda ser atendido con su historia clínica electrónica, pero además si el paciente lo autoriza permite que el médico tratante pueda acceder a traces del RENHICE, a visualizar o leer sus otras historias clínicas electrónicas generadas en otros establecimientos de salud o servicios médicos de apoyo. El sistema de información debe estar diseñado para presentar a requerimiento y por separado los datos de filiación, la información clínica tanto básica como sensible de cada historia clínica.

Se define como trazabilidad como : "Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad, dejando rastro del respectivo acceso".

La autorización de acceso que brinda el paciente o usuario de salud o su representante legal al profesional de salud que lo atiende, para la visualización o lectura de sus historias clínicas electrónicas, debe ser dado con la capacidad autónoma, libre y de manera informada, en concordancia con la normativa de salud y de protección de datos personales[105].

El paciente o usuario de salud es el titular de su historia clínica electrónica en tanto es el propietario de su información clínica allí contenida. El establecimiento de salud o servicio médico de apoyo es el propietario de su información clínica allí contenida. El establecimiento de salud o servicio médico de apoyo es el propietario de las historias clínicas electrónicas y del sistema de información de historias clínicas electrónicas acreditado ante el RENHICE; y por tanto tiene la responsabilidad de conservar, custodiar y garantizar la seguridad de estas y de la información allí contenida[106].

La autenticación de la identidad del paciente o usuario de salud o su representante legal es para que reciba la atención de salud correspondiente, para que el paciente o su representante legal otorguen la autorización de acceso del paciente o su representante legal al RENHICE. Para la atención de salud, el paciente o usuario de salud deberá autenticar su identidad mediante cualquiera de los siguientes mecanismos: a) Autenticación biométrica mediante el uso del aplicativo Match OnCard del documento nacional de identidad electrónico-DNIe. Autenticación Digital mediante el correspondiente certificado digital para persona natural contenido en el documento nacional de identidad electrónico-DNIe[107].

2.2. Análisis de la Legislación de Firmas y Certificados Digitales y el Derecho de Identidad Digital

[105] Reglamento de la Ley que crea el Registro Nacional de Historia Clínicas Electrónicas. Art.5. D.S. 039-2015-SA. Publicado el 17 de Diciembre de 2015.

[106] Reglamento de la Ley que crea el Registro Nacional de Historia Clínicas Electrónicas. Art.52. . D.S. 039-2015-SA. Publicado el 17 de Diciembre de 2015.

[107] [107] D.S. 039-2015-SA, Reglamento de la Ley que crea el Registro Nacional de Historia Clínicas Electrónicas. Arts.74 y 75. Publicado el 17 de Diciembre del 2015

La Ley 27269, Ley de Firmas y Certificados Digitales, fue promulgada en el mes de mayo del año 2000. En su objeto establece: "La presente Ley tiene por objeto regular la utilización de la firma electrónica otorgándole la misma validez que una firma manuscrita u otra análoga que conlleve manifestación de voluntad"[108].

En este primer párrafo de la Ley 27269, se consagra el principio de equivalencia funcional por el cual "los actos jurídicos realizados por medios electrónicos que cumplan con las disposiciones legales vigentes poseen la misma validez y eficacia jurídica que los actos realizados por medios convencionales, pudiéndolo sustituir para todos los efectos legales. De conformidad con lo establecido en la ley y el reglamento, los documentos firmados digitalmente pueden ser presentados y admitidos como prueba en toda clase de procesos judiciales y procedimientos administrativos"[109].

La Ley peruana de firmas y certificados digitales, tiene una vigencia de más de quince años y su utilización es un proceso. A fin de lograr un verdadero desarrollo de las transacciones electrónicas es necesario regular un sistema integral que permita al ciudadano en forma efectiva y segura realizar procesos electrónicos de gobierno electrónico, comercio electrónico, negocios electrónicos y aprendizaje electrónico.

"El punto de partida en toda legislación en materia de firmas electrónicas es el de determinar es como un mensaje de datos se puede firmar y luego ser enviado, recibido, archivado o comunicado en forma electrónica…Firma electrónica es el término genérico y neutral para referirse al universo de tecnologías mediante las cuales una persona puede firmar un mensaje de datos…firma digital es el nombre que se le da a cierto tipo de firma electrónica basada en el uso de criptografía simétrica o de llave publica"[110].

[108] Ley 27269, Ley de Firmas y Certificados Digitales. Articulo 1º: Objeto de la Ley. Mayo del 2000.
[109] D.S. 052-2008-PCM, Reglamento de la Ley de Firmas y Certificados Digitales. Glosario de Terminos.
[110] TELLEZ VALDES, Julio: "Derecho Informático". Tercera Edición. Ed. McGrawHill. México DF. México. Pagina 203.

En el Perú, conforme la Ley 27269, se entiende por firma electrónica "a cualquier símbolo basado en medios electrónicos utilizado o adoptado por una parte con la intención precisa de vincularse o autenticar un documento cumpliendo todas o algunas de las funciones características de una firma manuscrita" y se define la firma digital "como aquella firma electrónica que utiliza una técnica de criptografía asimétrica, basada en el uso de un par de claves único; asociadas una clave privada y una clave pública relacionadas matemáticamente entre sí, de tal forma que las personas que conocen la clave pública no puedan derivar de ella la clave privada". El certificado digital es "el documento electrónico generado y firmado digitalmente por una entidad de certificación, la cual vincula un par de claves con una persona determinada confirmando su identidad".

En Colombia, conforme la Ley 527 de 1999 se entiende por firma digital " un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación".

En Argentina conforme el artículo 2º de la Ley 25506, se entiende por firma digital "al resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control. La firma digital debe ser susceptible de verificación por terceras partes, tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma.

Los procedimientos de firma y verificación a ser utilizados para tales fines serán los determinados por la Autoridad de Aplicación en consonancia con estándares tecnológicos internacionales vigentes".

Conforme el artículo 13 de la Ley 25506 se entiende por "certificado digital al documento digital firmado digitalmente por un certificador, que vincula los datos de verificación de firma a su titular".

Conforme el artículo 4º de la Ley 25506, las disposiciones de la ley argentina de firma digital no son aplicables: a) A las disposiciones por causa de muerte; b) A los actos jurídicos del derecho de familia; c) A los actos personalísimos en general; d) A los actos que deban ser instrumentados bajo exigencias o formalidades incompatibles con la utilización de la firma digital, ya sea como consecuencia de disposiciones legales o acuerdo de partes.

En España, conforme la Ley 59/2003 "1. La firma electrónica es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante. 2, La firma electrónica avanzada es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control. 3. Se considera firma electrónica reconocida la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma. 4. La firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel

En cuanto al objeto de algunas leyes sobre firmas y certificados digitales, tenemos las siguientes:

Paìs	Ley	Objeto	Comentarios
Perú	27269 de Firmas y Certificados Digitales.	"regular la utilización de la firma electrónica otorgándole la misma validez y eficacia jurídica que el uso de una firma manuscrita u otra análoga que conlleve manifestación de voluntad".	Regula Firma Electrónica. Principio de Equivalencia Funcional.

Colombia	Ley 527 de 1999 de Comercio Electrónico	"definir y reglamentar el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, así como establecer las entidades de certificación".	Regula mensaje de Datos, Comercio Electrónico y Firmas Digitales.
Argentina	Ley 25506 de Firma Digital	"reconocer el empleo de la firma electrónica y de la firma digital y su eficacia jurídica en las condiciones que establece la presente ley".	Firma Electrónica. Firma Digital. Eficacia Jurìdica.
España	*Ley 59/2003 de Firma Electrónica.*	*"*regular la firma electrónica, su eficacia jurídica y la prestación de servicios de certificación".	Firma Electrónica. Eficacia Electrónica. Prestación de Servicios de Certificación.

"El comercio y las demás operaciones electrónicas se caracterizan por la no presencia física y simultánea de los interesados, la inmediatez en la conclusión del negocio u operación y el celebrarse a través de un medio accesible a cualquier ciudadano del mundo. Por ello, el mecanismo clásico de la firma manuscrita debe ser sustituido por otro instrumento que reúna las mismas garantías de integridad y seguridad y que, además permita la confidencialidad"[111]

La firma electrónica y especialmente la firma digital permiten garantizar las autenticación por la cual se garantiza la comprobación

[111] PUIGCERVER ASOR, Carlos: "La Firma Digital y las Autoridades de Certificación: Regulación e Interacción en el proceso Español tras la regulación del Comercio Electrónico". En Revista de Derecho Comercial y de las Obligaciones. Nº 197. Ed. Depalma. Buenos Aires, Argentina. 2000. Página 136.

de la identidad del suscriptor del certificado digital; la integridad por la cual se garantiza que el mensaje de datos no ha sido modificado desde su envío por el iniciador hasta su recepción por el destinatario y el no repudio que garantiza que no pueda desconocerse la validez jurídica del documento firmado digitalmente dentro de la Infraestructura Oficial de Firma Electrónica.

"La firma electrónica se podría entender como el método, signo o símbolo de naturaleza electrónica incorporado por su titular a un documento preparado para ser tratado por medios telemáticos, con cualquiera de las finalidades previstas para la firma manual"[112]

La firma digital permite la manifestación de voluntad con efectos jurídicos en el entono digital, permitiendo que la persona que ha sido previamente identificada por la Entidad de Registro o Verificación pueda suscribir diversos documentos en la red con valor probatorio y efecto jurídico, siempre que se emita dentro de la Infraestructura Oficial de Firma Electrónica.

"La implantación de sistemas de firma electrónica y su utilización en el tráfico jurídico constituye uno de los mayores desafíos mundiales en materia de comunicación. No es exagerado afirmar que la consecución de un elevado grado de seguridad en la transmisión de datos mediante la firma electrónica podría convertir a los sistemas telemáticos en el cauce ordinario del tráfico jurídico entre particulares y entre éstos y los poderes públicos. De hecho, la expansión y consolidación del comercio electrónico, muy desarrollado en la actualidad, depende en buena parte del perfeccionamiento de este medio de autenticación, sobre todo por lo que se refiere a las operaciones o transacciones de un valor o entidad elevados. Sin un sistema de autenticación como la

[112] MOLINA MATEOS, José María: "Firma Electrónica y Fe Pública Extrajudicial" En Revista Iberoamericana de Derecho Informático. Nºs. 30,31,32 Ed. Universidad Nacional a Distancia. Centro Regional de Extremadura, Merida, España.. 2000. Página 421.

firma electrónica,… puede quedarse … debilitada y resultar un cauce poco atractivo el inseguro para desarrollar el tráfico jurídico…"[113]

2.2.1.. Criptografía y Firma Digital.

2.2.1.1. La Criptografía:

"La criptografía es un conjunto de técnicas empleadas para conservar segura la información. Con ella es posible transformar palabras escritas y otros tipos de mensajes de forma que sena incomprensibles para receptores no autorizados. Un receptor autorizado puede después regresar las palabras o mensajes a un mensaje perfectamente comprensible"[114]

Los sistemas de encriptación modernos constan de dos procesos complementarios: la encriptación y la desencriptación. La encriptación es el proceso mediante el cual el mensaje (el texto llano) se transforma en un segundo mensaje (el texto cifrado) mediante una función compleja (el algoritmo de encriptación) y una llave de codificación (encriptación) especial. Desencriptación: Proceso inverso, en el cual el texto cifrado (encriptado) se convierte nuevamente en el texto llano original mediante una segunda función compleja y una llave de desencriptación.

La encriptación es la tecnología que protege fundamentalmente la información al viajar a través de Internet. Los sistemas criptográficos que se utilizan en forma amplia hoy en día pueden dividirse en dos categorías[115].

El primer grupo lo forman los programas y protocolos utilizados para encriptar mensajes de correo electrónico. Estos programas toman un mensaje en texto llano, lo encriptan y almacenan el texto cifrado o lo envían a otro usuario en Internet. También pueden ocuparse para

[113] ORMAZABAL SANCHEZ, Guillermo: "La prueba documental y los medios e instrumentos idóneos para reproducir imágenes o sonidos o archivar y conocer datos". Editorial La Ley. Madrid, España. 2000. Página 209.
[114] GARFINKEL, Simson y SPAFFORD, Gene: Ob.cit. Página 187.
[115] Vid. GARFINKEL, Simson y SPAFFORD, Gene: Ob. Cit. Páginas 212 a 219.

encriptar archivos guardados en las computadoras para darles mayor protección , por ejemplo:

i)El PGP o Pret Good Privacy, es uno de los primeros programas de encriptación de llave pública en adquirir popularidad, escrito por Phil Zimmermann y liberado en Internet en Junio de 1991. PGP es un sistema completo para la protección de correo electrónico y archivos. También es un conjunto de estándares que describen los formatos de los mensajes encriptados, llaves y firmas digitales. PGP es un sistema híbrido que utiliza encriptación de llave pública RSA para la administración de llaves, y el código simétrico IDEA para la encriptación de los datos.

ii)El S/MIME. o Extensiones Multipropósito de Correo en Internet (MIME, Multipurpouse Internet Mail Extensions) son un estándar para enviar mensajes con archivos binarios anexos a través de internet. Secure/MIME (MIME seguro) extiende el estándar MIME para proporcionar correo electrónico firmado. En principio fue implementada como una biblioteca diseñada para agregarse a los paquetes de correos existentes. Como esta biblioteca proviene de RSA Data Security e incluye licencias de todos los algoritmos y patentes necesarias, y debido a que las principales empresas que venden sistemas de correo electrónico ya tienen una relación de negocios con RSA Data Security, es posible que muchos proveedores de correo lo adopten prefiriéndolo a PGP. S/MIME ofrece confidencialidad mediante algoritmos de encriptación especificados por el usuario; integridad mediante una función hash especificada por el usuario; autenticación mediante certificados de llave pública X.509 v3, y no repudio mediante mensajes firmados criptográficamente. El sistema puede usarse tanto con encriptación fuerte como débil.

La segunda categoría de sistemas criptográficos se compone de protocolos de red utilizados para proporcionar confidencialidad, autenticación, integridad y no repudio en un ambiente de red. Algunos de estos sistemas que encuadran dentro de esta categoría son:

a) SSL.- Nivel de Conexiones Seguras (SSL, Secure Sockets Layer) es un protocolo criptográfico de propósito general para asegurar canales de comunicación bidireccionales. SSL se utiliza comúnmente junto con el protocolo TCP/IP, y es el sistema de encriptación que usan sistemas como Navigator de Nestcape e Internet Explorer de Microsoft, pero puede emplearse con cualquier servicio basado en TCP/IP . SSL ofrece confidencialidad mediante algoritmos de encriptación especificados por el usuario; integridad, mediante funciones hash criptográficas especificadas por el usuario, y no repudio mensajes firmados criptográficamente.

b) PCT (Private Communications Technology o Tecnología de Comunicaciones Seguras) es un protocolo de seguridad de nivel de transporte similar a SSL desarrollado por Microsoft y es usado entre otros, por sus clientes de intranets corporativas.

c) SET (Secure Electronic Transactions o Transacciones Electrónicas Seguras) es un protocolo criptográfico diseñado para envío de número de tarjetas de crédito por Internet. SET proporciona confidencialidad para los números de tarjeta de crédito, pues se encriptan mediante el algoritmo RSA, proporciona además integridad, autenticación y no repudio mediante funciones de compendio de mensajes y firmas digitales.

d) CyberCash (Ciberefectivo) es un protocolo de pagos electrónicos de propósito similar al SET. Es un sistema basado en tecnología de llave pública. Antes de utilizar CyberCash, el consumidor debe descargar un programa especial del sitio web Cybercash en http://www.cybercash.com . Al programa se le llama billetera Cybercash, y mantiene una base de datos de las tarjetas de crédito y otros instrumentos de pago del usuario. Cuando se ejecuta por primera vez, el software de billetera crea una combinación de claves pública y privada.

Al respecto, hay que tener en cuenta los distintos sistemas de identificación digital, entre los que tenemos los siguientes:

a) Uno de los sistemas de identificación digital es el que se basa en claves de acceso: se le asigna a cada usuario del sistema un nombre de usuario y una clave de acceso (o contraseña). Para probar la identidad a la computadora sólo se le teclea la clave de acceso. Si es idéntica a la que está almacenada en la computadora, el usuario debe ser quién dice ser.

b) Una segunda forma en que las personas pueden probar su identidad son las tarjetas de acceso: un objeto físico que llevan consigo y que, de alguna forma , comprueba su identidad y proporciona el acceso. Las tarjetas de acceso son utilizadas para comprobar la identidad en el mundo de negocios actual. Para acceder a un sistema o abrir una "puerta" se inserta la tarjeta en una lectora, cada tarjeta tiene un número único, a su vez, el sistema tiene una lista de las tarjetas autorizadas para abrir "puertas" específicas a determinadas horas. Para que el sistema sea efectivo las personas no deben prestar sus tarjetas a otros[116].
c) Otra técnica que las computadoras utilizan para determinar la identidad de las personas es hacerles una medición física y compararla con un perfil almacenado con anterioridad. Esta técnica se conoce como biométrica, ya que se basa en la medición de algún rasgo de una persona viva.

"Una computadora es segura si puede confiar en ella y su software se comporta como usted espera...la seguridad en el Web es un conjunto de procedimientos, prácticas y tecnologías para proteger a los servidores y usuarios del web y las organizaciones que los rodean. La seguridad es una protección contra el comportamiento inesperado"[117]

El problema de la seguridad en el web consta de tres principales partes. A) Asegurar el servidor y los datos que contiene. B) Asegurar

[116] Vid. GARFINKEL, Simson y SPAFFORD, Gene: "Seguridad y Comercio en el Web" Ed. Mc Graw Hill. México D.F., México. 1999. Página 106.
[117] GARFINKEL, Simson y SPAFFORD, Gene: Ob.cit. Página 3.

la información entre el servidor web y el usario. C) Asegurar la computadora del usuario.

"El comercio y las demás operaciones electrónicas se caracterizan por la no presencia física y simultánea de los interesados, la inmediatez en la conclusión del negocio u operación y el celebrarse a través de un medio accesible a cualquier ciudadano del mundo. Por ello, el mecanismo clásico de la firma manuscrita debe ser sustituido por otro instrumento que reúna las mismas garantías de integridad y seguridad y que, además permita la confidencialidad"[118]

Al respecto, hay que tener en cuenta que "La firma electrónica se podría entender como el método, signo o símbolo de naturaleza electrónica incorporado por su titular a un documento preparado para ser tratado por medios telemáticos, con cualquiera de las finalidades previstas para la firma manual"[119] . La tecnología permite reforzar la seguridad y la acreditación de la identidad digital cuando hay manifestación de voluntad.

Por tanto, "La implantación de sistemas de firma electrónica y su utilización en el tráfico jurídico constituye uno de los mayores desafíos mundiales en materia de comunicación. No es exagerado afirmar que la consecución de un elevado grado de seguridad en la transmisión de datos mediante la firma electrónica podría convertir a los sistemas telemáticos en el cauce ordinario del tráfico jurídico entre particulares y entre éstos y los poderes públicos. De hecho, la expansión y consolidación del comercio electrónico, muy desarrollado en la actualidad, depende en buena parte del perfeccionamiento de este medio de autenticación, sobre todo por lo que se refiere a las operaciones o transacciones de un valor o entidad elevados. Sin un sistema de autenticación como la firma electrónica,… puede

[118] PUIGCERVER ASOR, Carlos: "La Firma Digital y las Autoridades de Certificación: Regulación e Interacción en el proceso Español tras la regulación del Comercio Electrónico". En Revista de Derecho Comercial y de las Obligaciones. Nº 197. Ed. Depalma. Buenos Aires, Argentina. 2000. Página 136.
[119] MOLINA MATEOS, José María: "Firma Electrónica y Fe Pública Extrajudicial" En Revista Iberoamericana de Derecho Informático. Nºs. 30,31,32 Ed. Universidad Nacional a Distancia. Centro Regional de Extremadura, Merida, España.. 2000. Página 421.

quedarse… debilitada y resultar un cauce poco atractivo el inseguro para desarrollar el tráfico jurídico…"[120]. Lo que reafirma la necesidad de la encriptación y de contar con seguridad en el mundo digital en la comunicación electrónica de las personas.

2.2.2. Comunicación Segura con La firma digital

La comunicación es segura es posible si el receptor toma parte activa del proceso de cifrado. La cuestión fundamental a resolver es si puede enviarse de forma segura un mensaje cifrado digitalmente sin un intercambio previo de claves. Para lo cual, en vez de utilizar una clave secreta única se utiliza un par de claves. Una clave es capaz de cifrar el mensaje original, para que extraños no pudieran leerla, la otra clave es una llave que abre la puerta del mensaje y permite a su dueño leer su contenido.

Mediante la clave pública una persona puede generar una pareja de claves, una pública y otra privada, y ningún intruso tendría acceso a la parte secreta de la clave. Entonces serían posibles las verdaderas comunicaciones privadas. La clave pública proporciona el medio para autenticar al remitente de un mensaje electrónico. Si el remitente envía el mensaje cifrado utilizando la clave pública de una persona, sólo podrá leerlo el destinatario del mensaje. Pero, si se invierte el proceso, si alguien cifra un texto utilizando su clave privada, el texto cifrado resultante sólo podrá ser descifrado por la clave pública que encaja con su compañera. En otras palabras, aplicar la clave secreta de uno a un mensaje equivale a firmarlo con su nombre: una firma digital.

En la práctica, la firma digital está integrada con los dígitos que constituyen el contenido del propio mensaje, así si el documento es interceptado el intruso no podrá extraer de él la firma del remitente en otro documento. Esta técnica asegura la autenticación, integridad y no repudio de todo el documento. En consecuencia, "..la firma digital sirve..para asegurar la identidad de remitente y destinatarios de

[120] ORMAZABAL SANCHEZ, Guillermo: "La prueba documental y los medios e instrumentos idóneos para reproducir imágenes o sonidos o archivar y conocer datos". Editorial La Ley. Madrid, España. 2000. Página 209.

mensaje de datos, impidiendo así la remisión o recepción o acceso por parte de terceras personas [no autorizadas]"[121]

2.2.3 Los Certificados Digitales, atributos de la firma y la Identidad

"El certificado digital es el documento electrónico generado y firmado digitalmente por una entidad de certificación, la cual vincula un par de claves con una persona determinada confirmando su identidad"[122].

El certificado digital identifica indubitablemente a su titular y a la entidad de certificación que lo emitió, indicando su periodo de vigencia y los datos que permitan su identificación única.

Los atributos de la firma digital que se emiten basado en un certificado digital, emitido por una entidad de certificación acreditada son:

"Autenticidad: La firma garantiza que las personas que intervienen son quienes dicen ser. Es decir, el contenido del mensaje se encuentra resguardado por medio de algoritmos matemáticos, salvaguardando la autenticidad del mensaje inicial"[123].

Integridad: Es la característica que indica que un documento electrónico no ha sido alterado desde la transmisión por el iniciador hasta su recepción por el destinatario. Ningún carácter puede ser modificado para que mantenga su validez la firma digital.

"No repudio: Es la imposibilidad de una persona de desdecirse de sus actos cuando ha plasmado su voluntad en un documento y lo ha firmado en forma manuscrita o digitalmente con un certificado emitido por una Entidad de Certificación acreditada en cooperación con una Entidad de Registro o Verificacion acreditada, salvo que la misma entidad tenga ambas calidades, empleando un software de firmas

[121] IGLESIAS, Lidia Viviana: "Firma Digital. Seguridad en Internet. Certificados. En Memorias del VIII Congreso Iberoamericano de Derecho e Informática. TEC de Monterrey. México. Noviembre 2000. Página 515.
[122] Ley 27269, Ley de Firmas y Certificados Digitales, articulo 6º
[123] Sistema Economico Latinoamericano y del Caribe (SELA): "Fundamentos de la firma digital y su estado de arte en America Latina y el Caribe". Mayo del 2012. Pagina 9.

digitales acreditado y siempre que se cumpla lo previsto en la ley civil"[124].

Los certificados digitales se basan en la confianza y vinculan un par de claves con el titular de la firma digital, verificando y autenticando su identidad. Permite verificar que una clave específica pertenece efectivamente a una persona, previniendo la suplantación de identidad.

Para la obtención de un certificado digital, el solicitante debe acreditar lo siguiente: Tratándose de personas naturales, tener plena capacidad de ejercicio de sus derechos civiles, Tratándose de personas jurídicas, acreditar la existencia de la persona jurídica y su vigencia mediante los instrumentos públicos o norma legal respectiva, debiendo contar con un representante debidamente acreditado para tales efectos.

Los certificados digitales dentro de la Infraestructura Oficial de Firma Electrónica (IOFE)[125] deben contener como minino para las personas naturales, nombres completos, número de documento oficial de identidad, tipo de documento, dirección oficial de correo electrónico. Tratándose de personas jurídicas debe contener como mínimo la razon social, el número de Registro Único de Contribuyente, nombres completos del suscriptor[126], facultades del suscriptor, correo electrónico del suscriptor, dirección del correo electrónico del suscriptor, dirección oficial del correo electrónico del suscriptor, dirección oficial del correo electrónico de la persona jurídica.

La firma digital generada dentro de la IOFE tiene la misma validez y eficacia jurídica que el uso de una firma manuscrita. En tal sentido, cuando la ley exija la firma de una persona, este requisito se entenderá cumplido en relación con un documento electrónico si se utiliza digital generada en el marco de la Infraestructura Oficial de

[124] D.S. 052-2008-PCM, Reglamento de la Ley de Firmas y Certificados Digitales. Glosario de Términos.
[125] Conforme el Glosario de términos del reglamento, Infraestructura Oficial de Firma Electrónica (IOFE) es el sistema confiable, acreditado, regulado por la Autoridad Administrativa Competente, provisto de instrumentos legales y técnicos que permiten generar firmas digitales y proporcionar diversos niveles de seguridad respecto de la integridad de los documentos y sobre la identidad de su autor.
[126] Es la persona natural responsable de la generación y uso de la clave privada, a quien se le vincula de manera exclusiva con un documento electrónico firmado digitalmente utilizando su clave privada.

Firma Electrónica. Por otra parte, los documentos electrónicos firmados digitalmente dentro de la IOFE deberán ser admitidos como prueba en los procesos judiciales y o procedimientos administrativos siempre y cuando la firma digital haya sido emitida por una entidad acreditada. La firma digital generada en el marco de la IOFE garantiza el no repudio del documento original.

Dentro de la IOFE, la responsabilidad de los efectos jurídicos generados por la utilización de una firma digital corresponde al titular de un certificado. Tratándose de personas naturales, estas son titulares y suscriptores del certificado digital. En el caso de personas jurídicas, estas son titulares del certificado digital. los suscriptores son las personas naturales responsable de la generación y uso de la clave privada.

Hay un caso especial y es el de los certificados digitales para su utilización a través de agentes automatizados[127], situación en el cual las personas jurídicas asumen las facultades de titulares y suscriptores del certificado digital.

La comprobación de la validez de un documento firmado digitalmente se realiza en un ambiente electrónico aplicando el software de verificación de firma digital.

Una firma digital generada bajo la IOFE carece de validez, además de los supuestos que prevé la legislación civil, cuando es utilizado en fines distintos para los que extendido el certificado y cuando el certificado haya sido cancelado.

La cancelación del certificado digital puede darse a solicitud del titular del certificado digital o del suscriptor; por decisión de la Entidad de Certificación; por expiración del plazo de vigencia; por interdicción civil judicialmente declarada o declaración de ausencia o muerte presunta, del titular del certificado; por extinción de la personería jurídica o declaración judicial de quiebra; por muerte, o por inhabilitación o

[127] Agentes automatizados son los procesos y equipos programados para atender requerimientos predefinidos y dar respuesta automática sin intervención humana en dicha fase.

incapacidad declarada judicialmente de la persona natural suscriptor del certificado.

2.2.4. Prestadores de Servicios de Certificación Digital.

Los Prestadores de Certificación Digital son la Entidad de Certificación; la Entidad de Registro o Verificación; los Prestadores de Servicios de Valor Añadido.

La Entidades de Certificación emiten certificados digitales manteniendo una secuencia correlativa en el número de serie; cancelan certificados digitales. Las Entidades de Registro o Verificación identifican a los titulares y/o suscriptores del certificado digital mediante el levantamiento de datos y comprobación de la información brindada por aquel; aprobar o denegar, según sea el caso , las solicitudes de emisión, modificación, re-emisión, suspensión o cancelación de certificados digitales, comunicándolo a la respectiva Entidad de Certificación, según lo declarado en la correspondiente Declaración de Practicas de Certificación[128]. Los Prestadores de Servicios de Valor Añadido certifican los documentos electrónicos con fecha y hora cierta (sello de tiempo) o en el almacenamiento de tales documentos, aplicando medios que garanticen la integridad y no repudio de los datos de origen y recepción (sistema de intermediación digital).

La Autoridad Administrativa Competente[129] , aprueba las Políticas de Certificación; las Declaraciones de Practicas; las Políticas de seguridad, las políticas y planes de privacidad. Asimismo, la Autoridad acredita a los Prestadores de Servicios de Certificación Digital. Supervisa, fiscaliza y sanciona ante infracciones e incumplimiento a la ley, el reglamento y la declaraciones y prácticas de certificación, entre otras normas.

[128] Es el documento oficialmente presentado por una Entidad de Certificación a la Autoridad Administrativa Competente, mediante el cual define sus prácticas de certificación.
[129] La Autoridad Administrativa Competente, actualmente es INDECOPI, según ley modificatoria por Decreto Suoremo podrá designarse otra autoridad.

Los Prestadores de Servicios de Certificación acreditados son incluidos en un registro especial denominado TSL. La lista de servicios de confianza (TSL) contiene los nombres y, en varios casos los certificados digitales raíces de las Entidades Prestadoras de Servicios de Certificación Digital (PSCs) consideradas de confianza. Para el diseño de su formato se ha tomado como referencia la Norma Técnica ETSI TS 102.231.

La inscripción de una Prestadora de Servicios de Certificación (PSCs) en la lista de servicios de confianza (TSL) significa que ésta se encuentra acreditada por el INDECOPI conforme el Reglamento de la Ley de Firmas y Certificados Digitales , aprobado por D.S.052-2008-PCM.

"La TSL garantiza la interoperabilidad entre las entidades acreditadas por el INDECOPI. La TSL esencialmente reemplaza al par de certificados cruzados. La parte que confía (receptor del documento firmado digitalmente), en realidad, lo que hace es confiar en la TSL y, por tanto, en las entidades inscritas en la misma. La TSL provee información especialmente significativa para las transacciones internacionales e interdominios de una manera inteligible y a la vez procesable por el software del usuario, a efectos de permitir una verificación automática de la información sobre el estado del certificado"[130]

2..2.4.1. En el Sector Privado.

Dentro de la lista de servicios de confianza[131], encontramos las siguientes entidades privadas acreditadas:

a) Con software de firma digital: Acist Perú SAC. Bit 4ID Ibèrica SL. CELSAT (Perù) . Com SAC. Colegio de Notarios de Lima-

[130] http://www.indecopi.gob.pe

[131] https://iofe,indecopi.gob.pe/WebAppConsultas/faces/pages/IofeWeb/Principal.jspx?adf.ctrl-state=101nr4b57r4 Fecha de Consulta: 04 de Diciembre de 2015.

CNL. INDENOVA S.L: Microsoft Perù SRL. Perù Media Server SAC. Realia Technologies SL. Soft & Net SAC. Z y Trust SA.

b) Entidad de Certificacion Raiz y Entidad de Certificacion Nivel subsiguiente:
-ENTRUST. AC CARMERFIRMA. DIGI SIGN. SWISSING Platinium. Intercambio Electronico de Datos y Comunicaciones. COMODO CA. FIRMA PROFESIONAL S.A.

c) Entidad de Registro de Persona Juridica
IOFE SAC

d) Prestador de Servicio de Valor Añadido:
- Indenova SL (Sistema de Intermediación Electrònica-SIE).
- IOFE SAC (Sistema de Intermediaciòn Electrònica-SIE)
- Gestión de Soluciones Digitales SAC (Sellado de Tiempo).
- Soft & Net SAC (Sellado de Tiempo)
- Salmon Corp SAC (Sellado de Tiempo)
Z y Trust SA (Sellado de Tiempo).

2..2 4..2. En el Sector Público.

a) Con Software de Firma Digital
- Registro Nacional de Identificación y Estado Civil (RENIEC).
- Superintendencia de Banca y Seguros y AFP (SBS).
- Superintendencia del Mercado de Valores (SMV)
- Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI).

b) Entidad de Certificación Raìz del Estado Peruano (ECERNEP)
- Registro Nacional de Identificación y Estado Civil (RENIEC).

c) Entidad de Registro o Verificación para Persona Natural.
- Registro Nacional de Identificación y Estado Civil (RENIEC).

d) Entidad de Registro o Verificación para Persona Juridica.
- Registro Nacional de Identificación y Estado Civil (RENIEC).

e) Entidad de Certificación Digital (ECEP)
- Registro Nacional de Identificación y Estado Civil (RENIEC).

- 2..2.5 . Ley de firmas y certificados digitales y normas concordantes.

La creciente utilización de técnicas de autenticación digital en sustitución de firmas manuscritas, dentro de la Infraestructura Oficial de Firma electrónica (IOFE) ha originado la necesidad de crear un marco jurídico específico. En el Perú, mencionamos las siguientes normas jurídicas, con jerarquía de ley:

a) Ley Nº 27269, Ley de Firmas y Certificados Digitales, de Mayo del 2000, que establece el principio de equivalencia funcional, define la firma electrónica, establece su ámbito de aplicación, define la firma digital, precisa las obligaciones del titular, define el certificado digital, precisa su contenido, incide en la confidencialidad de la información, señala los casos de cancelación del certificado digital, precisa los casos de revocación del certificado digital y de reconocimiento de los certificados emitidos por entidades extranjeras. Regula el régimen jurídico de las Entidades de Certificación y las Entidades de Registro. .
b) Ley Nº 27310 que modifica el artículo 11º de la Ley 27269 precisando que: "Los Certificados de Firmas Digitales emitidos por Entidades Extranjeras tendrán la misma validez y eficacia jurídica reconocidas en la presente ley, siempre y cuando tales certificados sean reconocidos por la autoridad administrativa competente.
c) Ley Nº 28403, de Noviembre de 2004, que dispone la recaudación de un aporte por supervisión y control anual por parte del INDECOPI de las Entidades de Certificación y de Verificación y Registro de Firmas Digitales acreditadas bajo su ámbito.
d) Ley Nº 30224, de Julio de 2014, que incorpora el articulo 15-A de la Ley 27269, que establece el Régimen de Infracciones y Sanciones, estableciendo que: "La autoridad competente tiene la facultad de tipificar las infracciones por incumplimiento de lo establecido en la Ley 27269, Ley de Firmas y Certificados Digitales, su Reglamento y las Guías de Acreditación de la Autoridad Administrativa Competente. La Autoridad podrá

imponer las siguientes sanciones: 1. Multa hasta un monto de 50 UIT. 2. Suspensión temporal de la acreditación. 3. Cancelación de la acreditación. Las infracciones serán establecidas como leves, graves y muy graves, teniendo en cuenta criterios de proporcionalidad.

e) Ley Nº 27291, que modifica el artículo 141º del Código Civil que establece: "la manifestación de voluntad puede ser expresa o tácita. Es expresa cuando se realiza en forma oral o escrita, a través de cualquier medio directo, manual, mecánico, electrónico u otro análogo…".

2.2.6. Normas complementarias de la legislación de firmas y certificados digitales.

Entre las normas complementarias de la legislación de firmas y certificados digitales, mencionamos las siguientes:

a) La Ley Nº 28677, Ley de Garantía Mobiliaria, de Febrero del 2006, en su artículo 17, establece que "el acto jurídico constitutivo de la Garantía Mobiliaria constara por escrito y podrá instrumentarse por cualquier medio fehaciente que deje constancia de la voluntad de quien lo otorga, incluyendo intercambio electrónico de datos, correo electrónico y medios ópticos o similares, de conformidad con la Ley 27269 Ley de Firmas y Certificados Digitales…".

ii) La Ley 30229 de Julio de 2014, que incorpora el articulo 155-A a la Ley Orgánica del Poder Judicial, estableciendo que: "la notificación electrónica debe contar con firma digital y debe ser utilizada en el marco de la Ley 27269, Ley de Firmas y Certificados Digitales, su reglamento, asi como la normativa relacionada".

iii) La Ley 30224, Ley que crea el Registro Nacional de Historias Clínicas Electrónicas, de Mayo de 2013, establece en su artículo 8.1: "RENIEC, entidad de certificación del Estado Peruano, y las demás entidades de certificación digital brindan los servicios de certificación digital para la autenticación de la identidad de las

personas naturales y jurídicas, mediante los certificados y firmas digitales, en el marco de la Ley 27269, Ley de Firmas y Certificados Digitales".

iv) Decreto Legislativo 1049, Ley del Notariado, de Junio de 2008, que en su artículo 24 establece: "*Los instrumentos públicos notariales otorgados con arreglo a lo dispuesto en la ley, producen fe respecto a la realización del acto jurídico y de los hechos y circunstancias que el notario presencie.*
Asimismo, producen fe aquellos que autoriza el notario utilizando la tecnología de firmas y certificados digitales de acuerdo a la ley de la materia".

v) Ley 26612, que modifica la legislación de microforma digital, de Mayo de 1996, establece, en su artículo 5º inciso e) que: "los procedimientos técnicos empleados en la confección de las microformas, microduplicados y copias fieles deben garantizar los resultados siguientes: ".. Que las microformas obtenidas bajo la modalidad de documentos producidos por procedimientos informáticos y medios similares tengan sistemas de seguridad de datos e información que aseguren su inalterabilidad e integridad. Asimismo, cuando en esta modalidad de microformas se incluya signatura o firma informática, ésta deberá ser inalterable, fija y durable y comprobable su autenticidad en forma indubitable, esta comprobación deberá hacerse por medios idóneos".

2.2.7. Acuerdos Comercial con normas referentes a la Certificación Digital.

Con respecto a los Acuerdos Comerciales suscritos por el Perú, que contienen normas referentes a la certificación digital, tenemos los siguientes:

1) Acuerdo Comercial con la Unión Europea (TLC). Título VI, Comercio de Servicios, en el artículo 109, inciso g) establece que: "En la medida que sea necesario y justificado, el Comité de Comercio, podrá establecer un grupo de trabajo con el fin de establecer mecanismos de cooperación en materia de

acreditación y certificación digital para transacciones electrónicas y el reconocimiento mutuo de certificados digitales".

2) Acuerdo Comercial con Estados Unidos (TLC). Capitulo Quince. Comercio Electrónico. Articulo 15.6. Autenticación. " Ninguna parte podrá adoptar o mantener legislación sobre autenticación electrónica que: a) prohíba a las partes en una transacción electrónica determinar en forma mutua los métodos apropiados de autenticación para dicha transacción; o b) impida a las partes tener la oportunidad de establecer ante las instancias judiciales o administrativas que la transacción electrónica cumple con cualquier requerimiento legal con respecto a la autenticación".
3) Alianza del Pacifico (Peru, Chile, Colombia, Mèxico). Capitulo 13: Comercio Electronico. Articulo 13, numeral 2: "Las partes establecerán mecanismos y criterios de homologación que fomenten la interoperabilidad de la autenticación electrónica entre ellas de acuerdo a estándares internacionales. Con este propósito podrán considerar el reconocimiento de certificados de firma electrónica avanzada o digital, según corresponda, emitidos por prestadores de servicios de certificación, que operen en el territorio de cualquier parte de acuerdo al procedimiento que determine su legislación, con el fin de resguardar los estándares de seguridad e integridad".

Con respecto a las normas reglamentarias, el Reglamento vigente es el Decreto Supremo Nº 052-2008-PCM, cuenta con 75 artículos. Como normas modificatorias y complementarias tenemos al D.S. 070-2011-PCM y al D.S. 105-2012-PCM.

En Artículo 5 del D.S. 070-2011-PCM, referido a los partes notariales electrónicos, se señala:

"Artículo 5.- Presentación y tramitación de partes notariales electrónicos firmados digitalmente

Los partes notariales electrónicos firmados digitalmente, en el marco de la Infraestructura Oficial de Firma Electrónica (IOFE), constituyen ***instrumento legal con valor suficiente*** *para dar mérito a la calificación e inscripción registral, siempre que hayan sido expedidos conforme al Decreto Legislativo Nº 1049,* ***Decreto Legislativo del Notariado y su Reglamento,*** *y sean presentados respetando los lineamientos contenidos en los* ***Convenios*** *que suscriban los Colegios de Notarios del Perú, con la Superintendencia Nacional de los Registros Públicos (SUNARP)."*

Otras normas peruanas relacionadas a la certificación y firma digital, son las siguientes:

a)D.S. 003-2015-JUS que aprueba el Reglamento de la Ley Nº 30229, Ley que adecua el uso de las Tecnologías de Información y Comunicaciones en el Sistema de Remates Judiciales y en los Servicios de Notificaciones Judiciales.

b) Resolución del Superintendente Nacional de Registros Pùblicos Nº 179-2015-SUNARP del 14 de Julio de 2015, que dispone la ampliación del servicio de presentación electrónica, del parte notarial de firma digital, a través del sistema SID-Sunarp, y la implementación y funcionamiento de dicho sistema en las oficinas registrales para actos de constitución de empresas en el Registro de Personas Jurídicas y otorgamiento de poderes en el Registro de Personas Naturales.

c) Resolución SMV Nº 010-2013-SMV/01 del 02 de Mayo de 2013, que aprueba el Reglamento del Sistema MVnet y SMV Virtual que regula el intercambio de información mediante plataformas electrónicas entre personas naturales y jurídicas con la Superintendencia del Mercado de Valores-SMV. El MV net es un sistema WEB de intercambio de información, que permite el

almacenamiento de información, utiliza la firma digital, autenticación y canales para el intercambio de información segura, garantizando lo siguiente: autenticación, confidencialidad, integridad, no repudio, sello de tiempo.

2.3. La autenticación biométrica de la identidad y otra legislación relacionada a la identificación.

2.3.1. La Biometría , la identidad y RENIEC

La "Biometría Informática" es la aplicación de técnicas biométricas[132] a la autentificación e identificación automática de personas en sistemas de seguridad informática. Las técnicas biométricas se basan en medir al usuario directa o indirectamente para reconocerlo automáticamente aplicando técnicas estadísticas y de Inteligencia Artificial (lógica borrosa, redes neuronales, etc).

El RENIEC ha implementado el Servicio de "Identificacion de Personas al Instante mediante el moderno sistema AFIS", compuesto por el software de consultas biométricas, kit de identificación y peritos dactiloscópicos expertos en identificación humana, proceso que se inicia con la captura de los dedos dactilares de los índices mediante el lector biométrico y se logra la identificación de la persona en forma indubitable en un "tiempo record de 5 segundos". Las personas NN identificadas acceden a los múltiples servicios de manera inmediata: salud, identidad, beneficios y programas sociales. Asimismo, la identificación de las personas fallecidas, evita que sean derivados a la fosa común y reciban digna sepultura[133]

"Las huellas dactilares y el reconocimiento del iris son dos aplicaciones en un nuevo campo conocido como biometría. Mediante almohadillas de lectura de huellas dactilares o con cámaras muy sensibles se puede capturar en un segundo información que prueba

---

[132] *Biometría: el concepto tradicional de biometría se refiere a la aplicación de las técnicas matemáticas y estadísticas a las ciencias de los seres vivos .en medicina, biología, etc.*

[133] Vid. Folleto de RENIEC titulado "Identificación de Personas al Instante mediante el Moderno Sistema AFIS" (Automated Fingerprint Identification System. Lima, Perù. Marzo de 2013.

que el usuario es, en efecto, quien dice ser, de forma más definitiva que , incluso, una contraseña muy segura. Estas aplicaciones... pueden ahorrar a una empresa una cantidad considerable de dinero, no sólo eliminando una plétora de problemas asociados con las contraseñas (las contraseñas se pueden perder, robar o corromper), sino gracias a que introducen otro obstáculo en el camino que debe recorrer un empleado de la empresa para burlar los sistemas de seguridad"[134]

"En el año 1996 se inicia el servicio de identificación de personas a través de las impresiones dactilares con la captura, homologación y determinación de la identidad de manera manual, con un plazo de atención de dos a tres semanas, recibiéndose de diferentes entidades (Policia Nacional del Perú, Poder Judicial, Ministerio Público, Fiscalía, hospitales, clínicas, morgues, albergues, entre otros) solicitudes para determinar la identidad de las personas (nombres, apellidos y dirección), que se encontraban como "NN" para resolver problemas administrativos y riesgos quirúrgicos de ser el caso, o ubicar o notificar a sus familiares, para su atención o darle sepultura en el caso de los fallecidos"[135]

En el año 2006, el RENIEC adquiere el Sistema Automatizado de Identificación de Impresiones Dactilares (AFIS), a efectos de contar con una Base de Datos AFIS-RENIEC (Impresiones Dactilares) de todos los peruanos "lográndose almacenar para el año 2010, las impresiones de diecinueve millones ochocientos dieciséis mil novecientos sesenta idos peruanos, reduciendo los plazos de atención a 24 horas. A partir del 2010, se implementa el servicio "Identificación de personas al instante mediante el moderno Sistema AFIS" reduciéndose el plazo máximo de atención a cinco segundos, cuyo proceso es "1 a N" (comparación de una impresión dactilar contra el universo de la Base de Datos AFIS-RENIEC). Este servicio se realiza,

[134] MC CARTHY, Mary Pat y CAMPBELL, Stuart: "Seguridad Digital" Ed. Mc Graw Hill Madrid, España 2002. Páginas 54 y 55.
[135] http://portales.reniec.gob.pe/web/seminario_biometrico/biometria Fecha de Consulta: 21 de Octubre de 2014.

a través de un "Kit de identificación" compuesto por un lector biométrico y una computadora portátil con conexión a Internet, que contiene el sistema de identificación biométrica"[136].

Mediante Resolución Jefatural Nº 264-2010-JNAC/RENIEC se crea el Servicio de Verificación Biométrica, el cual constituye una herramienta avanzada que facilita a las instituciones públicas o privadas a enfrentar la suplantación de identidades e impedir fraudes mediante la identificación automática de las personas.
La seguridad jurídica permite entre otras cosas la formalización de los agentes económicos, a través de la verificación oportuna de la identidad de las personas, lo que a su vez consolida la confianza en las operaciones comerciales y financieras que se realizan cotidianamente; todo lo cual contribuye a dinamizar la economía del país. El RENIEC al suministrar el servicio de verificación biométrica se convierte en uno de los pilares en la salvaguarda de la seguridad jurídica.

2.3.2. La obligatoriedad de uso del sistema de verificación biométrica en trámites notariales.

La legislación peruana establece la Obligatoriedad del Uso de Sistema de Verificación Biométrica de Huellas Dactilares en Trámites Notariales.

El uso de verificación biométrica de huellas dactilares en las notarías del país es obligatorio, con la finalidad de brindar seguridad respecto a la identidad de los otorgantes y/o intervinientes que realizan trámites notariales. El sistema de verificación biométrica se empleará para todo instrumento público notarial, sea de carácter protocolar o extraprotocolar.

Conforme la ley del Notariado[137] "el notario dará fe de conocer a los otorgantes y/o intervinientes o de haberlos identificado, conforme lo siguiente:

[136] http://portales.reniec.gob.pe/web/seminario_biometrico/biometria Fecha de Consulta: 21 de Octubre de 2014
[137] Artículo 55 de la Ley del Notariado, Decreto Legislativo Nª 1049, modificado por Decreto Legislativo Nº 1222 del 26 de Setiembre del 2015.

a) Cuando en el Distrito donde se ubica el oficio notarial tenga acceso a Internet, el notario exigirá el documento nacional de identidad y deberá verificar la identidad de los otorgantes o intervinientes utilizando la comparación biométrica de las huellas dactilares, a través del servicio que brinda el Registro Nacional de Identificación y Estado Civil- RENIEC.
b) Cuando no se pueda dar cumplimiento a la comparación biométrica de las huellas dactilares por causa no imputable al notario, éste exigirá el documento nacional de identidad y la consulta en línea para la verificación de las imágenes y datos del Registro Nacional de Identidad y Estado Civil- RENIEC con la colaboración del Colegio de Notarios, si fuera necesaria”.

Los Colegios de Notarios deberán informar al Consejo del Notariado, en el plazo que éste establezca, sobre los avances de la implementación del uso del sistema de verificación biométrica en su respectivo distrito notarial. El Registro de Identificación y Estado Civil (RENIEC) brindará a la notarías del país el acceso a su Base de Datos para la verificación de la identificación al costo real del servicio. Los usuarios realizan el pago correspondiente a dicho costo en la tarifa notarial".

El artículo 55º del Decreto Legislativo Nº 1049 establece que: "el notario, tiene el deber de dar fe, de conocer o haber identificado a los otorgantes y/o intervinientes en instrumentos públicos notariales, por lo que se encuentra obligado a acceder a la base de datos del RENIEC, en aquellos lugares donde se cuente de acceso a Internet, para proceder a verificar la identidad de los referidos otorgantes y/o intervinientes mediante la verificación de su fotografía, datos y/o a identificación por comparación biométrica de sus huellas dactilares".

En el considerando, de la norma en comentario, se afirma: "Que, sin perjuicio de existir mecanismos de control de identidad, como la verificación biométrica, se advierte la contínua comisión de operaciones fraudulentas efectuadas mediante instrumentos públicos notariales, como consecuencia de un inadecuado proceso de identificación de los intervinientes. Que, ante la referida problemática que afecta el correcto desempeño de la función notarial, a la ciudadanía y al Estado peruano, resulta necesario disponer la obligatoriedad del uso del sistema de verificación biométrica en todos los oficios notariales del país- que cuenten con acceso a internet- con

la finalidad de elevar los niveles de certeza del proceso de identificación de los otorgantes y/o intervinientes en actos notariales".

2.3.3. Identificación de abonados de teléfonos móviles mediante autenticación biométrica

El Decreto Supremo Nº 023-2014-MTC del 07 de Diciembre de 2014 establece el uso de herramientas que permitan cautelar la seguridad en los servicios públicos de telecomunicaciones, de modo que sea posible identificar a sus abonados a partir de los registros existentes, prevenir conductas que puedan afectar la normal prestación de los servicios públicos móviles, a fin de cautelar el derecho de las personas a utilizar libremente los servicios públicos móviles y salvaguardar la seguridad ciudadana, para lo cual regula el uso del sistema de verificación biométrica de huella dactilar.

Modifica el artículo 9° del D.S. 024-2010-MTC, disponiendo que las empresas operadoras de los servicios públicos móviles son responsables de realizar una adecuada identificación y registro de los abonados que contratan sus servicios. La contratación del servicio público móvil se realiza en forma previa o simultánea a su activación, debiendo verificarse la identidad de los abonados mediante los mecanismos previstos en los artículos 9° A , 9°B y 9° C.

En el artículo 9° A , se afirma que para efectos de la contratación del servicio, las empresas operadoras de los servicios públicos móviles deberán verificar la identidad de sus abonados, para lo cual se encuentran obligadas a utilizar:

El Sistema de Verificación Biométrica de Huella Dactilar, que es el sistema que consiste en la identificación de las personas a partir de la característica anatómica de la huella dactilar, empleando para tal efecto un dispositivo analizador, que permitirá la validación de la información en la base de datos de RENIEC. Este sistema será implementado obligatoriamente en los centros de atención de las

empresas operadoras y en las distribuidoras autorizadas por las mismas.

De no ser factible la verificación de identidad a través de este sistema, debido a la discapacidad física del solicitante, o por problemas con la base de datos de RENIEC o por falta de conectividad debidamente acreditada; la información de identidad del solicitante, en el caso de personas naturales, deberá ser verificada conforme el Sistema de Verificación de la Identidad No Biométrico.

El Sistema Verificación de Identidad No Biométrico, este sistema consiste en requerir al solicitante del servicio, la exhibición del documento legal de identificación, y solo puede ser utilizado por los distribuidores autorizados, para la confirmación de ciertos datos personales del solicitante del servicio que obren en la base de datos del RENIEC, mediante el uso de mensajes de texto (SMS) o mensajes del Servicio Suplementario de Datos No estructurados (USSD) o llamadas telefónicas.

En el artículo 9° E , se afirma que en el caso de las personas extranjeras, que no están registradas en el RENIEC, a quienes no les resulta aplicables los sistemas de verificación, en tanto se implemente el sistema de acceso en línea que permita validar el movimiento migratorio de los extranjeros o sus datos personales contenidos en el Registro Central de Extranjería, la contratación del servicio se realizará previa presentación del original y copia del Carnet de Extranjería o Pasaporte, con la finalidad que la empresa operadora proceda a registrar los datos personales del abonado y archivar copia del documento legal de identificación.

En el artículo 9° H , se establece que el RENIEC brindará a las empresas operadoras de servicios públicos móviles el servicio de verificación biométrica de huella dactilar, así como la atención en línea de las consultas que resulten necesarias para la operación del Sistema No Presencial de Verificación de la Identidad, al costo real del servicio. La determinación de las tasas o derechos a favor de RENIEC que resulten aplicables, se sujetará a lo previsto en los artículos 44 y

45 de la Ley 27444- Ley de Procedimiento Administrativo General, al Código Tributario y al Decreto Supremo N° 064-2010-PCM.

2.3.4. La Ley de Dinero Electrónico y la identificación

Por Ley Nº 29985 se regula emisión de dinero electrónico, se determina las empresas autorizadas a emitirlo y se establece el marco regulatorio y de supervisión de las Empresas Emisoras de Dinero Electrónico.

"Los soportes mediante los cuales se puede hacer uso del dinero electrónico pueden ser las siguientes: a) Teléfonos Móviles. b) Tarjetas prepago. C) Cualquier otro equipo o dispositivo electrónico"[138].

Titular es la persona que contrata con el emisor de dinero electrónico la prestación del servicio de emisión de dinero electrónico. También se considera titular a los menores de edad que tengan más de dieciséis años, que cuenten con autorización de su tutor o apoderado legal o que cuenten con capacidad de ejercicio.

Conforme el Reglamento de la Ley[139], las cuentas de dinero electrónico solo pueden ser abiertas por personas naturales nacionales o extranjeras. La emisión propiamente dicha de dinero electrónico, es la conversión de dinero a dinero electrónico, por el mismo valor que se recibe, a través de su almacenamiento en un soporte electrónico, siendo esta función exclusiva del emisor electrónico.

La emisión de dinero electrónico constituye un servicio financiero y la información del usuario electrónico y de las operaciones que realice están sujetas a la Ley de Protección de Datos Personales.

[138] Resolución SBS Nº 6283-2013, Reglamento de Operaciones con dinero electrónico. Lima, 18 de Octubre de 2015.
[139] Decreto Supremo Nº 090-2013-EF, Reglamento de la Ley Nº 29985, arts.2 y 5.

En el marco del proceso de implementación del Documento Nacional de Identidad Electrónico (DNIe), el Registro Nacional de Identificación y Estado Civil (RENIEC) en coordinación con los sectores pertinentes, habilita las aplicaciones correspondientes para que en dicho documento se almacene información para usos financieros, bancarios y no bancarios, con autorización del usuario.

Con esta disposición complementaria se visualiza la importancia que da el legislador a la autenticación biométrica y al uso del documento nacional de identidad electrónico para operaciones de dinero electrónico. De forma tal de que le documento credencial electrónico permita dentro del contexto de la inclusión digital, la inclusión financiera.

2.3.5. La identificación mediante el uso de clave y contraseña

Las claves de acceso, códigos secretos o password son el sistema de identificación más popular en el mundo computacional. Hay que tener en cuenta que la computadora debe tener la clave de acceso archivada antes de intentar comprobar la identidad del usuario; que la clave de acceso puede ser interceptada al enviarse a la computadora, por lo que requieren medidas de seguridad; las personas pueden olvidar las claves de acceso; las personas eligen claves predecibles con facilidad; las personas pueden confiar sus claves a otra personas. Por tanto, es necesario el uso responsable de las claves y contaseñas, de forma tal que el ciudadano tome conciencia sobre la necesidad de su uso responsable.

Al respecto, cabe señalar que en materia tributaria, la Superintendencia Nacional de Administración Tributaria (SUNAT), para efecto de las actuaciones o procedimientos tributarios que se realicen a través de medios electrónicos, telemáticos e informáticos, la SUNAT deberá asignar la Clave SOL[140] que permita acceder al buzón electrónico a todos los sujetos que deban inscribirse en sus registros, que le permita realizar las notificación electrónica.

[140] Conforme el articulo 86º A del Código Tributario, modificado por Ley Nº 30296, Ley que promueve la Reactivación de la Economía del 31 de Diciembre del 2014.

Asimismo, se establece que los administrados están obligados[141] a facilitar las labores de fiscalización y determinación que realice la Administración Tributaria y en especial deberán inscribirse en los registros de la Administración Tributaria así como obtener con ocasión de dicha inscripción la clave SOL que permita el acceso la buzón electrónico y a consultar periódicamente el mismo.

El administrado debe aportar todos los datos personales necesarios para la inscripción en los registros de la Administración Tributaria, así como actualizar los mismos en la forma y dentro de los plazos establecidos por las normas pertinentes. También, deberán cambiar el domicilio fiscal, de ser necesario.

En general, el código secreto o "password" es una forma de autenticación de la identidad utilizado en gran número de sistemas de información. Puede complementarse para mayor seguridad, con el uso de la biometría y la firma digital. La regulación y protección del derecho a la identidad en Internet debe contemplar el uso adecuado de estas formas de autenticación e identificación en un canal seguro de comunicación.

2.3.6. La Contratación Electrónica, legislación e Identidad Digital

"Es necesario prever que las partes estén correctamente identificadas en la celebración del contrato; pero a su vez que sea posible reconocer una serie de datos e informaciones relativos al contrato mismo o a los documentos administrativos de las partes. En cuanto a la identificación de las partes es necesario establecer la identidad del tipo de la persona física o jurídica, individual o plural, o de los representantes que actúan por ellas y el poder respectivo, a fin de determinar la responsabilidad de cada una de ellas"[142].

[141] Conforme el artículo 87º del Código Tributario, modificado por Ley Nº 30296, Ley que promueve la Reactivación de la Economía del 31 de Diciembre del 2014.

[142] FERREYROS SOTO, Carlos; GONZALES AGUILAR, Audilio; CARRASCOSA LOPEZ, Valentín: "Los Contratos en la Sociedad de la Información". Ed. Fondo Editorial del Pedagógico de San Marcos. Primera Edicion en el Peru. Lima, Perú. Octubre del 2004. Página 97.

En un entorno electrónico los contratos se celebran verificando la identidad digital de las partes. Sea que se trate de personas naturales o jurídicas la identificación de las partes es fundamental. Ya sea que se traten de contratación electrónica, contratos informáticos o los "smart contract" también llamados contratos inteligentes, la identificación segura en un entorno digital va a permitir que las obligaciones de las partes sean asumidas por las partes contractuales, disminuyendo el riesgo de la suplantación de identidad y del uso indebido de las múltiples identidades.

En el contexto de la contratación electrónica hay que tener en cuenta el artículo 1374 del Código Civil Peruano el cual establece que: "la oferta, su revocación y cualquier otra declaración contractual dirigida a determinada persona se consideran conocidas en el momento que llegan a la dirección del destinatario, a no ser que este pruebe haberse encontrado sin culpa, en la imposibilidad de conocerla. Si se realiza a través de medios electrónicos, ópticos u otro análogo, se presumirá la recepción de la declaración contractual, cuando el remitente reciba el acuse de recibo". El acuse de recibo puede ser automático a través del sistema o software que facilita la comunicación electrónica de las partes en una relación contractual o puede ser manifestado expresamente por las partes en la relación contractual, para la identificación digital tiene un papel preponderante.

"La contratación electrónica o telemática determina el nacimiento de derechos y obligaciones tanto personales como patrimoniales en línea, tanto en internet como en intranet, requiriéndose la adecuada atención del jurista en orden a su regulación, control y previsión de las consecuencias. La propia naturaleza digital de los contratos celebrados plantean nuevos problemas y características, tanto en el ámbito de los contratos privados, como en la contratación con el Estado y la contratación pública en general"[143].

[143] NUÑEZ PONCE, Julio: "La Contratación Electrónica" . En Tratado de Derecho Mercantil. Tomo III. Contratos Mercantiles y Bancarios. Ed. Gaceta Juridica S.A. Lima, Perù. Abril, 2008. Página 35.

Por la contratación electrónica entendemos a los contratos que en su formación y/o ejecución utilizan medios electrónicos. Los contratos informáticos son aquellos que tienen por objeto bienes o servicios informáticos. Los "smart contract" o contratos inteligentes son protocolos informáticos que facilitan, verifican y hacen cumplir el objeto de un contrato. "Los contratos inteligentes están escritos en código de programación, es decir son programas informáticos que ejecutan autónoma y automáticamente los términos de un contrato. El programa puede definir las reglas y las consecuencias estrictas del mismo, de la misma manera que lo haría un contrato tradicional, pero a diferencia…también puede obtener información como input y procesarla según las reglas establecidas en el contrato, para, a continuación, adoptar las medidas que se requieran como consecuencia de ello"[144].

Ya sea que se trate de contratación electrónica, de contratos informáticos o de contratos inteligentes consideramos que la identidad digital de las partes tiene gran importancia para la formación y ejecución del contrato. La forma de ejercer el derecho de identidad digital en internet en materia contractual está directamente relacionada a que esta identidad sea segura y se minimice técnica y legalmente la suplantación o el uso indebido de esta identidad.

La práctica y utilización a través de internet de la contratación electrónica a nivel global, ha llevado que la Comisión de Naciones Unidas para el Derecho Mercantil Internacional (UNICITRAL) promueva y desarrolle la Convención de Naciones Unidas *sobre la utilización de las comunicaciones electrónicas en los contratos internacionales*[145]*. En el Preambulo de esta Convencion se afirma:*

[144] ¿Qué son los contratos inteligentes o smart contract? En: https://www.oroyfinanzas.com/2015/11/que-son-contratos-inteligentes-smart-contracts/ 17 de Noviembre de 2015.

[145] Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales (Nueva York, 2005). En http://www.uncitral.org/uncitral/es/uncitral_texts/electronic_commerce/2005Convention.html

a) *"Convencidos* de que si se adoptaran normas uniformes para eliminar los obstáculos que se oponen al uso de las comunicaciones electrónicas en los contratos internacionales, incluidos los que se deriven de la aplicación de los instrumentos internacionales vigentes de derecho mercantil, aumentaría la certidumbre jurídica y la previsibilidad comercial de los contratos internacionales y se ayudaría a los Estados a obtener acceso a las rutas comerciales modernas"

b) "*Estimando* que las normas uniformes deben respetar el derecho de las partes de escoger medios y tecnologías apropiados, teniendo en cuenta los principios de neutralidad tecnológica y equivalencia funcional, siempre y cuando los métodos escogidos por las partes cumplan el propósito de las normas jurídicas pertinentes".

Por otra parte, en el artículo 1º de esta Convención se establece que: "La presente Convención será aplicable al empleo de las comunicaciones electrónicas en relación con la formación o el cumplimiento de un contrato entre partes cuyos establecimientos estén en distintos Estados".
Con el desarrollo de internet y su uso global, las comunicaciones electrónicas en materia contractual son frecuentes y aceptadas en forma general tanto con respecto a la contratación electrónica, los contratos informáticos, como con los contratos inteligentes.

En este orden de ideas, es importante analizar las disposiciones contenidas en el Articulo 3º de la Convención, que establece que: "Cuando la ley requiera que una comunicación o un contrato sea firmado por una parte, o prevea consecuencias en el caso de que no se firme, ese requisito se dará por cumplido respecto de una comunicación electrónica:
a) Si se utiliza un método para determinar la identidad de esa parte y para indicar la voluntad que tiene tal parte respecto de la información consignada en la comunicación electrónica; y
b) Si el método empleado) O bien es tan fiable como sea apropiado para los fines para los que se generó o transmitió la comunicación electrónica, atendidas todas las circunstancias del caso, inclusive todo

Acuerdo aplicable; o ii) Se ha demostrado en la práctica que, por sí solo o con el respaldo de otras pruebas, dicho método ha cumplido las funciones enunciadas en el apartado *a) supra".*

Con esta disposición la Convención da un papel fundamental a la determinación de la identidad digital con respecto a la información consignada en internet. Resalta la fiabilidad y seguridad de la identidad digital para que una persona sea parte del contrato, pudiendo acreditarse esta identidad con firma digital o con otro mecanismo que de certeza de la identidad como prodrian ser los certificados digitales de autenticación que dan seguridad que la persona es la que dice ser con la verificación de sus datos biométricos que confirman su identidad en forma fehaciente.

Por otra parte, el Articulo 12, sobre *empleo de sistemas automatizados de mensajes para la formación de un contrato, de la Convención de Naciones Unidas sobre la utilización de las comunicaciones electrónicas en los contratos internacionales*[146]*, establece: "*No se negará validez ni fuerza ejecutoria a un contrato que se haya formado por la interacción entre un sistema automatizado de mensajes y una persona física, o por la interacción entre sistemas automatizados de mensajes, por la simple razón de que ninguna persona física haya revisado cada uno de los distintos actos realizados a través de los sistemas o el contrato resultante de tales actos ni haya intervenido en ellos". En este contexto, permite la utilización de certificados digitales de agente automatizado, asi como de programas informáticos que en los contratos inteligentes ejecuten un contrato. Consideramos que en los casos de contratación electrónica, contratos informáticos y contratos inteligentes la identidad digital formal garantizada por el

[146] La Convención tiene como fecha de adopción: 23 de noviembre de 2005. Fecha de entrada en vigor: 01 de Marzo de 2013. "La aplicabilidad de la Convención a una determinada operación comercial internacional se determinará en función de las reglas jurídicas del Estado del foro (*lex fori*) que aplique el tribunal de ese Estado que esté llamado a dirimir la controversia. Así pues, si las reglas de derecho internacional privado de ese Estado requieren la aplicación del derecho sustantivo de un Estado Contratante para resolver la controversia, la Convención será aplicable como derecho de ese Estado Contratante, independientemente del lugar en que se encuentre el tribunal. La Convención también será aplicable cuando las partes en un contrato hayan convenido válidamente en que las disposiciones de la Convención constituirán el derecho aplicable al contrato. Además, los Estados podrán también plantearse adoptar las disposiciones de la Convención a nivel interno. Esa decisión promovería la uniformidad, al ahorrar recursos judiciales y legislativos, e incrementaría la seguridad jurídica respecto de las operaciones comerciales, especialmente habida cuenta del auge de la utilización de aparatos móviles para realizar operaciones electrónicas. La adopción de la Convención se recomienda especialmente a los Estados que aún no hayan promulgado legislación en materia de comercio electrónico. Por lo demás, las comunicaciones puramente nacionales no se verán afectadas por la Convención y seguirán rigiéndose por el derecho interno" .En: http://www.uncitral.org/uncitral/es/uncitral_texts/electronic_commerce/2005Convention.html

Estado a través de un sistema jurídico coherente con la el uso adecuado de la plataforma tecnológica, va a ser necesario y fundamental para garantizar seguridad jurídica y técnica en este tipo de contratos.

La validez y fuerza de los contratos en internet esta directamente relacionados a la robustez de los mecanismos seguros que garanticen la identidad digital de las personas que son parte de un contrato. La interacción del sistema automatizado con otras personas u otros sistemas debe garantizar la identidad de las partes en cada una de las declaraciones contractuales en internet. Los datos de las personas, los certificados digitales y otras instituciones jurídicas propias del derecho informático deben ser tratadas y reguladas en forma coherente teniendo como elemento esencial de cohesión la identidad digital formal segura.

Capítulo 3.

Necesidad de un Sistema Funcional de Identidad Digital que garantice la seguridad y confianza en los procesos electrónicos.

3.1. Necesidad de un Sistema Funcional de Identidad Digital

Los sistemas como: "los conjuntos de principios, normas, procedimientos, técnicas e instrumentos mediante los cuales se organizan las actividades de la Administración Pública que requieren ser realizadas por todas o varias entidades de los Poderes del Estado, los Organismos Constitucionales y los niveles de Gobierno" [147]. .

Son de dos tipos: Sistemas Funcionales. Sistemas Administrativos. Los Sistemas Funcionales tiene por finalidad asegurar el cumplimiento de políticas públicas que requieren la participación de todas o varias entidades del Estado… Las normas del Sistema establecen las atribuciones del Ente Rector del Sistema"[148]. En cambio, "los sistemas administrativos tienen por finalidad regular la utilización de los recursos en las

[147] Ley Nº 29158, Ley Organica del Poder Ejecutivo. Articulo 43º
[148] Ley Nº 29158, Ley Organica del Poder Ejecutivo. Articulo 45º

entidades de la administración pública, promoviendo la eficacia y eficiencia en su uso"[149]

Los sistemas funcionales tienen por finalidad asegurar el cumplimiento de políticas públicas. Las Políticas de Estado en el Perú son definidas por el Acuerdo Nacional[150], que ha establecido cuatro grandes objetivos: I. Democracia y Estado de Derecho (9 políticas de Estado). II. Equidad y Justicia Social (7 políticas de Estado). III. Competitividad del País (7 políticas de Estado). IV. Estado Eficiente, Transparente y Descentralizado (8 Políticas de Estado). Son treintaicinco las políticas públicas aprobadas en la actualidad[151].
Los sistemas funcionales requieren la participación de todas o varias entidades del Estado que permitan que la política pública se cumpla y se aplique en la realidad.

Solo por ley se crea un sistema. Para su creación se debe contar con la opinión favorable de la Presidencia del Consejo de Ministros. "Los Sistemas están a cargo de un Entre Rector que se constituye en su autoridad técnico-normativa a nivel nacional; dicta normas y establece los procedimientos relacionados con su ámbito; coordina su operación técnica y es responsable de su correcto funcionamiento en el marco de la presente Ley, sus leyes especiales y disposiciones complementarias"[152].

Para crear el sistema funcional de identidad digital, protección de datos personales, certificación y registro digital, se necesita que

[149] Ley Nº 29158, Ley Organica del Poder Ejecutivo. Articulo 46. Los Sistemas administrativos de aplicación nacional están referidos a gestión de recursos humanos; abastecimiento; presupuesto publico; tesorería; endeudadmiento publico; contabilidad; inversión publica; planeamiento estratégica; Defensa Judicial del Estado; Control; Modernizacion de la Gestion Publica.
[150] http://acuerdonacional.pe/politicas-de-estado-del-acuerdo-nacional/politicas-de-estado%e2%80%8b

[151] Entre estas políticas publicas tenemos: 3. Afirmación de la identidad nacional. 20. Desarrrollo de la Ciencia y la tecnología. 22. Politica de comercio exterior para la ampliación de mercados con reciprocidad. 28. Plena vigencia de la constitución y de los derechos humanos y acceso a la justicia e independencia judicial. 29. Acceso de la información, libertad de expresión y libertad de prensa.
[152] Ley Nº 29158, Ley Organica del Poder Ejecutivo. Articulo 44º

se incluya como política pública numero 35. Esta Política Pública proponemos se incluya dentro del objetivo IV Estado eficiente, Transparente y Descentralizado, donde se ubica la política publica 28. Plena vigencia de la Constitución y de los derechos humanos y acceso a la justicia e independencia judicial. 29. Acceso a la información, libertad de expresión y libertad de prensa. El establecimiento de la Política Publica 35 identidad digital, protección de datos personales, certificación y registro digital, lograría equilibrio en la aplicación coordinada de estas políticas en la sociedad peruana.

3.1.1. Fundamentos desde el punto de vista de la Teoría General de Sistemas.

"Lo que distingue a los sistemas es que, en si, son una materia que puede hacer referencia acerca de otros temas…, es una meta-disciplina, cuya materia sustancial se puede aplicar dentro de otra disciplina… ¿Qué es un enfoque de sistemas?...es un enfoque a un problema que toma una amplia visión, que trata de tomar en cuenta todos los aspectos, que se concentra en interacciones entre las diferentes partes del problema…"[153].

La Identidad Digital tiene incidencia en todas las actividades del ser humano. Un sistema que garantice el derecho a la identidad digital del ciudadano resguardando sus derechos fundamentales como el nombre, el honor, la reputación, la intimidad, entre otros, permitirá un tratamiento coherente de los derechos del ser humano en un entorno digital, tomando en cuenta todos los aspectos que interactúan entre sí, buscando solucionar el problema de uso indebido de las múltiples identidades y la suplantación de identidad.

La protección de datos, la certificación y registro digital están interrelacionadas para asegurar el ejercicio del derecho a la

[153] CHECKLAND, Peter: "Pensamiento de sistemas, practica de sistemas". México DF. Grupo Noriega Editores, 1993, pagina 19.

identidad digital en internet, por tanto un sistema funcional debe incluir estos conceptos.

"…se puede describir una sociedad como funcionalmente diferenciada a partir del momento en el cual forma sus principales subsistemas en la perspectiva de problemas específicos que deberán ser resueltos en el marco de cada sistema funcional"[154].

El enfoque de sistemas permite tratar la identidad digital en una forma funcional teniendo en cuenta los problemas específicos que origina el uso inseguro de las múltiples identidades y los riesgos de ser pasibles de suplantación de identidad y otros cibercrimenes, asi como su utilización en el teletrabajo en el ámbito público y privado.

"Consecuencia de la existencia de propiedades generales de sistemas es la aparición de estructuras similares… en diferentes campos…La teoría general de sistemas es capaz en principio de dar definiciones exactas de conceptos semejantes…"[155]. Por tanto, la identidad digital constituye un concepto unificador y base del sistema funcional que proteja y garantice los derechos fundamentales de una persona en un entorno digital, permite utilizar las estructuras similares de la protección de datos personales y de la certificación digital.

"La diferenciación en sistemas funcionales se comprende a través del modelo de la producción por el sistema de lo que lo constituye y de lo que lo limita…cada sistema observa la

[154] URTEAGA, Eguski: "La Teoria de Sistemas de Niklas Luhman".En Contrastes. Revista Internacional de Filosofia. Vol XV (2010).(Pags.301 a 317) Recibido 26-11-2008. Aprobado 22-01-2009. Niklas Luhman es in sociólogo alemán (1927-1998) ha elaborado una teoría ambiciosa y coherente en la que describe la sociedad moderna como un sistema. Se divide en sistemas funcionales cerrados a través de códigos especializados. Página 307. En http://www.uma.es/contrastes/pdfs/015/ContrastesXV-16.pdf

[155] VON BERTALANFFY, Ludwig: "Teoria General de Sistemas: Fundamentos, desarrollo, aplicaciones". Ed. Fondo de Cultura Económica". México D.F. Primera Edicion en español, Séptima Reimpresión, 1989. Páginas 33 y 34.

sociedad a partir de su propia función"[156]. La identidad digital, permite ejercer los derechos de la persona en un entorno digital, permitiendo crear las condiciones tanto a nivela nacional como a nivel global de la "conectividad de persona a persona, donde hay que hacer el esfuerzo necesario para reducir las barreras existentes a la interacción y la movilidad y desarrollar actividades..que apoyen el flujo de personas"[157].

En el contexto global "…la comprensión científica de las sociedad humana y sus leyes…no solo nos enseñara lo que tienen en común con otras organizaciones el comportamiento y la sociedad humanos, sino también cual es su unicidad…Los valores reales de la humanidad…son los que proceden de la mente individual…[158]"

La unicidad del yo, base la construcción de la identidad moderna, reúne y consolida los valores inherentes de las persona humana en un entorno digital. Específicamente la información fehaciente y fiable de la persona que garantice su identidad digital permitirá una movilidad turística, laboral y social de las personas en los distintos países del mundo.

3.1.2. Fundamentos desde el punto de vista de la protección de datos personales.

Conforme se afirma en el Informe del Comité Jurídica Interamericano sobre Privacidad y Protección de Datos Personales[159], los principios de la Organización de Estados Americanos (OEA) reflejan los conceptos de autodeterminación en lo que respecta a la información, la ausencia de restricciones arbitrarias del acceso a los datos, y la protección a la privacidad,

[156] URTEAGA, Eguski: ob.cit. Pagina 308.
[157] 22ª Declaracion de los Lideres dAPEC. Beijing, China. 11 de Noviembre de 2014. Anexo D. Plan de Conectividad APEC para 2015-2025, numeral 7. En http://www.acuerdoscomerciales.gob.pe
[158] VON BERTALANFFY, Ludwig: ob.cit. Pagina 53.
[159] Principios de la OEA sobre la Privacidad y la Proteccion de Datos Personales con anotaciones. OEA/CJIdoc.474 rev 2. 26 de Marrzo de 2015. 86º Periodo Ordinario de Sesiones. Rio de Janeiro, Brasil. En http://www.oas.org/es/sla/ddi/docs/CJI-doc_474-15_rev.pdf

la identidad, la dignidad y la reputación. El derecho a la privacidad no es absoluto y puede tener limitaciones razonables relacionadas de manera racional con metas apropiadas.
"Tal como se usa en estos principios, la frase "datos personales" abarca la información que identifica o puede usarse de manera razonable para identificar a una persona de forma directa o indirecta, especialmente por referencia a un número de identificación o a uno o más factores referidos específicamente a su identidad física, fisiológica, mental, económica, cultural o social"[160].
Por tanto, incluir como Política de Estado la identidad digital, la protección de datos personales, la certificación y registro digital está acorde con los principios de la OEA. Asimismo, el sistema funcional[161] estaría en concordancia con estos principios.

Los principios de la OEA sobre Privacidad y los Datos Personales con anotaciones[162], que pueden incluirse como principios del sistema funcional propuesto de identidad digital, protección de datos personales, certificación y registro digital, son los siguientes:

Principio Uno: Propósitos Legítimos y Justos.- Este principio abarca dos elementos: i) Los fines legítimos para los cuales inicialmente se recopilan los datos personales y ii) los medios justos y legales con los cuales se efectúa la recopilación inicial.
La premisa es que muchas o incluso la mayoría de las intrusiones en los derechos de las personas pueden evitarse si se respetan los conceptos conexos de legalidad y justicia desde el comienzo, cuando se recopilan inicialmente los datos. Desde luego, estos principios se aplican y deben respetarse en todo el proceso de recopilación, compilación, almacenamiento, utilización, divulgación y eliminación de datos personales, no solo en el momento de su recopilación.

[160] Principios de la OEA sobre la Privacidad y la Proteccion de Datos Personales con anotaciones. OEA/CJIdoc.474 rev 2. 26 de Marrzo de 2015. 86º Periodo Ordinario de Sesiones. Rio de Janeiro, Brasil. En http://www.oas.org/es/sla/ddi/docs/CJI-doc_474-15_rev.pdf
[161] El sistema funcional de identidad digital, protección de datos personales, certificación y registro digital, que se basaría en la política 35 propuesta para incluirse en el Acuerdo Nacional.
[162] Principios de la OEA sobre la Privacidad y la Proteccion de Datos Personales con anotaciones. OEA/CJIdoc.474 rev 2. 26 de Marrzo de 2015. 86º Periodo Ordinario de Sesiones. Rio de Janeiro, Brasil. En http://www.oas.org/es/sla/ddi/docs/CJI-doc_474-15_rev.pdf

El requisito de legalidad del fin para el cual se recopilan, retienen y procesan datos es una norma fundamental y directamente relacionada con la protección de derecho a la identidad digital en internet. Por otra, parte los datos personas, incluidos los que permiten verificar la identidad digital de una persona en internet se recopilan por medios justos y legales cuando la recopilación es compatible tanto con los requisitos jurídicos pertinentes como con las expectativas razonables de las personas basadas en su relación con el controlador de datos[163] o con otra entidad que recopile los datos y en el aviso o los avisos dados a las personas en el momento que se recopilen sus datos.

Principio Dos: Claridad y Consentimiento. Se deben especificar los fines para los cuales se recopilan los datos personales en el momento que se recopilen. Como regla general, los datos personales solamente deben ser recopilados con el consentimiento a la persona que se refieran. Se basan en el principio de transparencia sobre los fines para los cuales se recopilan los datos y el de consentimiento por el cual la persona debe ser capaz de dar su consentimiento libremente respecto de la recopilación de los datos personales, de la forma y con los fines previstos.

Principio Tres. Pertinencia y necesidad. Los datos deben ser verídicos, pertinentes y necesarios para los fines expresos de su recopilación. Los datos personales y especialmente los referidos al derecho de identidad digital en internet deben ser correctos, exactos y completos y estar actualizados según sea necesario con respecto a los fines para los cuales se haya recopilado.

Principio Cuatro. Uso Limitado y Retención. Los datos personales deben ser mantenidos y utilizados solamente de manera legítima con incompatible con el fin o fines para los cuales se recopilaron, No deberán mantenerse mas del tiempo necesario para su propósito y de conformidad con la legislación nacional correspondiente.
Principio Cinco: Deber de confidencialidad. Los datos personales no deben divulgarse, ponerse a disposición de terceros ni

[163] Controlador de datos significa la persona física o jurídica, entidad privada, autoridad pública u otro organismo u organización (solo o junto con otros) procesa los datos en cuestión.

emplearse para otros propósitos que no sean aquellos para los cuales se obtuvieron, excepto con el consentimiento de la persona en cuestiono bajo la autoridad de la ley.

Principio Seis: Protección y Seguridad. Los datos personales, incluido los concernientes al derecho de identidad digital en internet, deben ser protegidos mediante salvaguardas razonables y adecuadas contra accesos no autorizados, perdida, destrucción, uso, modificación o divulgación.

La protección de la privacidad de las personas implica mantener la seguridad de sus datos personales y permitir que las personas controlen su experiencia “en línea”. Además de tomar medidas de seguridad eficaces, los controladores de datos deberían tener flexibilidad para proporcionar a sus usuarios medios efectivos para controlar el intercambio de datos personales como parte de las medidas generales de protección de la privacidad.

Principio Siete: Fidelidad de los datos. Los datos personales deben mantenerse fieles y actualizados hasta donde sea necesario para los propósitos de su uso.

Cuando se recopilan datos personales y se los retiene para seguir usándolos, el controlador de datos tiene la obligación de tomar medidas para que los datos se mantengan actualizados y sean exactos en la medida de lo necesario para los fines para los cuales se hayan recopilado y se usen.

Principio Ocho: Acceso y Corrección. Se debe disponer de métodos razonables para permitir que aquellas personas cuyos datos personales hayan sido recopilados puedan solicitar el acceso a dichos datos y puedan solicitar al controlador de datos que los modifique, corrija o elimine. En caso de que fuera necesario restringir dicho acceso o corrección, deberían especificarse las razones concretas de cualquiera de estas restricciones de acuerdo con la legislación nacional.

Principio Nueve: Datos Personales Sensibles. Algunos tipos de datos personales, teniendo en cuenta su sensibilidad en contextos particulares susceptibles de causar daños

considerables a las personas si se hace mal uso de ellas. Los controladores de datos deberían adoptar medidas de privacidad y de seguridad que sean acordes con la sensibilidad de los datos y su capacidad de hacer daño a los individuos sujetos de la información.

Principio Diez: Responsabilidad. Los controladores de datos deberán e implementaran las medidas correspondientes para el cumplimiento de estos principios.

La protección efectiva se basa tanto en la conducta responsable de los controladores de datos como en las personas y en las autoridades gubernamentales del caso. Los sistemas de protección de la privacidad deben reflejar un equilibrio apropiado entre la reglamentación gubernamental y la implementación efectiva por aquellos que tienen responsabilidad directa por la recopilación, el uso, la retención y la difusión de datos personales.

Un enfoque contemporáneo eficaz consiste en requerir que los controladores de datos incorporen la privacidad en el diseño y la arquitectura de sus sistemas de tecnologías de la información. Los controladores de datos deben estar preparados para demostrar sus programas de gestión de la privacidad cuando se los solicite, en particular a petición de una autoridad competente.

Principio Once: flujo Transfronterizo de Datos y Responsabilidad. Los Estados miembros de la OEA cooperaran entre sí en la creación de mecanismos y procedimientos que aseguren que los controladores de datos que operen en más de una jurisdicción puedan ser efectivamente hechos responsables por el incumplimiento de estos principios.

Principio Doce: Publicidad de las Excepciones. Cuando las autoridades nacionales establezcan excepciones a estos principios por motivos relacionados con la soberanía nacional, la seguridad interna o externa, el combate de la cibercriminalidad, el cumplimiento de normativas u otras prerrogativas de orden público, deberían poner en conocimiento del publico dichas excepciones.

3.1.3 Fundamentos desde el punto de vista de la certificación y Registro Digital

Los Principios contenidos en el Proyecto de Ley 3900-2014-RENIEC de Identidad Digital, contiene los principios que desde el punto de vista de la certificación y registro digital, fundamentan que se cree un sistema funcional de identidad digital, protección de datos personales, registro y certificación digital. Entre estos principios, señalamos los siguientes:

Principio Uno: Principio de equivalencia funcional, por el cual el ejercicio de la identidad digital para el uso y prestación de servicios de gobierno y comercio electrónico seguros, confiere y reconoce a las personas las mismas garantías que otorgan los modos tradicionales de relación entre las personas o en la relación con las entidades de la Administración Pública.

. Principio Dos: Principio del deber de cuidado, por el cual las personas deben observar y tomar las medidas necesarias para la debida salvaguarda en el uso de su identidad digital.

Principio Tres: Principio de responsabilidad y calidad en la veracidad y autenticidad de la información y dentro de los servicios de gobierno electrónico seguro, ofrecidos por las entidades de la Administración Pública. En todos los casos, las entidades de la Administración Pública responden por los actos realizados por medios electrónicos seguros de la misma manera y con iguales responsabilidades que por los realizados a través de medios tradicionales.

Principio Cuatro: Principio de normalización, según el cual los estándares y patrones establecidos por el Estado, para la prestación de servicios de gobierno electrónico seguro, deberán mantener la mayor correspondencia posible con los estándares internacionales de reconocimiento mundial y regional.

Principio Cinco: Principio de uso de factores de autenticación, por el cual la identidad digital se verificará mediante un proceso de autenticación digital que utilice distintos factores de autenticación.

3.2. Ubicación de una Ley de Identidad Digital dentro del Sistema Funcional Propuesto y contenido de Proyecto de Ley.

3.2.1. Proyecto de Ley de Identidad Digital: importancia y contenido

"La identidad digital es el conjunto de rasgos propios de un individuo o un colectivo que los caracteriza frente a los demás a través de los medios digitales. La autenticación es la verificación fehaciente de la identidad de una persona a través de mecanismos tecnológicos basados en una característica del individuo. En este sentido, la autenticación vendría a ser la confirmación verificada de la identidad digital de una persona, brindando evidencias que descartan la suplantación de identidad"[164].

Una Ley de Identidad Digital, complementa y cohesiona y complementa el sistema funcional propuesto de identidad digital, protección de datos personales, certificación y registro digital. Asimismo, refuerza los fundamentos para establecer la Política de Estado 35 Identidad Digital, Protección de Datos Personales, Certificación y Registro Digital.

Un sistema funcional de identidad digital que tenga como marco jurídico una ley de identidad digital, complementada por una ley de protección de datos personales y una ley de firma y certificados digitales, promueve y facilita la implementación de servicios electrónicos seguros al ciudadano, resguardando su identidad digital en Internet. Asimismo, estas normas deben complementarse con normas concordantes y sistémicas que inciden en una utilización por el ciudadano de la identidad digital, como son la ley y reglamento sobre

[164] ESTRADA VILLEGAS, Carina: "Servicio de Consultoría para el análisis de los modelos para la identificación y autenticación digital en los servicios electrónicos". Consultoria solicitada por el Consejo Nacional de Competitividad. Lima, Perú. Mayo 2015. Página 6. En: http://www.cnc.gob.pe/

teletrabajo, la ley de delitos informáticos y las normas sobre votación electrónica.

"La implementación de servicios electrónicos permite a un país crear nuevas oportunidades comerciales y de desarrollo profesional para sus ciudadanos y empresas, superando las barreras espaciales y optimizando los procesos administrativos públicos. Asi como en el uso de servicios de solicitud presencial, los servicios electrónicos requieren de salvaguardas de seguridad que eviten la suplantación de identidad de los solicitantes, asi como medidas que permitan garantizar la protección de los datos personales de los ciudadanos. Sin embargo, la implementación de estas salvaguardas debe considerar no crear dificultades que puedan reducir el grado de aceptación de estos servicios por parte del ciudadano"[165].

En la Exposición de Motivos del Proyecto de Identidad Digital se afirma: "a la luz del estado actual de desarrollo de la sociedad, en particular de las herramientas tecnológicas, es imperativo para los Estados modernos adoptar el uso de las denominadas Tecnologías de la Información y las comunicaciones (TIC) a fin de mejorar la prestación de servicios públicos, pero también para mejorar el acceso de procedimientos administrativos y el ejercicio de acceso a la tutela jurisdiccional…todo lo cual precisa que se efectúe el reconocimiento a todas la personas en el ámbito nacional de los derechos…a la inclusión e identidad digital"[166].

CONTENIDO DEL PROYECTO DE IDENTIDAD DIGITAL[167]

El Proyecto de Ley 3900/2014 de Identidad Digital, con las modificaciones introducidas, presentado el 22 de Octubre de 2014 por RENIEC ante el Congreso de la Republica, tiene la siguiente estructura:

Exposición de motivos. Título Preliminar: DISPOSICIONES GENERALES. -Titulo Primero: INCLUSION E IDENTIDAD DIGITAL. Capítulo I. De la Inclusión Digital. Capítulo II. De la Identidad Digital.

[165] ESTRADA VILLEGAS, Carina: ob.cit. Página 4.
[166] Exposicion de Motivos del Proyecto de Ley Nº 3900-2014-RENIEC, presentado al Congreso de la Republica del Peru, en Octubre de 2014. En http://www.congreso.gob.pe
[167] El texto completo esta contenido como anexo de la presente tesis.

Capítulo III: Documento Nacional de Identidad Electrónico (DNIe) Capítulo IV: Derechos y Deberes de la Persona.

Titulo Segundo: DEL RÉGIMEN JURÍDICO DEL GOBIERNO ELECTRÓNICO. Capítulo I: Obligaciones y Garantías de las Entidades de la Administración Pública y Ámbito Jurisdiccional.. Capítulo III Del Valor Probatorio de los Documentos Electrónicos y del Archivo Electrónico.

Título Tercero: DE LA INTEROPERABILIDAD, REUTILIZACIÓN DE APLICACIONES INFORMÁTICAS Y TRANSFERENCIA DE TECNOLOGÍAS ENTRE ENTIDADES DE LA ADMINISTRACIÓN PÚBLICA. Capítulo I: De la interoperabilidad.. CAPÍTULO II. De La Reutilización de Aplicaciones Informáticas y Transferencia de Tecnologías. TÍTULO CUARTO DEL INCUMPLIMIENTO DE LAS DISPOSICIONES DE LA LEY. CAPÍTULO ÚNICO**.** DISPOSICIONES COMPLEMENTARIAS FINALES. PRIMERA

El Proyecto de Identidad Digital busca impulsar el desarrollo de los servicios electrónicos, la interoperabilidad, la inclusión digital. Busca dar cohesión a las normas dispersas y en base al ejercicio de la identidad digital dar seguridad jurídica.

3.2.2. Objeto, Alcance, fines, principios rectores del Proyecto de Ley de Identidad Digital

El Titulo Preliminar Disposiciones Generales, comprende los artículos 1º al 6º. El articulo 1º del Objeto establece: “La presente Ley tiene por objeto reconocer el derecho de todas las personas a la inclusión digital y regular el derecho a la identidad digital para el uso de los servicios

de gobierno electrónico seguro, prestados por las entidades de la Administración Publica..". La inclusión digital se define como "el derecho de todas las personas al establecimiento e implementación de las condiciones mínimas necesarias provistas por el Estado para hacer uso de servicios de gobierno electrónico seguros; empleando para tales efectos, su identidad digital en el marco de las disposiciones previstas en la presente ley"[168].

Por identidad digital se define a "aquella basada en un documento credencial electrónico, emitido en el marco de la Infraestructura Oficial de Firma Electrónica (IOFE), y conforme las disposiciones legales vigentes. La identidad digital permite la identificación y autenticación de modo fehaciente en medios electrónicos, para el uso de los servicios de gobierno y comercio electrónico seguros, prestados dentro de la Infraestructura Oficial de Firma Electrónica (IOFE)"[169].

El segundo párrafo del artículo 1º establece: "… Para efectos de esta Ley entiéndase por personas, a las personas naturales y jurídicas, quienes asimismo podrán usar su identidad digital para el uso de los servicios de comercio electrónico, en la medida que estos se implementen observando los establecido en la presente Ley". En los alcances de la Ley, precisados en el artículo 2º del Proyecto de Ley se señala que: "la presente Ley comprende el uso de gobierno y comercio electrónico seguros", consideramos que en los alcances debiera

[168] Art. 7ª del Proyecto de Ley 3900/2014-RENIEC presentado al Congreso de la Republica del Perú el 22 de Octubre de 2014.
[169] Art. 9º del Proyecto de Ley 3900/2014-RENIEC presentado al Congreso de la Republica del Perú el 22 de Octubre de 2014.

también incluirse los procesos de negocios electrónicos y de aprendizaje electrónico.

El artículo 3º del Proyecto, sobre ámbito de aplicación de la ley señala que la presente Ley será de aplicación a todas las entidades de la Administración Publica referidas en el Articulo I del Título Preliminar de la Ley Nº 27444, Ley del Procedimiento Administrativo General, tanto a las relaciones entre las distintas entidades de la Administración Publica y a las relaciones entre personas naturales y/o personas jurídicas y de estas con las entidades de la Administración Publica. Consideramos que será necesario concordarla con las políticas públicas y con el conjunto de normas que regulan el Poder Ejecutivo, el Poder Legislativo, el Poder Judicial, los Gobiernos Regionales y Locales.

El articulo 5º sobre finalidades, precisa, entre otras las siguientes: a) Instituir la inclusión digital como un derecho de todas las personas impulsando la puesta en disposición y el aprovechamiento de los servicios de gobierno electrónico seguro. b) Establecer la identidad digital como un derecho de las personas y un deber del Estado para garantizar el ejercicio de la misma en los servicios de gobierno electrónico seguro. c) Establecer las condiciones idóneas para la prestación de servicios de gobierno electrónico seguro. d) Promover la masificación de los servicios y procedimientos administrativos por medios electrónicos seguros mediante el uso de la identidad digital. e) Favorecer el ejercicio del acceso a la tutela jurisdiccional a través del uso de medios electrónicos seguros, contribuyendo al fortalecimiento de los órganos jurisdiccionales.

En el artículo 6º se establecen los principios rectores, entre los que tenemos: i) Principio de equivalencia funcional. ii) Principio de no discriminación iii) Principio de protección de datos personales. iv) Principio de seguridad de la información. v) Principio de deber de cuidado, por el cual las personas deben observar y tomar las medidas necesarias para la debida salvaguardia en el uso de su identidad digital. vi) Principio de enfoque por procesos. vii) Principio de usabilidad.

3.2.3. La Identidad Digital Nacional, el Documento Nacional de Identidad Electrónico (DNIe) y otros Proyectos relacionados.

Una de las precisiones importantes que realiza el Proyecto de Ley es el de la Identidad Digital Nacional, definiéndola como: "aquella identidad digital que es reconocida a las personas naturales nacionales y contenida en su Documento Nacional de Identidad electrónico (DNIe), emitido por el Registro Nacional de Identificación y Estado Civil (RENIEC)".

Debe tenerse en cuenta que: " La Identidad digital conlleva una serie de cambios y adaptaciones técnicas y jurídicas...se emparenta a varias nociones jurídicas conocidas de la persona pero en el ámbito digital, una parte de éste se refiere a las redes sociales…se requiere, que "alguien", una entidad pública oficialice o no la identidad digital nacional, expida los certificados en los cuales se porta ésta…"[170]. La identidad digital nacional es reconocida a las personas naturales nacionales por una Entidad Pùblica que es RENIEC y esta contenida en el DNIe, convirtiéndose en una identidad digital oficial que garantiza los derechos de la persona en un entorno electrónico.

[170] FERREYROS SOTO, Carlos: "Ejecuttivos, Redes Sociales e Identidad Digital". Blog Derecho y Nuevas Tecnologias, Sabado, 29 de Diciembre del 2012. En http://derecho-ntic.blogspot.pe/search?updated-min=2012-01-01T00:00:00-08:00&updated-max=2013-01-01T00:00:00-08:00&max-results=19

Asimismo, el Proyecto define la identificación digital como "el proceso a través del cual una persona ejerce su identidad digital en medios electrónicos seguros" y define la "autenticación digital" como "el proceso por el cual se confirma la identidad digital de una persona, permitiéndosele el uso de servicios de gobierno y comercio electrónico seguros"[171].

La identificación es la acción o efecto de identificar o identificarse. La identificación permite verificar la identidad y ejercer el derecho de la identidad en la sociedad digital actual. La identificación digital permite autenticar, registrar y validar la identidad digital de una persona en internet en forma oficial, lográndose que los datos personales contenidos en su documento nacional de identidad electrónica acrediten en forma indubitable y segura su identidad en internet.

El Documento Nacional de Identidad electrónico (DNIe), es el Documento Nacional de Identidad emitido por el Registro Nacional de Identificación y Estado Civil (RENIEC), que acredita presencial y no presencialmente la identidad de su titular, permitiendo en este último caso reconocer a las personas naturales nacionales su identidad digital nacional.

El Documento Nacional de Identidad electrónico (DNIe), almacena dos (2) certificados digitales: el de autenticación y el de firma digital emitidos por el Registro Nacional de Identificación y Estado Civil (RENIEC), lo cual permite a su titular autenticar su identidad digital nacional en un medio electrónico y firmar digitalmente documentos electrónicos o mensajes de datos.

El Documento Nacional de Identidad Electrónico (DNIe) es de policarbonato, un material rígido durable con resistencia al calor, al doblado y a los rayos ultravioleta. Contiene un chip criptográfico con

[171] Vid. Arts. 10, 11, 12 y 13 del Proyecto de Ley 3900/2014-RENIEC presentado al Congreso de la Republica del Perú el 22 de Octubre de 2014.

certificación y sistema operativo[172]. "Almacena en la memoria del chip las minucias (plantillas) obtenidas a partir de las imágenes de las huellas dactilares del titular de la inscripción. Adicionalmente contiene la aplicación MOC (Match-On-Card) que ejecuta la comparación, dentro del propio chip, de las minucias almacenadas con respecto a las que se obtengan del ciudadano, respondiendo con resultado positivo o negativo acerca de dicha comparación"[173].

Asimismo, el Documento Nacional de Identidad electrónico (DNIe), permite a su titular el uso de servicios de gobierno y comercio electrónico seguro y el ejercicio del derecho al voto electrónico presencial y no presencial en los procesos electorales de conformidad con las disposiciones vigentes sobre la materia.

El Documento Nacional de Identidad electrónico (DNIe) es reconocido como documento de viaje dentro del territorio nacional, así como en aquellos países con los cuales el Perú cuente o suscriba acuerdos o convenios para dicho fin.

El Documento Nacional de Identidad electrónico (DNIe), a solicitud expresa del usuario podrá almacenar información para usos financieros, bancarios y no bancarios.

El Dictamen Proyecto de Ley 3591/2013-CR[174], propone lo siguiente: "Declárese de interés nacional el uso del Documento Nacional de Identidad Electrónico (DNIe) en todas las actividades servicios u otros aspectos relacionados con el gobierno electrónico. Para tal efecto, facúltese al RENIEC a entregar conjuntamente con el DNIe, los

[172] La Resolucion Jefatural Nº 212-2013/JNAC/RENIEC del 02 de Julio de 2013, establece las especificaciones técnicas del Documento Nacional de Identidad Electronico (DNIe), entre ellas tenemos: certificación Common Criteria EAL5 y Sistema Operativo que implementa las especificaciones JavaCard 2.2. y Global Plataform 2.1.1.

[173] La Resolución Jefatural Nº 212-2013-JNAC/RENIEC del 02 de Julio de 2013. También precisa como utilizando la información dentro del chip contenido en el DNI Electrónico se realiza la verificación biométrica dactilar.

[174] Dictamen del Proyecto de Ley 3591/2013-CR que propone la Ley que dispone que las entidades publicas envíen a tarves de medios electrónicos o aplicativos informáticos la información o documentación que por mandato legal presentan a la Comisión de Presupuesto y Cuenta General del Congreso de la Republica. Dictamen de la Comisión de Presupuesto y Cuenta General de la Republica. Periodo Anual de Sesiones 2013-2014. En http://www.congreso.gob.pe

dispositivos que permitan su uso como lectores de tarjeta inteligente, lectores de huella digital u otros , en aquellas circunscripciones, localidades o distritos en los cuales no existan proveedores locales de tales dispositivos que satisfagan la demanda”.

El empleo del Documento Nacional de Identidad electrónico (DNIe), se encuentra sujeto a lo dispuesto en Ley N° 26497, Ley Orgánica del Registro Nacional de Identificación y Estado Civil y demás normas complementarias, quedando prohibida, bajo ninguna circunstancia, que sea requisado o retenido, bajo responsabilidad.

Ley Nº 26497. Articulo 26º “El Documento Nacional de Identidad (DNI) es un documento público, personal e intransferible. Constituye la única cedula de Identidad Personal para todos los actos civiles, comerciales, administrativos, judiciales y, en general, para todos aquellos casos en que, por mandato legal, deba ser presentado. Constituye también el único título de derecho al sufragio de la persona a cuyo favor ha sido otorgado”.

El RENIEC puede determinar las características técnicas y contenido del circuito integrado o solución tecnológica del Documento Nacional de Identidad electrónico (DNIe).

El Capítulo III del Proyecto, el artículo 14º regula el Documento Nacional de Identidad Electrónico precisando que “permite a su titular autenticar su identidad digital nacional en un medio electrónico y firmar documentos electrónicos o mensajes de datos.

Al respecto, cabe señalar: “El DNI Digital es la más importante de las iniciativas para la generalización de la firma electrónica entre la ciudadanía, e incluso es una iniciativa que de implantarse seriamente será demostrativa del importante papel que puede tener un Estado cabal y responsable en la dinamización de la economía…la extensión y correspondiente “normalización” de la firma digital entre los

ciudadanos sienta las mas solidas bases tecnológicas y sociales, para el desarrollo del comercio electrónico. Y lo que es más, si los ciudadanos en principio tienen firma digital, no hay razon para que la Administración, que se la ha proporcionado, cierre sus puertas y no haga posible su utilización en absolutamente TODOS los procedimientos que se llevan a cabo en cualquiera de las Administraciones Públicas"[175].

Por tanto, regular el Documento Nacional de Identidad Electrónico (DNIe) garantizando la autenticación de su identidad digital nacional y el uso de la firma digital fortalece el marco jurídico que permite generalizar el uso de la firma digital y fortalecer la prestación de los servicios electrónicos públicos por parte del Estado que permite al ciudadano ejercer en forma segura su derecho de identidad digital en Internet.

El artículo 15º establece que: "El Código Único de Identificación (CUI) contenido en el Documento Nacional de Identidad (DNI), se efectuará utilizando el código de ocho dígitos que resulte de la conversión de la cadena genética de cada persona natural, utilizando el análisis genético de la sangre de la persona que deberá efectuarse en su nacimiento, utilizando tecnologías informáticas y genéticas seguras. Este procedimiento se hará en forma gradual y progresiva"[176].

[175] SUÑE LLINAS, Emilio: "La Ventanilla Única Electrónica". En Memorias del X Congreso Iberoamericano de Derecho e Informática. Celebrado en Santiago de Chile del 6 al 9 de Setiembre de 2004. Ed. Biblioteca del Congreso Nacional de Chile, Facultad de Derecho de la Universidad de Chile. Santiago de Chile, 2004. Chile. Página 42.

[176] En el texto sustitutorio en la Comisión de Justicia del Congreso de la Republica, de Noviembre de 2015 se varia la redacción de la siguiente forma: "El Código Único de Identificación (CUI) contenido en el DNIe, se efectúa utilizando el código que resulte de la conversión de la cadena genética de cada persona natural, utilizando el análisis genético de la persona que deberá efectuarse en su nacimiento, utilizando tecnologías

En el Capítulo IV del Proyecto se establece en el artículo 15º el derecho del reconocimiento de la Identidad Digital en medios electrónicos seguros, señalando que "las personas tienen el derecho al uso de servicios de gobierno electrónico seguro, prestado en el marco de la Infraestructura Oficial de Firma Electrónica (IOFE). Asimismo, se precisan los derechos conexos que son los relacionados al uso de los servicios de gobierno electrónico seguro, entre los cuales tenemos el de relacionarse con las Entidades de la Administración Publica para el ejercicio de sus derechos y cumplimiento de sus obligaciones, empleando su identidad digital y presentar solicitudes, escritos y/o comunicaciones a través de medios electrónicos seguros todos los días del año, las veinticuatro horas del día.

3.2.4. La Identidad Digital, la prestación de servicios de gobierno electrónico por medios seguros, Sede Electrónica y Notificación.

El Titulo Segundo del Proyecto se refiere al Régimen Jurídico del Gobierno Electrónico que incluye, entre otros, los siguientes temas: a) De las obligaciones de las entidades de la Administración Publica para la la prestación de servicios electrónicos seguros). De la garantías para la prestación de servicios de gobierno electrónico por medios electrónicos seguros.

El artículo 22º regula el uso de los documentos credenciales contenidos en el DNIe por parte de funcionarios y personal de servicio

informáticas y genéticas seguras. En el procedimiento señalado, se garantiza la identificación única de la persona natural. El reglamento de la presente ley establece las acciones y medidas necesarias para evitar duplicidad de los códigos generados con base genética y los existentes antes de su implementación"

de las entidades de la Administración Pública. Se precisa que los documentos credenciales electrónicos contenidos en el DNIe solo otorgan garantía sobre la identificación de la persona natural, mas no del cargo, rol, atribuciones o facultades que ostenta el funcionario o personal al servicio de dichas entidades. Se establece que es responsabilidad de las entidades de la Administración Pública gestionar las autorizaciones de acceso y las facultades de sus funcionarios y personal a través de sus aplicaciones de gobierno electrónico seguro.

Con respecto al uso del Documento Nacional de Identidad Electrónico (DNIe) por los funcionarios públicos hay distintos criterios que deben ser concordados y prevalecer el propuesto en el Proyecto de Ley de Identidad Digital. Cabe mencionar que el Proyecto de Ley Nº 3591/2013-CR[177] propone que "la identificación electrónica del cargo que ocupan los funcionarios o el personal en las entidades públicas es mediante un certificado digital de función o cargo público, incorporado en el DNIe". En cambio, la propuesta contenida en el Proyecto de Ley de Identidad digital permite utilizar los certificados digitales contenidos en el DNIe para autenticar a la persona natural como funcionario público, quedando como responsabilidad de la Administración Pública autorizar el acceso y ejercicio de su facultades conforme su rol y cargo respectivo. Se diferencia la autenticación de la autorización con lo cual

[177] Dictamen del Proyecto de Ley 3591/2013-CR que propone la Ley que dispone que las entidades públicas envíen a tarves de medios electrónicos o aplicativos informáticos la información o documentación que por mandato legal presentan a la Comisión de Presupuesto y Cuenta General del Congreso de la Republica. Dictamen de la Comisión de Presupuesto y Cuenta General de la Republica. Periodo Anual de Sesiones 2013-2014. En http://www.congreso.gob.pe

se facilita y sistematiza la utilización de los DNI electrónicos y del derecho de la identidad digital en internet por los funcionarios públicos.

En el artículo 25º del Proyecto se define la sede electrónica como "aquella dirección electrónica de cada entidad de la Administración Pública, mediante la cual brinda los servicios de gobierno electrónico seguro comprendidos en el alcance de la presente Ley y que se encuentra disponible para las personas como un canal de comunicación único a través de Internet. La sede electrónica pondrá a disposición de las personas un catalogo de servicios.

El concepto de sede electrónica, en el derecho comparado lo encontramos en la legislación española. En efecto, el artículo 10º de la Ley Nº11/2007[178], de acceso electrónico de los ciudadanos a los servicios públicos, establece que: "La sede electrónica es aquella dirección electrónica disponible para los ciudadanos a través de redes de telecomunicaciones cuya titularidad, gestión y administración corresponde a una Administración Pública, órgano o entidad administrativa en el ejercicio de sus competencias. El establecimiento de una sede electrónica conlleva la responsabilidad del titular respecto de la integridad, veracidad y actualización de la información y los servicios a los que pueda accederse a través de la misma..."

El artículo 26º del Proyecto de Ley de Identidad Digital precisa que la sede electrónica utilizara para identificarse y garantizar las personas una comunicación segura, certificados digitales de agentes automatizados de acuerdo a lo establecido en la Ley de Firmas y Certificados Digitales. Se precisa que la autenticación y generación de documentos electrónicos por parte de la Administración Pública, se utiliza firmas y certificados digitales usando sus documentos

[178] Ley 11/2007, Ley española de acceso electrónico de los ciudadanos a los servicios públicos del 22 de Junio de 2007. https://www.boe.es/diario_boe/txt.php?id=BOE-A-2007-12352

credenciales electrónicos contenidos en el DNIe por parte de los funcionarios y personal al servicio de las entidades de la Administración Pública.

El articulo 27º dispone que los registros electrónicos deben emitir automáticamente un acuse de recibo y la constancia de presentación del documento electrónico, escrito, solicitud o comunicación de que se trate, la que deberá incluir fecha y hora cierta del servicio del sellado de tiempo[179], así, como numero de entrada de registro. El servicio de sellado de tiempo es provisto por un Prestador de Servicio de Valor Añadido (PSVA) acreditado ante la Autoridad Competente.

El numeral 29.2 del Proyecto de Identidad Digital dispone lo siguiente: "El RENIEC proporciona el domicilio electrónico oficial del ciudadano, que se habilita para todo ciudadano que obtenga un Documento Nacional de Identidad Electrónico (DNIe) y al que pueda acceder todas las entidades de la Administración Pública para propósitos de la notificación electrónica. El acceso al domicilio electrónico Oficial es a través del DNIe".

El domicilio electrónico oficial del ciudadano, conforme el glosario del Reglamento de la Ley de Firmas y Certificados Digitales: "es la dirección…del ciudadano, reconocida por el Gobierno Peruano para la realización confiable y segura de las notificaciones electrónicas personales requeridos en los procesos públicos". Al precisar el Proyecto de Ley de Identidad Digital que el RENIEC proporciona el

[179] El servicio de sellado de tiempo es un mecanismo online que ofrece evidencias técnicas y jurídicas para demostrar lo siguiente: Que un dato ha existido desde un instante específico del tiempo y que el dato no ha sido alterado desde ese momento, cumpliendo el estándar RFC 3161.

domicilio electrónico oficial del ciudadano, que se habilita para todo ciudadano que obtenga un DNIe, se está regulando el domicilio procesal electrónico del ciudadano que se autentica con el uso de los documentos credenciales electrónicos contenidos con el DNIe y que están en concordancia con el concepto de sede electrónica. Estas disposición permite utilizar distintas soluciones tecnológicas[180], que permitan un acceso seguro del ciudadano a su información, garantizando su derecho de identidad digital en internet.

En los artículos siguientes se regula la prueba de los documentos electrónicos y el expediente electrónico. Cabe señalar que el artículo 31 del Proyecto de Ley de Identidad Digital regula la verificación de las copias de documentos electrónicos, de la siguiente forma: "Para la verificación de las copias en papel de documentos electrónicos firmados digitalmente y que hayan sido generados dentro de la IOFE , los documentos impresos deben incluir la impresión de un código de verificación generado electrónicamente o un enlace que guarde relación con el documento original".

Con respecto al expediente electrónico se precisa en el artículo 33 del Proyecto de Identidad Digital que "se constituye en los tramites, procedimientos administrativos o procesos judiciales en la entidad que agrupa una serie de documentos o anexos identificados como archivos, sobre los cuales interactúan los usuarios internos o externos a la entidad que tengan los perfiles de acceso o permisos autorizados".

[180] Estas soluciones tecnológicas pueden incluir el uso de casillas electrónicas que garanticen la autenticación de la identidad digital del ciudadano y combinen el uso de sede electrónica, sistemas de casillas electrónicas y comunicación de aviso y/o información al correo electrónico del ciudadano.

Asimismo, en el Proyecto de Identidad Digital[181] se señala que: "El expediente electrónico debe tener un número de identificación único e inalterable que permita a lo largo de la prestación de los servicios de gobierno electrónico seguro su identificación univoca dentro de la entidad de la administración pública que lo origine. Dicho número permite a su vez su identificación para efectos de un intercambio de información entre entidades o por las partes interesadas…cada documento electrónico incorporado en el expediente electrónico debe ser enumerado correlativamente de modo que se origine un índice electrónico el cual es firmado digitalmente por el personal responsable de la entidad de la Administración Pública..".

Dentro de los documentos electrónicos incluidos en el expediente electrónico tenemos los producidos utilizando tecnologías de información y comunicaciones, como es el caso de las videoconferencias. Al respecto cabe mencionar la Sentencia del Tribunal Constitucional que ha validado el uso de la videoconferencia en un proceso penal que fue impugnado mediante el Proceso de Hábeas Corpus al que se refiere el expediente 02738-2014-PHC/TC[182], promovido en beneficio de un interno de un centro penitenciario ubicado en la ciudad de Nazca, quien consideraba que al no encontrarse físicamente presente en la audiencia de apelación de sentencia, la misma que se llevó a cabo a través de una videoconferencia, se afectaba su derecho al debido proceso. En esta sentencia destacamos lo siguiente:

[181] Texto Sustitutorio del Proyecto de Ley Nº 3900-2014-RENIEC, Ley de Identidad Digital. Comisión de Justicia del Congreso de la Republica del Perú. Noviembre de 2015.
[182] Sentencia del Tribual Constitucional del 30 de Julio de 2015. Expediente 02738-2014-PHC/TC. Publicado en: http://www.tc.gob.pe

a) La videoconferencia es un sistema aceptado y regulado administrativamente en cumplimiento del principio de celeridad procesal, así como un mecanismo que no atenta contra el principio de inmediación, puesto que cumple con los elementos necesarios, a saber: la interacción de las partes, la contradicción, la observación, el lenguaje no verbal y la comprobación de identidad del declarante.
b) A criterio del supremo intérprete de la Constitución, " el sistema de videoconferencia no impide que el procesado y el juzgador puedan comunicarse oralmente, pudiéndose observar que cuando se realiza bajo las condiciones técnicas adecuadas no obstaculiza la mejor percepción sensorial”. Asimismo, en la medida que permita el acceso al contenido de las audiencias, no afecta la publicidad.
c) Respecto a la contradicción, se aprecia que con las partes comunicadas en tiempo real, esta pueden expresarse fluidamente, tal y como estuvieren presentes físicamente el procesado y el juzgador en el mismo ambiente.
d) El Tribunal Constitucional Peruano "considera que la utilización del sistema de videoconferencia no transgrede *prima face,* los principios de oralidad, publicidad y contradicción, constituyéndose más bien, en un instrumento tecnológico que coadyuva los fines del proceso”.

3.2.5. La Interoperabilidad, la identidad digital y otros temas relacionados

En el Titulo Tercero se regula interoperabilidad en los artículos 36º al 42º. En el artículo 36º se establece que “las entidades de la Administración Pública deben establecer la interconexión de equipos de procesamiento de datos, a través del uso de estándares que permitan su interoperabilidad, a fin que sus respectivos sistemas y sus componentes puedan intercambiar información, con el objeto de facilitar el cumplimiento de sus respectivas funciones y la prestación de servicios de gobierno electrónico seguro, integrados o brindados en conjunto entre ellas.

La interoperabilidad permite que la información sea intercambiada electrónicamente identificando digitalmente a las personas en forma segura. Los datos personales deben ser fehacientemente verificados en relación con su identidad digital, de forma tal que la información intercambiada por las entidades de la Administración Pública garanticen los derechos de la persona en cuanto a la veracidad, finalidad, proporcionalidad, calidad y seguridad de los datos comunicados que pueden servir de base para actos administrativos que reconozcan o afecten derechos del ciudadano.

El artículo 37º establece que el “Sistema de Interoperabilidad del Estado Peruano está constituido por políticas, lineamientos, especificaciones, estándares e Infraestructura de Tecnologías de la Información, que permitan de manera efectiva la interoperabilidad para la prestación de servicios de gobierno electrónico seguro”.

Las políticas, lineamientos y especificaciones posibilitan la interconexión y transmisión de la información entre entidades de la administración publicas que se refiera a datos personales u otros datos que pueden ser vinculados a la identidad digital del funcionario o autoridad que remite esa información. El ejercicio del derecho de la identidad digital en internet para prestación de servicios de gobierno electrónico seguro implican que la autenticación y la autorización legal para trasmitir esa información este acorde con estándares internacionales y criterios seguros contenidos en las políticas, lineamientos y especificaciones que se utilizan.

En el artículo 38º se diferencia la interoperabilidad a nivel semántico de la interoperabilidad a nivel técnico. Con respecto, a la interoperabilidad a nivel semántico se precisa que “en este nivel, se ocupa del significado del uso de los datos y la información garantizando que el significado preciso de la información intercambiada pueda ser entendida por cualquier aplicación de otra entidad de la Administración Pública”. En cambio la Interoperabilidad a nivel técnico es “ejecutado por personal funcional relacionado con los objetivos de la entidad y personal especializado de tecnologías de la información de acuerdo a normas, actividades y desarrollos de proyectos de interoperabilidad”.

La interoperabilidad a nivel semántico y técnico permite que la información y los sistemas estén con estándares y lenguajes compatibles que permitan una eficaz comunicación vinculada a la identidad digital de los datos personales que se comunican y/o de los funcionarios o autoridades que se responsabilidad de esta

comunicación. En este sentido, es necesario utilizar la Plataforma de Interoperabilidad del Estado Peruano[183] que permitirá la implementación de servicios públicos por medios digitales y el intercambio electrónico de datos entre entidades del Estado a través de Internet.

En los artículos siguientes se regula reutilización de aplicaciones informática, también se establece la necesidad de establecer de un Plan Nacional de Identidad Digital y de Implementación de Servicios de Gobierno Electrónico Seguro.

Finalmente, se establecen las Disposiciones Finales Complementarias, entre las que es necesario mencionar las siguientes:

a) El RENIEC dictará las medidas reglamentarias referidas al DNIe. Con esta disposición se faculta a RENIEC que dicte las normas reglamentarias que permitirán el ejercicio de la identidad digital del las personas naturales incluyendo los adultos, personas de la tercera edad. Discapacitados, niños, entre otros.
b) Se implementará un Plan Nacional de Identidad Digital y de Implementación de Servicios de Gobierno Electrónico Seguro. El Plan deberá tener objetivos y estrategias, lo que permitirá consolidar un sistema de identidad digital que evite la suplantación de identidad y el uso indebido de las identidades multiples.

[183] El Decreto Supremo Nº 083-2011-PCM, crea la Plataforma de Interoperabilidad del Estado Peruano (PIDE).

c) Se encarga a RENIEC la elaboración del modelo de e-inclusión y la metodología de diseño de servicios y procedimientos que basados en la identidad digital, sean de aplicación para su implementación por las entidades de la Administración Publica. El modelo de inclusión electrónica permitirá disminuir la brecha digital y facilitar los servicios digitales que permitan una activa y plena participación del ciudadano.
d) Se autoriza a RENIEC a promover el uso de la autenticación de la identidad a través de la tecnología biométrica, así como el establecimiento progresivo y gradual del Código Único de Identificación de la Persona Natural con Base Genética.

3.3. Normas que complementan sistémicamente el sistema funcional propuesto: teletrabajo, delitos informáticos, votación electrónica.

3.3.1. Ley y Reglamento del Teletrabajo

3.3.1.1. Ley del Teletrabajo Nº 30036

El miércoles 05 de Junio de 2013, se ha publicado la Ley Nº 30036 que regula el Teletrabajo, tanto en instituciones públicas como privadas y que promueve políticas públicas para garantizar su desarrollo y su preferente utilización a favor de poblaciones vulnerables. Por la importancia y actualidad del tema regulado, consideramos necesario emitir el presente informe

La Ley que regula el teletrabajo, tiene el siguiente contenido:

a) La ley tiene por objeto regular el teletrabajo, como una modalidad especial de prestación de servicios caracterizada por la utilización de tecnologías de la información y las telecomunicaciones (TIC), en las instituciones públicas y privadas, y promover políticas públicas para garantizar su desarrollo.

“El teletrabajo es la actividad profesional desarrollada por personas que no están presentes físicamente en la empresa para la que trabajan. Esto exige, además de un perfil profesional, un dominio de las nuevas tecnologías de información y comunicación. Por tanto, es una forma de trabajo a distancia mediante el uso de telecomunicaciones. Es una nueva forma de trabajo que no requiere la presencia del empleado en el centro productivo, es decir, en la oficina o planta de la empresa[184]”.

b) El teletrabajo se caracteriza por el desempeño subordinado de labores sin la presencia física del trabajador, denominado "teletrabajador", en la empresa con la que mantiene vínculo laboral, a través de medios informáticos, de telecomunicaciones y análogos, mediante los cuales se ejercen a su vez el control y la supervisión de las labores. Son elementos que coadyuvan a tipificar el carácter subordinado de esta modalidad de trabajo la provisión por el empleador de los medios físicos y métodos informáticos, la dependencia tecnológica y la propiedad de los resultados, entre otros.

c) Cuando los equipos sean proporcionados por el empleador, el teletrabajador es responsable de su correcto uso y conservación, para lo cual evita que los bienes sean utilizados por terceros ajenos a la relación laboral. Cuando el teletrabajador aporte sus propios equipos o elementos de trabajo, el empleador debe compensar la totalidad de los gastos, incluidos los gastos de comunicación, sin perjuicio de los mayores beneficios que pudieran pactarse por acuerdo individual o convenio colectivo. Si el teletrabajador realiza sus labores en una cabina de internet o en un equipo proporcionado por terceras personas, el empleador asume los gastos que esto conlleva. El reglamento establece la forma como se efectuará esta compensación de condiciones de trabajo.

[184] TELEZ VALDES, Julio: “ Teletrabajo”. Biblioteca Juridica Virtual del Instituto de Investigaciones Juridicas de la UNAM. Pagina 730. En http://biblio.juridicas.unam.mx/libros/5/2458/43.pdf

d) Por razones debidamente sustentadas, el empleador puede variar la modalidad de prestación de servicios a la de teletrabajo, previo consentimiento del trabajador. El cambio de modalidad de prestación de servicios no afecta la naturaleza del vínculo laboral, la categoría, la remuneración y demás condiciones laborales, salvo aquellas vinculadas a la asistencia del centro de trabajo.

e) El teletrabajador puede solicitar al empleador la reversión de la prestación de servicios bajo esta modalidad. El empleador puede denegar dicha solicitud en uso de su facultad directriz. El empleador puede reponer al teletrabajador a la modalidad convencional de prestación de servicios que ejecutaba con anterioridad si se acredita que no se alcanzan los objetivos de la actividad bajo la modalidad de teletrabajo.

f) El teletrabajador tiene los mismos derechos y obligaciones establecidos para los trabajadores del régimen laboral de la actvidad privada. Pueden utilizarse todas las modalidades de contratación establecidas para dicho régimen. En todos los casos, el contrato de trabajo debe constar por escrito.

g) Las entidades públicas sujetas al régimen laboral del Decreto Legislativo 276, Ley de bases de la carrera administrativa y de remuneraciones del sector público, y a regímenes especiales, se encuentran facultadas para aplicar la presente norma cuando así lo requieran sus necesidades. El reglamento establece cuotas mínimas de personal sujeto a esta modalidad, de acuerdo a las necesidades de cada entidad.

h) Las acciones a cargo del Estado de los diferentes niveles de gobierno, que se deban implementar para el cumplimiento de lo dispuesto en la presente norma, se financian a cargo a sus respectivos presupuestos institucionales, sin demandar recursos adicionales al tesoro público.

i) Dentro de los noventa días hábiles de entrada en vigencia de la presente Ley, el Ministerio de Trabajo y de Promoción del Empleo formula políticas públicas referidas al teletrabajo para

garantizar su desarrollo y su preferente utilización a favor de las poblaciones vulnerables, para lo cual coordina con la Autoridad nacional del Servicio Civil (SERVIR), con la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI), con el Consejo nacional para la Integración de la persona con Discapacidad (CONADIS) y con la Comisión Multisectorial para el Seguimiento y Evaluación del Plan de Desarrollo de la Sociedad de la Información en el Perú (CODESI).

j) La Ley que regula el teletrabajo precisa que el teletrabajador tiene los mismos derechos y obligaciones establecidos para los trabajadores del régimen laboral de la actividad privada, por tanto tiene beneficios como vacaciones, compensación de tiempo de servicios, gratificaciones, entre otros.

k) Las entidades del sector público, se encuentran facultadas para aplicar la presente norma cuando así lo requieran sus necesidades. Por tanto, cada entidad deberá evaluar que necesidades pueden adecuarse a la incorporación de teletrabajadores, de acuerdo a la naturaleza de las labores de cada dependencia.

Las Políticas Públicas de teletrabajo deberán prever una preferente utilización a favor de las poblaciones vulnerables

3.3.1.2. Reglamento de la Ley del Teletrabajo

Por Decreto Supremo Nº 017-2015-TR, publicado el 03 de Noviembre de 2015, reglamentan la Ley Nº 30036, que regula el Teletrabajo. El Reglamento de la Ley de Teletrabajo tiene el siguiente contenido: Titulo Preliminar. Titulo I: Disposiciones aplicables al sector publico y privado. Capitulo I: Prestación de Servicios bajo la modalidad de teletrabajo. Capitulo II: Derechos y Obligaciones del teletrabajador. Titulo II Disposiciones aplicables al Sector Publico. Disposiciones Complementarias Finales. Disposiciones Complementarias Finales. Disposición Complementaria Modificatoria.

3.3.1.2.1. Principios del Teletrabajo establecidos en el Reglamento

Son principios que orientan la aplicación de la modalidad de teletrabajo los siguientes:

a) Voluntariedad: el empleador o entidad pública, por razones debidamente sustentadas, puede efectuar la variación de la prestación de servicios a la modalidad de teletrabajo, contando para ello con el consentimiento del trabajador o servidor civil. Este consentimiento debe ser libre, previo, expreso e inequívoco e informado. Cuando se utilice documentos electrónicos se realizara utilizando firmas y certificados digitales.

b) Reversibilidad: el empleador o entidad pública puede reponer al teletrabajador a la modalidad de prestación de servicios anterior a teletrabajo, si se acredita que no se alcanzan los objetivos bajo la modalidad de teletrabajo. Para lo cual es necesario identificar adecuadamente al teletrabajador para identificar sus labores y resultados utilizando las tecnologías de información y telecomunicaciones.

c) Igualdad de trato: el empleador o entidad pública debe promover la igualdad de trato en cuanto a las condiciones de trabajo de los teletrabajadores, en relación a quienes laboran presencialmente. La igualdad de trato requiere una adecuada gestión de identidad que permita al teletrabajador recibir un trato igual en línea que el trabajador presencial.

d) Conciliación entra la vida personal, familiar y laboral de los trabajadores o servidores civiles, a través de la modalidad de teletrabajo. En tal sentido, deberá existir una adecuada correspondencia entre la carga de trabajo y la jornada de labores o servicios asignada. Para lo cual una gestión de identidades del teletrabajador y de sus familiares y diferenciación de roles coadyuvarían con esta finalidad.

3.3.1.2.2. Requisitos formales

Los contratos, resoluciones de incorporación o designación y adendas o acuerdos por los que se establezca la modalidad de teletrabajo, o el cambio de modalidad presencial por la de teletrabajo, se celebran por escrito y se sujetan a las condiciones y requisitos previstos por las normas que les sean aplicables, según el régimen al que pertenezca cada teletrabajador. El empleador o entidad pública debe entregar a teletrabajador un ejemplar de aquellos documentos, según corresponda.

3.3.1.2.3. Formas de Teletrabajo

La modalidad de teletrabajo puede desarrollarse bajo las siguientes formas:

a) Forma completa: el teletrabajador presta servicios fuera del centro de trabajo o del local de la entidad pública; pudiendo acudir ocasionalmente a estos para las coordinaciones que sean necesarias.
En estos casos la identidad digital requiere ser fehacientemente comprobada, dado que el contrato de trabajo implica una prestación personal del trabajador. En estos casos el uso del documento nacional de identidad electrónico y de sus certificados de autenticación y firma digital coadyuvan con esta finalidad.

b) Forma mixta: el teletrabajador presta servicios de forma alternada dentro y fuera del centro de trabajo o local de la entidad pública. La identidad digital comprobada fehacientemente también es necesaria e importante en esta modalidad.

3.3.1.2.4. Derecho y beneficios del teletrabajador

El teletrabajador tiene los mismos derechos y beneficios de los trabajadores que prestan servicios bajo la modalidad convencional, de acuerdo al régimen al que pertenezca cada teletrabajador, salvo aquellos vinculados a la asistencia del centro de trabajo.
Entre los derechos que serán garantizados se encuentran:

a) Capacitación sobre los medios informáticos, de telecomunicaciones y análogos que emplearan para el desempeño de la ocupación especifica, así como las restricciones en el empleo de tales medios, la legislación vigente en materia de resguardo de la identidad digital, protección de datos personales, propiedad intelectual y seguridad de la información. La capacitación se realiza antes de iniciarse la prestación de servicios bajo la modalidad de teletrabajo y cuando el empleador introduzca modificaciones sustanciales a los medios informáticos de telecomunicaciones y análogos con los que el teletrabajador presta sus servicios.

b) Intimidad, privacidad, identidad digital e inviolabilidad de las comunicaciones y documentos privados del teletrabajador, considerando la naturaleza del teletrabajo.

c) Protección de la maternidad y periodo de lactancia de la teletrabajadora.
d) Seguridad y salud en el trabajo, en lo que fuera pertinente y considerando las características especiales del teletrabajo.
e) Libertad sindical, de acuerdo al régimen que resulte aplicable. En ningún caso, la aplicación o el cambio de modalidad de prestación de servicios de un trabajador o servidor civil a la modalidad de teletrabajo podrá afectar el ejercicio de sus derechos colectivos.

3.3.1.2.5. Registro en planilla electrónica
El empleador y la entidad pública registran en la planilla electrónica la condición de teletrabajador en la modalidad completa o mixta aplicada, y otros criterios que se establezcan mediante Resolución Ministerial.
En la planilla electrónica se registran los datos de la relación laboral del teletrabajador. En consecuencia, la boleta de pago también debiera ser electrónica.
La identidad digital y los datos personales consignados en la planilla electrónica requieren ser garantizados y protegidos por un tercero de confianza que acredite y respalde a las personas para evitar el uso indebido de las múltiples identidades y la suplantación de identidad.

Con respecto, a la Boleta de Pago Electrónica, dentro del ámbito laboral, se ha propuesto[185] que deba ser firmada digitalmente tanto por el empleador como por el trabajador. Se propone que el empleador pueda sustituir la emisión y entrega física de la boleta de pago por una boleta de pago electrónica, cuando el integro de la remuneración en dinero se efectúe en la modalidad de depósito en cuenta, sea registrada en el T-Registro de la Planilla Electrónica y se informe al trabajador de esta modalidad que para acceder a ella deberá autenticar su identidad digital utilizando su documento nacional de identidad electrónico (DNIe).

[185] Por Resolución Ministerial Nº 242-2014-TR, del 11 de Noviembre de 2014 se dispone la pre-publicación del Proyecto Normativo "Decreto Supremo que modifica el Decreto Supremo Nº 001-98-TR para implementar la Boleta de Pago Electrónica".

3.3.2. Ley de Delitos Informáticos

La Ley 30096 tiene por objeto prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidos mediante la utilización de tecnologías de la información o de la comunicación, con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia. La Ley Nº 30096 fue modificada por la Ley Nº 30171 del 14 de Marzo del 2014

La ley tipifica penalmente, las siguientes conductas en el Capítulo II: Delitos contra Datos y Sistemas Informáticos: el acceso ilícito a un sistema informático, los atentados contra la integridad de datos informáticos o sistemas informáticos. Conforme la Exposición de Motivos del Proyecto 2520/2012-PE, en estos casos los bienes jurídicos que se protegen y cuya lesión o puesta en peligro se sancionan son los sistemas informáticos y los datos informáticos, dado que, debido al avance las TIC, dichos bienes han alcanzado una importancia significativa para el desarrollo de la persona y la comunidad.

Acceso Ilícito se tipifica de la siguiente forma: El que deliberada e ilegítimamente accede a todo o parte de un sistema informático, siempre que se realice con vulneraciones de medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro y con treinta a noventa días multa. Será reprimido con la misma pena , el que que accede a un sistema informático, excediendo lo autorizado.

“Por la característica que presenta este tipo penal acceso ilícito se le puede calificar como un delito de mera actividad , porque esta figura exige el acto de acceder (entrar en un lugar o pasar a él) sin autorización a un sistema informático, vulnerar (transgredir, quebrantar, violar una ley o precepto)las medidas de seguridad, de esta manera se configura el ilícito; por tanto el delito queda consumado en el momento que se vulnera las medidas de seguridad

establecida para impedir el acceso ilícito, y para ellos es necesario que se realice esta conducta con dolo"[186].

Atentado a la integridad de datos informáticos, se tipifica: "El que deliberada e ilegítimamente daña, introduce, borra, deteriora, altera, suprime, o hace inaccesibles datos informáticos , será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa".

Un caso[187] en que encuadra este tipo penal de atentado a la integridad de datos informáticos es el siguiente: "se realiza un supuesto pago por deposito que acreditaba el pago correspondiente de multas de un vehículo internado en un depósito vehicular; el encausado ordena modificar la base de datos del área de Informática para así reducir el costo real de la deuda por concepto de internamiento de su vehículo y poder ordenar la liberación del vehículo, borrando y alterando datos informáticos"

Otros casos de atentado a la integridad de datos informáticos pueden ser producidos por malwares[188] creados por ciberdelincuentes que utilizando internet dañan, deterioran , suprimen o hacen inaccesibles datos informaticos.

Atentado contra la integridad de sistemas informáticos, se tipifica "El que deliberada o ilegítimamente inutiliza, total o parcialmente, un sistema informático, impide el acceso a éste, entorpece o imposibilita su funcionamiento, o la prestación de sus servicios, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa.

[186] VILLAVICENCIO TERREROS, Felipe: "Delitos Informaticos en la Ley 30096 y la Modificacion de la Ley 30171". En: http://www.derecho.usmp.edu.pe/cedp/revista/articulos/Felipe_Villavicencio_Terreros-Delitos_Informaticos_Ley30096_su_modificacion.pdf Pagina 11. Fecha de Consulta 30 de Noviembre de 2015.

[187] Jurisprudencia sistematizada del Poder Judicial del Peru. Sala Penal Permanente de la Corte Suprema. R.N. Nº 3372-2009. LIMA. En http://www.pj.gob.pe

[188] Malware es la abreviatura de ***"Malicious software",*** término que engloba a todo tipo de programa o código informático malicioso cuya función es dañar un sistema o causar un mal funcionamiento. Dentro de este grupo podemos encontrar términos como: Virus, Troyanos (Trojans), Gusanos (Worm), keyloggers, Botnets, Ransomwares, Spyware, Adware, Hijackers, Keyloggers, FakeAVs, Rootkits, Bootkits, Rogues, etc…. En: https://www.infospyware.com/articulos/que-son-los-malwares/. Fecha de consulta: Noviembre de 2015.

Se incluye como métodos informáticos para realizar estas conductas delictivas: el daño informático o el sabotaje informático, bombas lógicas, rutinas cáncer, gusanos.

Los daños informáticos pueden definirse como el deterioro, menoscabo o destrucción de hardware, software o información cuyo perjuicio patrimonial es evaluable económicamente.

"Actualmente se mantiene la perspectiva estrictamente patrimonial de todos los delitos de daños. Sin embargo, es una realidad que los daños informáticos poco tienen que ver con los daños tradicionales. La informática e internet han cambiado las reglas del juego. Ya no es necesaria la destrucción física de la cosa, ahora las acciones criminales se producen de forma remota, generando resultados muy difíciles de evaluar económicamente y causando perjuicios muy superiores al valor de los datos destruidos. El sabotaje informático es una conducta habitual en muchos perfiles de ciberdelincuentes..[189]".

"Las "bombas lógicas" son piezas de código de programa que se activan en un momento predeterminado, como por ejemplo, al llegar una fecha en particular, al ejecutar un comando o con cualquier otro evento del sistema"[190].

"Otra modalidad que actúa sobre los programas de aplicación es el llamado «cáncer de rutinas» («cancer routine»). En esta técnica los programas destructivos tienen la particularidad de que se reproducen, por sí mismos, en otros programas, arbitrariamente escogidos"[191].

"Un gusano es un programa que se reproduce por sí mismo, que puede viajar a través de redes utilizando los mecanismos de éstas y que no requiere respaldo de software o hardware (como un disco duro, un programa host, un archivo, etc.) para difundirse. Por lo tanto, un gusano es un virus de red"[192].

---

[189] Abogacia Española. Consejo General: "Análisis Jurídico del Sabotaje Informático". 9 de Marzo del 2015. En: http://www.abogacia.es/2015/03/09/analisis-juridico-del-sabotaje-informatico/

[190] Definición de Bombas Lógicas . Noviembre de 2015. En http://es.ccm.net/contents/742-bombas-logicas .

[191] Definicion de cáncer de rutinas. Fecha de Consulta: Noviembre de 2015. En Wikiteca. Apuntes. En http://www.wikiteka.com/apuntes/delitos-informaticos/

[192] Definición de Gusano Informático. Noviembre de 2015. En http://es.ccm.net/contents/755-gusanos-informaticos

La ley 30171 incorpora el artículo 154-A al código penal y deroga el artículo 6° de la Ley 30096; Ley de Delitos Informáticos. El Tráfico Ilegal de Datos, es tipificado en el artículo 154-A del Código Penal de la siguiente forma: "El que ilegítimamente comercializa y vende información no pública relativo a cualquier ámbito de la esfera personal, familiar, patrimonial, laboral, financiera u otro de naturaleza análoga sobre una persona natural, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años. Si el agente comete el delito como integrante de una organización criminal, la pena se incrementa hasta en un tercio encima del máximo previsto en el párrafo anterior".

Este tipo penal sanciona al que ilegítimamente comercializa y vende información no publica, por no contar con la autorización o consentimiento libre, previo, expreso e inequívoco en informado del titular de los datos personales que es individualizado por su identidad digital. Pudiendo determinarse que información obtenida ilegítimamente esta en el ámbito personal en que la persona ejercita su identidad estática y dinámica. Pero también esta información puede involucrar el ámbito familiar, patrimonial, laboral o financiera y ser utilizada por quien no tiene legitimidad para usar esta información que es atribuida por una persona a la que se le identifica digitalmente. .

La Interceptación de Datos Informáticos, es tipificada de la siguiente forma: "El que deliberada e ilegítimamente intercepta datos informáticos en transmisiones. no públicas, dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo, incluidas las emisiones· electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos, será reprimido con una pena privativa de libertad no menor de tres ni mayor de seis años.

La pena privativa de libertad será no menor de cinco años ni mayor de ocho años cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con la ley 27806, Ley de Transparencia y Acceso de Información Pública. La pena privativa de libertad será no menor de ocho años ni mayor de diez años cuando el delito comprometa la defensa, la seguridad o la

soberanía nacionales. Si el agente comete el delito como integrante de una organización criminal la pena se incrementa hasta un tercio por encima del máximo legal previstos en los supuestos anteriores".

"Este injusto penal interceptar datos informáticos es un delito de peligro abstracto y por ende, solo basta con demostrar la interceptación de datos informáticos para que el delito quede consumado. Por ende, se clasifica como un delito de mera actividad porque basta con el sólo hecho de interceptar datos informáticos para que se consuma el delito"[193].

El Capítulo IV tipifica el delito de Fraude Informático, de la siguiente forma: "El que deliberada e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero, mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de tres ni mayor de ocho años *y* con sesenta a ciento veinte días-multa".
La pena será privativa de libertad no menor de cinco ni mayor de diez años *y* de ochenta a ciento cuarenta días-multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social"
"Se clasifica como un delito de resultado porque no basta cumplir con el tipo penal para que se consume el delito de fraude informático, sino que además, es necesario que esa acción vaya seguida de un resultado separado de la misma conducta el que consiste en causar un perjuicio a tercero"[194].

El capítulo V de la ley regula la suplantación de la identidad, tipificándose de la siguiente forma: "El que, mediante las tecnologías de la información o de la comunicación suplanta la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años.

[193] VILLAVICENCIO TERREROS, Felipe: ob.cit. Página 17.
[194] VILLAVICENCIO TERREROS, Felipe: ob.cit. Pagina 19.

"La suplantación de identidad se puede calificar como un delito de resultado porque no basta con realizar la conducta típica de "suplantar " la identidad, sino que además es necesario que esa acción vaya seguida de un resultado separado de la misma conducta que consiste en causar un perjuicio, caso contrario quedaría en tentativa"[195].

La Ley 30171 incorpora el artículo 12 a la Ley de Delitos informático, estableciendo la exención de responsabilidad penal para el Hacking Etico, de la siguiente forma: "Artículo 12. Exención de Responsabilidad Penal. Está exento de responsabilidad penal el que realiza las conductas descritas en los artículos 2 (delito de acceso ilícito), 3 (delito de atentado a la integridad de datos informáticos), 4 (delito de atentado a la integridad de sistemas informáticos) y 10 (delito de abuso de mecanismos y dispositivos informáticos) con el propósito de llevar pruebas autorizadas y otros procedimientos autorizados destinados a proteger sistemas informáticos" .

La Ley en el capítulo VII regula las disposiciones comunes precisando el abuso de mecanismos y dispositivos informáticos de la siguiente forma: "El que fabrica, diseña, desarrolla, vende , facilita, distribuye, importa u obtiene para su utilización uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático específicamente diseñado para la comisión de los delitos previstos en la ley, o el que ofrece, o presta servicio que contribuya a este propósito, será reprimido con pena privativa de libertad no menor de uno ni mayor cuatro años y con treinta a noventa días multa.

3.3.3 Votación Electrónica

3.3.3.1. La votación electrónica en procesos electorales

El Sistema de votación electrónica "es el conjunto de software, hardware y red de comunicaciones que haciendo uso de la tecnología disponible permiten: comprobar los datos de identidad del elector; emitir y consolidar los votos; emitir reportes:

[195] VILLAVICENCIO TERREROS, Felipe: ob.cit. Página 19.

presentar y transmitir resultados de un proceso electoral, de referéndum y otras consultas populares"[196]

Esta definición que interrelaciona el software, el hardware y las redes con la tecnología y la identidad del elector ha evolucionado pasando de la concepción referida al número de votantes al de gradualidad de la automatización de las actividades y etapas propias de la jornada y el proceso electoral dando lugar a soluciones tecnológicas de voto electrónico, con una visión integral.

El sistema de votación electrónica integral "comprende la automatización de todas la etapas de la Jornada Electoral, así como la transmisión de los resultados. Permite la generación electrónica del Reporte de Puesta a Cero de Votantes y de Votos, Reporte de asistencia de los Miembros de Mesa y de lectores. Acta de instalación, Acta de sufragio y de Escrutinio. Constancia de Voto y Cartel de Resultados en el caso de votación electrónica presencial, así como la transmisión de resultados"[197].

Las soluciones tecnológicas de voto electrónico permiten al elector el libre ejercicio del derecho del sufragio, considerando las características propias de la identidad digital y de los datos personales identificativos como la edad, la condición física, el domicilio y otros que permitan utilizar las tecnologías de comunicación e información para facilitar el ejercicio del derecho de voto del ciudadano, en un entorno electrónico seguro.

El Voto Electrónico es el conjunto de procedimientos aplicados en las diversas etapas de los procesos electorales, de

[196] Reglamento de Voto Electrónico. Numeral 5.20. Version anterior aprobada por Resolución Jefatural 0171-2014-ONPE del 15 de Julio de 2014. En http://www.onpe.gob.pe.
[197] Reglamento de Voto Electrónico. Articulo 10º. Version Actual aprobada por Resolución Jefatural 022-2016-ONPE del 28 de Enero de 2016g. En http://www.onpe.gob.pe.

referéndum o de consultas populares en el que se incluye, específicamente, el acto mismo de la votación, permitiendo el ejercicio del derecho de sufragio de manera automatizada, a través del uso de medios electrónicos e informáticos. Forma parte del Sistema de voto electrónico integral. El voto electrónico puede ser de dos modalidades:

A) Presencial: Modalidad de Votación Electrónica, cuyos procesos se desarrollan en ambientes o lugares debidamente supervisados por las entidades competentes y requiere la concurrencia y participación del elector del elector en su mesa de sufragio a través del uso de equipos informáticos electorales, debidamente controlados.

B) No presencial: Modalidad de Votación electrónica que se realiza por Internet. No requiere la concurrencia del elector al local de votación, quedando a discrecionalidad del elector la determinación del equipo y lugar de emisión del voto, pero garantizándose la debida identificación de los electores en un entorno digital.

"El sistema de votación electrónica comprueba la identidad de los electores y garantiza la privacidad de los datos, la no vinculación de éstos con el voto emitido y que se refleje en el escrutinio. Asimismo, el sistema de votación electrónica registra y genera data fiable a fin de que la observación electoral sea óptima y transparente, garantizando la autenticidad, disponibilidad e integridad de la misma".[198]

Los principios reconocidos en el Reglamento de Voto Electrónico[199] son: a) Confiabilidad y seguridad. b) Continuidad del Proceso Electoral. c) Legalidad. d) Neutralidad Tecnológica. e) No repudio. f) Preclusión del acto electoral. g) Preservación

[198] Reglamento de Voto Electrónico. Numerales 4.4.1. y 4.4.2. Versión anterior Aprobada por Resolución Jefatural 0171-2014-ONPE del 15 de Julio de 2014. En http://www.onpe.gob.pe

[199] Reglamento de Voto Electrónico. Versión Actual aprobada por Resolución Jefatural 022-2016-ONPE del 28 de Enero de 2016g. En http://www.onpe.gob.pe.

del voto. i) Publicidad y Transparencia. Secreto del Voto. j) Sufragio Universal.

Por la confiabilidad y seguridad todos los votos son registrados y contados en forma igualitaria, precisa y transparente. Por continuidad del proceso electoral, entendemos que hay una secuencia ininterrumpida de las etapas del proceso electoral. Por legalidad los electores y las autoridades deben actuar conforme a la Constitución y la Ley de acuerdo a sus atribuciones y finalidades. Por neutralidad tecnológica, las soluciones tecnológicas del voto electrónico no realizan preferencia por algún tipo de tecnologías sino que priorizan los requisitos y resultados. Por no repudio no se negará la validez jurídica de la manifestación de voluntad de la persona identificada debidamente y que utiliza un sistema controlado y auditable.

Por preclusión del acto electoral se entiende que el proceso electrónico de votación y las soluciones tecnológicas respectivas, se realiza en etapas sucesivas, en que cada una de ellas concluye la anterior. Por el principio de preservación del voto se privilegia la validez del voto frente a las dudas en su interpretación siempre que se hayan realizado con la solución tecnológica adecuada. Los procesos son públicos y transparentes y se garantiza el sufragio universal.

3.3.3.2. Votación Electrónica en las elecciones del Colegio de Abogados de Lima

En el año 2015 el Comité Electoral del Colegio de Abogados de Lima[200] "acordó por unanimidad que el proceso de elecciones gremiales a realizarse con fecha 28 de noviembre de 2015 y la segunda vuelta a realizarse el 12 de Diciembre de 2015, serán

[200] Comunicado del Comité Electoral del Colegio de Abogados de Lima. Octubre de 2015. En http://www.cal.org.pe

totalmente electrónico (presencial y no presencial), por los siguientes fundamentos:

a) Permitirá a sus colegiados la facilidad de ejercer su voto de manera remota y rápida, utilizando computadores, tabletas, "smatphones" y otros dispositivos electrónicos..
b) Resultados de la elección en forma inmediata colaborando con el reconocimiento de los ganadores.
c) Se incrementara el porcentaje de participación en elecciones[201].
d) Marcara un precedente para que los siguientes procesos electorales del Colegio de Abogados de Lima sean electrónicos. El uso de los medios electrónicos permite que el abogado se familiarice con la identidad digital y con su manifestación por medios electrónicos con equivalencia funcional.
e) El Colegio de Abogados de Lima no incurrirá en costos de compra de ningún equipo para el proceso de votación. Lo que permite un uso racional de los recursos, porque los equipos necesarios para el proceso electoral electrónico presencial y no presencial son proporcionados para este proceso, por la empresa contratada para este fin.

El Comité Electoral del Colegio de Abogados de Lima[202], informo lo siguiente:

- Primero: El Comité Electoral vio por conveniente convocar a tres empresas especializadas en prestar el Servicio del "Software" con soporte lógico y técnico para llevar a cabo dicha elección gremial, habiéndose recibido, atendido y evaluado.
- Segundo: El Comité Electoral optò por contratar a una de las tres empresas convocadas[203], la empresa escogida, afirma el Comité

[201] Según Comunicado del Comité Electoral del Ilustre Colegio de Abogados de Lima, el 50% de los miembros hábiles (aproximadamente 37.000), sufragaron en la primera vuelta del 28 de Noviembre en forma electrónica no presencial.
[202] Ibidem
[203] La Empresa HIPER S.A. es la empresa que ha sido encargada por el Comité Electoral del Colegio de Abogados de Lima, de llevar a cabo el proceso de votación electrónica presencial y no presencial.

Electoral: otorga transparencia, seguridad y confianza, siendo la entidad que llevara a cabo el proceso del Voto Electrónico, en primera y segunda vuelta, si fuera el caso, porque cumple, a criterio del Comité, con los siguientes requisitos:

- A) Solución Integral (Hardware, Software, Operación, Soporte). Esta solución implica prever la utilización de computadoras, tabletas y otros dispositivos electrónicos, software de votación electrónica, operación de las maquinas y sistemas, soporte técnico frente a contingencias.
- B) Instalación y desmontaje de sesenta (60) cabinas de votación. En las elecciones celebradas se distribuyeron estas cabinas de votación en tres locales del Ilustre Colegio de Abogados de Lima: Miraflores, Palacio de Justicia y Cono Norte.
- C) Infraestructura basada 100% en Cloud Services (Nube). Lo que significa que la información producida en el proceso electoral se procesa y almacena en la "nube" y puede accesarse desde cualquier punto, previa identificación de las personas autorizadas con privilegios de acceso vigentes.
- D) Implementación Sufragio electrónico presencial.
  "Se dice que el proceso de votación es presencial cuando se identifica manualmente al elector, autorizándolo a utilizar una máquina —que en este caso genéricamente se denomina DRE (direct recording electronic) o sistema de registro electrónico directo— dispuesta en un lugar específico (colegio electoral). En dicho caso, el proceso de identificación es independiente y no debe de existir la posibilidad de relacionarlo con el voto depositado. De esta manera, toda la información necesaria está in situ; por tanto, se utiliza para ello un equipo específico"[204].

- E) Implementación de Sufragio electrónico remoto (Computadoras, Laptops y dispositivos móviles)

  "Cuando el voto es ejercido no presencialmente, es decir, de forma remota, a través de Internet —votación telemática— , el

[204] PANIZO ALONSO, Luis: "Aspectos Tecnológicos del Voto Electrónico". Lima. Oficina Nacional de Procesos Electorales (ONPE) 2007. Documento de Trabajo 17. Página 17. Información publicada en http://www.web.onpe.gob.pe/modEducacion/Publicaciones/I-2-2-017.pdf

sistema lo hace todo (identificar y enviar el voto) y, probablemente, con independencia del dispositivo (ordenador personal o equipamiento equivalente)"[205].

- F) Impresión de Votos No Remotos (en impresora instalada en CAL). En la votación electrónica presencial una vez identificada la persona y emitido su voto electrónicamente, se imprime su voto y se deposita en un ánfora como respaldo en caso de ser necesario un cotejo.
- G) Implementa Mesa de Votación (Presencial y No Presencial). Los equipos y personal necesario fueron proporcionados por la empresa contratada.
- H) Validación Biométrica. Se menciona un proceso de recarnetizacion con archivo de huella digital para ser almacenado en circuito integrado a ser incorporado en los nuevos carnets. La fecha a de entrega de carnets se han programado para fecha posterior del proceso electoral electrónico. Por tanto, en este proceso[206] no se utilizó la validación biométrica, la verificación de la identidad en el voto electrónico presencial se hizo con el cotejo visual en base al carnet anterior o su respectivo documento nacional de identidad.
- I) Pantallas intuitivas y fáciles de usar. Implementa Escrutinio de Votos. Cierre y Emisión de Reportes. Backup de Auditoria. Soporte Presencial y Remoto. Capacitación (antes, durante y después de la elección). Simulacro de elección.
- J) Procesamiento de votos. Proceso de segunda vuelta. Prototipo técnico. Plan de trabajo detallado. Plan de seguimiento y control del proyecto. Sistema de aseguramiento de la calidad del software. Seguridad.
- Tercero: El Comité Electoral del Colegio de Abogados de Lima, afirma que el proceso de Elecciones 2016-2017, que el Comité Electoral viene elaborando es un proceso integral con las siguientes características:

[205] PANIZO ALONSO, Luis: ob.cit. Página 18.
[206] De la primera vuelta realizada el 28 de Noviembre y el de la segunda vuelta del 12 de Diciembre de 2015, de las elecciones de la Junta Directiva del Ilustre Colegio de Abogados de Lima..

- I) Seguridad, confidencialidad y auditabilidad.
- II) Resultados casi inmediatos (Según cierre cada mesa).
- III) Voto Electrónico Presencial y Remoto.
- IV) Votos impresos para Escrutinio manual, si se requiere.
- V) Validación Biométrica de Identidad (VE Presencial)
- VI) Clave Web y Clave Especial Única para Votación (VENP)
- VII) Solución y Servicios Integrales: Hardware, software, operación, soporte y Backup.
- VIII) Soporte presencial y remoto: Call center de apoyo al usuario.

3.4. Lineamientos sobre el Ente Rector del Sistema Funcional propuesto

Para la propuesta de establecer un sistema funcional de Identidad Digital, Protección de Datos, hay que tener en cuenta que: "Los sistemas están a cargo de un Ente Rector que se constituye en su autoridad técnica-normativa a nivel nacional, dicta las normas y establece los procedimientos relacionados con su ámbito; coordina su operación técnica y es responsable de su correcto funcionamiento en el marco de la presente ley , sus leyes especiales y disposiciones complementarias"[207].

En la Política de Estado Peruano 24[208]: Afirmación de un Estado eficiente y transparente se afirma: "Nos comprometemos a construir y mantener un Estado eficiente, eficaz, moderno y transparente al servicio de las personas y sus derechos…". Por tanto el Ente Rector que asuma autoridad técnica normativa del sistema funcional propuesto de contribuir con su organización y tecnología a defender y proteger el derecho a la identidad digital de la persona en Internet.

[207] Ley Nº 29158, Ley Organica del Poder Ejecutivo, articulo 44.
[208] En http://acuerdonacional.pe/politicas-de-eestado-del-acuerdo-nacional/ . Vid. CUEVA VALVERDE, Enrique: "Ingeniería, Planificación y Desarrollo", donde se explican los grandes objetivos del Acuerdo Nacional. En: www.cip.org.pe/index.../158_9b07fe4268cf3283c4f9eefa1ce2dc8d.html . *Fecha de consulta: 28 de Noviembre del 2015.*

El Ente Rector del sistema funcional propuesto de identidad digital, protección de datos personales, certificación y registro Digital debe ser el Registro Nacional de Identificación y Estado Civil (RENIEC) por los siguientes fundamentos:

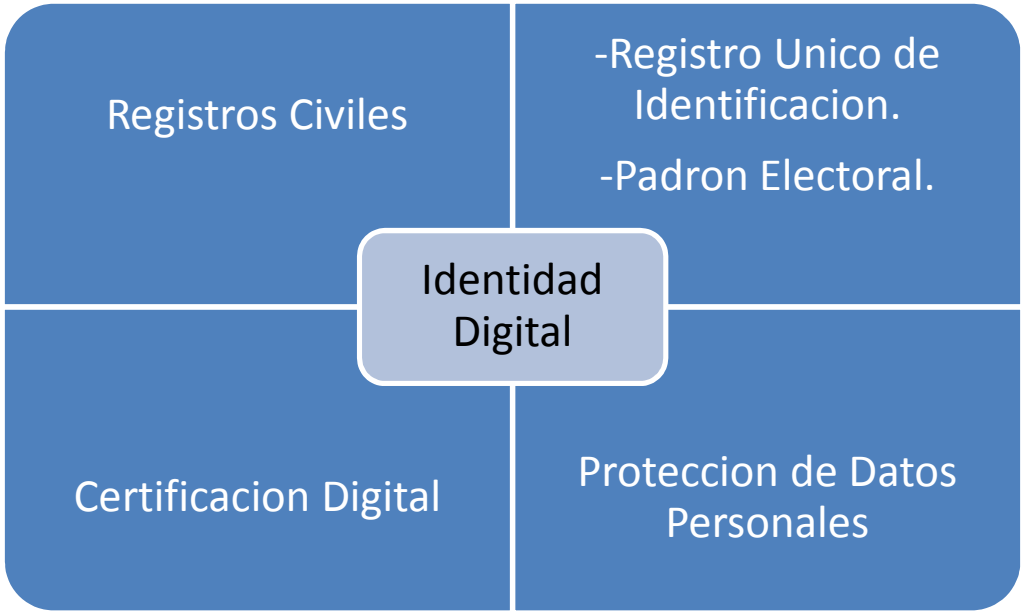
a) Conforme el artículo 183º de la Constitución Política del Perú, el RENIEC tiene a su cargo "la inscripción de nacimientos, matrimonios, divorcios, defunciones y otros actos que modifican el estado civil. Emite las constancias correspondientes. Prepara y mantiene actualizado el Padrón Electoral. Proporciona al Jurado Nacional de Elecciones (JNE) y a la Oficina Nacional de Procesos Electorales ONPE la información necesaria para el cumplimiento de sus funciones. Mantiene el registro de identificación de los ciudadanos y emite los documentos que acreditan su identidad. Ejerce las demás funciones que la ley señala".

b) Conforme el artículo 48º del D.S. 052-2008-PCM el RENIEC será la única Entidad de Certificación Nacional del Estado Peruano y actuara también como Entidad de Certificación del Estado Peruano y Entidad de Registro o Verificación para el Estado Peruano: Todas las Entidades de Certificación del Estado Peruano y las Entidades de Registro o Verificación para el Estado Peruano deben seguir las políticas y estándares propuestos por la Entidad de Certificación Nacional para el Estado Peruano aprobados por la Autoridad Administrativa Competente.

c) Es necesario modificar el artículo 32º de la Ley 29733, Ley de Protección de Datos Personales y designar al RENIEC como Autoridad Nacional de Protección de Datos Personales en sustitución del Ministerio de Justicia, que ejerce esta función a través de la Dirección General de Protección de Datos Personales.

d) El Proyecto de Ley de Identidad Digital fortalece el derecho de la identidad digital y la inclusión digital para su utilización de servicios de gobierno y comercio electrónico seguros, utilizando para tal efecto como documento nacional de identidad electrónico (DNI). Por tanto, es necesaria la aprobación de la ley respectiva.

e) Con estos supuestos el Sistema Funcional de Identidad Digital, Protección de Datos Personales, certificación y registro digital estaría conformado de la siguiente forma:



Este sistema Funcional propuesto tendría en RENIEC el Ente Rector y permitiría que la institución asegure el cumplimiento de la política pública propuesta coordinando la participación de todas o varias Entidades del Estado para lograr proteger y regular adecuadamente el derecho de la identidad digital en Internet. En Registros civiles se registran el nacimiento, el matrimonio, el divorcio, la muerte, la viudez; todos estos datos personales inciden en la protección coherente de la identidad digital.

Conforme la Ley Nº 26497, RENIEC es un "organismo autónomo que cuenta con personería jurídica de derecho público interno y goza de atribuciones en materia registral, técnica, administrativa, económica y financiera". Le corresponde planear, dirigir, coordinar y controlar las actividades de registro e identificación de las personas. Entre sus funciones tiene la de "velar por el irrestricto respeto del derecho a la intimidad e identidad de la persona y los derechos inherentes a ella derivados de su inscripción en el registro.

f) Conforme la Ley Nº 26497, modificada por la Ley 30338, RENIEC administra la plataforma de interoperabilidad electrónica en materia domiciliaria con la finalidad de articular esta información geo-referenciada con las Entidades del Sistema Electoral y demás entidades que así lo requieran.
g) El Proyecto de Ley de Identidad Digital establece que RENIEC debe elaborar el Modelo de E-inclusión y la metodología de diseño de servicios y procedimientos. Asimismo, establece que RENIEC conjuntamente con ONGEI deben elaborar el Plan Nacional de Identidad Digital.

3.5. Procesos Electrónicos donde el Sistema Funcional de Identidad Digital, Proteccion de Datos, Certificación y Registro Digital tiene incidencia.

3.5.1. Comercio Electrónico y Negocios Electrónicos

El comercio electrónico global, promovido por el desarrollo de Internet, será un motor importante para el crecimiento de la economía mundial del siglo XXI. "El comercio electrónico ofrece nuevas oportunidades para los negocios y ciudadanos de todas las regiones del mundo. En particular, las compañías pequeñas podrán conseguir un acceso sin precedentes a los mercados mundiales a bajo coste y los consumidores podrán escoger entre un amplio abanico de

productos y servicios"[209]. El mundo desarrollado ha emprendido un transición de una economía industrial a otra basada en la información.

El comercio electrónico aumentará la productividad en todos los sectores de nuestras economías, además de promover el intercambio de bienes y servicios y la inversión, creará nuevos sectores de actividad, nuevas formas de marketing y venta, nuevos sistemas de obtención de ingresos, nuevos puestos de trabajo. La liberación de los servicios particularmente de los servicios básicos de telecomunicaciones, juega un papel clave en el crecimiento del comercio electrónico.

Con respecto al Comercio Electrónico, debemos distinguir distintas modalidades de llevarlo a cabo: a) Empresa-Empresa (Bussines to Bussines) que implica operaciones y negocios electrónicos en la actividad empresarial que incluye la complementación económica y otras transacciones del mercado virtual. Como por ejemplo empresas que se complementan entre sí en sus procesos de producción en cuánto a la producción de insumos, envases u otros materiales necesarias realizando el planeamiento y control de la producción en forma electrónica. Es la modalidad que tiene más desarrollo en internet y con mayor rapidez en su crecimiento. b) Empresa-Consumidor (Bussines to Consumer) que supone las operaciones y negocios entre las empresas y los consumidores individualizados según sus necesidades que son atendidas en línea y satisfechas con eficiencia en corto tiempo y con menos costos. C) Gobierno Digital (e-goverment) que implica que las actividades gubernamentales estén al servicio del ciudadano y este pueda acceder a sus servicios en un entorno virtual con eficiencia y rapidez.

El uso de la información cambiará las reglas de la competencia comercial. Por cuánto la expansión del comercio electrónico global estará orientado esencialmente al mercado y será manejada por la iniciativa privada. El papel de los gobiernos es proporcionar un marco legal claro y consistente, promover un entorno competitivo en el que el

[209] Declaración Conjunta Unión Europea y Estados Unidos sobre Comercio Electrónico. En Contract-soft onnet. URL:http://www.onnet.es/08001009.htm. Fecha de acceso: 13 de Diciembre de 1999.

comercio electrónico pueda florecer y asegurar la protección adecuada de objetivos de interés público como la intimidad, los derechos de propiedad intelectual, la prevención del fraude, la protección del consumidor y la seguridad nacional.

En el Perú, la legislación del Comercio Electrónico recientemente ha tenido un intenso desarrollo con la dación de normas sobre la transmisión de datos y tarifa plana en Internet, protección al consumidor, de los datos personales y del derecho de autor aplicables al comercio electrónico, modificaciones al código civil sobre el acto jurídico electrónico y la contratación electrónica, la dación de la ley sobre firmas y certificados digitales que incluye normativa sobre la firma electrónica en general, títulos valores electrónicos, prueba del documento informático, delitos informáticos y otros temas relacionados.

En cuanto a la solución de las implicancias jurídicas que origina Internet, éstas están intrínsecamente relacionadas con la dación de la normatividad aplicable al Comercio Electrónico. En este sentido, hay que tener en cuenta que "Internet ha ofrecido nuevas posibilidades más ágiles, baratas y rápidas para comerciar electrónicamente de un lado, a través del almacenamiento y reenvío de mensajes (correo electrónico) y, por otro, a través de transacciones electrónicas interactivas (on line). Su mayor virtud, aunque también su principal riesgo, radica en que se trata de una red abierta a la que puede acceder cualquier persona.. Esta circunstancia justifica la necesidad de establecer mecanismos de seguridad" [210]. Esta seguridad debe ser tanto jurídica como técnica.

"El término "negocio electrónico", "negocio virtual" o e-business, se refiere a las a las actividades de comercio por Internet, que van desde la compraventa de productos y servicios hasta la colaboración con socios de negocios. IBM acuñó el término en 1997, dando a Wall

[210] RECALDE CASTELLS, Andrés : "Comercio y Contratación Electrónica" . En Revista Iberoamericana de Derecho Informático. Nºs 30,31,32 sobre Jornadas de Contratación Electrónica, Privacidad e Internet. UNED, Mérida, España. 1999. Página 42.

Street una llamada de atención para que pusiera sus ojos sobre las dimensiones de las nuevas redes de intercambio global. Hoy en día, las grandes empresas están revisando sus estrategias de negocio para incluir la cultura de Internet. Las empresas están comprando piezas y suministros en línea, se están promocionando en sitios web e incluso están recopilando en línea todos los datos para sus investigaciones de mercado. Los negocios electrónicos son convenientes y están a la vanguardia. Amazon.com es sólo un ejemplo exitoso de lo que un negocio electrónico puede llegar a ser"[211].

3.5.2. Gobierno Electrónico

El Gobierno Electrónico consiste en el uso que hace tanto el gobierno central como los gobiernos locales de las Tecnologías de información y comunicaciones, en particular Internet, para mejorar los servicios e información ofrecidos a los ciudadanos, incrementar la eficiencia y eficacia de la gestión pública, proveer a las acciones de gobierno un marco de transparencia y crear mecanismos para facilitar la participación ciudadana en la toma de decisiones de la administración pública.

"La implantación del Gobierno Electrónico comporta el reconocimiento por parte de los Estados Iberoamericanos del derecho de los ciudadanos a relacionarse electrónicamente con sus Gobiernos y Administraciones Públicas. Lo que supone que las Administraciones estén interrelacionadas entre sí a fin de simplificar los procedimientos. Las leyes de acceso a la información pública establecidas en algunos países de la región apuntan en esa dirección"[212].

Conforme el artículo 40º del Decreto Supremo Nº 052-2008-PCM: "el ciudadano tiene el derecho al acceso a los servicios públicos a través de medios electrónicos seguros para la realización de transacciones

[211] http://www.ehowenespanol.com/ejemplos-negocios-electronicos-ebusinesses-info_113401/ Fecha de consulta 23 de Octubre de 2014.
[212] CARTA IBEROAMERICANA DE GOBIERNO ELECTRÓNICO Aprobada por la IX Conferencia Iberoamericana de Ministros de Administración Pública y Reforma del Estado Pucón, Chile, 31 de mayo y 1° de junio de 2007 Adoptada por la XVII Cumbre Iberoamericana de Jefes de Estado y de Gobierno Santiago de Chile, 10 de noviembre de 2007 (Resolución No. 18 de la Declaración de Santiago).

de gobierno electrónico con las entidades de la administración pública , como manifestación de voluntad y en el marco establecido en la Ley de Procedimiento Administrativo General – Ley Nº 27444".

Por Decreto Supremo N°081-2013-PCM, publicado el miércoles 10 de Julio de 2013, se ha aprobado la Política Nacional de Gobierno Electrónico 2013-2017.

La Política Nacional de Gobierno Electrónico se 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, Plan de Desarrollo de la Sociedad de la Información en el Perú, aprobada mediante Decreto Supremo N° 066-2011-PCM.

La Política Nacional de Gobierno Electrónico 2013-2017, ha sido desarrollado con la participación de entidades del Estado, sector privado, sociedad civil y la académica. Se han realizado talleres en diversas regiones del país, entre las que se encuentran Arequipa, La Libertad, Puno, Cusco, Tacna Madre de Dios, Piura, Ucayali, Ayacucho, Apurímac y Loreto, en las cuales se han recogido iniciativas y sugerencias vinculadas a actividades y proyectos regionales sobre el desarrollo del Gobierno Electrónico, lo cual hace que esta Política cuente con el consenso e identificación nacional en su desarrollo.

La Presidencia del Consejo de Ministros a través de la Oficina Nacional de Gobierno Electrónico e Informática- ONGEI, como ente Rector del Sistema Nacional de Informática, en el marco del proceso de Modernización y Descentralización del Estado con inclusión social, y le desarrollo del Gobierno Electrónico en el país, presenta la Política Nacional de Gobierno Electrónico 2013-2017.

La Política Nacional de Gobierno Electrónico, es el principal instrumento que permitirá el desarrollo y despliegue el Gobierno Electrónico en el Perú. Es de alcance nacional y cumplimiento obligatorio por parte de todas las entidades de la Administración Pública a nivel del gobierno nacional, gobiernos regionales y gobiernos

locales, las mismas que se implementan en el ámbito de sus funciones y competencias.

"El Gobierno Electrónico en el Perú se encuentra en una etapa de fortalecimiento de los marcos normativos y regulatorios que permitan soportar necesidades futuras de comunicación, participación, seguridad y transparencia. La infraestructura tecnológica del Perú todavía se encuentra en una desventaja frente a otros países de la región, con niveles bajos de penetración de acceso a Internet, telefonía celular y banda ancha".

"El Gobierno Electrónico constituye una materia transversal a todas la entidades de la administración pública y por ende es responsabilidad de todas las autoridades, funcionarios y servidores del Estado".

Los objetivos de la Política Nacional de Gobierno Electrónico 2013-2017, son los siguientes:
-Fortalecer el gobierno electrónico en las entidades de la administración Pública, garantizando su interoperabilidad y el intercambio de datos espaciales con la finalidad de mejorar la prestación de los servicios brindados por las entidades del Estado para la sociedad, fomentando su desarrollo.
Acercar el Estado a los ciudadanos de manera articulada, a través de las tecnologías de la información que aseguren el acceso oportuno e inclusivo a la información y participación ciudadana como medio para contribuir a la gobernabilidad, transparencia y lucha contra la corrupción en la gestión del estado.

-Fomentar la inclusión digital de todos los ciudadanos, a través del Gobierno Electrónico, especialmente de los sectores vulnerables, a través de la generación de capacidades y promoción de la innovación tecnológica respetando la diversidad cultural y el medio ambiente.

-Promover a través del uso de las tecnologías de la información y en coordinación con los entes competentes la transformación de la sociedad peruana en una Sociedad de la Información y el Conocimiento, propiciando la participación activa de las entidades del Estado y la sociedad civil, con la finalidad que sea íntegra, democrática, abierta, inclusiva y brinde oportunidades para todos.

Se han establecido los siguientes lineamientos estratégicos para el desarrollo del Gobierno Electrónico en el Perú:

-Transparencia.- Promover el conocimiento de la gestión del Estado a través de nuevos canales que permitan la participación del ciudadano en las funciones públicas con información confiable, oportuna y accesible. Además la transparencia generará mayor visibilidad de los asuntos del Estado y contribuirá a los objetivos de la Política Nacional de Modernización de la gestión Pública.

-E-inclusión.- Incluir a todos los ciudadanos sin distinción de origen, credo, idioma, sexo, edad u otra variable de exclusión a la Sociedad de la Información y el Conocimiento a través de proyectos y programas de Alfabetización Digital que permiten el fortalecimiento de las capacidades de los ciudadanos.

-E-Participación.- Generar la participación activa del ciudadano a través de su Identidad Digital en la gestión pública a través de plataformas de Internet como redes sociales, foros, chats en línea u otras formas de interacción a fin de satisfacer eficientemente necesidades de información, control y consultas públicas en nuevas Políticas de Estado.

E-Servicios.- Habilitar los medios electrónicos necesarios al ciudadano para que pueda accedea los servicios públicos por medios electrónicos seguros, a través del uso de su identidad digital, con seguridad, comodidad y satisfacción desde cualquier lugar. E-Servicios necesita de un rediseño de los procesos en las entidades del Estado, así como el aseguramiento de estándares tecnológicos en interoperabilidad (web-services). Adicionalmente, se requiere construir una plataforma tecnológica intergubernamental que facilite los servicios, trámites y consultas del ciudadano. Finalmente, se necesita apoyar las iniciativas de identidad digital, firmas y certificados digitales, mecanismos de seguridad para la privacidad y protección de datos en general y datos personales en particular.

Tecnología e innovación.- Se debe promover el crecimiento de la Tecnología e Innovación a través de la provisión de una Infraestructura adecuada a través del desarrollo de plataformas que permitan llevar a cabo innovaciones impulsando la cultura emprendedora y, al mismo tiempo dando respuestas a problemáticas sociales concretas.

Seguridad de la Información.- El paradigma de todo a disposición de todos debe manejarse de la manera más cuidadosa, velando por la integridad, seguridad y disponibilidad de los datos, apara ello se debe establecer lineamientos en seguridad de la información a fin de mitigar el riesgo de exposición de información sensible al ciudadano.

Infraestructura.- El requisito fundamental para la comunicación efectiva y la colaboración dentro del Estado es contar con una red informática y de telecomunicaciones que integre a todas las dependencias y a sus funcionarios públicos, incluyendo hardware, software, sistemas, redes, conectividad a la internet, base de datos, infraestructura para la capacitación en línea (e-learning) y recursos humanos especializados.

Como factores críticos de éxito, para garantizar el éxito en la difusión, uso y alineamiento de las diferentes entidades del Estado con la Política nacional de Gobierno Electrónico, se necesita del compromiso y cumplimiento de los siguientes factores: i) Apoyo Político al más alto Nivel. b) Liderazgo Institucional y compromiso interinstitucional. c) Disponibilidad de recursos: financieros, humanos y tecnológicos. d) Conectividad y Accesibilidad a nivel nacional. e) Contar con un marco normativo actualizado en materia de Gobierno Electrónico. f) Difusión, capacitación y sensibilización en Gobierno Electrónico.

Es necesario señalar que el Gobierno Electrónico está en constante evolución llegando a evolucionar en el denominado gobierno abierto y el gobierno inteligente[213] donde la identidad digital tiene un papel cohesionador fundamental. La convergencia tecnológica de la computación en la nube, los grandes datos (bigdata), los smartphones, las redes sociales, la internet de las cosas y la impresión en tercera

[213] Según la consultora Gartner la fusión del Gobierno abierto y del gobierno inteligente da lugar al Gobierno Digital. Vid. http://www.gartner.com/newsroom/id/3069117 Fecha de consulta Agosto de 2015.

dimensión y su aplicación al ámbito gubernamental han permitido la evolución del gobierno electrónico donde el ciudadano y su identidad digital es el centro de atención y el paradigma en los servicios gubernamentales electrónicos seguros.

En el Derecho Comparado, es necesario asimismo, tener en cuenta el caso italiano con el Decreto del Presidente del Consejo de Ministros de Italia del 24 de Octubre de 2014 sobre la Definición de la características del sistema público de la gestión de la identidad digital (SPID). El contenido de esta norma es la siguiente: Definiciones. Objeto y finalidad. Sujetos participantes en el sistema público de gestión de la identidad digital (SPID). Rol de la Agenzia del SPID. Atributos de la Identidad Digital. Seguridad. Expedición de la Identidad Digital. Gestión de la Identidad Digital. Uso Ilícito de la Identidad Digital. Acreditación del Gestor de la Identidad Digital. Obligaciones del Gestor de la Identidad Digital. Cesación y revocación de la actividad del gestor de identidad digital[214].

La identidad digital es expedida a solicitud del interesado, al gestor de la identidad digital, previa verificación de la identidad mediante la entrega de una modalidad segura de la credencial de acceso. Este decreto del Presidente del Consejo de Ministros de Italia tiene como base legal el Decreto Legislativo del 21 de Junio de 2013 que regula el sistema público de la gestión de la Identidad Digital (SPID).

Asimismo, es necesario tener en cuenta la Electronic Identity Mangement Act de Virginia (Estados Unidos de Amèrica) que entró en vigor el 01 de Julio de 2015[215]. Esta norma regula la identidad electrónica en temas como identificación, firma, integridad, fecha, prueba de envió y recepción, fiabilidad, seguridad de datos.

3.5.3. Aprendizaje Digital

[214] Decreto del Presidente del Consjeo de Ministros de Italia del 24 de Octubre de 2014. Gazzeta Ufficiale de la Republica Italiana. 09 de Diciembre de 2014.
[215] https://log1.state.va.us/cgi-bin/legp504.exe?151+ful+CHAP0483. Fecha de Consulta: 08 de Enero de 2016.

A) El aprendizaje electrónico y la Alfabetización Digital.

Conforme el artículo 44 del Reglamento de la Ley de Promoción de Banda Ancha y Construcción de Red Dorsal Nacional de Fibra Optica, aprobado por D.S. N° 014-2013-MTC: "El Ministerio de Educación, en coordinación con el ONGEI y el Ministerio de Transportes y Comunicaciones diseñará el Plan Nacional de Alfabetización Digital, poniendo especial énfasis en la formulación de contenidos educativos y aplicaciones orientados a la fácil comprensión de los educandos, adultos mayores, minorías idiomáticas, personas con discapacidad y demás grupos étnicos y culturales ; complementando dicha labor con actividades orientadas al fortalecimiento de capacidades, el uso y aprovechamiento de las tecnologías de la información y comunicaciones, herramientas informáticas y terminales (computadoras, tabletas, teléfonos inteligentes, entre otros)".

B) El aprendizaje electrónico a nivel escolar y la identidad digital.

"Cabe señalar que, la intervención del MTC permitirá la articulación de las políticas de Banda Ancha con las políticas educativas, facilitando que éstas se diseñen y apliquen en una realidad concreta predefinida por la tecnología (conectividad, protocolos, aplicaciones, terminales de Banda Ancha) y en un mercado que cuenta con disparidades en el grado de desarrollo. A su vez, la participación de ONGEI permitirá que la alfabetización se coordine con las políticas de Gobierno Electrónico, en modo tal que pueda priorizarse la enseñanza de aplicativos que, por ejemplo, faciliten la provisión de servicios a cargo del Estado, promuevan la eficiencia en el desempeño de la Administración Pública, o impulsen la competitividad"[216]

C) El aprendizaje electrónico a nivel universitario y la identidad digital.

Conforme la Ley Universitaria 30220, publicada el 09 de Julio de 2014, se establece lo siguiente:

[216] Exposición de Motivos del Reglamento de la Ley N° 29904, Ley de Promoción de la Banda Ancha y construcción de Red Dorsal Nacional de Fibra Optica. Diario Oficial El Peruano. Jueves, 13 de Junio de 2013. Lima, Perú. Página 497078.

a) "La universidad es una comunidad académica orientada a la investigación y la docencia, que brinda una formación humanista, científica y tecnológica con una clara conciencia de nuestro país como realidad multicultural. Adopta el concepto de educación, como derecho fundamental y servicio público esencial. Está integrada por docentes, estudiantes y graduados …" (art.3º)
b) Dentro de los fines de la universidad tenemos: "preservar, acrecentar, y transmitir de modo permanente la herencia científica, tecnológica, cultural y artística de la humanidad". (art. 6, numeral 6.1) y "afirmar y transmitir las diversas identidades culturales del país· (art. 6, numeral 6.7.).
c) Son funciones de la universidad la formación profesional; investigación; extensión cultural y proyección social; educación continua; contribuir al desarrollo humano. (art. 7).
d) Las universidades pueden desarrollar programas de educación a distancia, basados en entornos virtuales de aprendizaje. Los programas de educación a distancia deben tener los mismos estándares de calidad que las modalidades presenciales de formación. (art. 47).
e) Para ser elegido Rector se requiere tener el Grado Académico de Doctor, el mismo que debe ser obtenido con estudios presenciales. (art. 61, numeral 61.3).
f) Son requisitos para ser Decano "tener grado de Doctor o Maestro en su especialidad, el mismo que debe haber sido obtenido con estudios presenciales" (art. 69, numeral 69.3).
g) Para ser profesor principal se requiere grado de Doctor el mismo que debe haber sido obtenido con estudios presenciales. (art. 83, numeral 83.1). Lo que implica una discriminación para los estudios virtuales, la que debe ser corregida legislativamente.

D) Importancia del Sistema Funcional de Identidad Digital, Protección de Datos Personales, Registro y Certificación Digital para el Aprendizaje electrónico.

Con un sistema funcional de Identidad Digital, Protección de Datos Personales, Registro y Certificación Digital los proceso de aprendizaje digital podrán efectuarse con seguridad, certeza, confianza, permitiendo una adecuada planificación del uso de las Tecnologías de Información y Comunicaciones a nivel nacional en todos los niveles escolares y de educación superior.

En la Sociedad de la Información donde tenemos “nativos digitales” los niveles de aprendizaje digital se extienden desde muy temprana edad hasta los adultos mayores. Por lo cual un sistema funcional de identidad digital coadyuva a una mayor seguridad jurídica en Internet.

El documento nacional de identidad electrónico acredita presencialmente y virtualmente la identidad de una persona en Internet, permitiendo que el docente se identifique, que los alumnos se identifiquen y se forme la clase virtual donde cada parte interviniente en el proceso de enseñanza virtual tenga la certeza de quien está enseñando, quien está aprendiendo y quien está evaluando en un entorno electrónico seguro.

Capítulo 4:

Problemática e Hipótesis. Investigación de Campo

4.1. Problemática

En este capítulo planteamos la problemática desarrollada en esta investigación, que es la siguiente:

a) La protección y regulación jurídica del derecho de identidad digital en internet debe ser adecuada y suficiente. El problema es cómo lograr sistematizar el derecho aplicable en internet que dé seguridad a las personas naturales o jurídicas intervinientes acreditando su identidad.
b) El derecho de identidad digital permite garantizar el ejercicio de los derechos de las personas en internet. El problema es determinar cómo el Estado debe garantizar al ciudadano el

ejercicio de sus derechos armonizando las políticas proteccionistas del Estado y la legislación informática existente.

c) Los procesos electrónicos para realizarse en forma segura deben basarse en una identidad digital fehaciente. El problema es cómo regular esta identidad digital para que las personas eviten el uso fraudulento de las múltiples identidades y la suplantación de identidad.
d) La relación que se entabla por Internet es siempre un acto jurídico bilateral en el que no hay certeza ni de la identidad, ni de la capacidad de las partes, siendo inciertos igualmente los domicilios que se señalan. No existe seguridad jurídica suficiente para las partes intervinientes en la relación jurídica bilateral que se entabla por Internet, aun cuando ésta no tenga implicancias patrimoniales, pudiendo vulnerar la buena fe, la moral y las buenas costumbres. El eje central de esa problemática está en la certeza y la garantía de la identidad de las partes

   ¿Puede el Derecho procurar a la humanidad y, específicamente, a la sociedad nacional la solución de esa problemática? ¿Qué podemos hacer frente a esta problemática planteada utilizando la visión sistémica del Derecho Informático?

4.2. Hipótesis

Para superar la problemática planteada, considero que es necesario un sistema funcional digital mediante el cual el documento credencial electrónico emitido por èl garantice la identidad digital formal. Las hipótesis son las siguientes:

a) Este problema se va a resolver estableciendo un sistema funcional de identidad digital donde el documento credencial electrónico garantice la identidad digital formal por parte del Estado en Internet.
b) Para garantizar a las personas el ejercicio seguro de sus derechos en las relaciones plurilaterales ejercidas mediante técnicas informáticas es necesario que este sistema funcional de

identidad digital integre la protección de datos personales y el uso de las firmas y certificados digitales, estableciéndose una legislación sistemática en torno a la identidad digital que cohesione y sistematice en forma jerárquica las instituciones jurídicas relacionadas al derecho informático en Internet.

c) Para regular la identidad digital y evitar el uso indebido de las múltiples identidades es necesario que se establezca una política de Estado, se cree por ley un sistema funcional y establezca un ente rector, que coordine la acción efectiva de las instituciones del Estado para dotar de seguridad jurídica a las personas para darle seguridad jurídica al ciudadano en internet, tanto nacional como internacionalmente, para lo cual debiera proponerse un Tratado Internacional de Seguridad Informática. Derecho Informático con su enfoque sistémico, permite dar una solución jurídica eficaz a la regulación y protección del derecho de identidad digital en internet.

En la contratación electrónica, los contratos informáticos y los "smart contracts" o contratos inteligentes, la identidad digital formal debe tener un papel fundamental dando certeza en cuanto a la identidad de las partes, a su capacidad, su domicilio y datos e información que generen confianza y seguridad en el ciberespacio. La identidad digital fortalece la seguridad jurídica de las partes intervinientes en la relación jurídica bilateral que se entabla en Internet, teniendo o no implicancias patrimoniales. La identidad digital garantiza y da certeza a la buena fe de las partes en Internet y asegura el desarrollo de la economía digital a nivel global.

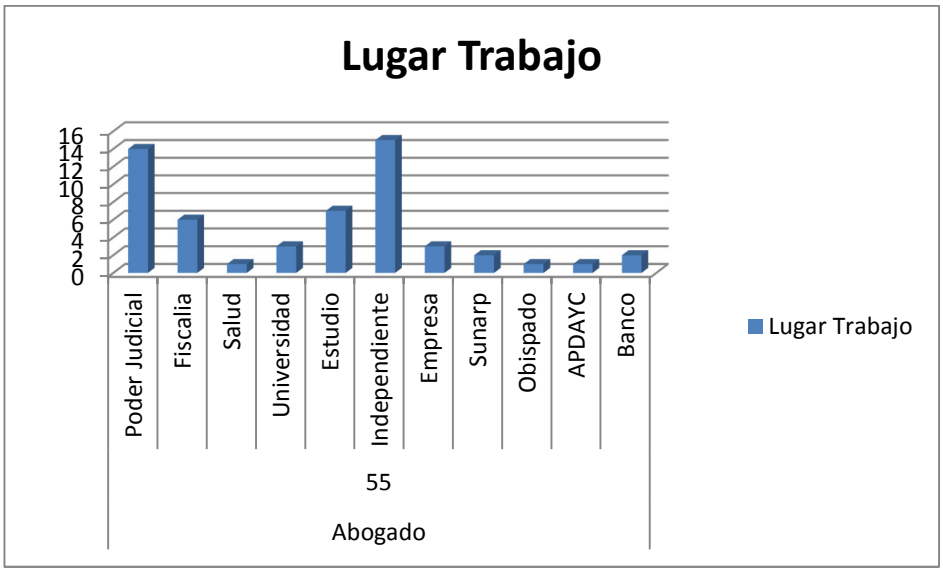
4.3. Instrumentos de campo aplicados

4.3.1. Encuestas.

- Encuestas a alumnos de la Maestría de Derecho Constitucional y Gobernabilidad de la UNPRG, en el curso de Metodología de Investigación.
- Encuesta a alumnos del curso de Derecho Informático en la carrera de Ingeniería de Tecnologías y Sistemas de la Universidad ESAN.

- Encuesta a alumnos del curso de Derecho de las Nuevas Tecnologías en la carrera de Derecho Corporativo en la Universidad ESAN.
- Encuestas a alumnos de Curso para ejecutivos de Seguridad de la Información (CISO).

- **I. Identificación de las personas encuestadas**

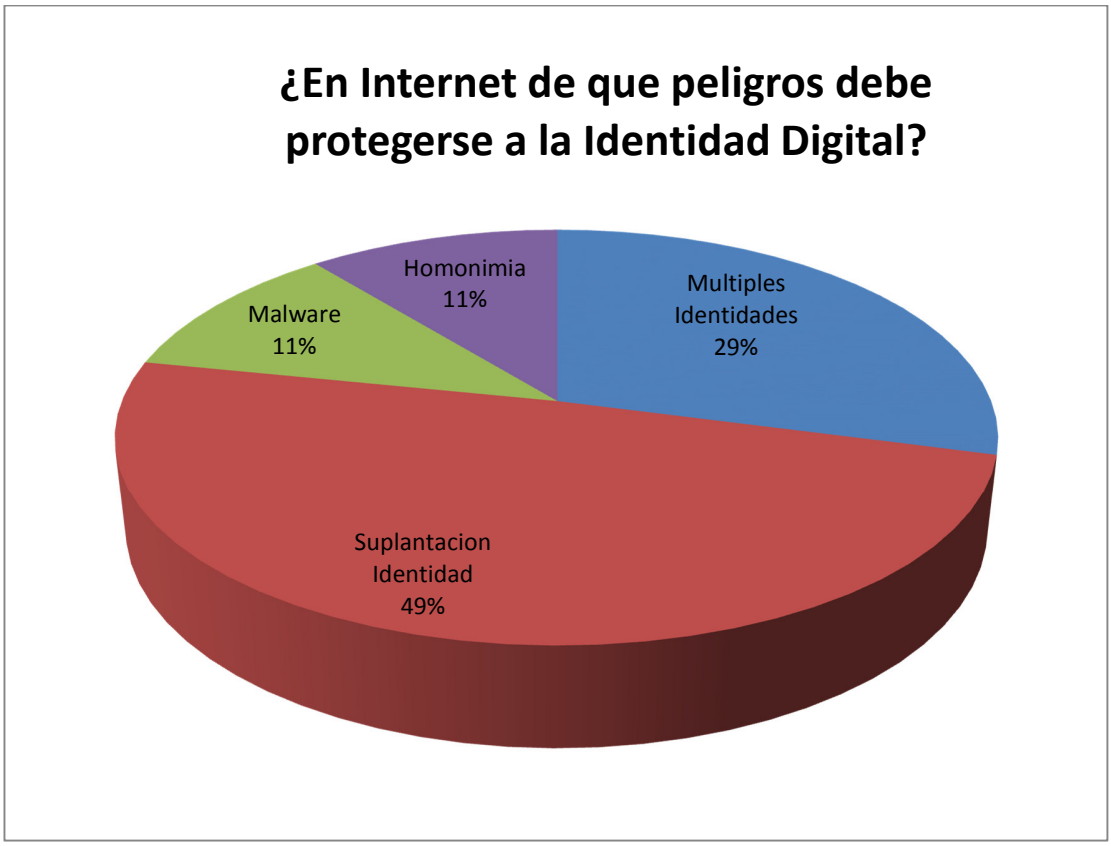


-

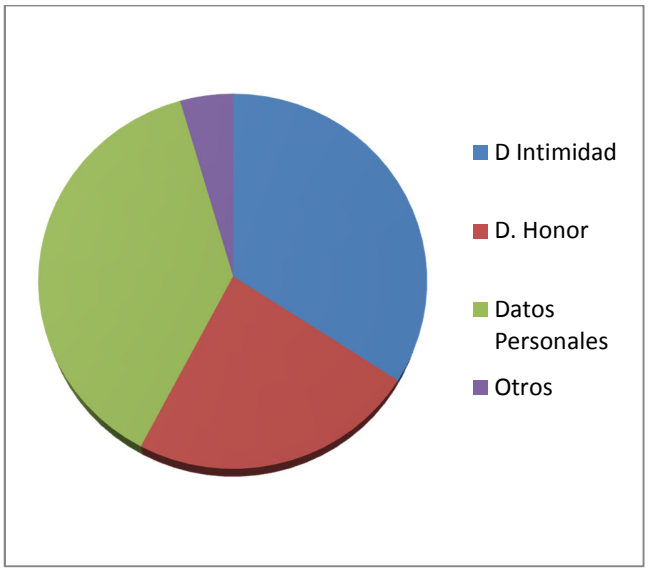
Profesion	Nº Profesion	Trabajo	Lugar Trabajo
Abogado	55	Poder Judicial	14
		Fiscalia	6
		Salud	1
		Universidad	3
		Estudio	7
		Independiente	15
		Empresa	3
		Sunarp	2
		Obispado	1
		APDAYC	1
		Banco	2

II. Sobre Identidad en Internet

A) En Internet de que peligros debe protegerse la Identidad Digital?

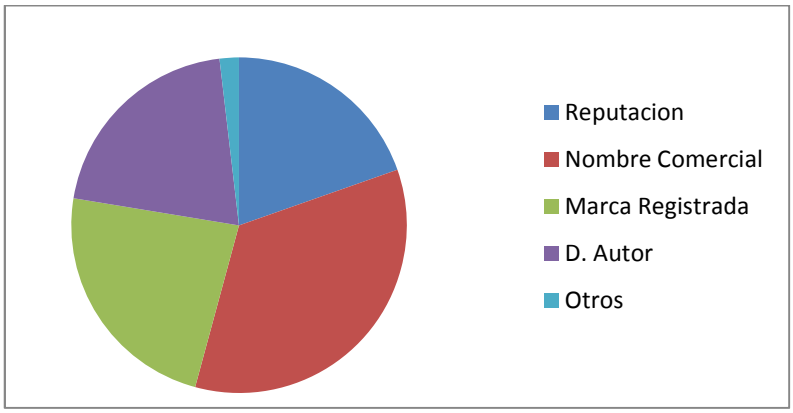


B) En Internet proteger la identidad de la persona natural permite proteger los siguientes derechos:



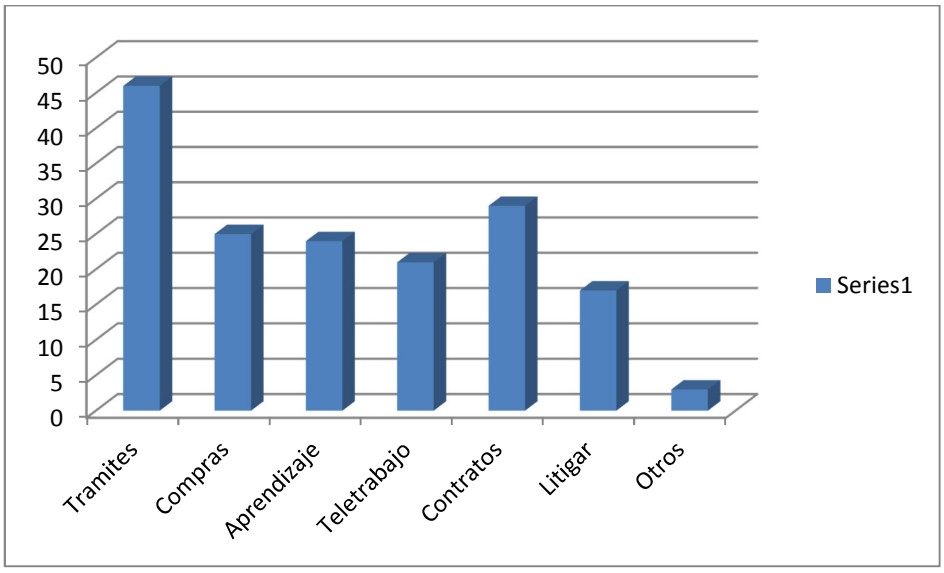
D Intimidad	D. Honor	Datos Personales	Otros
38	26	42	5

C) En Internet proteger la identidad de la persona jurídica permite proteger los siguientes derechos:



Reputacion	Nombre Comercial	Marca Registrada	D. Autor	Otros
21	37	25	22	2

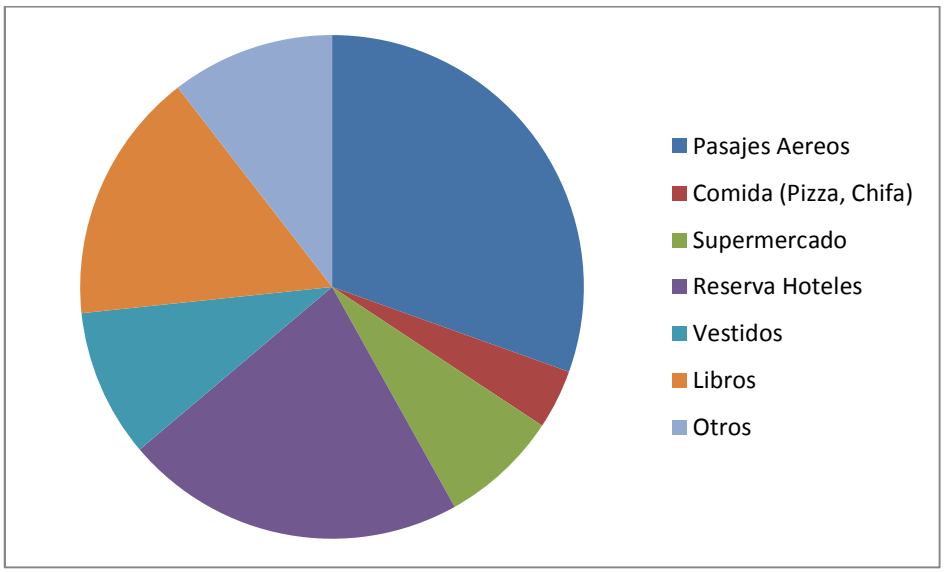
D) ¿Qué ventajas tendría para usted tener un Documento Nacional de Identidad Electrònico?



Tramites	Compras	Aprendizaje	Teletrabajo	Contratos	Litigar	Otros
46	25	24	21	29	17	3

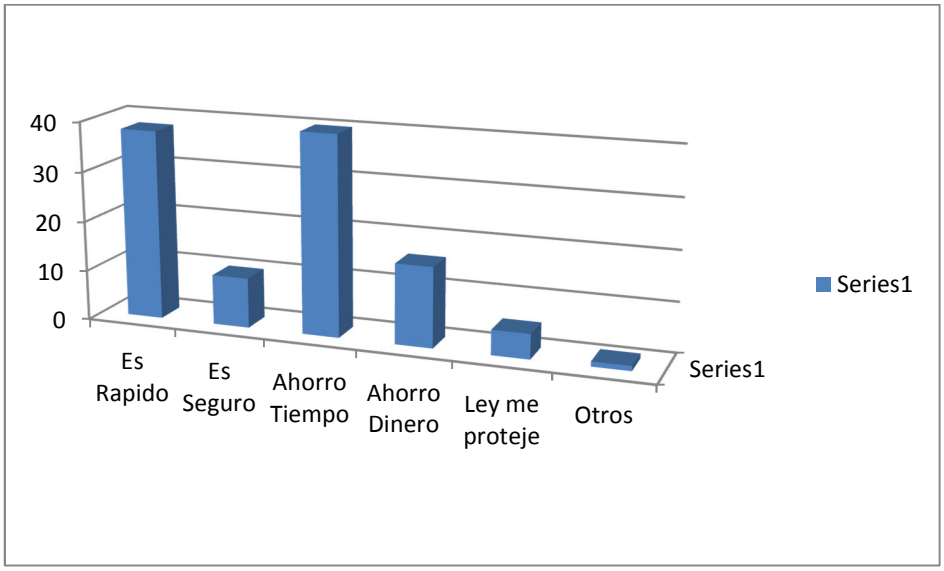
III. Identidad Digital en el Comercio Electrónico

E) Marque las opciones que correspondan, si usted ha realizado alguna de estas operaciones de comercio electrónico por Internet:

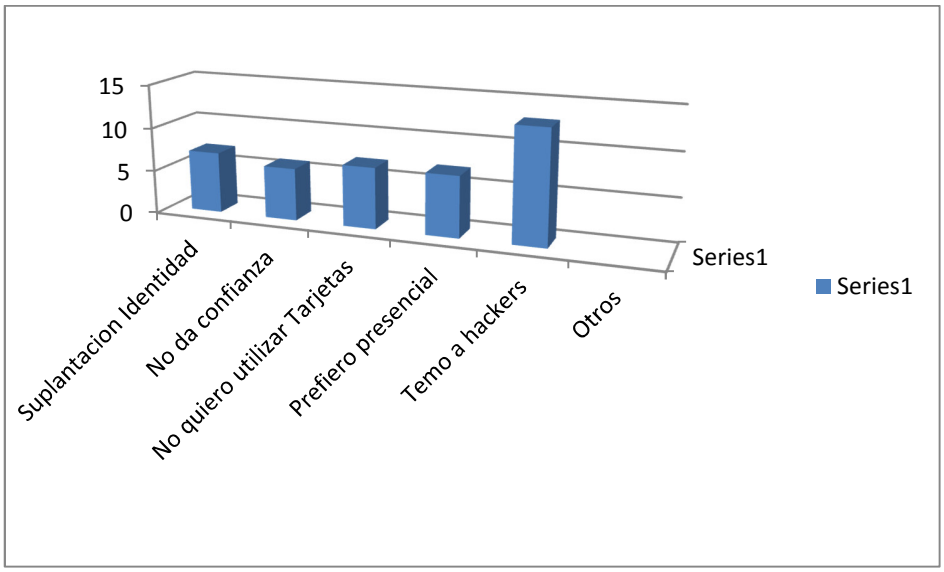


Pasajes Aereos	Comida (Pizza, Chifa)	Supermercado	Reserva Hoteles	Vestido
32	4	8	23	

F) ¿Qué razones le convencen para si realizar operaciones de comercio electrónico?

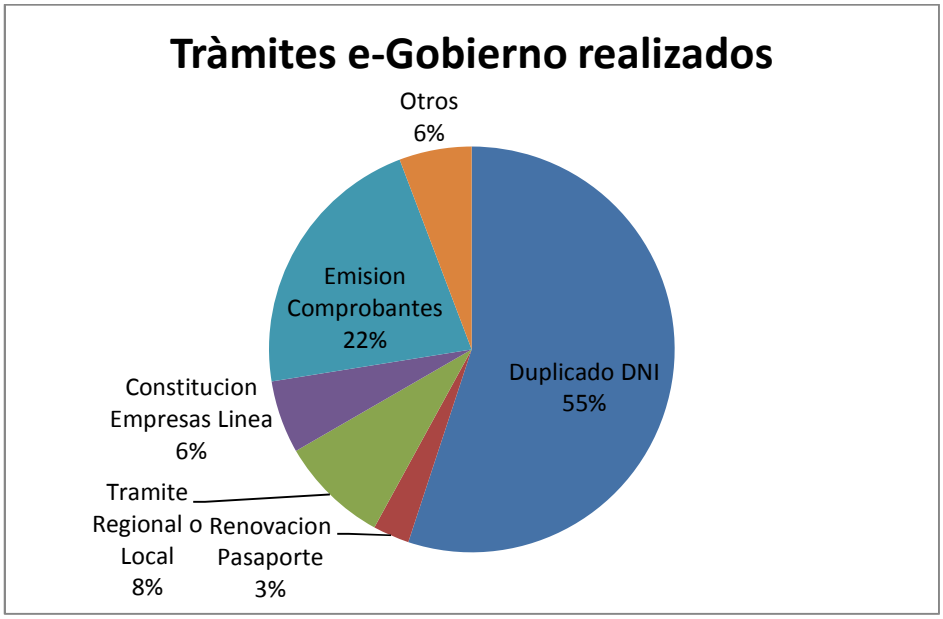


G) Si la respuesta es NO, señale las razones por las que no ha realizado operaciones de comercio electrónico:

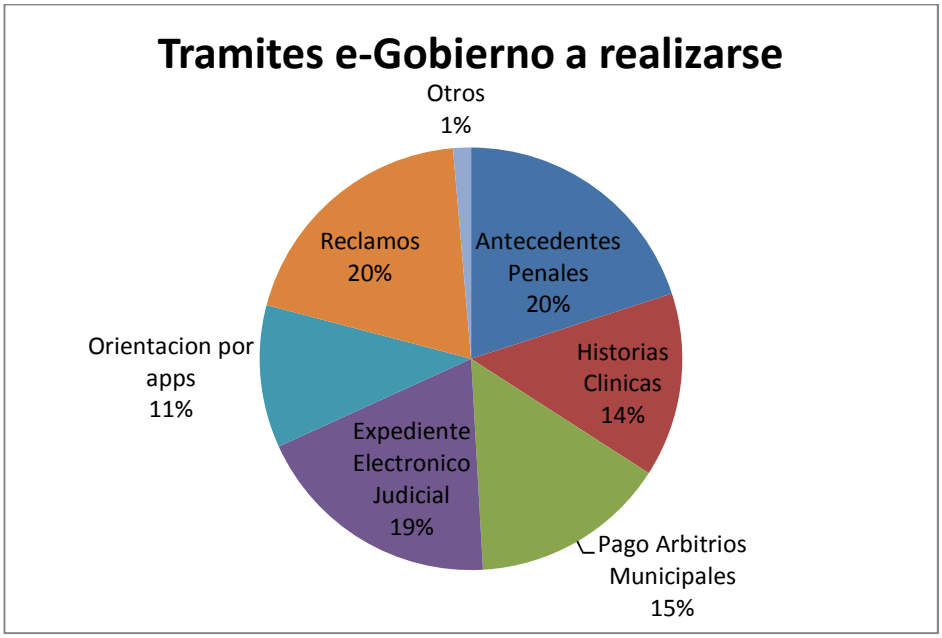


IV. Identidad Digital en el Gobierno Electrónico

H) ¿Qué trámites de Gobierno Electrónico ha hecho usted por Internet?

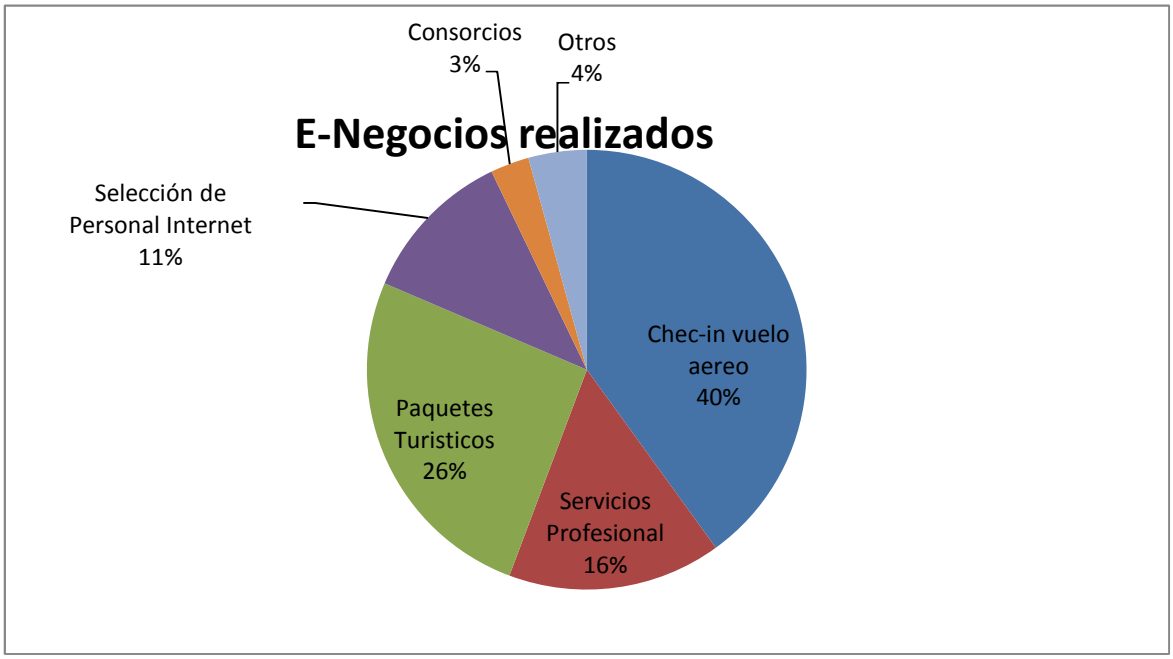


I) ¿Qué trámites de los siguientes utilizaría si se implementaran en el contexto del Gobierno Electrónico?

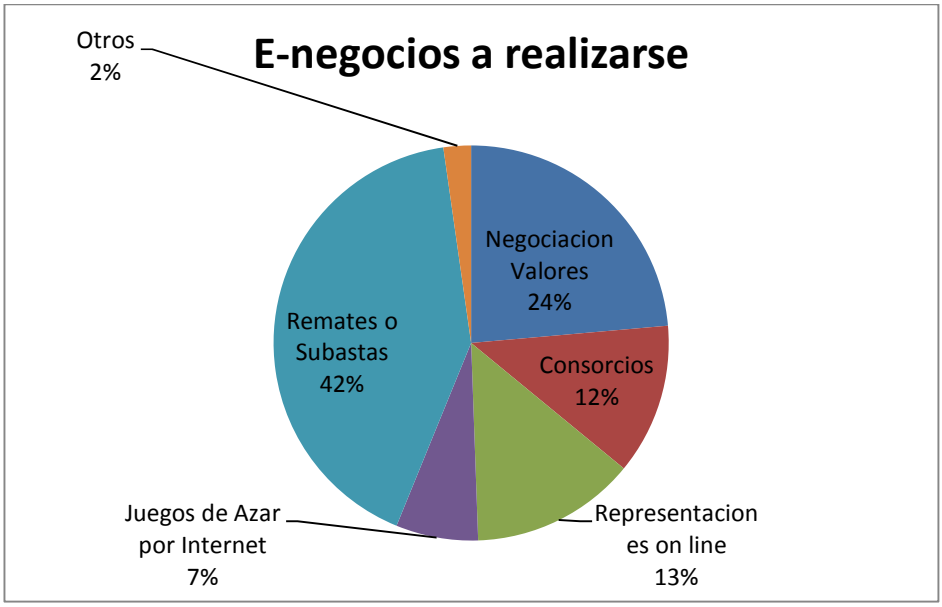


V. Identidad Digital en los Negocios Electrónicos

J) ¿Qué actividades de Negocios Electrónicos ha hecho usted por Internet?

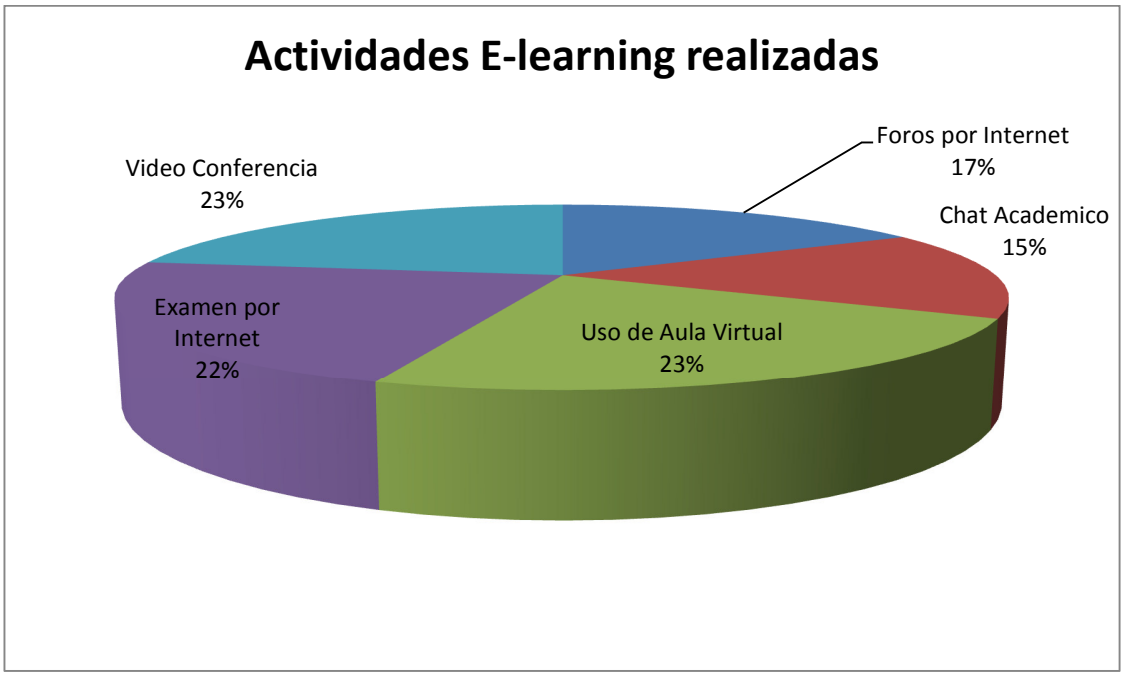


K) ¿Què actividades de negocios electrónicos estaría dispuesto a realizar en forma segura?

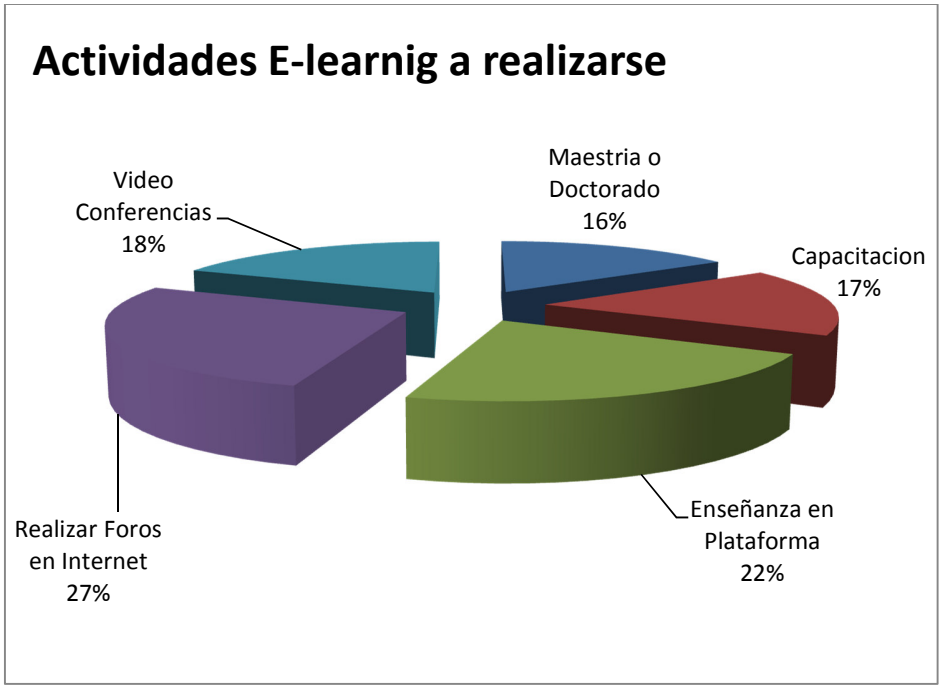


VI. Identidad Digital en el Aprendizaje Electrónico

L) ¿Qué actividades relacionadas al Aprendizaje electrónico a realizado usted?



LL) ¿Què actividades de aprendizaje electrónico estaría usted dispuesto a realizar en un entorno seguro?



M) ¿Por qué es importante un sistema funcional de identidad digital?

Respuestas:

a) Porque la Identidad Digital es necesaria para ejercer los derechos de la persona en Internet. 69%
b) Porque si cada Entidad Publica pide una identidad digital diferente van a proliferar las multiples identidades generando inseguridad.

- **4.3.2. Entrevista.**
- **Entrevista al Dr. Thomas J. Smedinghoff.**
- Thomas Smedinghoff es Experto estadounidense de Chicago en Derecho Informático. Representante de Estados Unidos desde 1997 a la fecha en UNCITRAL (Comisión de Naciones Unidas para el Derecho Mercantil Internacional) , su práctica profesional se centra en las nuevas cuestiones jurídicas relacionadas con el campo en desarrollo de la ley de las tecnologías de la

información y actividades comerciales electrónicas. Tom es reconocido internacionalmente por su liderazgo al abordar las cuestiones jurídicas emergentes respecto a las transacciones electrónicas, gestión de identidad , privacidad, seguridad de la información , y los problemas de autenticación en línea , tanto desde el punto de vista transaccional y la política pública. Ha sido contratado para estructurar e implementar iniciativas de la primera de su tipo de comercio electrónico, transacciones electrónicas, y gestión de la identidad y de las infraestructuras jurídicas seguridad de la información para el gobierno federal y las empresas nacionales e internacionales, incluyendo bancos, compañías de seguros, sociedades de inversión , y las autoridades de certificación. También ha participado activamente en el desarrollo de la legislación y las políticas públicas en el área de comercio electrónico a nivel estatal, nacional, e internacional.

- La entrevista fue realizada en Agosto de 2015, en el contexto del Seminario Internacional de Identidad Digital[217], donde Thomas Smedinghoff fue Expositor.
- Las preguntas y respuestas[218] fueron las siguientes:

Pregunta 1: ¿Según su experiencia, ¿Qué importancia tiene la Legislación sobre Identidad Digital para el Gobierno Electrónico?

Respuesta 1: Estoy consciente que tanto el gobierno de los Estados Unidos como el gobierno del Reino Unido están buscando activamente el uso de la identidad digital en conexión con la prestación de servicios públicos. De igual modo, la Regulación de las Identidades Digitales recientemente adoptada en la Unión Europea está diseñada para permitir a los ciudadanos de cualquier país de la Unión Europea a utilizar la Identidad digital emitida para ellos en dicho país en conexión con la obtención de acceso a los servicios del gobierno en otro país de la UE.

[217] Seminario Internacional de Identidad Digital, Lima 5, 6 y 7 de Agosto de 2015. Organizado por RENIEC. Certificado por la UNMSM Facultad de Ingeniería de Sistemas e Informática. Lugar. Auditorio de la UTP.
[218] Las preguntas y respuestas fueron formuladas en ingles. Han sido traducidas por el autor con asesoría de la Licenciada Mirtha Orihuela, traductora del idioma inglés al español. Se adjunta como anexo el texto original en inglès.

En los Estados Unidos. Estados Unidos está buscando el desarrollo de un programa de identidad digital para propósitos de permitir a los ciudadanos a acceder a los servicios gubernamentales/del gobierno en línea. Dicho programa es llamado "Connect Gov". El objetivo es utilizar los proveedores de identidad del sector privado para emitir credenciales de identidad digital a ciudadanos individuales. Esto no operaría como un identidad digital nacional, y las personas podrían obtener una credencial digital de cualquiera de los muchos proveedores de identidad del sector privado autorizados por el gobierno federal. Ellas podrían entonces utilizar dichas credenciales digitales para acceder a los servicios gubernamentales/del gobierno en línea. Esta información está disponible en http://www.connect.gov/.

En el Reino Unido. En el Reino Unido el gobierno también está buscando un programa similar, es el programa "GOV.UK.Verify". Igual que el programa de los Estados Unidos, el objetivo de GOV.UK.Verify es utilizar los proveedores de identidad del sector privado para emitir credenciales de identidad digital para los ciudadanos individuales. Esto no operaría como un Identificacion nacional, y las personas podrían obtener una credencial digital de cualquiera de los muchos proveedores de identidad del sector privado autorizados por el gobierno del Reino Unido. Más información disponible en https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify

En la Unión Europea. La Unión Europea también se ha comprometido activamente en un programa para facilitar el uso de identidades digitales emitido por cualquier país de la UE para las transacciones del sector público con gobiernos en otro país de la Union Europea. Para lograr dicho objetivo, la Unión Europea adoptó su Regulación de Identidad electrónica en Julio del 2014. La Regulación de la Identidad Electronica se centra en sistemas de identidad que emiten credenciales para el uso de transacciones en línea con organismos del sector público. Su objetivo principal es el reconocimiento mutuo de dichas credenciales en las transacciones del sector público en el extranjero. Así, la Regulación de Identidad electronica habilita a los individuos que tienen una credencial de identidad emitida en cualquier estado miembro de la Union Europea para usar la misma credencial para tener acceso a servicios públicos en línea en otro Estado miembro. La regulación de la Identidad electrónica (técnicamente denominada "Regulación (UE) No.

910/2014 del Parlamento Europeo y del Consejo del 23 de julio de 2014 sobre identificación electrónica y servicios la confianza… para las transacciones electrónicas en el mercado interno y la Directiva derogada 1999/93/EC") está disponible en varios idiomas en: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv: OJ.L_.2014.257.01.0073.01.ENG.

Legislación. No creo que ni los programas de gobierno electrónico de los E.E.U.U. ni los del Reino Unido mencionados líneas arriba contemplen la aplicación de cualquier nueva legislación. En lugar de ello, aparecen persiguiendo aquellos programas usando lo que me referí en mi charla como ley privada de "Nivel 3" (basada en un contrato). Sé, por ejemplo, que el gobierno del Reino Unido ha firmado contratos que dirigen la operación de su sistema de identidad del Gobierno electrónico con ocho proveedores de identidad por separado. Creo que el gobierno de los E.E.U.U. está haciendo algo similar. Sin embargo, en ambos casos entiendo que los proveedores de identidad han expresado su preocupación sobre diversos problemas, incluyendo responsabilidad, y se han presentado por lo menos algunas discusiones sugiriendo que dicha legislación sobre este problema podría ayudar.

La Unión Europea, por el contrario, está utilizando la legislación para lograr sus metas en relación a la identidad del Gobierno electrónico. Específicamente, porque el foco del esfuerzo de la unión europea es permitir el uso internacional de las credenciales para los servicios gubernamentales (por ejemplo, un ciudadano de cualquier país puede utilizar la credencial de identidad que se le emitió a él en ese país para tener acceso a los servicios gubernamentales de otro país de la UE), se consideró que dicha legislación (conocida como la Regulación Identidad Electrónica) era necesaria para lograr esa meta.

Mi sensación general es que muchos de los problemas de identidad se pueden abordar con un acercamiento basado en un contrato., los problemas fronterizos y asuntos internacionales a menudo requerirán de una legislación para resolverse.

Pregunta 2: ¿Cuál es la importancia para el comercio electrónico?

Respuesta 2: Desde mi punto de vista, creo que la gestión de la identidad digital es de suma importancia para el comercio electrónico, por lo menos las transacciones de comercio electrónico de naturaleza significativa. Mientras que muchos individuos pueden comprar mercancías por Internet usando una tarjeta de crédito, y sin ninguna identidad digital confiable (por lo menos en los Estados Unidos y en la Unión Europea), la identidad digital es a menudo necesaria para facilitar las transacciones que son significativas debido al monto de dinero involucrado, o la sensibilidad de la información involucrada.

Por ejemplo, la industria de defensa y aeroespacial en los Estados Unidos a menudo tiene la necesidad de permitir que los proveedores y manufactureros tengan acceso a varias bases de datos que contienen información sensible y confidencial. Dicha industria cuenta con credenciales de identidad para asegurar que solo las personas correspondientes tengan acceso a los datos solicitados.

De manera similar, la identidad digital puede ser crítica en situaciones que involucran la ejecución on-line de contratos importantes. Las firmas electrónicas que rigen según la ley hacen importante poder probar en la corte la identidad de la persona que firma.

Pregunta 3: ¿Por qué es importante la legislación de identidad digital para los negocios electrónicos y la enseñanza en línea?

Respuesta 3: Pienso que una legislación sobre identidad digital será necesaria (o por lo menos deseable) para el uso de la identidad digital en los negocios electrónicos y en el aprendizaje electrónico. . Dicha legislación podría ayudar a lograr una serie de metas importantes, incluyendo las siguientes:

. Remover las barreras para el uso de la identidad en línea que puedan existir bajo la actual legislación.

. Solucionar los problemas con la legislación existente.

. Ayudar a definir y promover la confianza en los sistemas de identidad.

. Facilitar el reconocimiento legal de la identidad y la autenticación.

. Facilitar la interoperabilidad de los sistemas de identidad en el exterior.

4.3.3. Observación.

-Observación de uso Aula Virtual de la Academia de la Magistratura en el dictado como profesor asociado del curso de Derecho Informático en Agosto y Setiembre de 2014.

-
- Se ingresa a la página web: http://www.amag.edu.pe
- Se elige el ítem Aula Virtual y se entra al siguiente sitio:
- http://aulavirtual.amag.edu.pe
- Aparece una pantalla:
- Academia de la Magistratura
- Bienvenido (a) al Aula Virtual
- Nombre del Usuario:……..
- Contraseña
- ¿Olvidó su nombre de Usuario o Contraseña?
- Acceso a la Pantalla y tengo las siguientes opciones: Agenda Académica. Biblioteca. Registro Académico. Boletín Institucional.
- Tengo también la opción de entrar al Curso Derecho Informático 18º PROFA.
- Seguidamente tengo las siguientes opciones:
- Información General:
- Hoja Informativa Nº 07-2014-AMAG SPA-PROFA.
- Espacio de Interacción:
- Foro de Consultas. Donde hay mensajes y respuestas y se puede interrelacionarse con los alumnos. Cada profesor y alumno está identificado con nombre apellido y foto.
- Material del Curso:
- Manual Auto instructivo de Derecho Informático.
- Lecturas.
- Diapositivas del Curso.
- Videos de Derecho Informático.

- Foro:
- Criterios de calificación del Foro.
- Foro/ Docente Julio Núñez/ Aula 6 Arequipa
- Restringido: "Disponibles desde el 18 de Agosto de 2014 hasta 22 de Agosto de 2014", 23:55.
- En el Foro se plantea la siguiente pregunta:
- ¿Cuáles considera que son los elementos básicos de la legislación vigente en materia de derecho y nuevas tecnologías que más se utilizan en el quehacer de jueces y fiscales?
- El alumno responde en formulario con formato virtual, donde el docente califica en línea sobre veinte.
- Chat:
- Puede comunicarse el docente con su alumnos vía chat.
- Primer Control:
- 1er Control de Lectura desde las 23:55 horas del 23 de Agosto hasta las 23:55 horas del 25 de Agosto de 2014.
- 31 alumnos del Aula 6 de Arequipa fueron calificados en este control de lectura que fue con preguntas objetivas, que el mismo sistema calificó.

- **Practica Calificada**
- La evaluación consistió en una pregunta principal calificada sobre doce puntos, desarrollado por cada alumno, redactando la respuesta en formulario virtual y dos preguntas para escoger una sola de ocho puntos también con redacción de respuesta en formulario virtual. Rindieron este examen en el curso a mi cargo del Aula 6 de Arequipa de 35 alumnos. Para calificar como docente leí cada pregunta y puse la nota, hay opción que como docente comente cada respuesta.
- Examen Final
- Fue escrito en papel y tuve que recogerlo en las oficinas administrativas y calificar las respuestas redactadas por cada alumno. Después de calificar tuve que ingresar al sistema del aula virtual para registrar las notas de cada prengunta e ingresar

el promedio final. Luego devolví los exámenes en físico a las oficinas administrativas, pero las notas ya estaban cargadas en el sistema.

- **Observación Directa de obtención del Documento Nacional de Identidad Electrónico (DNIe) en la Oficina respectiva de la Entidad de Registro Digital (EREP) de RENIEC.**

- **Fechas:** Martes 18 de Agosto de 2015 y Jueves 27 de Agosto de 2015 en las Oficina de RENIEC primero en el Centro Cívico y después en la Avenida Javier Prado en San Isidro.

- **Descripción del hecho observado:** El martes 18 de Agosto pago en la plataforma virtual de RENIEC del Centro Cívico mi tasa de S/. 40 soles por DNI electrónico y pago con mi tarjeta VISA. Con el voucher y una foto me acerco a la Oficina de EREP del Centro de Cívico de RENIEC. La señorita que me atiende amablemente me pregunta mi datos de correo electrónico y teléfono celular y si mis otros datos personales registrados en el sistema los mantengo igual. Mi respuesta es afirmativa, me hace firmar el formulario y me da mi comprobante de presentación, para recoger mi DNI electrónico en siete días hábiles.

- El Jueves 27 de Agosto me comunico por teléfono con el numero telefónico consignado en el comprobante y me indican que me acerque a la Oficina de san Isidro. A las 10 de la mañana me apersono a la oficina y con mi comprobante solicito mi DNI electrónico. Me hacen sentar y poner mi dedo índice en el huellero digital para comprobar mi identidad. Luego me entregan el Contrato de Prestación de Servicios de Certificación Digital, lo leo y firmo; las disposiciones que me llaman la atención son: El titular del DNIe se constituye en suscriptor de los certificados digitales emitidos por la ECEP-RENIEC y es el único tenedor de los mismos. La aceptación de los certificados digitales supone que el titular reconoce estar de acuerdo y acepta los términos y

condiciones contenidos en el presente documento, el cual rige sus derechos y obligaciones, asi como de la EREP-RENIEC y de la ECEP-RENIEC.

- Seguidamente la persona que me atiende me muestra mi DNI electrónico, lo coloca en el lector de tarjeta inteligente y me pide que digite mi clave de seis a ocho digitos, luego de confirmar la clave, espero un breve momento en que los certificados digitales son inyectados y luego me entrega mi DNI electrónico.
- **Comentarios:** Ha sido una experiencia importante obtener mi DNI electrónico que sustituye al DNI azul y que acredita mi identidad en forma presencial y en forma virtual.

-**Observación Directa de uso de tecnología de información de persona discapacitada visual para identificarse y comunicarse, dentro de transporte público en Lima, Perú.**

Fecha: viernes 27 de marzo de 2015. Hora: 21:05. Lugar: Lima. Trayecto del Metropolitano desde Estación Lampa-Colmena hasta Av. 28 de Julio. (Saliendo del Curso de Repaso de Inglés de la UPG de la UNMSM, para prepararme para mi examen de suficiencia en idioma inglès).

Descripción del Hecho Observado: A las 21.05 en el Paradero del Metropolitano subió una persona ciega de nacimiento pidiendo asiento preferencial, al estar los asientos ocupados, por una mujer gestante, le dieron un asiento plomo que estaba justo delante de mí, que estaba parado. Ahí observé como la persona ciega sacaba su Smartphone marca Samsung, lo prendía marcaba dos teclas con sonido y acercaba sus orejas para escuchar. Luego de su maletín saco un audífono grande y lo conecto a su celular y a sus orejas. Luego en la pantalla hizo aparecer un teclado con fila de números encima y al costado una tecla especial con símbolo resaltado en negrita. Luego escribió mensaje y se veía como con el tacto ubicaba la tecla y después de marcarla, apretaba la tecla especial y era como si escuchase cada

letra. Luego de escrito el mensaje volvía a marcar la tecla pero más tiempo y se observaba que oía la totalidad del mensaje y luego con otra tecla enviaba. Observe como se conectaba a Whatsapp y a Messenger y se vio que mando una foto.

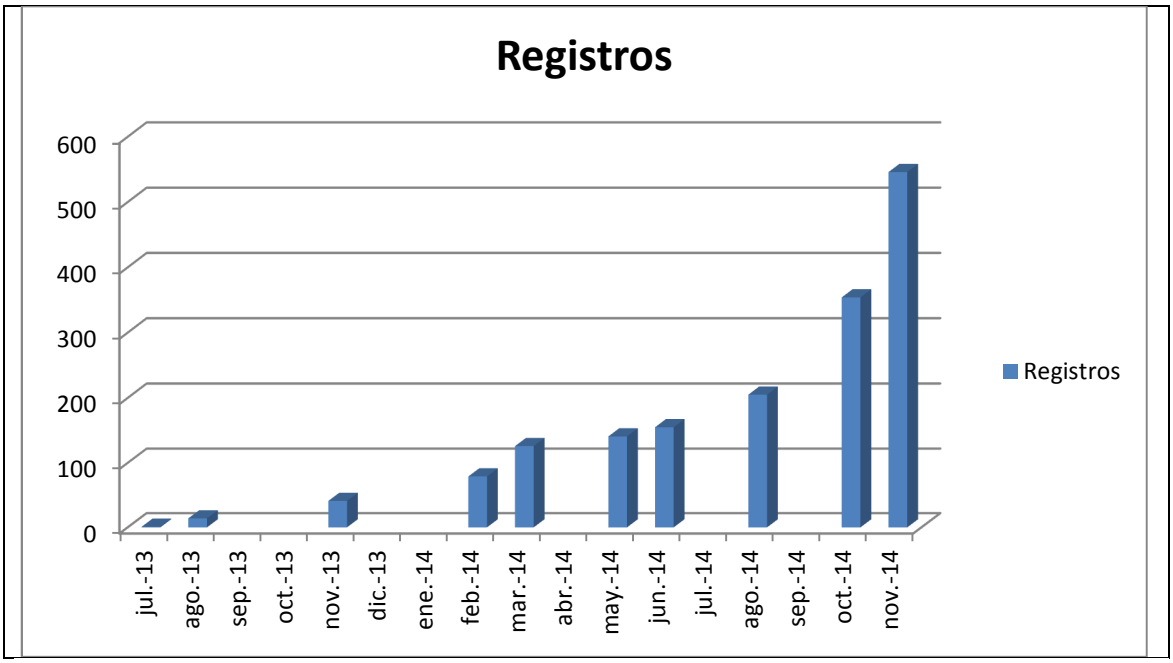
Comentarios: Esta es una muestra práctica del ejercicio de la identidad digital por una persona discapacitada que utiliza la tecnología para comunicarse y el sonido para comprobar que el mensaje es tal cual está escrito. Considero que su aplicación en el DNI electrónico es factible, porque la persona discapacitada utilizando un sistema como el descrito puede identificarse digitalmente en forma segura usando internet y dispositivos móviles.

- **4.3.4. Análisis Documental.**
- Análisis del Registro Nacional de Protección de Datos Personales, administrado por la Dirección General de Protección de Datos Personales del Ministerio de Justicia y Derechos Humanos del Perù.

- **REGISTRO NACIONAL DE PROTECCION DE DATOS PERSONALES**

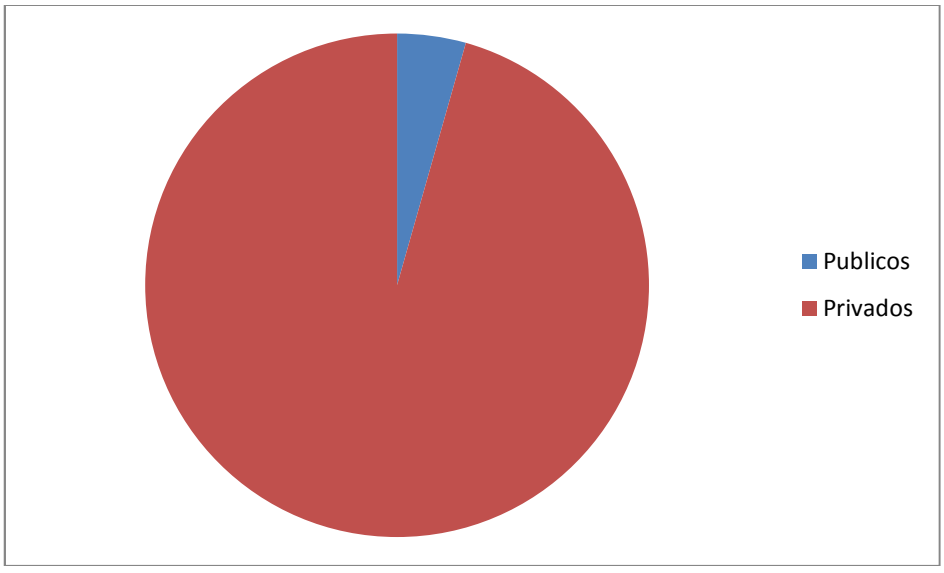
  - Al 12 de Julio de 2013 se inscribió el primer banco de datos personales en el Registro Nacional del Ministerio de Justicia.
  - Al 22 de Agosto de 2013 existían catorce (14) Banco de datos personales registrados, en el Registro Nacional de Protección de Datos Personales del Ministerio de Justicia.
  - Al 11 de Noviembre de 2013 existían cuarenta un (41) Banco de Datos personales registrados, en el Registro Nacional de Protección de Datos Personales del Ministerio de Justicia.
  - Al 14 de Febrero de 2014 existían setentainueve (79) banco de datos personales registrados, en el Registro Nacional de Protección de Datos Personales del Ministerio de Justicia.

- Al 22 de Marzo de 2014 existían ciento veintiseis (126) Banco de datos personales registrados, en el Registro Nacional de Protección de Datos Personales del Ministerio de Justicia.
- Al 22 de Mayo de 2014 existían ciento cuarenta un (141) Banco de datos personales registrados, en el Registro Nacional de Protección de Datos Personales del Ministerio de Justicia.
- Al 29 de Agosto de 2014 existían doscientos cinco (205) banco de datos personales registrados, en el Registro Nacional de Protección de Datos Personales.
- Al 16 de Octubre de 2014 existían trescientos cincuentaicuatro (354) banco de datos personales registrados, en el Registro Nacional de Protección de Datos Personales del Ministerio de Justicia.
- Al 13 de Noviembre de 2014, existían quinientos cuarenta seis (546) banco de datos personales registrados, en el Registro Nacional de Protección de Datos Personales.
- Puede verse la evolución del registro desde el 08 de Mayo del 2013 al 13 de Noviembre de 2014 , con el siguiente detalle:

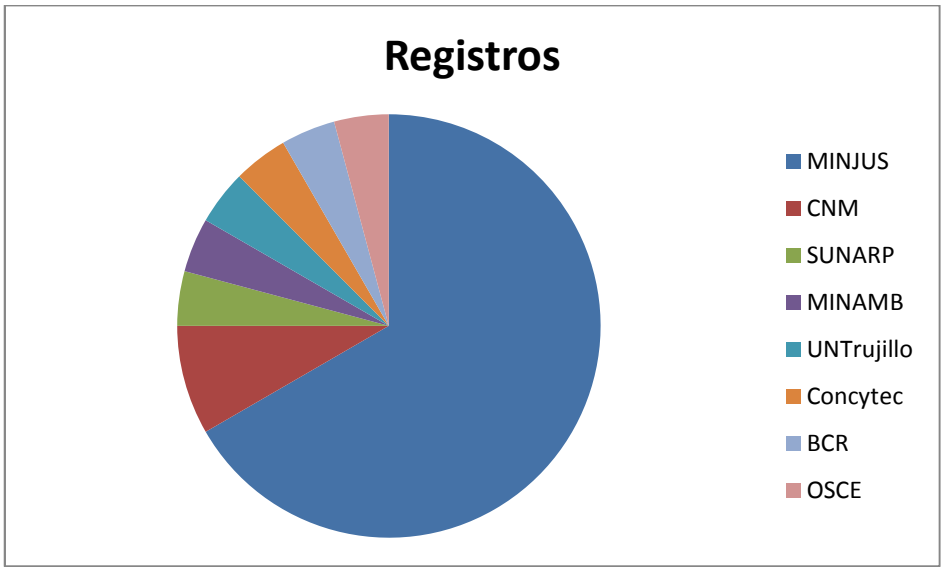


jul-13	1
ago-13	14
nov-13	41
feb-14	79
mar-14	126
may-14	141
jun-14	155
ago-14	205
oct-14	354
nov-14	546

De los 546 banco de datos personales inscritos al 13 de Noviembre de 2014, el registro de banco de datos personales de Entidades Publicas es de veinticuatro, (Ministerio de Justicia (16); SUNARP (1); Ministerio del Ambiente (1); Universidad Nacional de Trujillo (1); CONCYTEC (1); BCR (1); OSCE (1)); conforme puede apreciarse en los siguientes cuadros:

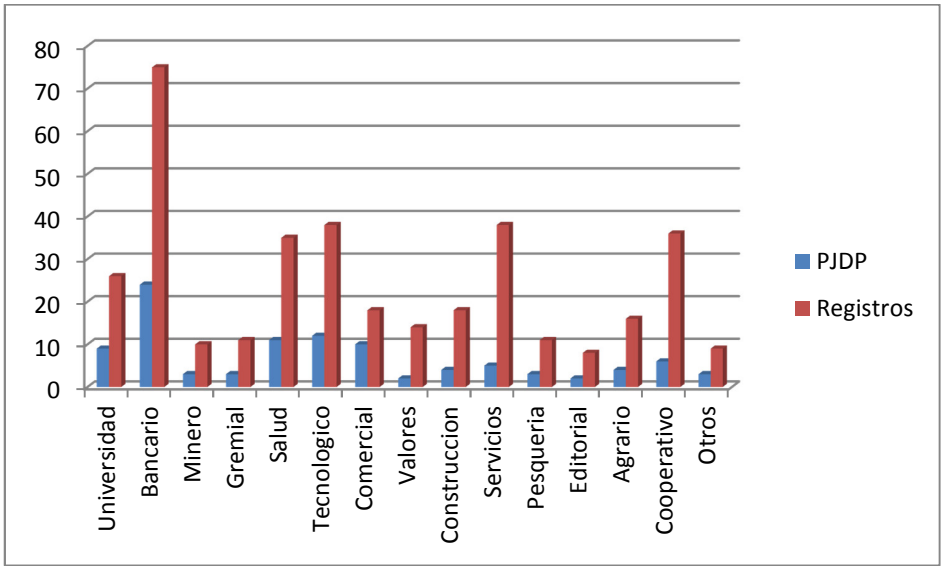


Registro de Banco de Datos Personales de Entidades Públicas: 24.
Registro de Banco de Datos Personales de Personas Jurídicas Privadas: 522.



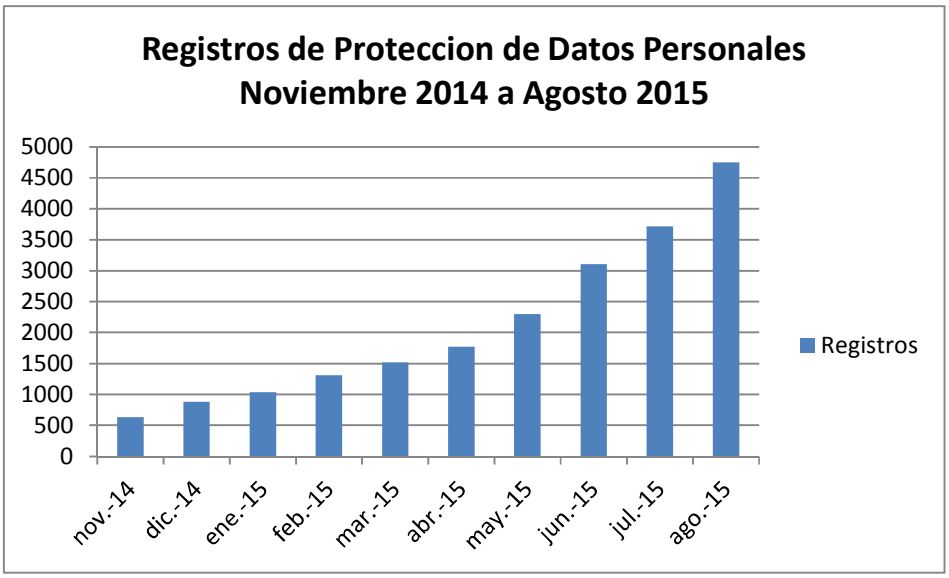
De las Entidades Públicas: MINJUS: 16 registros. CNM: 2 Registros. SUNARP: 1 Registro. MINAMB : 1 Registro. Universidad Nacional de Trujillo (UNT): 1 Registro. Concytec: 1 Registro. BCR: 1 Registro. OSCE: 1 Registro.

En los Banco de Datos Personales de Personas Juridicas de Derecho Privado identificamos en los primeros 354 banco de datos personales inscritos los siguientes:



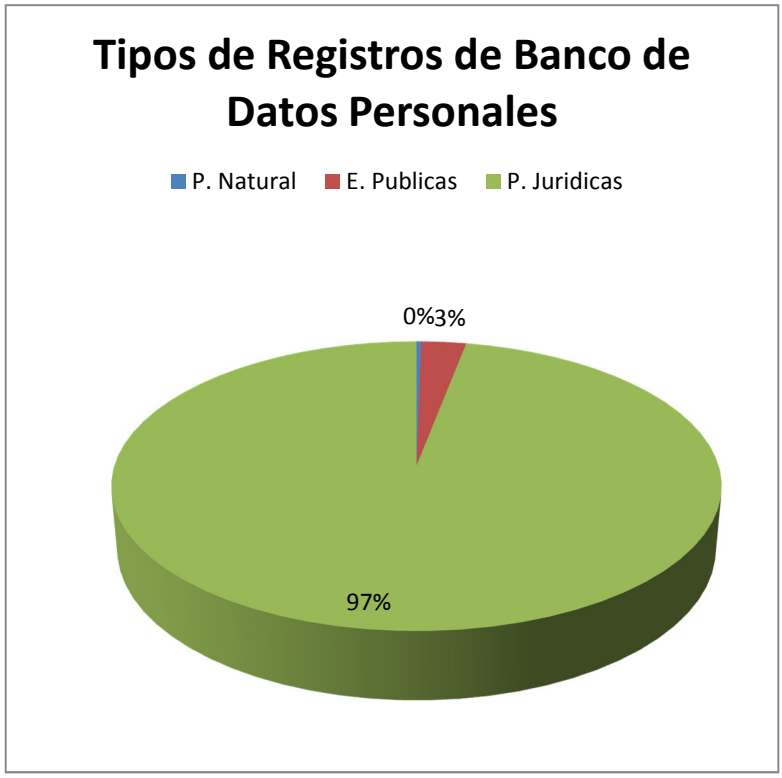
Sector	PJDP	Registros

Universidad	9	26
Bancario	24	75
Minero	3	10
Gremial	3	11
Salud	11	35
Tecnologico	12	38
Comercial	10	18
Valores	2	14
Construccion	4	18
Servicios	5	38
Pesqueria	3	11
Editorial	2	8
Agrario	4	16
Cooperativo	6	36
Otros	3	9



Mes	Registros
nov-14	632

dic-14	878
ene-15	1033
feb-15	1313
mar-15	1517
abr-15	1771
may-15	2297
jun-15	3102
jul-15	3715
ago-15	4754



P. Natural	E. Publicas	P. Juridicas
14	129	4611

Al 28 de Noviembre de 2014 se han inscrito 632 Bancos de Datos personales.
Al 23 de Diciembre de 2014 se han inscrito 878 Bancos de Datos Personales.

Al 30 de Enero de 2015 se han inscrito 1033 Bancos de Datos Personales.
Al 27 de Febrero de 2015 se han inscrito 1313 Bancos de Datos Personales.
Al 31 de Marzo de 2015 se han inscrito 1517 Bancos de Datos Personales.
Al 30 de Abril de 2015 se han inscrito 1771 Bancos de Datos Personales.
Al 29 de Mayo de 2015 se han inscrito 2297 Bancos de Datos Personales.
Al 30 de Junio de 2015 se han inscrito 3102 Bancos de Datos Personales.
Al 31 de Julio de 2015 se han inscrito 3715 Bancos de Datos Personales.
Al 26 de Agosto de 2015 se han inscrito 4754 Bancos de Datos Personales.
El 01 de Setiembre de 2015 se inscribió los Banco de Datos Personales 4794 al 4796 del Instituto Nacional de Entidades Neoplasias (INEN). Asimismo, se inscribió los Banco de Datos Personales 4816 al 4823 del Ministerio de Relaciones Exteriores.
Los tipos de Banco de Datos Personales inscritos del 28 de Noviembre de 2014 al 26 de Agosto de 2015 tenemos que son: 14 inscritos por Persona Natural. 129 inscritos por 41 Entidades Públicas. 4661 inscritos por Personas Jurídicas.

Banco de Datos Personales inscritos al 30/11/2015	
Personas Jurídicas de Derecho Publico	**372**
Personas Jurídicas de Derecho Privado	**7726**
Personas Naturales	**108**
Total	**8206**

Banco de Datos Personales inscritos al 12/02/2016	
Personas Jurídicas de Derecho Publico	**418**
Personas Jurídicas de Derecho Privado	**8600**
Personas Naturales	**165**
Total	**9183**

Procedimientos Trilaterales de Tutela presentados a la Dirección General de Protección de Datos Personales del Ministerio de Justicia del Perú, durante al año:

Nº	Procedimiento Trilateral de Tutela	Sumilla
1	2015 016-2015-JUS/DGPDP 16 de junio de 2015	**Derecho de cancelación.** El reclamante solicitó la tutela del derecho a la **cancelación** de sus datos personales en la **Empresa Editora El Comercio S.A.**La APDP solicitó al reclamante subsane las observaciones, sin haberse procedido a presentar ante la APDP la información requerida.La APDP declaró improcedente la reclamación.
2	013-2015-JUS/DGPDP 02 de junio de 2015	**Derecho de cancelación**. El reclamante solicitó la tutela del derecho a la **cancelación** de sus datos personales en el **Ministerio de Economía y Finanzas.** El reclamante presentó desistimiento de la pretensión. La APDP dio por desistida la reclamación y dio por concluido el procedimiento trilateral de tutela.
3	015-2015-JUS/DGPDP 15 de junio de 2015	Derecho de cancelación. El reclamante solicitó la tutela del derecho a la **cancelación** de sus datos personales en el **Fondo de Cooperación para el Desarrollo Social.** La APDP declaró improcedente la reclamación, en atención a que el tratamiento objeto de la reclamación cesó, según se constató de los enlaces de internet. La APDP ordenó al reclamado adoptar las medidas necesarias que permitan mantener el bloqueo y la eliminación de los datos personales del reclamante.
4	022-2015-JUS/DGPDP30 de julio de 2015	La reclamante solicitó la tutela del derecho a **acceso** de sus datos personales en el **Banco Ripley Perú S.A.** La APDP ordenó al reclamado atienda la solicitud de revocación de consentimiento de la reclamante. La APDP declaró fundada la reclamación. La APDP impuso la sanción de multa de cuatro (4) UIT.

Procedimientos Administrativos Sancionatorios de la Dirección General de Protección de Datos Personales del Ministerio de Justicia del Perú:

Nº	Procedimientos Administrativos Sancionadores	Sumilla
1	2015 Resolución de la Dirección de / Resolución de la Dirección General de Protección de	. Resolución Directoral Nº 003-2015-JUS/DGPDP-DS del 19 de febrero de 2015, que sanciona, en primera instancia administrativa, con multas a SUPERMERCADO LA CANASTA E.IR.L.;

	Sanciones	Datos Personales	Resolución Directoral Nº 008-2015-JUS/DGPDP del 17 de abril de 2015, que resuelve en segunda instancia administrativa la apelación interpuesta.
	Resolución Directoral Nº 003-2015-JUS/DGPDP-DS del 19 de febrero de 2015	Resolución Directoral Nº 008-2015-JUS/DGPDP del 17 de abril de 2015	
2	Resolución Directoral Nº 014-2015-JUS/DGPDP-DS del 20 de abril de 2015	Resolución Directoral Nº 014-2015-JUS/DGPDP del 12 de junio de 2015	. Resolución Directoral Nº 014-2015-JUS/DGPDP-DS del 20 de abril de 2015, que sanciona, en primera instancia administrativa, con multas a UNIVERSIDAD INCA GARCILASO DE LA VEGA; Resolución Directoral Nº 014-2015-JUS/DGPDP del 12 de junio de 2015, que resuelve en segunda instancia administrativa la apelación interpuesta.
3	Resolución Directoral Nº 017-2015-JUS/DGPDP-DS del 27 de abril de 2015	Resolución Directoral Nº 017-2015-JUS/DGPDP del 26 de junio de 2015	Resolución Directoral Nº 017-2015-JUS/DGPDP-DS del 27 de abril de 2015, que sanciona, en primera instancia administrativa, con multa a CLINICAS MAISON DE SANTE; Resolución Directoral Nº 017-2015-JUS/DGPDP del 26 de junio de 2015, que resuelve en segunda instancia administrativa la apelación interpuesta.
4	Resolución Directoral Nº 034-2015-JUS/DGPDP-DS del 03 de julio de 2015	No hay Resolución de Segunda Instancia, debido a que la Resolución de Primera Instancia quedó consentida.	. Resolución Directoral Nº 034-2015-JUS/DGPDP-DS del 03 de julio de 2015, que sanciona con multa, en primera instancia administrativa, a UNIVERSIDAD ALAS PERUANAS S.A.
5	Resolución Directoral Nº 037-2015-JUS/DGPDP-DS del 14 de julio de 2015	No hay Resolución de Segunda Instancia, debido a que la Resolución de Primera Instancia quedó consentida.	Resolución Directoral Nº 037-2015-JUS/DGPDP-DS del 14 de julio de 2015, que sanciona con multa, en primera instancia administrativa, a AIS HOSPITAL SANTA ROS
6	Resolución Directoral Nº 035-2015-JUS/DGPDP-DS del 08 de julio de 2015.	Resolución Directoral Nº 025-2015-JUS/DGPDP del 16 de setiembre de 2015.	Resolución Directoral Nº 025-2015-JUS/DGPDP del 16 de setiembre de 2015, declara infundado el recurso de apelación interpuesto por el Hospital Nacional Arzobispo Loayza.
7	Resolución Directoral Nº 040-2015-JUS/DGPDP-DS del 16 de julio de 2015.	Resolución Directoral Nº 026-2015-JUS/DGPDP del 16 de setiembre de 2015.	Resolución Directoral Nº 026-2015-JUS/DGPDP del 16 de setiembre de 2015, el cual contiene el recurso de apelación presentado por Farmacia Universal S.A.C.
8	Resolución Directoral Nº 043-2015-JUS/DGPDP-DS del 31 de julio de 2015.	Resolución Directoral Nº 028-2015-JUS/DGPDP del 21 de setiembre de 2015.	Resolución Directoral Nº 028-2015-JUS/DGPDP del 21 de setiembre de 2015, el cual contiene el recurso de apelación interpuesto por la Clínica San Felipe S.A. Sancionan a Clínica San Felipe con 5UIT por utilizar formas de consentimiento invalidas para el tratamiento de datos personales de sus usuarios web. Impone la sanción de 25 UIT de multa por no inscribir el Banco de Datos Personales de sus Pacientes en el Registro Nacional de Protección de Datos Personales.

4.4. Análisis de Resultados.

Los resultados demuestran la necesidad de interrelacionar la identidad digital con los procesos de comercio electrónico, negocios electrónicos, gobierno electrónico y aprendizaje electrónico.

En las Encuestas sobre Identidad Digital, en la pregunta A) ¿En Internet de que peligros debe protegerse la Identidad Digital? El 11% respondieron de malware; el 11% de la Homonimia, el 29% del uso indebido de las múltiples identidades, el 49% la Suplantación de la Identidad.

Por tanto, en la variable peligros de los cuales hay que proteger la identidad digital en Internet el 49% de los encuestados dan como resultado la suplantación de identidad. ***Phishing*** o **suplantación de identidad** es un término informático que denomina un modelo de abuso informático y que se comete mediante el uso de un tipo de ingeniería social, caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito otra información bancaria).

El 29% de los encuestados señalan que el peligro a la identidad digital en internet es el uso indebido de las múltiples identidades. Los seres humanos tenemos varias identidades, por ejemplo y simplificando con algunas dicotomías conocidas: a) identidad de género, mujer/hombre; b) identidad nacional, peruano/extranjero; c) identidad político-ideológica, centroizquierda/derecha; d) identidad étnica, indígena/shipibo; e) identidad religiosa, católico/metodista. f) abogado; g) docente universitario; h) padre de familia; i) titular de tarjeta de crédito. j) titular de tarjeta del metropolitano; k) titular de cuenta de facebook; l) titular de cuenta de linkedin; m) titular de cuenta de correo electrónico, etc. El uso indebido de estas múltiples identidad puede generar daño y perjuicio a la identidad digital de la persona y a su reputación "on line".

El 11% de los encuestados respondió Malware. El ***malware*** (del ingles *"**mal**icious soft**ware**"*), también llamado *badware*, **código maligno**, **software malicioso** o **software malintencionado**, es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario. El término *malware* es muy utilizado por profesionales de la informática para referirse a una variedad de software hostil, intrusivo o molesto.

También el 11% de los encuestados respondió Homonimia. Se aplica el termino homónimo si la persona tiene el mismo nombre que otra.

En la pregunta B) de la Encuesta se pregunta que derechos son protegidos al resguardar el derecho a la identidad digital en internet, afirmando el 35% que se protegen los datos personales, 30% el Derecho a la Intimidad, seguidos del derecho al honor con un 25% y un 20% de otros derechos. Por tanto, las personas son conscientes que al proteger el derecho de identidad digital de la persona en internet se están protegiendo todos los otros derechos de la persona.

En la pregunta C) de la Encuesta se pregunta si se protege la identidad de la persona jurídicas que derechos se están protegiendo, los encuestados precisan que el derecho a la reputación, el derecho al nombre comercial, la marca registrada y el derecho de autor.

En la pregunta D) se pregunta ¿Qué ventajas tendría tener el Documento Nacional de Identidad Electrónico?- El 45% de los encuestados contesto para trámites; el 28% para compras; el 24% para aprendizaje; el 21% para teletrabajo; el 32% contratos; el 20% para litigar; el 5% otros. En esta pregunta se permitió las respuestas múltiples, razon por la cual los resultados reflejan estos porcentajes.

En la pregunta E) sobre las operaciones de comercio electrónico realizadas responde el 30% Pasajes aéreos; el 5% comida; el 7% supermercado; el 12% reserva de hoteles; el 8% vestidos; el 10% libros.

En la pregunta F) sobre las razones que si convencen para realizar operaciones de comercio electrónico, en orden de jerarquía son: 1. Es

rápido. 2. Ahorro de Tiempo. 3. Ahorro de Dinero. 4. Es seguro. 5. Ley me protege.

En la pregunta G) en la respuesta a las razones por las que no han realizado operaciones de comercio electrónico en orden de jerarquía se dan las siguientes razones: 1. Temo a los Hackers. 2. Prefiero Presencial. 3. No quiero utilizar tarjetas. 4. Temo la suplantación de Identidad. 5. No da confianza.

En la pregunta H) que tramites de Gobierno Electrónico ha realizado en Internet, el 55% de los encuestas contesta el Duplicado de DNI, el 22% emisión de comprobantes, el 6% constitución de empresas en línea: el 6% tramites regionales o locales, 3% renovación de pasaporte, 6% otros.

En la pregunta I) sobre que tramites utilizaría si se implementaran en el contexto del Gobierno Electrónico, el 20% de los encuestados contesto tramites; el 25% el pago de arbitrios; el 20% Antecedentes Penales; el 19% Expediente Electrónico Judicial; el 14% Historia Clínica Electrónica, el 11% orientación por apps.

En la pregunta J) de que actividades de negocios electrónicos ha hecho usted por Internet el 40% contesto ckeck in aéreo; 26% paquetes turísticos; el 16% servicios profesionales; el 12% selección de personal por internet.

En la pregunta K) sobre las actividades de negocios electrónicos qu estaría dispuesto a realizar en forma segura tenemos al 42% Remates o subastas; 24% negociación de valores; 13% representación on line; 12% consorcios; 7% Juegos de Azar por Internet.

En la pregunta L) que actividades relacionadas al Aprendizaje electrónico ha realizado usted tenemos el 23% uso de aula virtual; 23% Video Conferencia; 22% Examen por Internet; 17% Foros por Internet; 15% Chat Académico.

En la pregunta LL) sobre que actividades de aprendizaje electrónico estaría usted dispuesto a realizar en un entorno seguro contesto el

28% Foros por Internet; el 22% enseñanza en plataforma de Internet; 17% Capacitación; 16% Maestría o Doctorado.

En la pregunta M) de por que es importante un Sistema Funcional de Identidad Digital el 69% contesto porque es necesario y el 31% para evitar el uso indebido de las múltiples identidades.

Por tanto es valorado por los encuestados la importancia y necesidad de estabelecer un sistema funcional de identidad digital donde el documento credencial electrónico garantice la identidad digital formal por parte del Estado en Internet, para que el ciudadano pueda realizar en forma segura los procesos de gobierno electrónico, comercio electrónico, negocios electrónicos y aprendizaje digital.

El derecho a la identidad digital en Internet tiene la regulación y protección establecida en la Constitución Política del Perú, en la Convención Universal de Derechos Humanos de las Naciones Unidas, el Marco de la Privacidad de la APEC, la Carta Iberoamericana de Gobierno Electrónico, los resultados del Grupo de Trabajo IV (Comercio Electrónico) de la Comisión de Naciones Unidas) para el Derecho Mercantil Internacional, la Ley 29733 de Protección de Datos Personales, la Ley 27269 de Firmas y Certificados Digitales, los reglamentos y diversas normas que regulan la materia investigada.

En la Encuesta efectuada al Dr. Thomas J. Smedinghoff , el entrevistado a la preguntas formuladas. afirma lo siguiente:

a) Es consciente que el Gobierno de Estados Unidos y el de Reino Unido está buscando activamente el uso de identidad digital en conexión con la prestación de servicios públicos.
b) La Regulacion de Identidades Digitales recientemente adoptada por la Union Europea esta diseñada para permitir a los ciudadanos de cualquier país de la Union Europea a utilizar la identidad digital emitida para ellos en dicho país en conexión con la obtención de acceso a los servicios del gobierno en otro país de la Union Europea.

c) Estados Unidos está buscando el desarrollo de un programa de identidad digital para propósitos de permitir a los ciudadanos acceder a los servicios gubernamentales del gobierno en línea. Dicho programa es llamado Conect Gov.
d) El objetivo de Conect Gov es utilizar los proveedores de identidad del sector privado para emitir credenciales de identidad digital a ciudadanos individuales. Que no operaria como una identidad digital nacional, sino en forma específica.
e) En Europa la regulación de la Identidad Digital se centra en sistemas de identidad que emiten credenciales para el uso de transacciones del sector público en el extranjero.
f) Desde su punto de vista la gestión de identidad digital es de suma importancia para el comercio electrónico, sobre todo para transacciones de naturaleza significativa.
g) Piensa que una legislación sobre identidad digital será necesaria (o por los menos deseable) para el uso de la identidad digital en los negocios electrónicos y en el aprendizaje electrónico. Dicha legislación podría ayudar a lograr una serie de metas importantes, incluyendo las siguientes: i) Remover las barreras para el uso de la identidad en línea que pueda existir bajo la actual legislación. Ii) Ayudar a definir y promover la confianza en los sistemas de identidad. Iii) Facilitar el reconocimiento legal de la identidad y la autenticación. Iv) Facilitar la interoperabilidad de los sistemas de identidad en el exterior.

Con el instrumento de campo de investigación de Observación Directa, describimos el uso del Aula Virtual de la Academia de la Magistratura en el dictado como profesor asociado del curso de Derecho Informático en Agosto y Setiembre de 2014. Asimismo, por Observación Directa describimos la obtención del Documento Nacional de Identidad Electrónico (DNIe) en la Oficina respectiva de la Entidad de Registro Digital (EREP) de RENIEC. Seguidamente, por Observación Directa de uso de Tecnologías de Información de persona discapacitada visual para identificarse y comunicarse dentro de transporte público en Lima, Perú.

En el instrumento de campo Análisis Documental, en el Registro Nacional de Banco de Datos Personales observamos diversidad de inscripciones; de las cuales destacamos las siguientes que tienen relación con el ejercicio del derecho de la identidad digital en Internet:

a) Ministerio de Comercio Exterior y Turismo. Registro Nº 1404 de Personas Prohibidas de Acceder a las Salas de Juego de Casino y Maquinas Tragamonedas. La Finalidad es: Llevar un registro de personas impedidas de ingresar a las salas de juego y asi dar cumplimiento a lo dispuesto en la Ley Nº 29907, Ley para la prevención y el tratamiento de Ludopatía en las Salas de Juego de Casino y de Maquinas Tragamonedas y su Reglamento aprobado por D.S. 007-2013-MINCETUR.
b) Programa Nacional de Apoyo Directo a los más Pobres-JUNTOS. Registro Nº 1477 de Data de Beneficiarios Afiliados y Abonados del Programa JUNTOS. La Finalidad es: Llevar un control y monitoreo de los hogares afiliados al programa, realizar el monitoreo de los abonos realizados a los hogares que cumplen sus corresponsabilidades.
c) Ministerio de Trabajo y Promoción del Empleo. Registro Nº 3544. Planilla Electrónica. La Finalidad es: -Administrar con mayor eficiencia la información de los empleadores y trabajadores en materia económica, salarial y socio cultural. – Herramienta para optimizar la fiscalización laboral. – Coadyuva a la rápida solución de los procesos laborales según el artículo 27ª de la Ley Nº 29497, Ley Procesal del Trabajo.
d) INDECOPI. Instituto de Defensa de la Competencia y de la Propiedad Intelectual. Registro Nº 4000 de Usuarios asesorados. Registro Nº 4782 de Procedimientos Concursales. Registro Nº 4787 Registro de Derecho de Autor. Registro Nº 4788 Registro de Signos Distintivos. Registro Nº 4793 Expedientes Denuncias OP1 (Protección al Consumidor). Registro Nº 4798 Registro GRACIAS NO INSISTA. Registro Nº 4831 Denuncias de

Competencias Desleal, Registro Nº 4835 Reclamos de Usuarios. Registro Nº 4836 Denuncias de Barreras Burocráticas.

e) Instituto Nacional de Enfermedades Neoclásicas-INEN. Registro Nº 4794 Pacientes. Registro Nº 4795 Donantes. Registro Nº 4796 Trabajadores. Registro Nº 4798 Proveedores.
f) Ministerio de Relaciones Exteriores. Registro Nº 4816 Directorio Activo de Funcionarios. Registro Nº 4817 Escalafón. Registro Nº 4818 Fojas de servicio del Cuerpo Diplomático. Registro Nº 4819 Nombres de Funcionarios. Registro Nº 4820 Certificación de Firmas y Apostilla. Registro Nº 4821 Actividades Migratorias. Registro Nº 4822 Sistema de Registro Civil. Registro Nº 4823 Visita a Funcionarios.

Los Procedimientos Trilaterales de Tutela y Sancionatorios realizados por la Autoridad Nacional de Protección de Datos Personales del Ministerio de Justicia durante el año 2015, demuestran un esfuerzo por aplicar y hacer cumplir la ley de protección de datos personales, pero consideramos que es insuficiente, porque consideramos que debiera haber procedimientos de fiscalización mas numerosos a nivel nacional. Lo que nos lleva a afirmar que la infraestructura y personal de la actual Autoridad Nacional de Protección de Datos Personales, limita su actuación, por lo que es necesario que se designe otra entidad pública para este efecto, la que proponemos sea RENIEC.

4.5. Contrastación de la Hipótesis.

- La identidad digital utilizada en forma segura permite evitar el uso inadecuado de múltiples identidades y disminuir la suplantación de identidad. La identidad digital como identidad formal permite proteger a la persona en internet.
- En el trabajo de campo se visualiza que las variables suplantación de Identidad y uso indebido de múltiples identidades son precisadas en forma significativa 49% y 29% respectivamente, como los peligros que en Internet debe protegerse a la Identidad Digital de la persona.

- En el trabajo de campo efectuado se ha podido constatar la diversas posibilidades de utilización de la identidad digital tanto en el ámbito público como en el ámbito privado. El uso de los sistemas informáticos para facilitar la vida del ciudadano se realiza tanto en los procesos de gobierno electrónico, comercio electrónico, negocios electrónicos y aprendizaje electrónico.

- La Identidad Digital Nacional se va a convertir en una Identidad Digital Formal respaldada en el Documento Nacional de Identidad Electrónico (DNI) como documento que permite su uso seguro y confiable en Internet. Para lo cual es necesario crear un sistema funcional de Identidad Digital. Protección de Datos Personales, Certificación y Registro Digital que cohesione en forma coherente las disposiciones contenidas en la Ley de Firmas y Certificados Digitales, Ley de Protección de Datos Personales y el Proyecto de Ley de Identidad Digital, que esperamos sea aprobado por el Congreso de la República y se convierta en Ley.

- Este sistema funcional de identidad digital que integre la protección de datos personales y el uso de las firmas y certificados digitales debe estar contenido en ley especifica, que establezca un marco legal coherente que este comprendido por: una Ley de identidad digital, la ley de protección de datos personales y la ley de firmas y certificados digitales, y la instituciones jurídicas relacionadas al derecho informático en internet donde el documento nacional de identidad electrónico (DNIe) acredita en forma segura la identidad digital de la persona en internet y le permite ejercer adecuadamente sus derechos.

- Para que pueda crearse un sistema funcional debe establecerse en el Acuerdo Nacional la Política de Estado 35 de identidad digital, protección de datos personales, certificación y registro digital.

- Este sistema funcional está a cargo de un Ente Rector que se constituye en su autoridad técnica-normativa a nivel nacional; dicta las normas y establece los procedimientos relacionados con su ámbito; coordina su operación técnica. En esta investigación proponemos que este Ente Rector sea RENIEC y que se interrelacione y coordine con la Oficina Nacional de Gobierno Electrónico (ONGEI) , el Ministerio de Justicia en el ámbito de la Protección de Datos Personales y con el INDECOPI en el ámbito de la certificación y registro digital, así como con otras entidades públicas.

- RENIEC conforme a ley es un organismo autónomo que cuenta con personería jurídica de derecho público interno y goza de atribuciones en materia registral, técnica, administrativa, económica y financiera, que al desempeñarse como Ente Rector de un Sistema Funcional coadyuvaría en forma decisiva en la protección y adecuado ejercicio del ciudadano del derecho a la identidad digital en Internet.

- 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. Se inscriben en el Registro Civil los nacimientos, los matrimonios, las defunciones, entre otros, datos que tienen incidencia en el ejercicio del derecho de identidad digital en Internet.
- En el trabajo de análisis documental se visualiza los procedimientos trilaterales de tutela (cuatro) y los procedimientos sancionatorios (ocho) realizados por la Autoridad de Protección de Datos Personales Peruana, durante el año 2015. Con lo cual se demuestra el accionar insuficiente de la Autoridad, para fortalecer la protección de datos personales en el Perú. Lo que refuerza nuestra propuesta de crear un sistema funcional de identidad digital, protección de datos personales, certificación y registro digital.

CONCLUSIONES

1. Se entiende por identidad digital de las personas, a aquella identidad electrónica basada en un documento credencial electrónico, emitido en el marco de la Infraestructura Oficial de Firma Electrónica (IOFE), y conforme a las disposiciones legales vigentes. En este sentido, la identificación y la autenticación digital permiten proteger en forma segura el derecho de identidad digital de la persona en internet.

2. La Identificación Digital es el procedimiento que mediante elementos seguros y acreditados, permite asignar una identidad con determinados atributos a una persona concreta, esto es a la comprobación de datos que acreditan que un individuo es efectivamente la persona que dice ser en internet, en forma indubitable.

3. Para intervenir y participar en los cuatro grandes procesos: el comercio electrónico, los negocios electrónicos, el aprendizaje electrónico y el gobierno electrónico necesitamos tener una identidad digital que sea segura, que evite el uso inadecuado de múltiples identidades y la suplantación de identidad. Para los cual

el Derecho Informático en Internet debe ser aplicado en forma sistemática y coherente.

4. El ejercicio de los derechos de la persona en internet, requiere la identificación plena de las personas, función que corresponde al Estado. El Estado es el responsable de la identificación de las personas y de garantizar la identidad de cada uno. El derecho de identidad digital y la identificación debe ser garantizada por la legislación de cada país, de forma tal de que los derechos de cada persona sean respetados en forma sistémica e integral en Internet.

5. Es necesario establecer en el Acuerdo Nacional del Perú. la Política de Estado 35 de identidad digital, protección de datos personales, Certificación y Registro Digital. De la siguiente forma: "Nos comprometemos a consolidar del derecho a la identidad digital en Internet, promover la protección de datos personales y desarrollar la infraestructura y Banda Ancha a Nivel nacional para la comunicación segura y rápida que utilice el registro y la certificación digital de toda persona como instrumento para desarrollar su inclusión digital en la Sociedad de la Información".

6. Es necesario crear por Ley, un sistema funcional de Identidad Digital, Protección de Datos Personales y Certificación y Registro Digital que asegure el cumplimiento de la Política de Estado 35 propuesta, que requiere la participación de todas o varias Entidades el Estado.

7. El sistema funcional de identidad digital, protección de datos personales, certificación y registro digital, cohesiona y permite la aplicación coherente de los derechos y obligaciones reconocidos en la Ley de Firmas y Certificados Digitales, Ley de Protección de Datos Personales y Proyecto de Ley de Identidad Digital.

8. Es necesario que el Congreso de la República apruebe el Proyecto de Ley de Identidad Digital que tiene por objeto reconocer el derecho de todas las personas a la inclusión digital y regular el derecho a la identidad digital para el uso de servicios de gobierno electrónico seguro, prestados por las entidades de la Administración Pública.

9. La Legislación Peruana de Teletrabajo, de Delitos Informáticos y de Votación Electrónica es necesario que sea concordada y aplicada en forma sistemática con la Legislación de Firmas y Certificados Digitales, Protección de Datos Personales y de Identidad Digital, para una aplicación coherente que permita cumplir en forma eficiente los objetivos de cada norma en forma específica.

10. Se requiere promover y fortalecer una Cultura de Identidad Digital y de Protección de Datos Personales. Para lo cual es necesario coordinar la inclusión de información sobre la importancia de la identidad digital y de la protección de datos personales en los planes de estudios de todos los niveles educativos y fomentar, asimismo la capacitación de los docentes en estos temas.

11. La validez y fuerza de los contratos en internet esta directamente relacionados a la robustez de los mecanismos seguros que garanticen la identidad digital de las personas que son parte de un contrato. La interacción del sistema automatizado con otras personas u otros sistemas debe garantizar la identidad de las partes en cada una de las declaraciones contractuales en internet. Los datos de las personas, los certificados digitales y otras instituciones jurídicas propias del derecho informático deben ser tratadas y reguladas en forma coherente teniendo como elemento esencial de cohesión la identidad digital formal segura.

12. El respeto y protección del derecho de identidad digital en Internet y la correspondiente protección de datos personales, bajo el marco de un sistema funcional eficiente, debe generar la confianza necesaria a nivel internacional, para permitir que un ciudadano peruano que tiene un Documento Nacional de Identidad Electrónico (DNIe) pueda tener acceso a servicios públicos en Línea en otros Estados, con los cuales el Perú tenga suscritos Acuerdos Comerciales como la Unión Europea, Estados Unidos, Canadá y Países que forman parte del Foro Asia Pacifico (APEC) , del Acuerdo Transpacífico (TPP) y la Alianza del Pacifico.

RECOMENDACIONES.

1. Se recomienda que el Registro Nacional de Identificación y Estado Civil (RENIEC) sea el Ente Rector del Sistema Funcional de Identidad Digital, Protección de Datos Personales, Certificación y Registro Digital.

2. Se recomienda que se designe como Autoridad de Protección de Datos Personales al organismo autónomo constitucionalmente RENIEC que permitiría la fiscalización del cumplimiento de la ley en corto plazo y que derecho fundamentales de la persona como es el derecho a la identidad se protejan en forma adecuada.

3. Se recomienda que la legislación universitaria y educativa se reconozca el valor jurídico a la educación virtual y del aprendizaje electrónico.

4. Se recomienda que la Comisión de Protección al Consumidor del INDECOPI forme parte de e-consumer que reúne a las entidades gubernamentales de distintos países buscan garantizar la atención de reclamos de consumidores, la protección de sus derechos y de la identidad digital.

5. Se recomienda que el curso de Derecho Informático sea de carácter obligatorio en las carreras de Derecho, Ingeniería Informática o de Sistemas de las Universidad del País. Asimismo, se recomienda en los programas de Postgrado conducentes a obtener el grado académico de Doctor en Derecho se incluya el curso de Derecho Informático.

6. Se recomienda la utilización en forma generalizada del documento nacional de identidad electrónico (DNIe) como medio seguro para realizar transacciones electrónicas en procesos de comercio electrónico, gobierno electrónico, negocios electrónicos y aprendizaje electrónico.

ANEXOS

ANEXO Nº 1

Banco de Datos Personales Registrados desde el 08 de Mayo de 2013 hasta el 16 de Octubre de 2014 (354 Banco de Datos Personales), en el Registro Nacional de Protección de Datos Personales del Ministerio de Justicia. Fuente: http://www.minjus.gob.pe

Numero	Tipo	Entidad/PJ	Denominación del banco de datos	Finalidad
001	Público	Ministerio de Justicia	Sistema de Notariado	Registrar a los Notarios del País.
002	Privado	Operadora de Carreteras SAC	Banco de datos de proveedores	Administrar la información de proveedores para adquirir bienes y servicios.
003	Privado	Operadora de Carreteras SAC	Banco de Datos de Trabajadores	Administra la información de los trabajadores para fines de compensación, bienestar social, salud y control interno del recurso humano.
004	Privado	Autopista del Norte SAC	Banco de Datos de Proveedores	Administrar la información de proveedores para la

				adquisición de bienes y servicios.
005	Privado	Autopista del Norte SAC	Banco de Datos de Trabajadores	Administra la información de los trabajadores para fines de compensación, bienestar social, salud y control interno del recurso humano.
006	Privado	Autopista del Norte SAC	Banco de Datos de Clientes	Administrar la información de los usuarios para fines de registro y verificación en el sistema de cobro de peaje.
007	Privado	PRI VFS PERU SAC	Spain Visa VFS Global	Tramitar solicitud de visado de corta duración Schnengen.
008	Privado	VFS PERU SAC	Canadian VISA	Tramitar solicitud de visa canadiense.
009	Privado	Iriarte Asociados SCRL	Banco de Datos de Cumpleaños	Realización de Actividades sociales.
010	Público	Ministerio de Justicia	Registro de Funcionarios y Servidores Procesados por presuntos delitos contra la	Promoción, ética, transparencia y erradicación de corrupción.

			Administración Pública.	
011	Público	Ministerio de Justicia	Registro de Deudores de Reparaciones Civiles por Delitos en agravio del Estado.	Contar con la información consolidada sobre las deudas por concepto de reparaciones civiles a favor del Estado que hayan incurrido en morosidad.
012	Privado	Grupo RPP SAC	Usuarios de Promociones Comerciales y envío de Información de servicios.	Realizar envío de comunicaciones en cualquier papel o medio electrónico.
013	Privado	Philip Morris	Registro de Empleados actuales, antiguos y posibles de Philip Morris Perú S.A.	Proceso de manejo de información de procesos de Recursos Humanos.
014	Privado	Google Perú SRL	Base de Datos de Recursos Humanos	Información de Recursos Humanos.
015	Privado	CETCO S.A.	Banco de datos de Proveedores de CETCO S.A.	Contar con lista de proveedores con los que CETCO S.A. contrata para fines contables.
016	Privado	ISTECEX	Planilla de Sueldos.	Pago de Haberes de Trabajadores.

017	Privado	ADEX	Planilla de sueldos	Pago de Haberes de Trabajadores.
018	Privado	PAPRINCO SAC	Planilla de sueldos	Pago de Haberes.
019	Privado	YCHIFORMAS S.A:	Planilla de trabajadores	Pago de Haberes de Trabajadores.
020	Privado	MYDANKETSU SAC	Planilla de trabajadores	Pago de Haberes.
021	Privado	La Caja Municipal de Ahorro y Crédito de Tacna S.A	Banco de Datos de Expedientes de los Clientes Activos.	Resguardo de documentación física de los clientes activos para el control en la gestión del proceso crediticio.
022	Privado	La Caja Municipal de Ahorro y Crédito de Tacna S.A	Banco de Datos de Clientes Activos.	Realizar Gestión de Clientes Activos.
023	Privado	La Caja Municipal de Ahorro y Crédito de Tacna S.A	Banco de Datos de Expedientes de Clientes Pasivos.	Resguardo de Documentos físicos de clientes.
024	Privado	La Caja Municipal de Ahorro y Crédito de Tacna S.A	Banco de Datos de Clientes Potenciales.	Realizar gestión de clientes potenciales para captarlos.
025	Privado	La Caja Municipal de Ahorro y Crédito de Tacna S.A	Banco de Datos de Pasivos	Realizar Gestión de Clientes Pasivos.
026	Privado	La Caja Municipal de Ahorro y Crédito de	Banco de Datos de Antecedentes Policiales y	Verificar que personal que ingresa a laborar

		Tacna S.A	Penales de los trabajadores.	no registra antecedentes policiales y registrales.
027	Privado	La Caja Municipal de Ahorro y Crédito de Tacna S.A	Banco de Datos de Bienes e Ingresos de Trabajadores	Conocer detalle de ingresos de trabajadores s y bienes muebles e inmuebles que posean.
028	Privado	La Caja Municipal de Ahorro y Crédito de Tacna S.A	Reporte de Trabajadores en Centrales de Riesgo	Verificar que el personal que ingresa a laborar no presenta deudas vencidas.
029	Privado	La Caja Municipal de Ahorro y Crédito de Tacna S.A	Banco de Datos de Consanguinidad y afinidad de trabajadores con accionistas.	Verificar que el personal que ingresa a laborar no tenga vínculos de consanguinidad con los miembros de la Junta General de Accionistas de la CMAC.
030	Privado	La Caja Municipal de Ahorro y Crédito de Tacna S.A	Convenio de Confidencialidad de los Trabajadores.	Acreditar el Compromiso de Confidencialidad.
031	Privado	La Caja Municipal de Ahorro y Crédito de Tacna S.A	Curriculum Vitae de Trabajadores.	Gestión de Curriculum Vitae de los trabajadores.

032	Privado	La Caja Municipal de Ahorro y Crédito de Tacna S.A	Banco de Datos de Identificación de los Trabajadores.	Contar con información para el pago de haberes de los trabajadores.
033	Privado	La Caja Municipal de Ahorro y Crédito de Tacna S.A	Banco de Datos de Inducción al Nuevo Trabajador.	Acreditar que nuevo trabajador conoce normativa interna vigente.
034	Privado	La Caja Municipal de Ahorro y Crédito de Tacna S.A	Clientes.	Control de hipotecas otorgadas a favor de CMAC Tacna.
035	Privado	La Caja Municipal de Ahorro y Crédito de Tacna S.A	Lista Negra de Clientes.	Registrar los clientes con problemas en el sistema financiero.
036	Privado	La Caja Municipal de Ahorro y Crédito de Tacna S.A	Atención a Clientes	Controlar la atención y comunicaciones periódicas enviadas a los clientes.
037	Privado	La Caja Municipal de Ahorro y Crédito de Tacna S.A	Reclamos	Atender reclamos de los clientes.
038	Privado	La Caja Municipal de Ahorro y Crédito de Tacna S.A	Proveedores	Registrar Proveedores.
039	Privado	La Caja Municipal de Ahorro y Crédito de Tacna S.A	Lista Preventiva de Clientes.	Remitir registros de operaciones.

040	Privado	La Caja Municipal de Ahorro y Crédito de Tacna S.A	Registro de Operaciones de Clientes	Remitir los registros de operaciones solicitadas por el ente supervisor de acuerdo a ley.
041	Privado	La Caja Municipal de Ahorro y Crédito de Tacna S.A	Cobranza Municipal	Realizar cobranza judicial.
042	Privado	La Caja Municipal de Ahorro y Crédito de Tacna S.A	Monitoreo Acceso Instalaciones.	Monitorear acceso a instalaciones a través de de CCTV
043	Privado	La Caja Municipal de Ahorro y Crédito de Tacna S.A	Acceso Centro Procesamiento de Datos.	Registrar accesos a ambientes restringidos.
044	Privado	La Caja Municipal de Ahorro y Crédito de Tacna S.A	Usuarios Red Interna.	Seguridad y control de accesos.
045	Privado	La Caja Municipal de Ahorro y Crédito de Tacna S.A	Usuarios que acceden a sistema de Información	Gestión y Control de Accesos.
046	Público	Ministerio de Justicia	Registro de Participantes de Programas de Capacitación.	Contar con Registro de Participantes.
047	Público	Ministerio de Justicia	Directorio de Asesores Jurídicos asistentes a las Convenciones de	Promover aplicaciones coherentes del Ordenamiento Jurídico.

			Asesores Jurídicos.	
048	Público	Ministerio de Justicia	Integrantes de las Comisiones que presentan Informe Final al Ministerio de Justicia.	Conocer personas que integran Comisiones.
049	Público	Ministerio de Justicia	Sistema de Registro de Usuarios del SPIJ	Enviar mensualmente a usuarios suscritos los DVDs del SPIJ y coordinar capacitación.
050	Público	Ministerio de Justicia	Registro Nacional de Fedatarios Juramentados con Especialización en Informática.	Mantener un Registro actualizado de fedatarios juramentados con Especialización en Informática y sus ratificaciones a efectos de brindar información a ciudadanía.
051	Público	Consejo Nacional de la Magistratura	Base de Datos del personal y apoyo del CNM	Contar con la información del personal de apoyo del CNM para efectos laborales y tributarios.
052	Público	Consejo Nacional de	Registro de	Administrar la información de

		la Magistratura	Jueces y Fiscales	los magistrados para su posterior servicio interno y externo.
053	Público	Consejo Nacional de la Magistratura	Registro de datos de funcionarios y autoridades del CNM	Administrar la información del Directorio, funcionarios y autoridades para invitación a eventos y actividades oficiales.
054	Privado	Comercial Líder S.A.	Planilla de Remuneraciones	Desarrollar correctamente las actividades de la empresa y permitir el pago de planilla de trabajadores.
055	Privado	Megacolor S.A.	Planilla Remuneraciones trabajadores	Desarrollar correctamente las actividades de la empresa y permitir el pago de planilla de trabajadores.
056	Privado	Agraria Santa Isabel SAC	Planilla Remuneraciones Trabajadores	Desarrollar correctamente las actividades de la empresa y permitir el pago de planilla de trabajadores.
057	Privado	Repuestos Nuevos S.A.	Planilla de Trabajadores	Desarrollar correctamente las actividades

				de la empresa y permitir el pago de planilla de trabajadores.
058	Privado	Automóviles S.A.	Datos personales de los Trabajadores de la Empresa.	Pagar Planilla de Remuneraciones.
059	Privado	Venator SAC	Planilla de Trabajadores	Pagar Planilla de Remuneraciones.
060	Privado	Consorcio Naviero Peruano	Planilla	Pago de Haberes de Trabajadores.
061	Privado	Supermarket Perú EIRL	Recursos Humanos	Administrar información de los trabajadores de la empresa.
062	Privado	Centro Carnes SRL	Recursos Humanos	Administrar información de los trabajadores de la empresa.
063	Privado	Centro Mar S.A.	Recursos Humanos	Administrar información de los trabajadores de la empresa.
064	Público	Ministerio de Justicia	Invitados a eventos de Difusión.	Promocionar eventos de difusión de la LPDP.
065	Público	Ministerio de Justicia	Banco de Datos de los SECIGRISTAS del Programa SECIGRA DERECHO.	Identificar a los participantes del programa SECIGRA DERECHO para hacer el seguimiento

				respectivo y evaluar el desarrollo de cada programa anual.
066	Privado	Sociedad Minera Cerro Verde S.A.A.	Base de Datos de Trabajadores.	Cumplir con lo normado por SUNAT y MINTRA respecto al pago de remuneraciones, registro de información en el T-Registro y PLAME; y pago de Planilla.
067	Privado	Gráficos Biblos S.A.	Banco de Datos del Personal.	Creación de Planillas de Pago de Personal.
068	Privado	Robert Bosch SAC	Clientes.	Realizar ventas al contado y al crédito.
069	Privado	Robert Bosch SAC	Proveedores.	Ingresar los datos en el sistema para generar la orden de compra y realizar el pago.
070	Privado	Robert Bosch SAC	Planilla Electrónica.	Manejo de la Planilla Electrónica para empleados de la Empresa.
071	Privado	ARACDIS PERU SAC	Trabajadores.	Trámites Administrativos

				propios de la relación contractual.
072	Privado	MITSUI SUMITOMO O INSURANCE CO LTDA	Trabajadores.	Pagos de Haberes e Impuestos.
073	Privado	CONSORCIO HBO SAC	Afiliados a Programas orientados a Pacientes.	Administrar el Banco de datos de los miembros afiliados orientados a pacientes.
074	Privado	RASAN S.A.	Trabajadores de la Empresa.	Planilla de Pago de Remuneraciones y administración de recursos humanos.
075	Privado	PANDERO S.A. EAFC	Sistema Empresarial de recursos Humanos de PANDERO	Administrar la información de los trabajadores.
076	Privado	PANDERO S.A. EAFC	Sistema Turbo Pandero.	Administrar la información de prospección de los asociados y clientes.
077	Privado	PANDERO S.A. EAFC	Sistema de Administración de los Fondo Pandero.	Administrar la información de los asociados y dar soporte a las operaciones del sistema de fondos colectivos.

078	Público	Ministerio de Justicia	Carga Procesal Defensa Pública	Almacenar carga procesal y la información personal de los patrocinados de la D. General de D. Público y acceso a la Justicia.
079	Privado	RECKITT BENCKISER PERU S.A.	Base de Datos de Participantes de Concursos	Recopilación de Datos con fines publicitarios.
080	Privado	**HOTELES SHERATON DEL PERU S.A.**	**STAR GUEST.**	**Registrar las preferencias, quejas y reclamos de los huéspedes del hotel por los servicios prestados.**
081	Privado	**ENTIDAD DE DESARROLLO DE LA PEQUEÑA Y MICRO EMPRESA CREDIVISION-EDPYME CREDIVISION S.A.**	**COLABORADORES CREDIVISIÓN.**	**Prestación laboral.**
082	Privado	**ENTIDAD DE DESARROLLO DE LA PEQUEÑA Y MICRO EMPRESA CREDIVISION-EDPYME CREDIVISION S.A.**	**CARTERA DE CRÉDITOS CREDIVISIÓN.**	**Prestación de servicios financieros**
083	Privado	**AVANCE LEGAL S.A.C.**	**REGISTROS DE RECURSOS HUMANOS Y POSTULANTES TELEAVANCE.**	**Administrar la información de los trabajadores para fines de pago de remuneraciones, salud, control interno de recursos humanos y de los postulantes**
084	Privado	**AVANCE LEGAL S.A.C.**	**REGISTRO DE PROVEEDORES TELEAVANCE.**	**Administrar la comercialización de bienes y servicios de los proveedores.**
085	Privado	**COMPARTAMOS FINANCIERA S.A**	**BANCO DE DATOS CNT (CONTABILIDAD).**	**Generar estados financieros, cumplimiento normativo de información tributaria.**
086	Privado	**COMPARTAMOS FINANCIERA S.A**	**BANCO DE DATOS MIS (MICROFINANCIAL INFORMATION SYSTEM).**	**Brindar servicios financieros de operaciones pasivas, activas y otros servicios**

				a los titulares de los datos personales, así como obtener información de los proveedores de bienes y servicios.
087	Privado	**COMPARTAMOS FINANCIERA S.A**	**BANCO DE DATOS OLAPMIS.**	**Análisis de resultados, toma de decisiones y fines estadísticos.**
088	Privado	**COMPARTAMOS FINANCIERA S.A**	**BANCO DE DATOS RCC (REPORTE CREDITICIO CONSOLIDADO).**	**Información de clientes con productos activos del sistema financiero peruano para evaluación de otorgamiento de créditos y principalmente análisis de riesgos.**
089	Privado	**COMPARTAMOS FINANCIERA S.A**	**BANCO DE DATOS RRHH (RECURSOS HUMANOS).**	**Administración de derechos y obligaciones de los colaboradores de Compartamos Financiera.**
090	Privado	**TECNOLOGÍA MASIVA S.A.C.**	**CHAMEA**	**Brindar publicidad segmentada de acuerdo a los gustos y preferencias de los usuarios de la página web www.chamea.com. Almacenar la información de perfiles e información de los anuncios**
091	Privado	**AT & T GLOBAL NETWORK SERVICES DEL PERU S.R.L.**	BASE DE DATOS DE EMPLEADOS DE AT & T GLOBAL NETWORK SERVICES DEL PERU S.R.L	**Procesar y manejar la información para diversos procesos de recursos humanos.**
092	Privado	**MITSUI AUTOMOTRIZ S.A.**	**RECURSOS HUMANOS**	**Manejo de personal en planilla y practicantes**
093	Privado	**MITSUI AUTOMOTRIZ S.A.**	**DEPARTAMENTO DE MARKETING.**	**Gestión de clientes y prospecto que cubren prospección, negociación, ventas, recompra y postventa.**
094	Privado	**PESQUERA ABC S.A.C.**	**REGISTRO DE PLANILLA DE**	**Cumplir con la obligación del**

			TRABAJADORES	**empleador de registrar en planilla a sus trabajadores**
095	Privado	**CORPORACIÓN REFRIGERADOS INY S.A.**	**REGISTRO DE PLANILLA DE TRABAJADORES**	**Cumplir con la obligación del empleador de registrar en planilla a sus trabajadores**
096	Privado	**BANCO AGROPECUARIO – AGROBANCO**	**BASE DE DATOS DEL PERSONAL DEL BANCO.**	**Registrar toda la información del personal del banco para realizar el pago de haberes, CTS y seguros.**
097	Privado	**CONSTRUCTORA GALILEA S.A.C.**	**BASE DE DATOS AREA COMERCIAL.**	**Manejo de información sobre clientes de forma interna.**
098	Privado	**CONSTRUCTORA GALILEA S.A.C.**	BASE DE DATOS - TRABAJADORES GALILEA	**Uso interno del área de recursos humanos.**
099	Privado	**TELEFÓNICA INGENIERÍA DE SEGURIDAD S.A. SUCURSAL DEL PERÚ**	**BANCO DE DATOS PERSONALES DE PROVEEDORES.**	**Administrar la información de proveedores para la adquisición de bienes o servicios, así como contar con una lista de proveedores con los que contrata la empresa e ingresar los datos en el sistema para generar la orden de compra y efectuar el pago**
100	Privado	**TELEFÓNICA INGENIERÍA DE SEGURIDAD S.A. SUCURSAL DEL PERÚ**	**BANCO DE DATOS PERSONALES DE RECURSOS HUMANOS.**	**Administrar la información de los trabajadores relacionada a la gestión de recursos humanos, así como desarrollar correctamente las actividades de la empresa y permitir el pago de planilla de los trabajadores y cumplir con lo normado por la SUNAT y MINTRA respecto al pago de remuneraciones.**
101	Privado	**TELEFÓNICA INGENIERÍA DE SEGURIDAD S.A. SUCURSAL DEL PERÚ**	**BANCO DE DATOS PERSONALES DE VIGILANCIA.**	**Captación de grabaciones de videovigilancia en las instalaciones de la empresa con la finalidad**

				de validar el ingreso de las personas a las instalaciones de la empresa.
102	Privado	**MOBIL OIL DEL PERU S.R.L.**	**BASE DE DATOS DE TRABAJADORES Y CONTRATISTAS DESTACADOS EN OFICINAS DE LA COMPAÑÍA.**	**Gestión del personal; desarrollo profesional y gestión de recursos; administración de contratistas; salud ocupacional; gestión de seguridad e incidentes; organización, planificación y administración de trabajo; verificación de identidad y seguridad, entre otros.**
103	Privado	**AUTOMARKET DEL PERU S.A.**	**BASE DE DATOS DE EX TRABAJADORES DE LA COMPAÑÍA.**	**Administración de la información de nómina, extender certificados de trabajo, entre otros.**
104	Privado	**EXXONMOBIL AVIACION PERU S.A.**	**BASE DE DATOS DE TRABAJADORES Y CONTRATISTAS DESTACADOS EN OFICINAS DE LA COMPAÑÍA.**	**Gestión del personal; desarrollo profesional y gestión de recursos; administración de contratistas; salud ocupacional; gestión de seguridad e incidentes; organización, planificación y administración de trabajo; verificación de identidad y seguridad, entre otros.**
105	Privado	**TARGET HR S.A.C**	**PLANILLA DE TRABAJADORES DE TARGET HR S.A.C.**	**Cumplir con la normatividad legal laboral que implica manejar información personal de los trabajadores en la planilla de pago. Ingresar toda la información personal en el software de planilla SS Human Resource que se encuentra alojada en el servicio web de la empresa.**
106	Privado	**TARGET HR S.A.C**	**RECLUTAMIENTO Y SELECCIÓN DE PERSONAL**	**Reclutar, evaluar y seleccionar personal con formación técnica y universitaria para poner a disposición de las empresas que solicitan personal con determinado perfil**

				técnico y/o profesional
107	Privado	**COMPAÑÍA MINERA ANTAMINA S.A.**	**COMPAÑIA MINERA ANTAMINA S.A.|**	**ADMINISTRACIÓN DE PERSONAL.**
108	Privado	**ICBC PERU BANK**	**BANCO DE DATOS DEL PERSONAL Y POSTULANTES.**	**Administrar la información personal de los trabajadores para: Comprobar la veracidad de los datos informados; transferir la información a las entidades relacionadas para la formalización; asignar y realizar de manera oportuna los abonos correspondientes al salario y otros beneficios legales.**
109	Privado	**WIGO S.A.**	**BANCO DE DATOS DE CLIENTES.**	**Administrar la información de los usuarios para fines de registro, verificación de identidad y publicitarios**
110	Privado	**CAJA MUNICIPAL DE AHORRO Y CREDITO DE TRUJILLO S.A.**	**BANCO DE DATOS DE CLIENTES.**	**Identificar, controlar, formular estadísticas a nivel operativo y estratégico para una mejor toma de decisiones; crear nuevos productos o servicios**
111	Privado	**CAJA MUNICIPAL DE AHORRO Y CREDITO DE TRUJILLO S.A.**	**BANCO DE DATOS DE TRABAJADORES.**	**Control de ingreso, cese, tiempo de servicio, cálculo de beneficios sociales, declaración de rentas, comunicación a AFPs, ESSALUD.**
112	Privado	**CAJA MUNICIPAL DE AHORRO Y CREDITO DE TRUJILLO S.A.**	**BANCO DE DATOS DE PROVEEDORES.**	**Promover la participación de pluralidad de proveedores en los procesos de adquisición de bienes y servicios que realiza la entidad**
113	Privado	**AGROINVERSIONES VALLE Y PAMPA PERÚ S.A.**	**BANCO DE DATOS DE VALLE Y PAMPA.**	**Administración de información, emisión de certificados, entre otros.**
114	Privado	**UNIVERSIDAD PERUANA CAYETANO HEREDIA - UPCH**	**BASE DE DATOS ACADÉMICA.**	**Registro, seguimiento y archivo del estado académico de los alumnos y docentes de la Universidad Peruana**

				Cayetano Heredia
115	Privado	**UNIVERSIDAD PERUANA CAYETANO HEREDIA - UPCH**	**BASE DE DATOS DE PROVEEDORES.**	**Transacciones comerciales.**
116	Privado	**UNIVERSIDAD PERUANA CAYETANO HEREDIA - UPCH**	**BASE DE DATOS DE PERSONAL DE LA UNIVERSIDAD PERUANA CAYETANO HEREDIA.**	**Registro, seguimiento y archivo de los datos del personal docente y no docente de la universidad**
117	Privado	**UNIVERSIDAD DE SAN MARTÍN DE PORRES**	**BASE DE DATOS ACADÉMICA - SICAT**	**Registrar los datos personales, académicos y pagos de los estudiantes de la universidad, como soporte de la gestión académica.**
118	Privado	**BSH ELECTRODOMESTICOS S.A.C.**	**BASE DE DATOS BSH PERÚ — RECURSOS HUMANOS.**	**Ser utilizada por el área de recursos humanos para tener un archivo histórico de los trabajadores, su estatus en la empresa y planilla.**
119	Privado	**BSH ELECTRODOMESTICOS S.A.C.**	**BASE DE DATOS BSH PERÚ — CONTABILIDAD Y FINANZAS.**	**Ser utilizada por el área de contabilidad y finanzas para tener un registro histórico de los clientes y proveedores con la finalidad de realizar cobros y pagos.**
120	Privado	**BSH ELECTRODOMESTICOS S.A.C.**	**BASE DE DATOS BSH PERÚ — MARKETING Y SERVICIO AL CLIENTE.**	**Ser utilizada por el área de marketing, servicio al cliente y ventas para enviar ofertas promocionales, novedades relacionadas a nuevos productos e invitaciones a eventos vía correo. Tener un registro de clientes y productos vendidos.**
121	Privado	**PERU MARINE OIL S.A.C — PEMO S.A.C.**	**PERSONAL PERU MARINE OIL.**	**Evaluar al personal para la contratación y almacenar los datos por el área de recursos humanos para atender lo que disponga e l Poder Judicial u otros organismos.**
122	Privado	**ESCUELA DE PERIODISMO JAIME BAUSATE Y MEZA**	**BANCO DE DATOS PERSONALES DE LOS ALUMNOS.**	**Fines académicos durante los años de estudios de los alumnos**

123	Privado	**WIGO S.A.**	**BANCO DE DATOS DE TRABAJADORES**	**Administrar la información de los trabajadores para fines de compensación, bienestar social, salud y control interno del recurso humano.**
124	Privado	**GENOMMA LAB PERÚ S.A.**	**CLIENTES Y/0 USUARIOS DE LA GARANTIA DE DEVOLUCIÓN**	**Identificar a los clientes y/o usuarios que compran productos importados por Genomma Lab Perú y que solicitan la garantía de devolución ante la insatisfacción de los resultados del producto adquirido.**
125	Privado	**UNIVERSIDAD PERUANA DE ARTE ORVAL S.A.C.**	**BANCO DE DATOS ALUMNOS UNIVERSIDAD**	**Comunicaciones varias**
126	Público	**MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS**	**SISTEMA DE DATOS DE LA DIRECCIÓN DE GRACIAS PRESIDENCIALES.**	**Registrar las solicitudes presentadas por los sentenciados que cumplen condena en los establecimientos penitenciarios o que se encuentran bajo regímenes de beneficios penitenciarios y por los procesados, según sea el caso.**
127	Privado	**AMÉRICA MÓVIL PERÚ S.A.C.**	**BASE DE DATOS DE CLIENTES (31 MDM).**	**Para la gestión de clientes en la prestación del servicio público de telecomunicaciones que brinda la empresa.**
128	Privado	**AMÉRICA MÓVIL PERÚ S.A.C.**	**BASE DE DATOS DE TRABAJADORES.**	**Mantener el registro actualizado de los datos de los trabajadores de la empresa.**
129	Privado	**AMÉRICA MÓVIL PERÚ S.A.C.**	**BASE DE DATOS DE PROVEEDORES (BI MDM).**	**Tener actualizada la información de proveedores para emitir órdenes de compra y realizar**
130	Público	**MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS**	**PROGRAMAS DEL CMAN**	**La base de datos del Plan Integral de Reparaciones permite conocer la afectación que sufriera la víctima del proceso de violencia ocurrido en el Perú entre los años 1980 al 2000 inscrita en el**

				Registro Único de Víctimas, lo que determinará la reparación a la que le asiste la Ley N° 28592.
131	Publico	**SUPERINTENDENCIA NACIONAL DE LOS REGISTROS PÚBLICOS**	**LEGAJO DE PERSONAL.**	**Contar con los datos personales de los trabajadores.**
132	Privado	**PRIME PROFESIONAL S.A.C**	**BANCO DE DATOS PRIME PROFESIONAL**	**Envío de información acerca de cursos de capacitación.**
133	Privado	**TIRE SERVICE PERÚ S.A. - P.T.S. S.A.**	**PLANILLAS.**	**Pagos de planillas.**
134	Privado	**TIRE SERVICE PERÚ S.A. - P.T.S. S.A.**	**FACTURACIÓN.**	**Emisión de boletas de venta.**
135	Privado	**COLEGIO DE NUTRICIONISTAS DEL PERÚ**	**BANCO DE DATOS DEL PERSONAL ADMINISTRATIVO DEL COLEGIO DE NUTRICIONISTAS DEL PERÚ.**	**Conocer los datos del personal que trabaja en la institución para brindar un servicio de calidad a los colegiados y favorecer al personal en su desarrollo profesional.**
136	Privado	**COLEGIO DE NUTRICIONISTAS DEL PERÚ**	**BANCO DE DATOS DE COLEGIADOS DEL COLEGIO DE NUTRICIONISTAS DEL PERÚ.**	**Conocer la información de los miembros de la orden prestos a ejercer la profesión en condición de colegiados y habilitados.**
137	Privado	**UNIVERSIDAD DE LIMA**	**BANCO DE DATOS PERSONALES DE LA UNIVERSIDAD DE LIMA.**	**La Universidad de Lima como institución académica de educación superior utiliza esta base de datos personales de miembros de su comunidad universitaria para fines educativos, y laborales en el caso de los datos del personal docente y no docente.**
138	Privado	**LIFE SOCIAL NETVVORK PERÚ S.A.C.**	**USUARIOS.**	**Gestión de los usuarios registrados en la red life social**
139	Privado	**GOULDS PUMPS (N.Y.) INCORPORATED SUCURSAL DEL PERU**	**BANCO DE DATOS DE RECURSOS HUMANOS.**	**Gestión de recursos humanos.**
140	Privado	**PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ**	**TRABAJADORES Y PROVEEDORES DE LA PUCP.**	**Administrar los pagos, beneficios, aportaciones de ley de los trabajadores y**

				proveedores de la universidad. Proporcionar a las entidades estatales los reportes que requieran
141	Privado	**PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ**	**PROSPECTO, POSTULANTES, ALUMNOS Y EX ALUMNOS DE LA PUCP.**	**Administrar los procesos de captación, admisión, enseñanza y fidelización de la institución**
142	Privado	**BTG PACTUAL PERÚ S.A. SOCIEDAD AGENTE DE BOLSA**	**BTG PACTUAL PERÚ S.A. SOCIEDAD AGENTE DE BOLSA.**	**Tener una base de datos de todos nuestros clientes nacionales y extranjeros, naturales y jurídicos que realizan operaciones bursátiles a través de nuestra empresa.**
143	Privado	**VIVA GYM S.A.**	**BANCO DE DATOS DE TRABAJADORES.**	**Administrar la información de los trabajadores para fines de compensación, bienestar social, salud y control interno de recursos humanos**
144	Privado	**VIVA GYM S.A**	**BANCO DE DATOS DE TRABAJADORES.**	**Administrar la información de los trabajadores para fines de compensación, bienestar social, salud y control interno de recursos humanos**
145	Privado	**AUSTRAL GROUP S.A.A.**	**ARCHIVO DE RECURSOS HUMANOS.**	**Trazabilidad de la información para efectos de procesos de RRHH (capacitación, desarrollo, entre otros). Prevenir riesgos laborales. Evidenciar cumplimientos legales ante las entidades fiscalizadoras estatales y privadas.**
146	Privado	**ASOCIACIÓN UNIVERSIDAD ANTONIO RUIZ DE MONTOYA**	**SISTEMA MAGIX.**	**Automatización de información de docentes, alumnos y personal administrativo**
147	Privado	**INNOVAR MARKETING S.A.C.**	**BASE DE DATOS DE CONCURSANTES.**	**Base de datos recolectada de los concursantes de juegos de lotería y/o similares para gestión de clientes.**

148	Público	**MINISTERIO DEL AMBIENTE**	**SISTEMA SIGFYS.**	**Sistema administrado por el sistema de informática y tecnologías de la información. Este sistema tiene entre sus módulos uno de datos personales cuya información es registrada por el sistema de recursos humanos. Asimismo, el sistema SIGFYS está previsto como soporte informático de los sistemas.**
149	Privado	**EDPYME ACCESO CREDITICIO SOCIEDAD ANÓNIMA**	**WFACR.**	**Generación de créditos, datos del personal**
150	Público	**UNIVERSIDAD NACIONAL DE TRUJILLO**	**PLANILLA DE PERSONAL DOCENTE Y ADMINISTRATIVO.**	**Ejecutar la relación contractual con el personal docente y administrativo.**
151	Privado	**THE BANK OF TOKYO-MITSUBISHI UFJ, LTD**	**INFORMACIÓN PERSONAL DE LOS EMPLEADOS DE LA OFICINA DE REPRESENTACIÓN EN LIMA DE THE BANK OF TOKYO-MITSUBISHI UFJ, LTD.**	**Gestión de recursos humanos**
152	Privado	**CAJA RURAL DE AHORRO Y CRÉDITO SIPAN S.A.**	**CLIENTES.**	**Registrar los datos de los clientes de cuentas activas (créditos, cartas fianza) y pasivas (cuentas de ahorros, órdenes de pago CTS, depósitos a plazo).**
153	Privado	**CAJA RURAL DE AHORRO Y CRÉDITO SIPAN S.A.**	**TRABAJADORES.**	**Registrar los datos personales de los trabajadores**
154	Privado	**CAJA RURAL DE AHORRO Y CRÉDITO SIPAN S.A.**	**PROVEEDORES.**	**Registrar los datos comerciales y contactos de proveedores.**
155	Privado	**UNIVERSIDAD DEL PACÍFICO**	**TRABAJADORES.**	**Contar con los datos de los trabajadores de la universidad con la finalidad de utilizarlos en gestiones institucionales y administrativas**

156	Privado	**UNIVERSIDAD DEL PACÍFICO**	**PADRES O TUTORES.**	**Utilizarlos en gestiones académicas, institucionales, administrativas y comerciales, así como procesar y manejar información para el adecuado desarrollo de la prestación de servicios educativos.**
157	Privado	**UNIVERSIDAD DEL PACÍFICO**	**ESTUDIANTES Y EGRESADOS.**	**Utilizarlos en gestiones académicas, institucionales, administrativas y comerciales, así como procesar y manejar información para el adecuado desarrollo de la prestación de servicios educativos.**
158	Privado	**UNIVERSIDAD DEL PACÍFICO**	**INTERESADOS / POSTULANTES.**	**Contar con los datos de los interesados y postulantes de las diversas carreras, maestrías, diplomados o programas educativos que ofrece la universidad, con la finalidad de utilizarlos en gestiones institucionales, administrativas y comerciales.**
159	Privado	**B2IMPROVE S.A.C.**	**RRHH.**	**Información para gestión de recursos humanos y pago de planillas**
160	Privado	**EMPRESA PERUANA DE SERVICIOS EDITORIALES S.A. - EDITORA PERÚ**	**GESPO - SISTEMA DE GESTIÓN DE PUBLICACIONES (TABLA DE CLIENTES).**	**Registrar datos de clientes para efectos de realizar tareas de venta y post-venta**
161	Privado	**EMPRESA PERUANA DE SERVICIOS EDITORIALES S.A. - EDITORA PERÚ**	**SISTEMA BAAN IV - PROVEEDORES.**	**Sistema integrado de datos para uso en procesos de compras.**
162	Privado	**EMPRESA PERUANA DE SERVICIOS EDITORIALES S.A. - EDITORA PERÚ**	**LEGAJO PERSONAL.**	**Soporte físico donde constan los documentos personales de los trabajadores y los que se generan durante la relación laboral, es utilizado como fuente de consulta para necesidades propias de la relación laboral.**

163	Privado	**EMPRESA PERUANA DE SERVICIOS EDITORIALES S.A. - EDITORA PERÚ**	**PROGRAMA ADRYAN - DATOS PERSONALES.**	**Fuente de donde se obtienen datos para emisión de boletas de pago y demás relacionados con la administración del personal que labora en Editora Perú.**
164	Privado	**COLEGIO DE ARQUITECTOS DEL PERÚ**	**PLANILLA DE TRABAJADORES - PDT PLAME.**	**Registrar a los trabajadores y cumplir con las disposiciones del Ministerio de Trabajo y Promoción del Empleo que regula el cumplimiento del T-Registro.**
165	Privado	**COLEGIO DE ARQUITECTOS DEL PERÚ.**	**REGISTRO DE MATRÍCULA DEL COLEGIO DE ARQUITECTOS DEL PERÚ.**	**Cumplir con lo dispuesto en la Ley N° 14085, Ley de Creación del Colegio de Arquitectos del Perú, en la Ley N° 16053, Ley que Autoriza a los Colegios de Arquitectos del Perú y al Colegio de Ingenieros del Perú para Supervisar a los Profesionales de Arquitectura e Ingeniería de la República y**
166	Privado	**ASTRAZENECA PERÚ S.A.**	**BASE DE DATOS DE EMPLEADOS.**	**Base de datos recolectada para la gestión de recursos humanos.**
167	Privado	**PURE BIOFUELS DEL PERÚ S.A.C.**	**BANCO DE DATOS PERSONALES PBF.**	**Recopilación de datos personales de nuestros trabajadores, clientes y proveedores para efectos legales, referidos a derechos y deberes laborales, tributarios, seguros, entre otros.**
168	Privado	**PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ**	**CENTURIA.**	**Dar soporte a la gestión administrativa.**
169	Privado	**BDO OUTSOURCING S.A.C.**	**BANCO DE DATOS DE TRABAJADORES.**	**Administrar la información de los trabajadores para fines de compensación, bienestar social, salud y control interno de recursos humanos**

170	Privado	**BBVA BANCO CONTINENTAL**	**RECLAMOS**	**Recoger información de las reclamaciones de los clientes para su estudio.**
171	Privado	**BBVA BANCO CONTINENTAL**	Clientes	**Marketing, información de gestión, información administración y gestión de relaciones con productos servicios BBVA.**
172	Privado	**CAJA MUNICIPAL DE AHORRO Y CRÉDITO DE ICA S.A.**	**BANCO DE DATOS DE VIDEO VIGILANCIA.**	**Captación, transmisión, conservación y almacenamiento de imágenes, incluida su reproducción o emisión en tiempo real con fines de video vigilancia de acuerdo a las políticas internas de la empresa.**
173	Privado	**CAJA MUNICIPAL DE AHORRO Y CRÉDITO DE ICA S.A.**	**BANCO DE DATOS PERSONALES DE PROVEEDORES.**	**Gestión administrativa de la información de proveedores para la adquisición de bienes, servicios u obras con la finalidad de cumplir con las obligaciones adquiridas, garantizando las operaciones de la empresa.**
174	Privado	**CAJA MUNICIPAL DE AHORRO Y CRÉDITO DE ICA S.A**	**BANCO DE DATOS DE RECURSOS HUMANOS.**	**Indica que realiza transferencia de datos personales a nivel nacional a entidades aseguradoras,(EPS), centros de salud, (AFP), colegios profesionales, instituciones educativas, seguro social, Oficina de Normalización Previsional (ONP), otras entidades públicas, administración tributaria.**
175	Privado	**CAJA MUNICIPAL DE AHORRO Y CRÉDITO DE ICA S.A.**	**BANCO DE DATOS DE CLIENTES.**	**Gestión administrativa de la información de clientes para el ofrecimiento de los productos y servicios de la empresa, así como la administración de los contratos celebrados.**

176	Privado	**BBVA BANCO CONTINENTAL**	**PRÉSTAMOS.**	**Gestión y administración de la cartera de préstamos.**
177	Privado	**MATTEL PERÚ S.A.**	**DATA CLIENTES.**	**Fines comerciales**
178	Privado	**MATTEL PERÚ S.A.**	**DATA PERSONAL MATTEL PERÚ.**	**Registro de información de los trabajadores de Mattel Perú para fines de control que toda entidad (empresa) necesita.**
179	Privado	**PRODUCTOS Y MERCADOS AGRÍCOLAS DE HUARAL CAJA RURAL DE AHORRO Y CRÉDITO - CAJA RURAL PRYMERA**	**DATOS DE CLIENTES.**	**Registro detallado de clientes.**
180	Privado	**PRODUCTOS Y MERCADOS AGRÍCOLAS DE HUARAL CAJA RURAL DE AHORRO Y CRÉDITO - CAJA RURAL PRYMERA**	**DATOS DE PROVEEDORES.**	**Registro de proveedores.**
181	Privado	**PRODUCTOS Y MERCADOS AGRÍCOLAS DE HUARAL CAJA RURAL DE AHORRO Y CRÉDITO - CAJA RURAL PRYMERA**	**DATOS DE TRABAJADORES.**	**Registro detallado de los colaboradores**
182	Privado	**CONEXIÓN ADULTO MAYOR E.I.R.L.**	**USUARIOS DEL PORTAL WEB CONEXIÓN ADULTO MAYOR.**	**Enviar información comercial o de publicidad mediante cualquier medio y soporte tanto de la empresa como de sus socios comerciales, responder consultas acerca de productos y servicios, cumplir obligaciones ante una eventual obligación contractual entre Conexión Adulto Mayor y el usuario, enviar invitaciones.**
183	Público	**CONSEJO NACIONAL DE CIENCIA, TECNOLOGÍA E INNOVACIÓN TECNOLÓGICA – CONCYTEC**	**DIRECTORIO NACIONAL DE INVESTIGADORES EN CIENCIA, TECNOLOGÍA E INNOVACIÓN.**	**Contribuir al ordenamiento de los profesionales que se dedican a la investigación en forma temporal o permanente. Ser referente único de capacidades humanas en las diferentes áreas temáticas del conocimiento científico**

				y tecnológico en
184	Privado	**COFACE SERVICES PERÚ S.A.**	**BANCO DE DATOS DE LOS EMPLEADOS Y POSTULANTES.**	**Administrar la información personal de los trabajadores relacionada a la gestión de recursos humanos, cumplir con la normativa laboral vigente respecto de la transferencia de esta información a las entidades relacionadas con la formalización de su permanencia en la empresa y del pago de remuneración**
185	Privado	**SUMITOMO METAL MINING PERÚ S.A.**	**BANCO DE DATOS DE TRABAJADORES.**	**Administrar la información de los trabajadores para fines de compensación, bienestar social, salud y control interno de recursos humanos.**
186	Privado	**AMERICATEL PERÚ S.A.**	**BANCO DE DATOS DE TRABAJADORES DE AMERICATEL PERÚ S.A.**	**Contar con una base de datos de los trabajadores**
187	Privado	**TYCO ELECTRONICS DEL PERÚ S.A.C.**	**BANCO DE DATOS DE LOS TRABAJADORES.**	**Gestionar el área de recursos humanos.**
188	Privado	**KROMASOL S.A.C.**	**LISTA DE DISTRIBUIDORES.**	**Base de datos recolectada para la gestión económica de los distribuidores para el pago de beneficios, comisiones, etc**
189	Privado	**INTERNET MEDIA SERVICES PERÚ S.R.L**	**BANCO DE DATOS DE EMPLEADOS.**	**Mantener la información de empleados actualizada para fines de recursos humanos.**
190	Privado	**BLUESTAR ENERGY S.A.C.**	**BANCO DE DATOS DE EMPLEADOS.**	**Mantener actualizada la información de los empleados para la correcta gestión de las remuneraciones y beneficios**
191	Privado	**BBVA BANCO CONTINENTAL**	**MEDIOS DE PAGO.**	**Fabricación y administración de tarjetas de crédito-débito y administración de comercios**
192	Privado	**BANCO CENTRAL DE RESERVA DEL PERÚ**	**BASE DE DATOS DEL PERSONAL Y PRACTICANTES DEL**	**Disponer de información general de los trabajadores y**

			BANCO.	**practicantes**
193	Privado	**NEXOS COMERCIALES S.A.C. - NEXCOM S.A.C**	**BASE DE DATOS DE LOS TRABAJADORES DE LA EMPRESA.**	**Gestión de recursos humanos de la empresa.**
194	Privado	**CETCO S.A.**	**BANCO DE DATOS PERSONALES DE COLABORADORES BELCORP.**	**Contar con un banco de datos de todas las personas que trabajan en CETCO S.A.**
195	Privado	**BBVA BANCO CONTINENTAL**	**CUENTAS PERSONALES.**	**Gestión y administración de la cartera de cuentas personales.**
196	Privado	**TELEFONICA DEL PERU**	**SISTEMA INTEGRADO DE VALORES (SIVA). ADMINISTRACIÓN DE LOS TÍTULOS VALOR DE LOS ACCIONISTAS DE TELEFÓNICA DEL PERÚ S.A.A.**	**Administración de los títulos valor, el cual abarca la administración integral de la base de datos de los accionistas de Telefónica del Perú S.A.**
197	Privado	**LAIN INTERCORP S.A.**	**BASE DE DATOS DE PACIENTES.**	**Recoger los datos de los pacientes con el objetivo de facilitar la asistencia médico nutricional**
198	Privado	**LAIN INTERCORP S.A.**	**BASE DE DATOS DE TRABAJADORES.**	**Contar con la base de datos de los trabajadores para la gestión de los recursos humanos**
199	Privado	**MICHELIN DEL PERU S.A.**	**ARCHIVO DE SERVICIO DE PERSONAL - PERÚ.**	**Mantener centralizada toda la información del personal contratado en un solo formato.**
200	Privado	**BANCO DE CRÉDITO DEL PERÚ**	**USUARIOS.**	**Administrar la información de clientes que tienen o han tenido productos del banco (activos o inactivos), así como la información de clientes potenciales. (No incluye información de colaboradores ni proveedores).**
201	Privado	**BANCO DE CRÉDITO DEL PERÚ**	**PROVEEDORES.**	**Administrar información de los proveedores con los que trabaja o trabajó la compañía que permita evaluar, controlar, compensar los trabajos realizados.**

202	Privado	**BANCO DE CRÉDITO DEL PERÚ**	**ATENCIÓN DE RECLAMOS.**	**Registrar, monitorear y gestionar los reclamos recibidos por las personas naturales para dar pronta respuesta a sus requerimientos.**
203	Privado	**BANCO DE CRÉDITO DEL PERÚ**	**ARCHIVO GDH.**	**Administrar los documentos físicos asociados a la gestión de recursos humanos.**
204	Privado	**BANCO DE CRÉDITO DEL PERÚ**	**REPRESENTANTES LEGALES.**	**Identificar las firmas autorizadas y poderes que permita controlar y gestionar el manejo de cuentas, las operaciones y contratos.**
205	Privado	**BBVA BANCO CONTINENTAL.**	**INTERVINIENTES OPERACIONES DE LEASING.**	**Información para la concesión, administración y gestión de operaciones de leasing.**
206	Privado	**CIBERTEC PERÚ S.A.C.**	**BASE DE DATOS DEL CONCURSO "PIMP MY PROFILE".**	**Ejecución del concurso "Pimp my Profile". Enviar información publicitaria sobre productos y servicios de CIBERTEC. Captación de**
207	Privado	**DELCA MEDICAL S.A.C.**	**BASE DE DATOS DE TRABAJADORES DE DELCA MEDICAL S.A.C.**	**Gestión de recursos humanos.**
208	Privado	**BBVA BANCO CONTINENTAL**	**EMPLEADOS.**	**Información para la gestión de recursos humanos (empleados-familiares relacionados) y elaboración de planillas del BBVA Banco Continental**
209	Privado	**CAVALI S.A. I.C.L.V.**	**VIDEO VIGILANCIA.**	**Grabación fílmica de las locaciones en las dos sedes de CAVALI (San Isidro y Lima) para fines de seguridad.**
210	Privado	**CAVALI S.A. I.C.L.V.**	**REGISTRO DE FIRMAS DE CLIENTES.**	**Registrar los datos de los representantes legales y personas autorizadas de nuestros clientes (Participantes y Emisores), quienes estarán facultados para solicitar los servicios brindados por CAVALI,**

				así como podrán enviar y recibir información.
211	Privado	**CAVALI S.A. I.C.L.V.**	**USUARIOS DEL BOLETÍN CAVALI.**	**Registrar a los usuarios del Boletín CAVALI, quienes reciben información y estadísticas sobre el mercado de valores.**
212	Privado	**CAVALI S.A. I.C.L.V.**	**USUARIOS DEL SERVICIO CAVALI WEB.**	**Registrar los datos personales de los titulares de valores anotados en cuenta, que deciden usar el servicio CAVALI WEB.**
213	Privado	**CAVALI S.A. I.C.L.V.**	**REGISTRO CONTABLE.**	**Registrar los datos personales de todos los titulares de valores anotados en cuenta**
214	Privado	**CAVALI S.A. I.C.L.V.**	**BANCO DE DATOS DE CURRICULUM VITAE DE TRABAJADORES Y POSTULANTES A PUESTOS DE TRABAJO EN CAVALI.**	**Registrar los curriculum vitae de los trabajadores y postulantes elegibles para un puesto de trabajo en CAVALI.**
215	Privado	**CAVALI S.A. I.C.L.V.**	**BASE DE DATOS DE COLABORADORES DE CAVALI.**	**Registrar los datos personales de los colaboradores que realizan labores en CAVALI**
216	Privado	**CAVALI S.A. I.C.L.V.**	**BASE DE DATOS DE PROVEEDORES PERSONAS NATURALES.**	**Identificar los datos de los proveedores personas naturales y los servicios que prestan a**
217	Privado	**NATURE'S SUNSHINE PRODUCTS DEL PERÚ S.A.**	**BASE DE DATOS DE CLIENTES MULTINIVEL AL 23 DE ENERO DEL 2012.**	**Nuestra empresa trabajó con el sistema de comercialización Multinivel desde su creación hasta el 23 de enero del 2012, posteriormente cambió a sistema Retail.**
218	Privado	**NATURE'S SUNSHINE PRODUCTS DEL PERÚ S.A.**	**BASE DE DATOS DE EMPLEADOS.**	**Registro de los empleados de la empresa.**
219	Privado	**NATURE'S SUNSHINE PRODUCTS DEL PERÚ S.A.**	**BASE DE DATOS DE CLIENTES RETAIL.**	**Relación de las personas que compran nuestros productos y se utilizan los datos para fines comerciales como informarles de promociones, lanzamientos de nuevos**

				productos, etc
220	Privado	**NATURE'S SUNSHINE PRODUCTS DEL PERÚ S.A.**	**BASE DE DATOS DE DEUDORES.**	**Cobranza de ex clientes de la empresa que mantienen deudas.**
221	Privado	**CLÍNICA SAN MARCOS S.A.**	**HISTORIAS CLÍNICAS.**	**Registrar el historial médico de los pacientes.**
222	Privado	**CLÍNICA FEIJOO E.I.R.L.**	**HISTORIAS CLÍNICAS.**	**Ordenar las historias clínicas.**
223	Privado	**PLEYADE PERU CORREDORES DE SEGUROS SAC**	**PLANILLAS.**	**Contar con información relevante para la ejecución de obligaciones laborales.**
224	Privado	**T-GESTIONA LOGÍSTICA S.A.C**	**PLANILLAS.**	**Contar con información relevante para la ejecución de obligaciones laborales**
225	Privado	**TELEFONICA INTERNATIONAL WHOLESALE SERVICES PERU S.A.C.**	**PLANILLAS**	**Contar con información relevante para la ejecución de obligaciones laborales.**
226	Privado	**TELEFONICA DEL PERU S.A.A.**	**PLANILLAS**	**Contar con información relevante para la ejecución de obligaciones laborales.**
227	Privado	**SERVICIOS GLOBALES DE TELECOMUNICACIONES S.A.C.**	**PLANILLAS**	**Contar con información relevante para la ejecución de obligaciones laborales.**
228	Privado	**MEDIA NETWORKS LATIN AMERICA S.A.C.**	**PLANILLAS**	**Contar con información relevante para la ejecución de obligaciones laborales.**
229	Privado	**TELEFONICA LEARNING SERVICES PERU S.A.C**	**PLANILLAS**	**Contar con información relevante para la ejecución de obligaciones laborales.**
230	Privado	**TELEFONICA MULTIMEDIA S.A.C.**	**PLANILLAS**	**Contar con información relevante para la ejecución de obligaciones laborales.**
231	Privado	**TFP S.A.C.**	**PLANILLAS**	**Contar con información relevante para la ejecución de obligaciones laborales.**
232	Privado	**TELEFONICA CENTROS DE COBRO S.A.C**	**PLANILLAS**	**Contar con información relevante para la ejecución de**

				obligaciones laborales.
233	Privado	**FUNDACION TELEFONICA DEL PERU**	**PLANILLAS**	**Contar con información relevante para la ejecución de obligaciones laborales.**
234	Privado	**WAYRA PERU ACELERADORA DE PROYECTOS S.A.C**	**PLANILLAS**	**Contar con información relevante para la ejecución de obligaciones laborales.**
235	Privado	**TELEFONICA MOVILES S.A.**	**SISTEMA INTEGRADO DE VALORES (SIVA). ADMINISTRACIÓN DE LOS TÍTULOS VALOR DE LOS ACCIONISTAS DE TELEFONICA MOVILES S.A**	**Administrar los títulos valor que abarca la administración integral de la base de datos de los accionistas de Telefónica Móviles S.A.**
236	Privado	**INC RESEARCH PERU LIMITED S.R.L.**	**BASE DE DATOS DE LOS EMPLEADOS.**	**Administración de personal.**
237	Privado	**INC RESEARCH PERU LIMITED S.R.L.**	**BASE DE DATOS DEL INVESTIGADOR.**	**Gestión de ventas, marketing y captación de clientes.**
238	Privado	**COMITE DE OPERACION ECONOMICA DEL SISTEMA INTERCONECTADO NACIONAL – COES**	**BASE DE DATOS COES.**	**Ingresar los documentos que aseguran la formación, experiencia y competencias solicitadas al trabajador, la información sobre sus familiares para el otorgamiento de beneficios, el historial médico-laboral del trabajador**
239	Privado	**GRAÑA Y ASOCIADOS CORREDORES DE SEGUROS S.A.**	**GIT INSURANCE TOOL - LASERFICHE.**	**Intermediación de seguros.**
240	Privado	**S.G. NATCLAR S.A.C.**	**ONLINEBD.**	**Recopilación de información.**
241	Privado	**COOPERATIVA DE AHORRO Y CREDITO PETROPERU LTDA**	**COOPERATIVA PETROPERU.**	**Efectuar operaciones de ahorro y crédito con sus socios respetando el principio cooperativo**
242	Privado	**THE BANK OF TOKYO-MITSUBISHI UFJ, LTD**	**INFORMACIÓN PERSONAL DE USUARIOS DEL SERVICIO BIZBUDDY.**	**La adecuada prestación del servicio de Bizbuddy que consiste en poner a disposición de sus usuarios información económica, política y social en idioma japonés.**

243	Privado	**FONDO MIVIVIENDA S.A.**	**BANCO DE DATOS DE SUB PRESTATARIOS.**	**Planificar, organizar, dirigir, supervisar y controlar la gestión de los desembolsos y cobranzas de los productos del Fondo Mivivienda S.A.**
244	Privado	**FONDO MIVIVIENDA S.A.**	**BANCO DE DATOS DEL PROGRAMA TECHO PROPIO.**	**Administración y otorgamiento del Bono Familiar Habitacional previo proceso de promoción, inscripción, registro, verificación de información y calificación de los grupos familiares elegibles. Programa Techo Propio del Fondo Mivivienda**
245	Privado	**FONDO MIVIVIENDA S.A.**	**BANCO DE DATOS DE COLABORADORES**	**Pago de haberes, beneficios sociales,declaraciones de rentas, control de asistencia y video vigilancia, exámenes médicos ocupacionales**
246	Privado	**BANCO INTERNACIONAL DEL PERU S.A.A. INTERBANK**	**BASE DE DATOS DE CLIENTES.**	**Realizar acciones comerciales (venta, retención, comunicación) a través de los diferentes canales (mailing, telefónico, presenciales, telefónicos o e-mailing).**
247	Privado	**BANCO INTERNACIONAL DEL PERU S.A.A. INTERBANK**	**BASE DE DATOS DE COLABORADORES.**	**Elaboración de las planillas de remuneraciones, retención y pago de los impuestos, aportaciones que establece la ley, control de asistencia y vacaciones.**
248	Privado	**BANCO INTERNACIONAL DEL PERU S.A.A. INTERBANK**	**BASE DE DATOS DE POSTULANTES.**	**Ofrecer a los postulantes puestos de trabajo de acuerdo a su perfil.**
249	Privado	**BANCO INTERNACIONAL DEL PERU S.A.A. INTERBANK**	**BASE DE DATOS DE PROVEEDORES.**	**Generar las órdenes de compra por los servicios requeridos.**
250	Público	**SUPERINTENDENCIA DEL MERCADO DE VALORES — SMV**	**REGISTRO DE DATOS PERSONALES Y LABORALES DEL PERSONAL DE LA**	**Gestión de documentación laboral para registros y pagos de remuneraciones,**

			SUPERINTENDENCIA DEL MERCADO DE VALORES.	**beneficios laborales, seguridad social y seguridad y salud en el trabajo.**
251	Privado	**CAE AVIATION TRAINING PERU S.A.**	**BANCO DE DATOS DEL PERSONAL DE LA EMPRESA.**	**Evaluación para contratación, contratación, pago de planillas, aportaciones en el sistema de pensiones, aportaciones de Essalud, registro de ingreso y salida.**
252	Privado	**CAE AVIATION TRAINING PERU S.A.**	**BANCO DE DATOS DE CLIENTES DE LA EMPRESA.**	**Facturación por servicios entregados, programación de turnos y registros de ingresos y salidas a las instalaciones.**
253	Privado	**CAE AVIATION TRAINING PERU S.A.**	**BANCO DE DATOS DE PROVEEDORES DE LA EMPRESA.**	**Pago por servicios prestados por los proveedores y registro de ingresos y salidas a las instalaciones**
254	Privado	**CAE AVIATION TRAINING PERU S.A.**	**BANCO DE DATOS DE VIDEO VIGILANCIA.**	**Registrar videos de las instalaciones por**
255	Privado	**CLINICA SAN ANTONIO DE VITARTE S.A**	**BANCO DE DATOS DE PACIENTES.**	**Gestión de recursos humanos**
256	Privado	**CLINICA SAN ANTONIO DE VITARTE S.A**	**BANCO DE DATOS DE CLIENTES.**	**Gestión de recursos humanos**
257	Privado	**CLINICA SAN ANTONIO DE VITARTE S.A**	**BANCO DE DATOS DE LOS TRABAJADORES.**	**Gestión de recursos del personal.**
258	Privado	**COMPAÑÍA ERICSSON S.A.**	**BASE DE DATOS RECURSOS HUMANOS.**	**Registrar la información de los empleados necesaria para todos los procesos de recursos humanos.**
259	Privado	**COOPERATIVA DE AHORRO Y CREDITO PROMOCION TAHUANTINSUYO 1946 LTDA N° 86**	**BANCO DE DATOS PERSONALES DE PROVEEDORES.**	**Identificar al proveedor que presta servicios a la cooperativa.**
260	Privado	**COOPERATIVA DE AHORRO Y CREDITO PROMOCION TAHUANTINSUYO 1946 LTDA N° 86**	**BANCO DE DATOS PERSONALES DE SOCIOS.**	**Identificar a los socios que realizan operaciones de ahorro y crédito**
261	Privado	**COOPERATIVA DE AHORRO Y CREDITO PROMOCION TAHUANTINSUYO 1946 LTDA N° 86**	**BANCO DE DATOS PERSONALES DE TRABAJADORES.**	**Identificar al personal que trabaja en la cooperativa**

262	Privado	**HOGAR CLÍNICA SAN JUAN DE DIOS**	**PROVEEDORES.**	**Adquisición de bienes y servicios.**
263	Privado	**HOGAR CLÍNICA SAN JUAN DE DIOS**	**RECURSOS HUMANOS.**	**Contratación laboral.**
264	Privado	**HOGAR CLÍNICA SAN JUAN DE DIOS**	**INFORMACIÓN MÉDICA - HISTORIAS CLÍNICAS.**	**Atención de pacientes.**
265	Privado	**LABORATORIO CLINICO INMUNOLOGICO CANTELLA S.A.C.**	**FICHAS MÉDICAS DE PACIENTES DE SALUD OCUPACIONAL.**	**Registrar las fichas médicas de exámenes ocupaciones.**
266	Privado	**INSTITUTO OFTALMOLOGICOS ESPECIALIZADOS DR CARLOS WONG CA. S.A.C.**	**HISTORIAS CLÍNICAS.**	**Archivo físico de historias clínicas de pacientes**
267	Privado	**CLINICA MIRAFLORES S.A.C.**	**DBCLINICA.**	**Almacenar datos de pacientes y personal que trabaja en la empresa.**
268	Privado	**EMPRESA FINANCIERA EDYFICAR S.A. - FINANCIERA EDYFICAR**	**BASE DE DATOS DE PROVEEDORES.**	**Contacto de proveedores.**
269	Privado	**EMPRESA FINANCIERA EDYFICAR S.A. - FINANCIERA EDYFICAR**	**BASE DE DATOS DE TRABAJADORES Y PRACTICANTES.**	**Registro de los datos personales de los colaboradores de la organización**
270	Privado	**EMPRESA FINANCIERA EDYFICAR S.A. - FINANCIERA EDYFICAR**	**BASE DE DATOS DE CLIENTES EDYFICAR CUENTAS ACTIVAS Y PASIVAS.**	**Evaluación de créditos y gestión comercial**
271	Privado	**CLINICA DE OSTEOPOROSIS S.A.C.**	**BANCO DE DATOS DEL PERSONAL.**	**Registrar la información personal de cada trabajador.**
272	Privado	**CLINICA DE OSTEOPOROSIS S.A.C.**	**BASE DE DATOS PROVEEDORES.**	**Registro y control de nuestros proveedores**
273	Privado	**CLINICA DE OSTEOPOROSIS S.A.C.**	**BASE DE DATOS DE PACIENTES.**	**Registrar la información y control de nuestros pacientes.**
274	Privado	**TELEFONICA GESTION DE SERVICIOS COMPARTIDOS PERU S.A.C.**	**PLANILLAS**	**Contar con información relevante para la ejecución de obligaciones laborales.**
275	Privado	**BECERRA BROKERS S.R.L. CORREDORES DE SEGUROS**	**REGISTRO DE PLANILLA DE TRABAJADORES.**	**Dar cumplimiento a las disposiciones y obligación del empleador de registrar a sus trabajadores en la planilla.**

276	Privado	**COOPERATIVA DE AHORRO Y CREDITO SAN PIO X LTDA**	**BPAC.**	**Registro y control de socios, apertura de cuentas, colocaciones y captaciones. Movimientos contables.**
277	Privado	**CLINICA LOS ANDES S.A.C.**	**REGISTRO DE DATOS - PERSONAL EN PLANILLA.**	**Tener un control detallado de las personas que laboran en forma dependiente**
278	Privado	**CLINICA LOS ANDES S.A.C.**	**PRESTADORES DE SERVICIOS DE 4TA. CATEGORIA.**	**Tener una relación del personal que presta servicios independientes a la Clínica Los**
279	Privado	**CLINICA LOS ANDES S.A.C.**	**HISTORIA CLÍNICA.**	**Contar con un registro de pacientes para fines estadísticos y el llenado de historias clínicas**
280	Privado	**EDPYME INVERSIONES LA CRUZ S.A.**	**PROVEEDORES**	**Prestación de bienes y servicios.**
281	Privado	**EDPYME INVERSIONES LA CRUZ S.A.**	**CLIENTES**	**Servicios financieros**
282	Privado	**EDPYME INVERSIONES LA CRUZ S.A.**	**COLABORADORES.**	**Prestación laboral.**
283	Privado	**UNIVERSIDAD TECNOLOGICA DEL PERU S.A.C.**	**ALUMNOS INSTITUTO SUPERIOR TECNOLÓGICO DEL PERÚ (IDAT).**	**Cumplimiento de finalidades contractuales**
284	Privado	**UNIVERSIDAD TECNOLOGICA DEL PERU S.A.C.**	**PROVEEDORES PERSONAS NATURALES**	**Cumplimiento de finalidades contractuales**
285	Privado	**UNIVERSIDAD TECNOLOGICA DEL PERU S.A.C.**	**GERENCIA DE DESARROLLO HUMANO**	**Cumplimiento de finalidades contractuales**
286	Privado	**UNIVERSIDAD TECNOLOGICA DEL PERU S.A.C.**	**ALUMNOS UNIVERSIDAD TECNOLÓGICA DEL PERÚ (UTP).**	**Cumplimiento de finalidades contractuales**
287	Privado	**ASOCIACIÓN MUTUALISTA DEL PERSONAL DE SUB OFICIALES Y ESPECIALISTAS DE SERVICIOS DE LA POLICIA NACIONAL DEL PERU — AMPSOES PNP**	**DATSIF.**	**Registrar los datos de asociados**
288	Privado	**SISTEMA DE PRÉSTAMOS BANQUITO ÁREA DE CRÉDITOS Y CONTROL.**	**SISTEMA DE PRÉSTAMOS BANQUITO ÁREA DE CRÉDITOS Y**	**Registro de datos personales, registro de solicitudes, listado de**

			CONTROL.	**clientes, préstamos**
289	Privado	**SCOTIA FONDOS SOCIEDAD ADMINISTRADORA DE FONDOS S.A.**	**PERSONAS.**	**Perfilamiento y gestión de clientes y prospectos**
290	Privado	**SCOTIA FONDOS SOCIEDAD ADMINISTRADORA DE FONDOS S.A.**	**COLABORADORES.**	**Administrar la información de los colaboradores de la empresa.**
291	Privado	**AON AFFINITY PERU - CORREDORES DE SEGUROS S.A.C**	**BAIS, AON ACCESS.**	**Intermediación de seguros**
292	Privado	**BBVA BANCO CONTINENTAL**	**INFORMES DE SALUD OCUPACIONAL.**	**Control de la salud de los empleados; responder consultas y realizar reconocimientos; adecuación de la persona al puesto de trabajo**
293	Privado	**SUSTAINABLE HARVEST AT ORIGIN LATIN AMERICA**	**PRESTACIÓN DE SERVICIOS.**	**Prestación de servicios**
294	Privado	**SUSTAINABLE HARVEST AT ORIGIN LATIN AMERICA**	**INVITACIÓN A EVENTOS.**	**Invitación a eventos.**
295	Privado	**SUSTAINABLE HARVEST AT ORIGIN LATIN AMERICA**	**RECURSOS HUMANOS**	**Recursos humanos**
296	Privado	**COOPERATIVA DE AHORRO Y CREDITO DE OFICIALES DE LA POLICIA NACIONAL DEL PERU CORONEL G.C. HUMBERTO FLORES HIDALGO**	**COOPERATIVA DE AHORRO Y CREDITO DE OFICIALES DE LA POLICIA NACIONAL DEL PERU CORONEL G.C. HUMBERTO FLORES HIDALGO - CACOP.**	**Intermediación financiera**
297	Privado	**COOPERATIVA DE SERVICIOS MULTIPLES ALAS PERUANAS**	**REGISTROS PERSONALES.**	**Mantener una fluida comunicación con los asociados.**
298	Privado	**BBVA BANCO CONTINENTAL.**	**SELECCION DE PERSONAL**	**Selección, evaluación de personal y recepción del currículo.**
299	Privado	**ASOCIACION MUTUALISTA DE TECNICOS Y SUBOFICIALES DE LA FUERZA AEREA DEL PERU — MUTUA**	**ASOCIACION MUTUALISTA DE TECNICOS Y SUBOFICIALES DE LA FUERZA AEREA DEL PERU — MUTUA.**	**Asociación sin fines de lucro, proporcionar a sus asociados y derechohabientes la asistencia y bienestar en el marco de la seguridad social bajo el principio de solidaridad**
300	Privado	**SERVICIOS MEDICOS DE DIAGNOSTICO S.A - CIMEDIC**	**BASE DE DATOS DE TRABAJADORES EN**	**Contar con información básica y actualizada de**

			PLANILLA	**los trabajadores.**
301	Privado	**SERVICIOS MEDICOS DE DIAGNOSTICO S.A - CIMEDIC**	**BASE DE DATOS DE PACIENTES CIMEDIC**	**Registro de los Pacientes.**
302	Privado	**BBVA BANCO CONTINENTAL**	**SISTEMA DE CONTROL DE VIDEO VIGILANCIA.**	**Fichero de imágenes en formato AVI para video vigilancia en cumplimiento con lo establecido en normas internas sobre tratamiento de datos personales con fines de video vigilancia**
303	Privado	**BANCO GNB PERU S.A.**	**CLIENTES BANCA PASIVA / ACTIVA.**	**Mantener la información almacenada sistemáticamente de los clientes activos y pasivos para la ejecución de los procesos crediticios requeridos y ante cualquier gestión o requerimiento de los clientes.**
304	Privado	**BANCO GNB PERU S.A.**	**BASE DE PROVEEDORES**	**Contar con una base para las cotizaciones de los diferentes servicios que el banco requiera**
305	Privado	**BANCO AGROPECUARIO – AGROBANCO**	**BANCO DE DATOS AGROPLAZA.**	**Registrar la existencia de una base de datos de usuarios del portal e-commerce Agroplaza, portal destinado a facilitar las transacciones comerciales en el sector agrario.**
306	Privado	**INSTITUTO DE CRIOPRESERVACION Y TERAPIA CELULAR S.A.C.**	**DATOS PERSONALES RECURSOS HUMANOS. DATOS CLIENTES CON CONTRATO.**	**Gestión de recursos humanos y gestión de datos para contacto con clientes**
307	Privado	**CENTRO DE REPOSO SAN JUAN DE DIOS (CREMPT) PIURA DE LA ORDEN HOSPITALARIA DE SAN JUAN DE DIOS**	**HISTORIA CLÍNICA DEL USUARIO.**	**Registrar la historia clínica del usuario.**
308	Privado	**EMPRESA FINANCIERA EDYFICAR SOCIEDAD ANONIMA FINANCIERA EDYFICAR**	**BASE DE DATOS DE POSTULANTES PARA UN PUESTO LABORAL EN EDYFICAR.**	**Contactó de posibles candidatos a puestos laborales.**
309	Privado	**EMPRESA FINANCIERA EDYFICAR SOCIEDAD ANONIMA FINANCIERA**	**REGISTRO DE ATENCIÓN DE**	**Registro de las atenciones a las reclamaciones recibidas**

		EDYFICAR	**RECLAMOS.**	**del público en general.**
310	Privado	**EMPRESA FINANCIERA EDYFICAR SOCIEDAD ANONIMA FINANCIERA EDYFICAR**	**VIDEO VIGILANCIA.**	**Seguridad interna de la oficina principal**
311	Privado	**DUPONT PERU S.AC.**	**GESTION DE EMPLEADOS.**	**Registrar todo lo concerniente a datos de empleados asociados a la gestión de recursos humanos.**
312	Privado	**DUPONT PERU S.AC.**	**GESTION DE CLIENTES**	**Registrar los datos personales asociados a la qestión de clientes.**
313	Privado	**DUPONT PERU S.AC.**	**GESTION DE PROVEEDORES.**	**Registrar los datos personales asociados a la i:iestión de proveedores.**
314	Privado	**ARGENPER S.A.**	**BANCO DE DATOS ARPERDB.W2.**	**Registro de operaciones para fines estadísticos y conocimiento dé la cartera de clientes**
315	Privado	**BBVA BANCO CONTINENTAL**	**CONTROL DE ACCESOS A EDIFICIOS DEL BANCO.**	**Seguridad y cpntrol de accesos de personas que ingresan a edificios del · BBVA Banco**
316	Privado	**CLINICA DEL PACIFICO, $.A.**	**BANCO DE DATOS DE TRABAJADORES.**	**Cumplir con las obligaciones formales con cada trabajador.**
317	Privado	**CLINICA DEL PACIFICO, $.A.**	**BANCO DE DATOS DE PACIENTES**	**Llevar el control de atención de pacientes particulares y convenios**
318	Privado	**MEDSALUD S.A.C.**	**REGISTRO DE PLANILLA DE LOS TRABAJADORES.**	**Dar cumplimiento a las disposiciones sobre la obligación remunerativa de los empleadores hacía sus trabajadores.**
319	Privado	**LA COOPERATIVA DE AHORRO Y CREDITO FORTALEZA DE AYACUCHO**	**COOPERATIVA DE AHORRO Y CREDITO FORTALEZA DE AYACUCHO SISTEMA DE INFORMACIÓN BESTERP FINANCIAL.**	**Ingresar datos para la generación de ahorro y crédito.**
320	Privado	**EDPYME ACCESO CREDITICIO SOCIEDAD ANÓNIMA**	**WFACR / PUBLIC.**	**Registrar los datos de los concesionarios.**
321	Privado	**EDPYME ACCESO CREDITICIO SOCIEDAD ANÓNIMA**	**MAE_PRO**	**Registrar los datos de los proveedores**

322	Privado	**EDPYME ACCESO CREDITICIO SOCIEDAD ANÓNIMA**	**MAE_PER.**	**Registrar los datos del personal de la empresa**
323	Privado	**FINANCIERA PROEMPRESA S.A.**	**MAESTRO PROVEEDORES.**	**Registrar los datos comerciales y contactos de proveedores.**
324	Privado	**FINANCIERA PROEMPRESA S.A.**	**MAESTRO TRABAJADORES.**	**Registrar los datos personales de los trabajadores**
325	Privado	**FINANCIERA PROEMPRESA S.A.**	**MAESTRO USUARIOS.**	**Registrar quejas o reclamos.**
326	Privado	**FINANCIERA PROEMPRESA S.A.**	**MAESTRO CLIENTES.**	**Registrar los datos de los clientes para la administración y gestión de relaciones con productos y servicios ofrecidos por la Financiera Proempresa:**
327	Privado	**CAJA RURAL DE AHORRO Y CREDITO CHAVIN S.A.A. — CREDICHAVIN S.A.A**	**CORENEVADO**	**Identificar al cliente para el envío de información de los productos y servicios contratados con Credichavin.**
328	Privado	**ASOCIACION PASTORAL DE SERVICIOS MEDICO ASISTENCIALES JULIACA DE LA IGLESIA ADVENTISTA DEL SEPTIMO DIA**	**CLINICA AMERICANA DE JULIACA**	**Registrar a pacientes y trabajadores.**
329	Privado	**FUNDACION OSWALDO KAUFMANN**	**FUNDACION OSWALDO KAUFMANN**	**Patrocinar al Hospital Andino del Alto Chicama- COINA, brindar asistencia médico-social en la recuperación, protección y prevención de la salud de los pobladores de escasos recursos económicos de las diferentes comunidades del Alto Chicama, La Libertad.**
330	Privado	**MIBANCO, BANCO DE LA MICRO EMPRESA S.A.**	**COLABORADORES**	**Administrar la información de los colaboradores para la gestión de planillas, selección y evaluación, capacitaciones, exámenes médicos y preventivos,**

				gestión de compensaciones, actualización de datos, convenios, comunicaciones y gestión de sanciones.
331	Privado	**MIBANCO, BANCO DE LA MICRO EMPRESA S.A.**	**PROVEEDORES**	Administrar información de los proveedores con los que trabaja o trabajó la compañía que permita evaluar, controlar y compensar los trabajos realizados.
332	Privado	**MIBANCO, BANCO DE LA MICRO EMPRESA S.A.**	**CLIENTES**	Administrar la información de clientes que tienen o han tenido productos, alguna transacción u operación con el banco (vigentes, fallecidos y desertores).
333	Privado	**HOSPIRAPERU SRL**	**BANCO DE DATOS DE TRABAJADORES**	**Administrar la información de los trabajadores para fines de compensación, bienestar social, salud y control interno de recursos humanos.**
334	Privado	**MEDSALUD SAC**	**REGISTRO DE HISTORIAS CLINICAS DE PACIENTES (CAJAMARCA)**	**Registrar los antecedentes para futuras atenciones médicas ocupacionales.**
335	Privado	**MEDSALUD SAC**	**REGISTRO DE PLANILLA DE TRABAJADORES (LIMA)**	Dar cumplimiento a las disposiciones sobre la obligación remunerativa de los empleadores hacia sus trabajadores.
336	Privado	**MEDSALUD SAC**	**REGISTRO DE HISTORIAS CLINICAS DE PACIENTES (LIMA)**	**Registrar los antecedentes para futuras atenciones médicas ocupacionales**
337	Privado	**BBVA CONTINENTAL**	**PROVEEDORES**	**Gestión contable y administrativa de proveedores (personas naturales con o sin negocio).**
338	Privado	**MEDSALUD SAC**	**BASE DE DATOS DE PACIENTES**	**Registrar los datos de los pacientes para la programación de citas, tratamientos, diaanósticos v oaaos.**
339	Privado	**MULTIDENT SRL**	**BASE DE DATOS DE TRABAJADORES**	**Uso y manejo de la base de datos de trabajadores para un adecuado control interno y presentación de impuestos, encuestas ante on:ianismos públicos y privados.**
340	Privado	**CLINICA DEL SEÑOR DE**	**HISTORIAS CLINICAS**	**Registro de datos de identificación y procesos secuenciales de atención en salud a**

		LUREN DE ICA SAC		**pacientes.**
341	Privado	BTG PACTUAL PERU S.A.C.	**BANCO DE DATOS PERSONALES BTG PACTUAL PERU S.A.C. - COLABORADORES.**	**Registrar los datos personales de los colaboradores.**
342	Privado	**BTG PACTUAL PERU S.A. SOCIEDAD AGENTE DE BOLSA - BTG PACTUAL PERU S.A. SAB.**	BTG PACTUAL PERU S.A. SAB. - COLABORADORES	**Registrar los datos personales de los colaboradores.**
343	Privado	**BTG PACTUAL PERU S.A SOCIEDAD ADMINISTRADORA DE FONDOS DE INVERSION**	**BTG PACTUAL PERU S.A. SAFI - COLABORADORES.**	**Registrar los datos personales de los colaboradores.**
344	Privado	**SCOTIABANK PERU S.A.A.**	**COLABORADORES**	**Administrar la información de los colaboradores del banco.**
345	Privado	**SCOTIABANK PERU S.A.A.**	**PERSONAS NATURALES**	**Perfilamiento y gestión de clientes y prospectos.**
346	Privado	**SCOTIABANK PERU S.A.A.**	**CANDIDATOS**	**Reclutamiento y selección de candidatos.**
347	Privado	**CLINICA SAN FRANCISCO DE ASIS SOCIEDAD ANONIMA**	**BANCO DE DATOS CLINICA SAN FRANCISCO DE ASIS SA CAJAMARCA**	**Registro de atenciones medicas a pacientes.**
348	Privado	**CAJA RURAL DE AHORRO Y CREDITO LOS ANDES SOCIEDAD ANONIMA**	**BASE DE DATOS DE CLIENTES**	**Mantener el registro de nuestros clientes de créditos y ahorros para realizar operaciones que brinda la CRAC Los Andes, así como cumplir la requlación dada por la SBS.**
349	Privado	**CAJA RURAL DE AHORRO Y CREDITO LOS ANDES SOCIEDAD ANONIMA**	**BASE DE DATOS DE TRABAJADORES.**	**Mantener el registro de datos de los trabajadores de la CRAC Los Andes relacionados al vinculo laboral empleador empleado,**

				para efecto de control, pago, derechos v deberes.
350	Privado	**B2IMPROVE S.A.C.**	**CLIENTES**	**Información para gestión comercial, publicidad v marketinq.**
351	Privado	**BANCO DE CREDITO DEL PERU**	**GRABACION DE LLAMADAS**	**Grabar por regulación como sustento todas las llamadas de los clientes hacia la entidad financiera (Call Center), grabar los contratos vía telefónica de ventas, servicios del banco y gestión de cobranza.**
352	Privado	**BANCO DE CREDITO DEL PERU**	**CONTROL DE VISITAS**	Registrar y controlar a personas que acceden a edificios específicos de la compañía (sede administrativa /tecnológica)
353	Privado	**BANCO DE CREDITO DEL PERU**	**INGRESO A AMBIENTES RESTRINGIDOS (BIOMETRICO)**	**Controlar el acceso a ambientes restringidos**
354	Privado	**BANCO DE CREDITO DEL PERU**	**VIDEO VIGILANCIA**	**Realizar el monitoreo de alarmas de agencias/sedes de la compañía para atender incidentes que se presenten en estas posiciones, análisis de incidentes al interior de agencias/sedes de la compañía.**

ANEXO Nº 2

Banco de Datos Personales de Entidades Públicas inscritos en el Registro Nacional de Protección de Datos Personales hasta el 01 de Setiembre de 2015

Nº	Titular	Nº de Registro	Comentarios. Banco de Datos Registrados.
1	Ministerio de Justicia	01, 010, 011, 0046, 047, 048, 049, 050, 064, 065, 078, 0130, 468, 469, 958, 959.	Sistema de Notariado. Registro de Funcionarios. Registro de Deudores de Reparaciones Civiles. Directorio Asesores Jurídicos. Registro de Fedatarios Juramentados. Entre otros.
2	Consejo Nacional de la Magistratura	051, 052, 053	Base de Datos del Personal de Apoyo del CNM. Registro de Jueces y Fiscales. Registro de datos de Funcionarios y Autoridades del CNM.
3	SUNARP	0131	Legajo Personal
4	Ministerio del Medio Ambiente	148	Sistema SYGFYS (Recursos Humanos)
5	Universidad Nacional de Trujillo	150	Planilla de Personal Docente y Administrativo.
6	CONCYTEC	183	Directorio Nacional

			de Investigadores
7	**BCR**	**192**	**Base de Datos de Personal y Practicantes**
8	**SMV**	**250**	**Banco de Datos Personales y Laborales.**
9	**OSCE**	**498**	**Banco de Datos de Trabajadores**
10	**Banco de la Nación**	**602, 603, 1012, 1013, 1014, 4362, 4363, 4364, 4365**	**Pensionistas. Clientes. Proveedores. Atención de Reclamos. Selección de personal. Prestamos Multired. Banca Seguros. Tarjeta de Credito. Crédito Hipotecario. Registro de Firmas.**
11	**Autoridad Nacional del Agua**	**957**	**Trabajadores.**
12	**Servicio Nacional de Sanidad Agraria SENASA**		**SIGA- Modulo de Mantenimiento de Personal.**
13	**CENFOTUR Chiclayo**	**1057**	**Estudiantes**
14	**CENFOTUR Cusco**	**1058**	**Estudiantes**
15	**CENFOTUR**	**1673**	**Trabajadores**
16	**Ministerio de Comercio Exterior y Turismo**	**1404**	**Registro de Personas Naturales prohibidas de acceder a las Salas de Juego de Casinos y de Maquinas Tragamonedas por Ludopatia.**
17	**Instituto Geográfico Nacional**	**1443**	**Recursos Humanos**
18	**Proyecto Especial Alto**	**1454**	**Trabajadores**

	Huallaga		
19	**Ministerio de Agricultura y Riego**	**1107. 1108. 1109.1110. 1111. 1112. 1113. 1114. 1116. 1117.**	**Proveedores y Contratistas. Pensionistas. Servidores Activos. Libro de Reclamaciones. Sistema integrado de gestión documentaria. Administración de Dominio de Red Local. Correos Electrónicos. Servidores Activos. Quejas y Denuncias. Control de llamadas telefónicas. Control de asistencia de personal.**
20	**Programa Nacional de Apoyo Directo a los más pobres - JUNTOS**	**1477. 1478**	**Data de Beneficiarios afiliados y abonados al Programa JUNTOS. Recurso Humanos de Empleados JUNTOS.**
21	**CENFOTUR- Cajamarca**	**1517**	**Estudiantes**
22	**SERFOR**	**1695**	**Servidores SERFOR**
23	**SEDAPAL**	**1722. 1781. 1586. 2025.**	**Trabajadores. Video Vigilancia, entre otros.**
24	**Superintendencia Nacional de Salud**	**1886. 1887. 1888. 1889. 1890. 1891. 1892. 1893. 1894. 1895. 1896.**	**Visitantes. Evaluadores. Asegurados. Entre otros.**
25	**Ministerio de Cultura**	**1934. 1935. 1936. 1937.**	**Remuneraciones. Consultas.**

			Profesionales. Arqueólogos.
26	**Instituto Nacional de Defensa Civil - INDECI**	**2024**	**Banco de Datos de Personal del INDECI**
27	**Proyecto Binacional Lago Titicaca**	**2046**	
28	**Defensoría del Pueblo**	**2132. 2133. 2134. 4141. 4142. 4143,**	**Sistema de Información Defensorial. Modulo de Personal de Defensoría del Pueblo, entre otros.**
29	**Instituto Nacional de Ciencias Neurológicas**	**2178. 2179. 2180. 2181. 2182. 2183. 2184.**	
30	**Ministerio de Vivienda, Construcción y Saneamiento.**	**2987. 2988. 2989.**	**Postulantes. Proveedores. Colaboradores.**
31	**Sistema Integral de Salud- SIS**	**3233. 3235. 3239.**	
32	**ONPE**	**3240. 3241. 3242. 3243. 3244. 3245.**	**Aportantes Organizaciones Politicas. Personas involucradas en demandas legales. Electores que figuran en padrones electorales. Personal. Atención ciudadana. Videovigilancia.**
33	**Academia de la Magistratura**	**3255**	**Visitas.**
34	**Ministerio de Trabajo y Promoción del Empleo**	**3543. 3544.**	**Legajo Personal. Planilla Electrónica.**
35	**OSIPTEL**	**3971. 3972**	**Supervisión de Servicios Público de Telecomunicaciones. Video Cámaras.**

36	**INDECOPI**	**3988. 3999. 4000. 4777. 4778. 4779. 4780. 4781. 4782. 4783. 4784. 4785. 4786. 4787. 4788. 4790. 4791. 4792. 4793. 4798. 4832. 4835. 4836.**	**Postulantes. Colaboradores. Usuarios Asesorados. Control de Accesos y Video Vigilancia. Expedientes de Supervisión y Fiscalización. Control de Acceso a la Biblioteca. Registro de Derecho de Autor. Registro de Signos Distintivos. Convenios. Material de Promoción y Difusión. Expedientes de Denuncia OPI (Protección al Consumidor). Registro Gracias No Insista. Procedimientos Concursales. Denuncias Barreras Burocráticas. Entre otros.**
37	**Ministerio de la Producción**	**4018**	**Pensionistas**
38	**IPEN**	**4377. 4378. 4379. 4380. 4381.**	**Trabajadores. Visitantes. Expedientes Procesos Judiciales. Administrados. Usuarios.**
39	**Contraloría General de la Republica.**	**4522. 4523. 4524. 4525.**	**Empleados y Pensionistas. Proveedores.**

			Sistema de Sociedades de Auditoria. Funcionarios y servidores públicos obligados a presentar declaración jurada de ingresos, bienes y rentas.
40	**Tribunal Constitucional**	**4745. 4746. 4747.**	**Personal. Publicidad Institucional. Proveedores.**
41	**Instituto Nacional de Enfermedades Neoplásicas. INEN.**	**4794. 4795. 4796. 4798.**	**Pacientes. Donantes. Trabajadores. Proveedores.**
42	**Ministerio de Relaciones Exteriores**	**4816. 4817. 4818. 4819. 4820. 4821. 4822. 4823.**	**Directivo Activo de Funcionarios. Escalafón. Fojas de Servicios del Cuerpo Diplomático. Nombres de Funcionarios. Certificación de Firmas y Apostilla. Actividades Migratorias. Sistema de Registro Civil. Visitas a Funcionarios.**

ANEXO Nº 3: Entrevista a Thomas Smedinghoff. Agosto de 2015.

Thomas Smedinghoff is Of Counsel at the Firm, where his practice focuses on the new legal issues relating to the developing field of information law and electronic business activities. Tom is internationally recognized for his leadership in addressing emerging legal issues regarding electronic transactions, identity management, privacy, information security, and online authentication issues from both a transactional and public policy perspective. He has been retained to structure and implement first-of-their-kind e-commerce initiatives, electronic transactions, and identity management and information security legal infrastructures for the federal government, and national and international businesses including banks, insurance companies, investment companies, and certification authorities. He has also been actively involved in developing legislation and public policy in the area of electronic business at the state, national, and international levels.

Representative Experience

- Chair of the American Bar Association Identity Management Legal Task Force, and working with private sector, federal government, and international organizations to address the challenges of developing an identity management legal framework
- Serves as counsel for companies, government agencies, and trade associations throughout the world in addressing new and developing legal issues relating to electronic business activities, online electronic transactions, identity management, information security, and data privacy.
- Has worked extensively with clients in newly developing legal areas such as identity management and online authentication, electronic negotiable instruments, digital signatures and voice signatures, PKI, e-notarization, and other unique forms of electronic transactions and e-business activities.
- Was a pioneer in the subject of PKI and digital signature law, representing the federal government, national banks, and certification authorities in developing first-of-their-kind public key legal infrastructures.
- Chaired the Illinois Commission on Electronic Commerce & Crime, and in that capacity wrote the Illinois Electronic Commerce Security Act (enacted in 1998). This Act had a significant influence on national and global e-commerce legislation, including the Uniform Electronic Transactions Act in the U.S., the European Union Electronic Signature Directive, the United Nations UNCITRAL Model Law on

Electronic Signatures, the Canadian Personal Information Protection and Electronic Transactions Act, and the Singapore Electronic Transactions Act.
- Helped to negotiate the 2005 United Nations Convention on the Use of Electronic Communications in International Contracts as part of the U.S. Delegation to the United Nations Commission on International Trade Law. This is the first international treaty that focuses on general cross-border e-commerce and electronic transactions, and is expected to have a major impact on international business.
- Assisted in development of a new identity management legal structure for browser-based online authentication. Resolved rights, responsibilities, and liabilities of participants in system to allow website users to verify the identity of the company they are dealing with, in order to address the problem of phishing and to promote secure commerce.

Texto de Entrevista en Inglés, en el mes de Agosto de 2015, en el contexto del Seminario Internacional de Identidad Digital, organizado por RENIEC el 5, 6 y 7 de Agosto de 2015. Lima, Peru.

Dear Julio,

It was a pleasure to meet you as well. I really enjoyed the opportunity to participate in the digital identity seminar and to learn more about what is happening in Peru.

Below I have provided answers to your questions.

1, According your experience. What importance has the digital identity legislation for the electronic government?

I am aware that both the US government and the UK government are actively pursuing the use of digital identity in connection with providing government services online. Similarly, the eIDAS Regulation recently adopted in the European Union is designed to allow citizens of one EU country to use a digital ID issued to them in that country in connection with obtaining access to government services in another EU country.

United States. The United States is actively pursuing development of a digital identity program for purposes of allowing citizens to access government services online. That program is called "Connect.Gov." The goal is to use private sector identity providers to issue digital identity credentials to individual citizens. This would not operate as a national ID, and individuals could obtain a digital credential from any one of several private sector identity providers authorized by the federal government. They could then use those digital credentials to access government services online. Further information is available at http://www.connect.gov/.

United Kingdom. In the UK, the government is also pursuing a somewhat similar program, which is referred to as "GOV.UK.Verify." Like the U.S. program, the goal of GOC.UK.Verify is to use private sector identity providers to issue digital identity credentials to individual citizens. This would not operate as a national ID, and individuals could obtain a digital credential from any one of several private sector identity providers authorized by the UK government. They could then use those digital credentials to access government services online. Further information is available at https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify.

European Union. The European Union has also actively been engaged in a program to facilitate the use of digital identities issued by one EU country for public sector transactions with governments in another EU country. To accomplish that goal, the European Union adopted its eIDAS Regulation in July 2014. The eIDAS Regulation focuses on identity systems that issue credentials for use in online transactions with public sector bodies. Its key goal is mutual recognition of such credentials in cross-border public sector transactions. Thus, the eIDAS Regulation enables individuals who have an identity credential issued in one EU member state to use that same credential to access online public services in another member state. The eIDAS Regulation (technically titled "**Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic**

identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC") is available in several languages at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG.

Legislation. I do not believe that either the US or the UK e-government programs noted above contemplate the implementation of any new legislation. Instead, they appear to be pursuing those programs using what I referred to in my talk as "Level 3" private (contract-based) law. I know, for example, that the UK government has entered into contracts governing the operation of its eGovernment identity system with eight separate identity providers. I believe the US government is doing something similar. However, in both cases I understand that the identity providers have been concerned about a variety of issues, including liability, and there have been at least some discussions suggesting that legislation on this issue might help.

The European Union, by contrast, is using legislation to accomplish its eGovernment identity goals. Specifically, because the focus of the European Union effort is to enable cross-border use of credentials for government services (i.e., a citizen of one country can use the identity credential issued to him in that country for use in accessing government services from another EU country), it was felt that legislation (known as the eIDAS regulation) was necessary to accomplish that goal.

My general sense is that many of the identity issues can be addressed through a contract-based approach, cross-border issues will often require legislation to resolve.

2, What is the importance for the e-commerce?

From my perspective, I think that digital identity management is critically important to e-commerce, at least e-commerce transactions of a significant nature. While many individuals are able to purchase goods over the Internet using a credit card, and without any reliable digital identity (at least in the U.S. and EU), digital identity is often needed to facilitate transactions that are significant because of the amount of money involved, or the sensitivity of the information involved.

For example, the aerospace and defense industry in the United States often has a need to allow suppliers and manufacturers to have access to various databases containing highly sensitive and confidential information. That industry relies on identity credentials to ensure that only appropriate persons are given access to the requested data.

Similarly, digital identity can be critical in situations involving the online execution of important contracts. The law governing electronic signatures makes it important to be able to prove in court the identity of the person who signed.

3. And tell me, why is the digital identity legislation important for the e-business and e-learning?

I believe that digital identity legislation will be necessary (or at least desirable) for the use of digital identity in e-commerce. Such legislation can help to accomplish a variety of important goals, including the following:

Remove barriers to the use of online identity that may exist under the current law

- Fix problems with existing law
- Help to define and promote trust in identity systems
- Facilitate legal recognition of identity and authentication
- Facilitate cross-border identity system interoperability
- Encourage and incentivize development of identity systems

I hope this is responsive to your questions. But if something is not clear, please let me know and I will provide additional information.

All the best,

Tom

Thomas J. Smedinghoff
Locke Lord LLP
111 S. Wacker Drive
Chicago, Illinois 60606
312-201-2021 Direct
312-545-1333 Mobile
Tom.Smedinghoff@lockelord.com
www.lockelord.com

From: Julio Nuñez Ponce [mailto:julionunezponce@gmail.com]
Sent: Thursday, August 06, 2015 8:50 PM
To: Smedinghoff, Tom; Julio Nuñez Ponce
Subject: Contact Digital Identity Law

ANEXO 4
Caso sobre Nombre de Dominio: Mario Vargas Llosa

Centro de Arbitraje y Mediación de la OMPI

DECISIÓN DEL PANEL ADMINISTRATIVO

Jorge Mario Pedro Vargas Llosa v. Instituto Cultural "Mario Vargas Llosa"

Caso No. D2004-0956

1. Las Partes

La parte demandante es Jorge Mario Pedro Vargas Llosa (en adelante el "Demandante") representada por Estudio Ghersi Abogados, con domicilio en San Isidro, Lima, Perú.

La parte demandada es el Instituto Cultural "Mario Vargas Llosa" representado por José Antonio Contreras (en adelante el "Demandado") quien tiene su domicilio en Miami, Florida, Estados Unidos de América.

2. El Nombre de Dominio y el Registrador

La demanda tiene como objeto el nombre de dominio <mariovargasllosa.org>.

El registrador del citado nombre de dominio es Arsys Internet, S.L. dba NICLINE.COM.

3. Historia del Procedimiento

El Centro de Arbitraje y Mediación de la OMPI (en adelante el "Centro") recibió el 12 de noviembre de 2004 la demanda por correo electrónico y en copia firmada en papel el 16 de noviembre del 2004.

El 15 de noviembre de 2004, el Centro envió a Arsys Internet, S.L. dba NICLINE.COM vía correo electrónico una solicitud de verificación registral en relación con el nombre de dominio en cuestión.

El 16 de noviembre de 2004, Arsys Internet, S.L. dba NICLINE.COM envió al Centro, vía correo electrónico, su respuesta, confirmando que el Demandado es la persona que figura como registrante, proporcionando a su vez los datos de contacto del titular del nombre de dominio, así como el contacto administrativo, técnico y de facturación.

En respuesta a una notificación del Centro en el sentido que la Demanda era administrativamente deficiente, el 17 de diciembre del 2004 la parte Demandante presentó una modificación a la Demanda.

El Centro verificó que la Demanda y su modificación cumplían los requisitos formales de la Política uniforme de solución de controversias en materia de nombres de dominio (la "Política"), el Reglamento de la Política uniforme de solución de controversias en materia de nombres de dominio (el "Reglamento"), y el Reglamento Adicional de la Política uniforme de solución de controversias en materia de nombres de dominio (el "Reglamento Adicional").

De conformidad con los párrafos 2.a) y 4.a) del Reglamento, el Centro notificó formalmente la Demanda al Demandado, dando comienzo al procedimiento el 23 de noviembre de 2004. De conformidad con el párrafo 5.a) del Reglamento, el plazo para contestar la Demanda se fijó para el 13 de diciembre de 2004.

El Escrito de Contestación a la Demanda fue presentado ante el Centro el 12 de diciembre de 2004.

El Centro nombró a Ada L. Redondo Aguilera como miembro único del Grupo Administrativo de Expertos el día 21 de diciembre de 2004, recibiendo la Declaración de Aceptación y de Imparcialidad e Independencia, en conformidad con el párrafo 7 del Reglamento. El Experto Único considera que su nombramiento se ajusta a las normas del procedimiento.

El 30 de diciembre del 2004, el Demandante presentó un documento adicional en el que se incluyeron otros documentos como medios de prueba.

4. Idioma del Procedimiento:

El idioma del acuerdo de registro es el inglés. Sin embargo, en virtud de haber sido planteados los escrito de demanda y de contestación a la demanda en idioma español, así como no haber recibido ninguna manifestación expresa que demuestre que las partes

desean que la disputa sea resuelta en otro idioma, la Panelista decidió que el idioma del procedimiento administrativo sea el español y dictar la presente resolución en el ya mencionado idioma, según el articulo 11 del Reglamento.

5. Antecedentes de Hecho

Con fecha 20 de marzo del 2003, el señor José Antonio Contreras Ramírez registró el nombre de dominio <mariovargasllosa.org>, tal y como aparece en la base de datos whois del registrador NICLINE.COM..

El nombre de dominio <mariovargasllosa.org> cuenta con los contenidos que corresponden al Instituto Cultural Iberoamericano "Mario Vargas Llosa".

La parte demandante es el Doctor Mario Vargas Llosa, peruano de nacionalidad y origen, escritor de profesión. El Doctor Mario Vargas Llosa es un prestigioso autor del género literario, ha sido laureado en su país y el ámbito internacional, tanto por su obra como por sus actividades académicas. Sus libros, comentarios y otros escritos han sido traducidos a varios idiomas, sus lectores provienen de todas partes del mundo y también tiene presencia en Internet, mediante el sitio "www.vargasllosa.com".

Antes de iniciarse el presente procedimiento, la parte demandante solicitó a la parte demandada, a través de una carta dirigida a José Antonio Contreras Ramírez, la devolución del nombre de dominio <mariovargasllosa.org>. El Demandado se negó a efectuar la transferencia del nombre de dominio.

6. Alegaciones de las Partes

A. Demandante

El Demandante presenta como base a su demanda y solicitud de transferencia del nombre de dominio <mariovargasllosa.org> los siguientes argumentos:

El Doctor Jorge Mario Pedro Vargas Llosa, quien es mejor conocido en el mundo de la cultura y la literatura como MARIO VARGAS LLOSA, goza de un gran prestigio nacional e internacional. Su fama se debe al fruto de una vida dedicada a la creatividad y al desarrollo profesional como autor de obras literarias.

Como consecuencia, cuenta con una vasta lista de galardones y premios que han sido otorgados a su persona y a su obra por varias instituciones de renombre tanto en el Perú como en el ámbito internacional.

La actividad profesional en el campo de la literatura y las letras del Demandante no solo se pone al público a través de sus obras escritas, sino que también cuenta con presencia en Internet a través del sitio <vargasllosa.com>, por lo que el nombre de dominio <mariovargasllosa.org> (registrado y utilizado por la parte demandada) causa confusión no solo con el nombre propio del autor (Doctor Mario Vargas Llosa) sino que también con

el sitio del Demandante "www.vargasllosa.com", pues los visitantes del sitio objeto del presente litigio creen que el origen, la administración y los contenidos del mismo están a cargo personalmente del Doctor Mario Vargas Llosa.

Que el nombre civil del Demandante Jorge Mario Pedro Vargas Llosa, o simplemente Mario Vargas Llosa (con el que es mejor conocido como autor), no ha sido registrado como marca. No obstante lo anterior, el Demandante aclara que los nombres propios o civiles de autores y de distintas personalidades del mundo artístico, de la política, de la cultura y de otras esferas han sido reconocidos como "marca de hecho" por lo que les ha sido aplicada la Política. El Demandante apunta a varios casos que han sido resueltos por Expertos ante el Centro de Arbitraje y Mediación de la OMPI en los que el nombre propio o civil de una persona ha obtenido esta especial protección, y argumenta que debido a la especial fama y mundialmente conocida obra del autor, el nombre " Mario Vargas Llosa" también debería tener la misma protección de marca de hecho.

El Demandado no tiene derechos ni intereses legítimos en el nombre de dominio <mariovargasllosa.org> ya que el Doctor Mario Vargas Llosa no tiene relación alguna con el Demandado, más que las varias solicitudes que ha efectuado para recuperar el nombre de dominio <mariovargasllosa.org> e incluye en su demanda las comunicaciones en las que el Demandante solicita al Demandado que se abstenga de usar el dominio antes señalado (Anexo Número 2 de la demanda).

El Demandado ha venido obteniendo ingresos con el uso del dominio materia del presente procedimiento, mediante la venta de banners, publicidad y uso comercial que hace en el sitio "www.mariovargasllosa.org".

El registro del nombre de dominio y su utilización, por parte del Demandado, ha sido y está siendo de mala fe. Según lo expuesto por el propio Demandante en su demanda, "el demandado, utilizando el dominio, ha venido atrayendo con ánimo de lucro a los usuarios de Internet (...)".

El registro y uso del nombre de dominio <mariovargasllosa.org> no solo es de mala fe por parte del Demandado, sino que también causa un serio perjuicio a la imagen y prestigio del Demandante, quien es ajeno a las actividades que se llevan a cabo en el sitio.

En apoyo a su demanda, la parte demandante aportó las pruebas documentales con las que fundamenta los hechos expuestos.

B. Demandado

Según extractos de su escrito de Contestación, la parte Demandada se defiende mediante los siguientes argumentos:

El Instituto Cultural Iberoamericano "Mario Vargas Llosa" inició sus actividades en la ciudad de Madrid hace más de siete años, en febrero de 1997 y que sus actividades de carácter cultural han sido reconocidas por universidades e instituciones de carácter intelectual en diferentes países de América Latina y Europa.

La Editorial ICIMAVALL es la encargada de editar las obras ganadoras de los premios internacionales que el Instituto Cultural Iberoamericano "Mario Vargas Llosa" otorga a los autores que entran a los concursos por ellos organizados.

El Instituto, a través de sus presidencias y representaciones, ha presentado conferencias en distintas instituciones académicas o culturales de gran prestigio internacional, de diferentes países del mundo, las cuales han versado sobre distintos temas de interés mundial.

El Instituto homenajea al Doctor Mario Vargas Llosa , razón por la que se eligió nombrar al Instituto "Instituto Cultural Iberoamericano Mario Vargas Llosa", motivo por el cual registró el nombre <mariovargasllosa.org>.

Que el Demandante conocía los proyectos de la parte demandada y que implícitamente aceptó que su nombre fuera incluido en el Instituto Cultural Iberoamericano "Mario Vargas Llosa" en su carta dirigida del 01 de febrero del 2003 documento que adjuntó a la demanda.

Que tiene derechos de Propiedad Intelectual (derechos de marca de hecho) sobre el nombre del Instituto Cultural Iberoamericano "Mario Vargas Llosa", pues en diversas decisiones de los Expertos de la OMPI han establecido que para que un nombre alcance el carácter de una marca de hecho, este debe ser suficientemente famoso en el campo de su actuación y que el Instituto Cultural Iberoamericano "Mario Vargas Llosa" goza de la fama y reputación necesaria para ser reconocida como marca.

Que el Instituto Cultural Iberoamericano "Mario Vargas Llosa" es una entidad sin fines de lucro, que tiene autorización directa, verbal e implícita del Escritor Mario Vargas Llosa para utilizar su nombre y por ende para registrar y utilizar el nombre de dominio <mariovargasllosa.org>.

Que existía una relación anterior a los requerimientos del nombre de dominio <mariovargasllosa.org> por parte del Doctor Mario Vargas Llosa a la parte demandante y lo prueba por medio de comunicaciones escritas que fueron anexadas al escrito de contestación.

Que no tiene ánimo de lucro, que jamás ha lucrado con el nombre del Demandado y que no ha ofrecido el nombre de dominio <mariovargasllosa.org> a la venta, ni a la parte Demandante ni a un tercero.

En apoyo a su escrito de contestación, el Demandado presentó al procedimiento pruebas documentales con las que sustenta su defensa.

7. Análisis y conclusiones

Con el fin de resolver la controversia generada por el registro y uso del nombre de dominio <mariovargasllosa.org>, a continuación se efectúa el análisis que toma en consideración tanto las circunstancias de hecho, las pruebas presentadas y los principios del derecho que hayan de ser aplicables al presente caso.

De conformidad con la Política, párrafo 4 que literalmente establece:

"a) Controversias Aplicables: Usted estará obligado a someterse a un procedimiento administrativo obligatorio en caso de que un tercero (un "demandante") sostenga ante el proveedor competente, en cumplimiento del Reglamento, que:

(i) usted posee un nombre de dominio idéntico o similar hasta el punto de causar confusión con respecto a una marca de productos o de servicios sobre la que el demandante tiene derechos; y

(ii) usted no tiene derechos o intereses legítimos respecto del nombre de dominio; y

(iii) usted posee un nombre de dominio que ha sido registrado y se utiliza de mala fe."

(i) Identidad o similitud del nombre de dominio hasta el punto de causar confusión con respecto a una marca de productos o servicios sobre la que el demandante tiene derechos:

El derecho de Marca del Demandante:

El tratamiento jurídico de marca que se le han atribuido a los nombres propios de personalidades o personajes del mundo de las artes, la cultura, la música, el entretenimiento, la política etc, que no se encuentren registrados, ha sido un tema ampliamente discutido por los Expertos de la OMPI del Centro lográndose establecer algunos criterios que sirven para definir cuando procede su tutela.

El propio Demandante aclaró en su demanda que no posee registro de marca que ampare la denominación "Mario Vargas Llosa". No obstante lo anterior, él mismo menciona dos factores que pueden ser tomados en consideración para que el nombre MARIO VARGAS LLOSA sea considerado una marca. En primer lugar, describe en forma detallada su historia literaria, sus galardones en todo el mundo y los distintos idiomas en los que ha sido traducida su obra, por lo que demuestra la fama y prestigio detrás del nombre MARIO VARGAS LLOSA. En segundo lugar, el Demandante también indica los casos que han sido resueltos ante el Centro en los que se han tutelado los derechos sobre nombres civiles de personalidades a tal grado que se han sido considerados como "marcas".

.El Panel procede a definir si el nombre civil de la parte demandante "Mario Vargas Llosa" es una marca (de servicios o de productos), se encuentre registrada o no para que la Política le sea aplicable.

En casos anteriores, los Expertos de la OMPI han aceptado que la Política se refiere al término marca (se encuentre o no registrada) en forma amplia y de esta se han tutelado los intereses de aquellos que si bien tienen un nombre o una denominación que puede ser considerada "marca" no cuentan con un registro oficial. No obstante lo anterior, los Expertos han sido cautelosos al brindar su apoyo o no a un nombre en particular, pues no todos los nombres propios o civiles de todas las personalidades pueden ser considerados marcas, son ciertos elementos que pueden llevar a un experto a determinar si un nombre propio o civil puede ser considerado marca o no Y los cuales serán analizados por el Panel más adelante.

Un ejemplo de protección de un nombre propio o civil de un autor como "marca" fue el caso de *Rosa Montero Gallo v. Galileo Asesores S. L.*, Caso OMPI No. D2000-1649, resuelto ante el Centro en el que se concluyó con el siguiente criterio: "Es un hecho notorio que las profesiones artísticas constituyen actualmente maneras de ejercicio de actividades lucrativas, dirigidas al mercado y sometidas a la competencia. En el mundo analógico, los ejemplares de obras (pinturas, esculturas, planos de arquitectura, programas de computación, etc.) son objeto de comercio activo. En el mundo virtual, no se discute que los "contenidos" protegidos bajo Derecho de Autor son materia prima privilegiada para el comercio electrónico y elemento básico para el desarrollo de la "Nueva Economía". Poca duda cabe entonces de que el nombre o seudónimo de un autor o artista intérprete de obras de cualquier género constituye a los efectos de la puesta en el mercado de ejemplares o "contenidos" una marca que distingue ante el público dicho ejemplar o contenido y le comunica el prestigio adquirido ante dicho público por el autor o artista intérprete en razón de los méritos y difusión de su obra o repertorio anterior. No existiendo registro, ese nombre o seudónimo deberá recibir el tratamiento de una marca de hecho." Ver también Caso OMPI No. D2000-0210, *Julia Fiona Roberts v. Russell Boyd*, Case OMPI No. D2000-0235, *Jeanette Winterson v. Mark Hogarth*).

Al igual que una marca el nombre propio del demandante, que a la vez es el nombre que lo identifica como autor de obras literarias en ejercicio del derecho del derecho a la paternidad de la obra "Mario Vargas Llosa" cumple las siguientes funciones:

a) Identificador del Origen de un Producto (Obra Literaria)

El derecho a la paternidad de la obra consiste en el facultad que tiene todo autor de que se reconozca su condición de creador de la obra. El derecho a la paternidad de la obra artística protege la íntima relación existente entre el autor y el fruto de su creatividad espiritual, y puede ser ejercido mediante el uso del nombre propio del autor (como es el caso de Mario Vargas Llosa) o mediante el uso de un seudónimo, a su vez el derecho a la paternidad de la obra puede ser analizado desde dos puntos de vista:

• Desde la perspectiva estricta del derecho del autor, como el derecho a la Paternidad de la Obra, mediante el cual se crea vinculo entre el sujeto que creo la obra y el objeto de la obra.

• Como un medio de identificación permitiendo asimilar algunas de las funciones de las marcas o identificadores comerciales.

b) El nombre de un autor como medio de identificación comercial.

El nombre del autor, en forma similar a una marca, puesto en su obra (producto) permite facilitar su comercialización a través de los distintos medios publicitarios.

Son innumerables los factores que llevan a una obra de arte, musical o literaria al éxito comercial. Uno de éstos factores es sin lugar a dudas, el nombre del autor o del artista que crea la obra o que está involucrado en la misma. En el presente caso, al tratarse de un autor de fama y prestigio internacional su nombre es comercialmente valioso y el mismo es un identificador que sin lugar a ninguna duda permite que su obra puesta en el mercado sea más atractiva al público que otras obras de otros autores del mismo genero.

El nombre de Mario Vargas Llosa cumple también con esta función, pues sus obras ya sean escritos, libros o documentos que se encuentren a disposición del publico ya sea por medios físicos o electrónicos pueden ser mejor comercializados con dicho nombre.

c) El Nombre del Autor como elemento de distinción:

Las marcas cumplen con la función de distinguir bienes o servicios de otros y de ser un signo que permita la comercialización de los mismos a través de los medios publicitarios. De la misma manera, el nombre de un autor (en ejercicio de su derecho a la paternidad de su obra) puede cumplir con la función de ser un signo distintivo, porque su nombre al ser plasmado en su obra permite distinguirla de otras obras en el mismo género.

El nombre del autor Mario Vargas Llosa, por sí mismo y en forma similar a una marca es suficientemente especial y notorio que estar impreso en un libro, revista o cualquier escrito, indubitablemente el lector asocie directamente al autor con su obra.

Teniendo en cuenta los antecedentes alegados y probados por el Demandante aludidos en el párrafo anterior, la Panelista considera que tal requisito de notoriedad o fama se llena más que suficientemente en el presente caso, por lo que establece que el nombre "Mario Vargas Llosa" si es una marca de hecho y que la parte demandante cumple con lo establecido en el párrafo 4.a)i) de la Política.

De la similitud de la marca y el nombre de dominio <mariovargasllosa.org>:

No cabe la menor duda de que el nombre <mariovargasllosa.org> es exacto al nombre propio y a los apellidos de Mario Vargas Llosa, ya que la terminación ".org" corresponde al Dominio Superior Genérico de Nombres de dominio en Internet.

Respecto a la exactitud del nombre de dominio <mariovargasllosa.org>, el Demandado no presentó oposición.

En conclusión, el Panelista considera que el nombre de dominio <mariovargasllosa.org> es exacto a la marca "de hecho" del Demandante Mario Vargas Llosa.

(ii) De los derechos o intereses legítimos

La parte demandante debe probar la ausencia de derechos o intereses legítimos de la parte demandada en el nombre de dominio objeto del presente procedimiento.

Según el Demandante, el Demandado no tiene intereses legítimos en el nombre de dominio <mariovargasllosa.org> porque no ostenta derechos de propiedad intelectual sobre el nombre del Demandante "Mario Vargas Llosa", en particular del nombre de dominio <mariovargasllosa.org>; porque el Demandante no ha otorgado su consentimiento o autorización expresa para que su nombre propio sea registrado y utilizado como nombre de dominio en Internet por un tercero, incluyendo al Demandado, y porque según el Demandante es evidente que el Demandado hace un uso comercial tanto del nombre como de la imagen y prestigio del autor.

La parte demandada manifiesta que si tiene intereses legítimos sobre el nombre de dominio <mariovargasllosa.org> en virtud de tener la autorización de utilizar el nombre de

Mario Vargas Llosa y porque, como lo indica él lo registró en representación del Instituto Cultural Iberoamericano "Mario Vargas Llosa", una entidad de carácter no lucrativo dedicada a actividades sin fines de lucro, tendientes a la divulgación de la literatura de lengua española.

A continuación se verificarán las circunstancias y las pruebas con las que sustentan las partes el interés legitimo sobre el nombre.

El párrafo 4.c) de la Política establece lo siguiente: "Cualquiera de las circunstancias siguientes, entre otras, demostrará sus derechos o sus legítimos intereses sobre el nombre de dominio a los fines del párrafo 4.a)ii) en caso de que el grupo de expertos considere que están probadas teniendo en cuanta la evaluación que efectúe de todas las pruebas presentadas: (…) ii) Usted (en calidad de particular, empresa u otra organización) ha sido conocido corrientemente por el nombre de dominio, aun cuando no haya adquirido derechos de marcas de productos o de servicios."

La parte demandada arguye que tiene derechos de Propiedad Intelectual del nombre "Instituto Cultural Iberoamericano Mario Vargas Llosa" razón por la que registró el nombre de dominio <mariovargasllosa.org>.

Así mismo, el Demandado argumenta, que el nombre "Instituto Cultural Iberoamericano Mario Vargas Llosa" es sobradamente conocido en el ámbito cultural, académico y de las letras en Latinoamérica y el mundo, razón por la cual debe considerarse como marca de hecho, al igual que han sido tutelados otros nombres propios por Expertos del Centro.

En cuanto al señalamiento que hizo el Demandante respecto a su derecho de marca (de hecho) del nombre "Instituto Cultural Iberoamericano Mario Vargas Llosa", el Panel opina que no todos los nombres de personas ya sean individuales o jurídicas han sido protegidos como marca de hecho. Reitero, los Expertos han sido muy cautelosos al reconocer el derecho de marca de hecho a ciertos nombres civiles o de persona, porque para que un nombre pueda alcanzar dicho reconocimiento debe cumplir con ciertos requisitos, en especial el valor distintivo que toda marca debe tener. En el presente caso, el valor distintivo de la denominación "Instituto Cultural Iberoamericano Mario Vargas Llosa" se debe precisamente a la inclusión del nombre de la parte Demandante "Mario Vargas Llosa", el cual si se encuentra tutelado como marca de hecho en virtud de la presente Política.

Por lo anteriormente expuesto, el Panel no reconoce el derecho de marca de hecho del nombre "Instituto Cultural Iberoamericano Mario Vargas Llosa", razón por la que no puede invocar éste presupuesto como interés legítimo para el registro del nombre de dominio <mariovargasllosa.org>.

En todas las pruebas, cartas y demás documentos que aporta la parte demandada, el Instituto Cultural Iberoamericano "Mario Vargas Llosa" también ha sido y es públicamente conocido con el nombre anteriormente citado o como Editorial ICIMAVALL. Dicho Instituto no ha sido públicamente conocido con el nombre propio del Demandante o "Mario Vargas Llosa" o únicamente con el nombre de dominio <mariovargasllosa.org> sino que ha empleado constantemente las denominaciones "Instituto Cultural Iberoamericano" a la par del nombre de la parte demandante, razón por la que tampoco puede invocar que es conocido con el nombre de "Mario Vargas Llosa" en forma independiente, pues su uso

está condicionado y ligado al del "Instituto". El Demandado tampoco puede invocar un interés legítimo basado en lo anterior, porque el uso del nombre "Mario Vargas Llosa" se encuentra condicionado a la autorización del titular del mismo.

La parte demandada argumenta que El Instituto Cultural Iberoamericano "Mario Vargas Llosa" es una entidad de carácter no lucrativo y cuenta con personería jurídica, hecho que no probó en ningún momento. En todo caso, fue el Demandante el que aportó documento legal que acredita la existencia del Instituto Cultural Iberoamericano ICIMAVALL, que ha sido dado a conocer por su representante legal el señor José Antonio Contreras como Instituto Cultural Iberoamericano "Mario Vargas Llosa" y que acredita que su existencia data desde el 23 de septiembre de 2002.

La resolución en el caso *José Luis Sampedro Saéz v. Galileo Asesores S. L*, Caso OMPI No. D2000-1650, señala:

"Es obvio y no precisa demostración que cualquier persona u organización puede organizar vastos repertorios de material cultural sin recurrir a la "ocupación" de nombres de dominio coincidentes con la firma de autores vivientes o cuyos derechos "patrimoniales" de autor se encuentren en vigencia. Cualquier usuario de Internet conoce la existencia de grandes repositorios virtuales de obra literaria.

Ninguno de los respetables y bienhechores organizadores de estas bibliotecas virtuales precisó recurrir al registro de nombres de dominio para cada uno de los autores de obras incluidas en su repertorio: se limitó a usar los recursos naturales y propios del lenguaje HTML para proporcionar a los usuarios de Internet las pistas necesarias destinadas a que los instrumentos de navegación y los agentes actuantes en la Red ubicaran con precisión la información pertinente a una búsqueda de material textual."

De la misma manera, es opinión del Panel que El Instituto Cultural Iberoamericano "Mario Vargas Llosa", o Instituto Cultural Iberoamericano ICIMAVALL, no se valió de recursos generales para llevar a cabo sus actividades culturales y sin fines de lucro, sino que se ha valido del nombre y de la imagen de la parte demandante registrando y utilizando el nombre de dominio <mariovargasllosa.org> aprovechándose de ésta forma, abiertamente, de la fama del autor.

Otros sitios que también brindan honores al Doctor Mario Vargas Llosa, no han sido registrado directamente como un nombre de dominio que contenga el nombre completo del autor, sino que han estructurado sus páginas en forma independiente, incluyendo segmentos en donde aparece el autor.

En los anteriores sitios y en un sinnúmero de otros sitios que el Panel visitó en Internet y en los que aparece el nombre completo o parcial del autor (Demandante), no se utilizó el recurso de registrar el nombre de dominio que lleva su nombre "Mario Vargas Llosa".

En conclusión se puede decir que las actividades sin fines de lucro que lleva a cabo en el sitio objeto del presente procedimiento no constituyen prueba de un "interés legítimo" es más el panel comprobó al visitar el sitio que las actividades que se llevan a cabo a través del sitio son de carácter mixto ya que el Instituto Cultural Iberoamericano Mario Vargas Llosa también lleva actividades comerciales utilizando el nombre de dominio objeto de la controversia.

En cuanto a la Autorización "implícita" por la parte demandante:

Con base a los hechos y pruebas presentadas, la parte demandada argumenta que tiene interés legítimo en el nombre porque en comunicaciones previas fue autorizada "implícitamente" por el Demandante a utilizar el nombre de Mario Vargas Llosa para que el señor José Antonio Contreras en representación del Instituto Cultural Iberoamericano "Mario Vargas Llosa" incluyera dicho nombre como parte de la denominación con la que se distingue el Instituto. Vale, en este punto, hacer las siguientes notas aclaratorias:

Si bien, la parte demandante pudo haber autorizado al señor José Antonio Contreras en forma personal o como representante legal del Demandado, la inclusión de su nombre "Mario Vargas Llosa" para que formara parte del nombre "Instituto Cultural Iberoamericano Mario Vargas Llosa", dicha autorización se encontraba limitada únicamente a ésta designación no así al registro y uso del nombre de dominio <mariovargasllosa.org>.

Es importante destacar que entre la parte demandante y la parte demandada no se dio una relación contractual o licencia escrita en la que conste que el Demandante autoriza en forma expresa al Demandado el utilizar su nombre propio (como autor) para registrarlo como nombre de dominio en Internet, en particular uno que fuera exacto al que el mismo Demandante utiliza como es el caso de <mariovargasllosa.org>. Al no existir pruebas o documentos que demuestren la existencia de una relación contractual entre el Demandante y el Demandado que estableciera las condiciones de la licencia de uso del nombre propio del autor, él estaba en su pleno derecho de prestar su nombre personal bajo las circunstancias que el haya establecido al momento de otorgar su autorización. Sin embargo, el Demandante al requerirle al Demandado que le ceda el nombre de dominio <mariovargasllosa.org> y que retire su nombre propio del Instituto Cultural Iberoamericano "Mario Vargas Llosa", lo hace porque las razones que lo motivaron en un principio a otorgarlo ya no están presentes y porque según el propio Demandante el proyecto que le presentaron se desvirtuó.

En todo caso, el Panel considera que para que el Demandado estuviera autorizado a utilizar una marca de hecho, como es el caso de la marca que corresponde a MARIO VARGAS LLOSA debió de obtener un contrato de licencia o la autorización expresa por parte del Demandante, preferiblemente por escrito, para conocer a ciencia cierta las condiciones bajo las cuales se le estaba autorizando utilizar el nombre y que en el mismo acuerdo o licencia estuviera expresamente autorizado a registrar el nombre de dominio objeto del presente procedimiento.

Es opinión del Panel que la autorización que en un momento dado pudo haber otorgado en forma implícita o verbal el Demandante al Demandado contenía las siguientes limitaciones: a) que el nombre propio del demandante se incluyera o formara parte integrante del nombre de un Instituto, esta autorización no es extensiva ni facultaba al Demandado a registrar y utilizar el nombre de dominio equivalente a los apellidos del Demandante y b) que también la autorización de la inclusión del nombre en la denominación del Instituto Cultural Iberoamericano "Mario Vargas Llosa" estaba condicionada al tipo de actividades que se llevaran a cabo en el mismo, a saber que las actividades fueran de carácter no lucrativo, algo que según el Demandante fue tergiversado.

En conclusión, El Panel estima que el Demandado no puede invocar como interés legítimo sobre el nombre de dominio <mariovargasllosa.org> la autorización "implícita" que se le hubiera otorgado por parte del Demandante porque la misma estaba limitada a la inclusión del nombre en la denominación del "Instituto" no al registro de nombres de dominio equivalentes a los nombres y apellidos propios del Demandante. Así mismo, el Panel declara que en virtud de ausencia de un contrato de licencia mediante el cual se establezcan las distintas condiciones bajo las cuales se otorga la autorización de uso de un nombre, signo distintivo o marca, el uso del nombre se encuentra condicionado a la autorización del titular del nombre (en este caso las condiciones del Demandante). Por lo anterior, el Demandante se encuentra plenamente facultado a limitar la autorización del uso de su nombre propio y de impedir que el mismo sea incluido como parte de cualquier denominación, si a su juicio las condiciones por las que se otorgó la autorización no subsisten o cambiaron.

Por los motivos anteriormente expuestos, la parte demandada no cuenta con la autorización por parte del Demandante para el registro y uso de su nombre como nombre de dominio en Internet y por ende no puede invocar éste argumento como parte de su interés legítimo en el nombre de dominio <mariovargasllosa.org>.

El párrafo 4.c)iii) de la Política reza: "Usted hace un uso legítimo y leal o no comercial del nombre de dominio, sin intención de desviar a los consumidores de manera equivoca o de empañar el buen nombre de la marca de productos o de servicios en cuestión con ánimo de lucro."

El Demandante alega que no hay un uso legítimo, leal o no comercial del nombre de dominio, ya que el Demandado no ha recibido autorización expresa por su parte para registrar el nombre y utilizar su imagen en las actividades abiertamente lucrativas que lleva a cabo la parte demandada.

Por su parte, el Demandado argumenta que las actividades que lleva a cabo por medio del sitio "www.mariovargasllosa.org" son de carácter no lucrativo, culturales y de promoción a las promesas de la literatura latinoamericana sin fines comerciales, sin embargo, no aportó pruebas que sustenten en forma fehaciente estas declaraciones.

Es evidente, y basta con ingresar al sitio "www.mariovargasllosa.org" para comprobar que el mismo se desarrolló sobre la base de la imagen del Doctor Mario Vargas Llosa. También, al visitar el sitio "www.mariovargasllosa.org" del Demandado se pudo detectar la mezcla entre las actividades culturales y las actividades lucrativas que tiene a su cargo en el sitio. En todo caso, el visitante, al ingresar al sitio "www.mariovargasllosa.org" se encuentra con un sitio de carácter mixto tanto de orden no lucrativo como comercial utilizando la imagen de la parte demandante.

El Panel concluye que el Demandado no tiene interés legítimo en el nombre de dominio <mariovargasllosa.org> ya que no ostenta derechos de Propiedad Intelectual sobre el nombre "Mario Vargas Llosa" o "mariovargasllosa.org", porque no cuenta con la autorización expresa de la parte demandante para registrar y utilizar su nombre o marca de hecho como nombre de dominio; porque hace uso comercial y no leal del nombre de dominio y porque pudiendo utilizar otro nombre como nombre de dominio para desarrollar su sitio, el Demandado decidió registrar y utilizar un nombre idéntico al del Demandante Mario Vargas Llosa.

C. Registro y uso del nombre de dominio de mala fe

Según el párrafo 4.b) de la Política, "a los fines del párrafo 4.a)iii), las circunstancias siguientes, entre otras, constituirán la prueba del registro y utilización de mala fe de un nombre de dominio, en caso de que el grupo de expertos constante que se hallan presentes:

i) circunstancias que indiquen que usted ha registrado o adquirido el nombre de dominio fundamentalmente con el fin de vender, alquilar o ceder de otra manera el registro del nombre de dominio al demandante que es titular de la marca de productos o de servicios o a un competidor de ese demandante, por un valor cierto que supera los costos diversos documentados que están relacionados directamente con el nombre de dominio; o

ii) usted ha registrado el nombre de dominio a fin de impedir que el titular de la marca de productos o servicios refleje la marca de productos o de servicios refleje la marca de un nombre de dominio correspondiente, siempre y cuando usted haya desarrollado una conducta de ésta índole; o

iii) usted ha registrado el nombre de dominio fundamentalmente con el fin de perturbar la actividad comercial de un competidor; o

iv) al utilizar el nombre de dominio, usted ha intentado de manera intencionada atraer, con ánimo de lucro, usuarios de Internet a su sitio Web o a cualquier otro sitio en línea, creando la posibilidad de que exista confusión con la marca del demandante en cuanto a la fuente, patrocinio, afiliación o promoción de su sitio Web o de su sitio en línea o de un producto o servicio que figure en su sitio Web o en su sitio en línea."

El Demandante manifiesta que el nombre de dominio es utilizado de mala fe, pues el Demandado ha intentado de manera intencionada atraer, con ánimo de lucro, usuarios de Internet a su sitio web o a cualquier sitio en línea, creando la posibilidad de que exista confusión con su marca en cuanto a la fuente, patrocinio, afiliación o promoción de su sitio Web o de su sitio en línea o de un producto o servicio que figure en su sitio web o en su sitio en línea.

Es indiscutible, que existe riesgo de confusión y de asociación causado por el registro de un nombre de dominio idéntico al nombre propio del Demandante. Incluso, el Demandado lo acepta en forma expresa en una de sus cartas dirigidas a la parte demandante en la que literalmente le dice: "Te envié varios e-mail de diferentes personas de diferentes partes del mundo para que visualices la magnitud del proyecto. Ellos nos consideran como una pagina oficial tuya y nos piden citas y nos envían invitaciones para congresos y desean enviarnos sus trabajos literarios. De miles de cartas que hemos recibidos, casi todas las hemos contestado y hemos resuelto su pedid. Otras las hemos ignorado, por su contenido absurdo, y otras te la hemos reenviado.(...)."

De ésta forma, queda demostrado que el Demandado está consciente de la vinculación y la asociación que harán las personas con el nombre de MARIO VARGAS LLOSA y en específico con el nombre de dominio <mariovargasllosa.org>.

Por otro lado, la parte demandante aportó como evidencia de la mala fe del Demandado un correo electrónico suscrito por el Presidente del Instituto Cultural Iberoamericano

"Mario Vargas Llosa", y que fuera enviado con fecha 18 de Mayo de 2004 del presente año al Demandante, que dice: "… si a esa fecha insistes en tu actitud pondrán a la venta los dominios www.vargasllosa.org y www.mariovargasllosa.org es de propiedad intelectual del Instituto que lleva tu nombre. No se de donde sacas la idea o el argumento de que es tuyo. Tú lo pagas, tu lo has comprado?, no, mi querido Mario… el dominio es legal, nosotros somos los propietarios y podemos hacer con el lo que nos plazca, pero todo en aras de la cultura y de la buena fe. Si el dominio cambia de dueño ya no será nuestra responsabilidad, sino consecuencia de tu actitud desestabilizadora…" (Anexo Número 4 de la demanda)

Si bien, la parte Demandante demuestra a través de la carta anteriormente citada que el Demandado tiene intenciones de vender o disponer de cualquier manera el nombre de dominio <mariovargasllosa.org>, lo cierto es que en el presente caso, el ánimo de lucro no se percibe únicamente con la oferta del nombre de dominio <mariovargasllosa.org> a la parte demandante (como sería el inciso a) de la norma de la Política arriba mencionada) sino también con el uso que del mismo se hace en el sitio de Internet. Ciertamente, hay un aprovechamiento de la fama, el prestigio y el renombre de la parte Demandante que es evidente para alcanzar el patrocinio tanto de personas individuales como de personas jurídicas en el mundo que confían que detrás del sitio "www.mariovargasllosa.org" se encuentra la solidez de la persona de Mario Vargas Llosa.

En el presente caso, al ingresar al sitio "www.mariovargasllosa.org" se puede detectar el uso de la imagen del Demandante, a tal punto que cualquier persona que ingrese al mismo pensará que el mismo esta siendo avalado o administrado directa o indirectamente por el Demandante así como los bienes y servicios que están a disposición del público en dicho sitio son autorizados o en cierta forma aprobados por el autor, hecho que ha sido negado por el propio Demandante.

A la luz de la Política arriba identificada, su ámbito de aplicación es limitada y únicamente tiene por objeto establecer si el registro y el uso del nombre de dominio ha sido de mala fe y no montos o sumas de dinero en la que materialmente se acredite cuanto ha perdido o ha dejado de percibir la parte demandante, basta que pruebe en forma fehaciente que existe el riesgo de confusión del origen para determinar que existe mala fe por parte del Demandado, según lo establecen otras resoluciones de los Expertos del Centro tal y como lo estableció en el procedimiento *David Valls Biosca v. Alex Blasi Mas*, OMPI Caso No. D2000-0749: "las marcas comerciales sobre las que se basa el reclamo coinciden con el nombre civil del demandante, que es a la vez el que usa para distinguirse como profesional de la moda y el que identifica su tienda. El uso deliberado del nombre ajeno se considera por el panelista un elemento corroborante de la mala fe en la conducta del demandado, que juega como una evidencia más de conducta de mala fe en el caso." En virtud de lo anteriormente expuesto, el Panel limita su decisión a establecer las circunstancias y hechos probados el registro y uso del nombre de dominio ha sido de mala fe o no.

La parte demandante manifiesta que el Demandado utilizando el dominio, ha venido atrayendo con animo de lucro a los usuarios de Internet, hasta hace poco tenían banners de diversas empresas dedicadas a la venta de libros por Internet y aun en la actualidad publican diversas ofertas en el link publicidad, lo que pone de manifiesto un afán de lucro y crean además, como hemos sostenido con anterioridad, un riesgo de asociación y confusión a los usuarios de Internet, quienes en su mayoría piensan que existe

vinculación entre el Demandante y la entidad que se aprovecha de un nombre ajeno, sin autorización ni derecho alguno para ello. Por su parte, el Demandado arguyó que el sitio "www.mariovargasllosa.org" cumple únicamente fines no lucrativos al igual que el Instituto Cultural Iberoamericano "Mario Vargas Llosa". Sin embargo, el Panel al efectuar la visita al sitio "www.mariovargasllos.org", detectó (como ya se manifestó arriba) que existe una yuxtaposición entre las actividades puramente culturales que lleva el Demandado y aquellas lucrativas, pues si existe un vinculo que apunta directamente hacia la comercialización de espacios de publicidad en la pagina http://www.mariovargasllosa.org/publicidad.html, y en el mismo sitio también se detectan otras actividades carácter editorial que tienen un tinte comercial.

El Panel comprobó que en el sitio "www.mariovargasllosa.org" existe una yuxtaposición de actividades comerciales con otras no lucrativas. Así mismo, para el Panel ésta combinación es una prueba de mala fe del Demandado, porque hay un aprovechamiento mediante el uso de la imagen, notoriedad, prestigio y fama del nombre del Demandante que se lleva a cabo en el sitio "www.mariovargasllosa.org".

En virtud de lo anterior y del uso de la fama del autor con fines comerciales en el sitio "www.mariovargasllosa.org" se considera que el registro y uso del nombre de dominio objeto de la presente controversia es de mala fe por parte del Demandado.

8. Decisión

El Panel decide que el nombre de dominio <mariovargasllosa.org> es idéntico al nombre del Demandante, el que es ampliamente conocido como "Mario Vargas Llosa", que éste nombre constituye una marca de hecho de la que es titular el Demandante, que el Demandado no probó tener un interés legítimo en el nombre de dominio y que el registro y uso del mismo se ha llevado a cabo de mala fe.

Por las razones expuestas, en conformidad con los párrafos 4.i) de la Política y 15 del Reglamento, el Panelista ordena que el nombre de dominio <mariovargasllosa.org> sea transferido al Demandante.

Ada L. Redondo Aguilera
Experto Único

16 de febrero de 2005

ANEXO 5
Caso sobre Nombre de Dominio: Mapfre v PRQ Inet KB

Centro de Arbitraje y Mediación de la OMPI

DECISIÓN DEL PANEL ADMINISTRATIVO

Mapfre Familiar, Compañía De Seguros Y Reaseguros, S.A. v. PRQ Inet KB

Caso No. D2013-0548

1. Las Partes

La Demandante es Mapfre Familiar, Compañía De Seguros Y Reaseguros, S.A. con domicilio en Madrid, España, representada por Elzaburu, España.

La Demandada es PRQ Inet KB con domicilio en Estocolmo, Suecia.

2. El Nombre de Dominio y el Registrador

La Demanda tiene como objeto el nombre de dominio <mapfre-teestafamos.com>.

El registrador del citado nombre de dominio es eNom.

3. Iter Procedimental

La Demanda se presentó ante el Centro de Arbitraje y Mediación de la OMPI (el "Centro") el 20 de marzo de 2013. El 20 de marzo de 2013 el Centro envió a eNom vía correo electrónico una solicitud de verificación registral en relación con el nombre de dominio en disputa. El 20 de marzo de 2013 eNom envió al Centro, vía correo electrónico, su respuesta confirmando que la Demandada es la persona que figura como registrante, proporcionando a su vez los datos de contacto. En el mismo día, la Demandante presentó documentación adicional.

El 27 de marzo de 2013 el Centro envió una comunicación vía correo electrónico e-mail a las partes en relación con el idioma del procedimiento. El 29 de marzo de 2013 la Demandante presentó sus comentarios acerca del idioma que debe ser usado en el presente procedimiento y solicitó que el idioma del procedimiento fuese el español.

El Centro verificó que la Demanda cumplía los requisitos formales de la Política Uniforme de Solución de Controversias en materia de nombres de dominio (la "Política"), el Reglamento de la Política Uniforme de Solución de Controversias en materia de nombres de dominio (el “Reglamento”), y el Reglamento Adicional de la Política Uniforme de Solución de Controversias en materia de nombres de dominio (el "Reglamento Adicional").

De conformidad con los párrafos 2.a) y 4.a) del Reglamento, el Centro notificó formalmente la Demanda a la Demandada, dando comienzo al procedimiento el 4 de abril de 2013. De conformidad con el párrafo 5.a) del Reglamento, el plazo para contestar la Demanda se fijó para el 24 de abril de 2013. La Demandada no contestó a la Demanda. Por consiguiente, el Centro notificó a la Demandada su falta de personación y ausencia de contestación a la Demanda el 25 de abril de 2013.

El Centro nombró a Rodrigo Velasco Santelices como miembro único del Grupo Administrativo de Expertos el día 8 de mayo de 2013, recibiendo la Declaración de Aceptación y de Imparcialidad e Independencia, en conformidad con el párrafo 7 del Reglamento. El Experto considera que su nombramiento se ajusta a las normas del procedimiento.

4. Antecedentes de Hecho

El Grupo Mapfre nace en España en agosto de 1933 como Mutua de Accidentes de Trabajo.

La empresa matriz del Grupo, Mapfre, S.A., tiene como misión principal gestionar, supervisar y administrar la actividad de todas sus filiales, entre otras Mapfre Familiar, a través de las cuales desarrolla su actividad no sólo en el campo de las aseguradoras y reaseguradoras, sino también en otros sectores como el financiero, inmobiliario o el sector servicios.

El Grupo Mapfre está presente en España a través de 423 oficinas directas y 2.732 delegadas, y en otros 46 países a través de sus 243 sociedades.

Mapfre Familiar, en sus más de tres décadas de actividad, ha venido ofreciendo seguros con una amplia gama de coberturas y servicios para el hogar, automóviles y salud, siendo además la división de seguros que mayores ingresos ha reportado en los últimos años en España al Grupo Mapfre, llegando a superar en el 2011 más de 4.500 millones de euros.

Toda la actividad del Grupo Mapfre gira desde su creación en torno a un signo distintivo: la marca MAPFRE. La elección del signo no es fruto de la casualidad, sino que responde a las siglas Mutua de Accidentes de Propietarios de Fincas Rústicas de España del año 1933.

Mapfre Familiar es titular de toda una familia de marcas en torno al distintivo MAPFRE tanto en España como a nivel comunitario e internacional (ver documento N°7)

El registro del nombre de dominio en disputa <mapfre-teestafamos.com>, fue realizado el 31 de diciembre de 2012.

5. Alegaciones de las Partes

A. La Demandante

La Demandante afirma que:

- Mapfre Familiar es titular de toda una familia de marcas en torno al signo distintivo MAPFRE tanto en España como a nivel comunitario e internacional (ver documento N°7)

- El nombre de dominio en disputa está formado de dos elementos unidos por un guión: El primer elemento está compuesto por el término “mapfre”, lo cual supone una reproducción literal de la denominación de la marca renombrada MAPFRE. El segundo elemento está compuesto por le expresión descriptiva “te estafamos”, que evidentemente juega con la denominación del programa de fidelización de “Mapfre Te Cuidamos”.

- El registro de un nombre de dominio que coincide con la marca de un tercero implica una infracción de los derechos de exclusiva del titular de la marca. La infracción es aún más grave si la marca que ha sido incorporada como nombre de dominio es notoria, como es el caso del registro MAPFRE de la actora.

- La Demandada PRQ Inet KB no es comúnmente conocida por el nombre de dominio en disputa.

- La Demandada PRQ Inet KB carece de registros de marca en torno al elemento MAPFRE.

- Mapfre Familiar en ningún momento ha autorizado el registro del nombre de dominio similar a sus marcas.

- El derecho a la libertad de expresión no legitima a PRQ Inet KB el registro de un nombre de dominio idéntico o similar hasta el punto de crear confusión con la marca MAPFRE.

- PRQ Inet KB tenía que conocer con anterioridad al registro del nombre de dominio la marca MAPFRE por ser un signo renombrado y aparecer los logotipos en la propia página web.

- PRQ Inet KB puede ejercer su derecho a la libertad de expresión haciendo uso de otro nombre de dominio que no sea idéntico o confundible con la marca MAPFRE.

- PRQ Inet KB no tiene necesidad de registrar el nombre de dominio en disputa en torno a una marca registrada para el ejercicio de su derecho a la libertad de expresión.

- PRQ Inet KB y Gottfrid Swartholm hacen uso de la expresión “te estafamos” junto a la marca MAPFRE con el manifiesto objeto de menoscabar el lema de la Demandante “te cuidamos” y su actividad a través del nombre de dominio <mapfretecuidamos.com>.

PRQ Inet KB tal y como se puso de manifiesto en los antecedentes de hecho, han formado parte de otros procedimientos en materia de nombres de dominio ante la OMPI (*General Steel Domestic Sales, LLC d/b/a General Steel Corporation v. PRQ Inet KB* Caso OMPI No. D2011-1845 <generalstreetscam.com>), así como ante la NAF (*Microsoft Corporation v. PRQ Inet KB / Gottfrid Swartholm* Caso NAF FA1206001450976 <xboxliverewards.com>), con decisiones desfavorables en ambos casos para los demandados. Además, son titulares de hasta un total de 417 nombres de dominio. Todo ello evidencia que PRQ Inet y Gottfrid Swartholm conocían a la perfección la política y reglamentación que rige en esta materia y que el registro del nombre de dominio en disputa es abusivo.
- En definitiva, son numerosas las circunstancias que revelan cómo la Demandada no sólo no ostenta derechos e intereses legítimos sobre el nombre de dominio en disputa, sino que ponen de manifiesto el registro y uso del mismo de mala fe.

B. La Demandada

La Demandada no contestó las alegaciones de la Demandante.

6. Debate y conclusiones

El artículo 15.a) del Reglamento encomienda al Experto la decisión de la Demanda sobre la base de:

- Las manifestaciones y los documentos presentados por las partes.- Lo dispuesto en la Política Uniforme y en el propio Reglamento.

- De acuerdo con cualesquiera reglas y principios de derecho que el panel considere aplicables.

Los presupuestos de admisibilidad de la Demanda contenidos en el apartado 4.a) de la Política Uniforme son:

- Que el nombre de dominio registrado por la Demandada sea idéntico, u ofrezca semejanza que produzca la confusión con una marca de productos o servicios sobre la que el Demandante tenga derechos.

- Que la Demandada carezca de derecho o interés legítimo en relación con el nombre de dominio en disputa y,

- Que el nombre de dominio en disputa haya sido registrado y usado de mala fe.

A. Idioma del Procedimiento

La Demandante ha presentado la Demanda en español y ha solicitado que éste sea el idioma de procedimiento, debido a que la página Web a la que redirecciona el nombre de dominio en disputa <mapfre-teestafamos.com> está íntegramente redactada y desarrollada en español, a su vez, la página va dirigida a los usuarios de habla hispana, ya que no hay posibilidad de visualizar la página en otro idioma distinta al español. En consecuencia, el Experto ha aceptado la solicitud y evidencia presentada por la Demandante para que el idioma del procedimiento en este caso sea el español.

B. Identidad o similitud hasta el punto de causar confusión

El nombre de dominio en disputa consiste en la conocida marca MAPFRE y la adición de los términos "teestafamos". En opinión del presente Experto, la inclusión en su totalidad de una marca notoriamente conocida en un nombre de dominio, independientemente de los elementos adicionales que la acompañan, no elimina la evidente identidad entre la una y la otra.

A su vez, la inclusión de elementos adicionales, sean estos peyorativos como en este caso en particular, o de cualquier otro tipo más neutral no disminuye ni elimina en la opinión de este Experto la identidad existente entre la marca registrada y la parte dominante del nombre de dominio en disputa.

En definitiva, este Experto concuerda con lo indicado por la Demandante en el sentido de que la mera adición de un término genérico o descriptivo a una marca renombrada o incluso cualquier otro signo distintivo no basta para disipar el riesgo de confusión.

Este Panel considera que el nombre de dominio en disputa <mapfre-teestafamos.com> es similar hasta el punto de crear confusión con la marca registrada MAPFRE por la Demandante. En consecuencia, este Experto constata que el artículo Política 4(a)(i) se ha cumplido.

C. Derechos o intereses legítimos

El segundo elemento requiere de la Demandante demostrar que la Demandada no tiene derechos o intereses legítimos respecto del nombre de dominio en disputa.

Según los términos indicados en el párrafo 4(a) de la Política, es claro que la carga global de la prueba recae sobre la Demandante, sin embargo, la Política proporciona a la Demandada medios para demostrar sus derechos e intereses legítimos sobre el nombre de dominio en disputa. Si la Demandada no hace uso de estos medios y la Demandante ha establecido una presunción conforme a lo señalado en el párrafo 4(a)(ii), la carga se desplaza a la parte demandada para demostrar lo contrario.

La Demandante afirma que la Demandada no tiene derechos o intereses legítimos sobre el nombre de dominio en disputa y no es titular de ninguna marca comercial en relación al nombre de dominio en disputa. La parte Demandada no ha utilizado la marca para la oferta de bienes o servicios y la Demandada no es conocida comúnmente por el nombre Mapfre. La Demandante no ha autorizado a la Demandada a utilizar la marca MAPFRE. No hay ninguna relación entre la Demandante y la Demandada.

La parte Demandada no ha dado respuesta a las alegaciones expuestas por la Demandante, a pesar de habérsele otorgado la oportunidad.

En virtud de lo anterior, uno ya podría considerar que no existen derechos o intereses legítimos por parte de la Demandada. Sin embargo, este Experto considera importante analizar el uso mismo que le está dando la Demandada al nombre de dominio en cuestión y si este uso es legitimo.

Primeramente, al revisar la página web del caso, este Experto ha podido verificar que la página web se encuentra actualmente activa. A su vez, conforme a lo disponible en dicha página es posible concluir que esta página no le otorga algún beneficio comercial o económico a la Demandada. Por tanto, este Experto debe analizar si el uso dado a este nombre de dominio es legítimo tomando en consideración que se trata de un nombre de dominio que contiene una marca notoriamente conocida seguida por un término peyorativo.

Importante es destacar que este tema ha sido analizado por otros Expertos; al respecto se puede concluir que hay principalmente dos puntos de vista. Aquella opinión de que el derecho a la crítica no se extiende necesariamente a registrar y utilizar un nombre de dominio que es idéntico o confusamente similar a la marca del demandante. Y aquellos que consideran que independientemente de si el nombre de dominio como tal conlleva crítica, el demandado tiene un interés legítimo en el uso de la marca como parte del nombre de dominio si dicho sitio Web tiene por objeto exclusivamente criticar al demandante, siendo este uso justo y no comercial.

Ahora, en la opinión de este Experto, los nombres de dominio en Internet no deberían servir como vehículo negativo para denostar a personas o empresas, ya que este Experto considera que el sistema de nombres de dominio se fundamenta en el principio de la identificación y ciertamente no en el de la descalificación.

En virtud de lo anterior, este Experto considera que no equivale a actuar de buena fe registrar un nombre de dominio cuya parte dominante es la marca de un tercero para criticar a este tercero. El Experto considera que el derecho de criticar no se extiende necesariamente a registrar y usar un nombre de dominio idéntico o similar a la marca de la Demandante. Aunque se podría creer, erróneamente, que el uso que le está dando la Demandada al nombre de dominio en disputa es fruto de su derecho a la libertad de expresión, en opinión de este Experto dicho derecho debe necesariamente ser ejercido sin vulnerar derechos de terceros, como ocurre en este caso con el derecho de propiedad industrial, al usarse sin ninguna autorización la marca registrada MAPFRE.

El Experto considera que esto es especialmente cierto, si además dicho uso produce o puede producir detrimento a la reputación del tercero ajeno, tal como ocurre en la especie, al relacionarse la referida marca comercial con una mención peyorativa como es la expresión “te estafamos”.

En ausencia de una respuesta, y conforme a lo antes indicado, este Experto considera que la Demandante ha cumplido con el segundo elemento, el párrafo 4 (a) de la Política, y ha establecido una presunción de que la Demandada no tiene derechos o intereses legítimos sobre el nombre de dominio en disputa.

D. Registro y uso del nombre de dominio de mala fe

Este tercer elemento exige que el demandante demuestre que (1) el nombre de dominio ha sido registrado de mala fe y (2) está siendo utilizado de mala fe.

El párrafo 4 (b) de la Política establece una lista no exhaustiva de circunstancias que de estar presente, a juicio del Experto, es prueba suficiente de registro y utilización de un nombre de dominio de mala fe.

El nombre de dominio en disputa se compone de la denominación <mapfre-teestafamos.com>.

Se entiende que cuando se procede al registro de un nombre de dominio, el apartado 2 de la Política implícitamente impone un esfuerzo de buena fe para evitar el registro y uso de nombres de dominio correspondientes a marcas de terceros. La responsabilidad recae sobre el solicitante de un nombre de dominio de realizar las averiguaciones necesarias para garantizar que el registro del nombre de dominio no infringe ni viola los derechos de terceros. Sin embargo en este caso en particular, es imposible presumir que el Solicitante, y ahora Demandada, registró el nombre de dominio en disputa sin ningún tipo de exploración de la posibilidad de violar derechos de terceros, y con aparente indiferencia de si el nombre de dominio en disputa que se registra corresponde a la marca de otra, dado que el nombre de dominio está compuesto por la marca registrada de la

Demandante y la mención peyorativa “te estafamos” y de hecho la página web que se encuentra activa alude directamente a la Demandante.

En virtud de lo antes indicado, y en concordancia con lo ya establecido en el apartado anterior, el Experto considera que no es posible concebir un registro y uso de buena fe del nombre de dominio en disputa por parte de la Demandada, ya que este Experto considera que no equivale a actuar de buena fe registrar un nombre de dominio cuya parte dominante es la marca de un tercero para criticar a este tercero. Es más, solo se puede presumir un registro y uso de mala fe ya que la única intención de la Demandada al registrar el nombre de dominio en disputa fue intentar de manera intencionada atraer usuarios de Internet a su sitio Web, con la única finalidad de dañar la reputación de la Demandante y mediante la incorporación de la marca MAPFRE en el nombre de dominio en disputa.

En consecuencia, por todas las razones expuestas, el Experto constata que la Demandante ha cumplido con los requisitos del párrafo 4 (a) (iii) de la Política.

7. Decisión

Por las razones explicadas precedentemente, y en conformidad con los párrafos 4.i) de la Política y 15 del Reglamento, el Experto ordena que el nombre de dominio <mapfre-teestafamos.com> sea transferido a la Demandante.

Rodrigo Velasco Santelices
Experto Único
Fecha: 29 de mayo de 2013

ANEXO 6

PROYECTO DE LEY Nº 3900-2014-RENIEC. Presentado al Congreso de la Republica el 22 de Octubre de 2014. TEXTO SUSTITUTORIO

EL PRESIDENTE DE LA REPÚBLICA

POR CUANTO:

EL CONGRESO DE LA REPÚBLICA

Ha dado la siguiente:

LEY DE IDENTIDAD DIGITAL

TÍTULO PRELIMINAR

DISPOSICIONES GENERALES

Artículo 1.- Del Objeto

La presente Ley tiene por objeto reconocer el derecho de todas las personas a la inclusión digital y regular el derecho a la identidad digital para el uso de servicios de gobierno electrónico seguro, prestados por las entidades de la Administración Pública.

Para efectos de esta Ley entiéndase por personas, a las personas naturales y a las personas jurídicas, quienes asimismo podrán usar su identidad digital para el uso de servicios de comercio electrónico seguro, en la medida que éstos se implementen observando lo establecido en la presente Ley.

Artículo 2.- Alcance de la Ley

La presente Ley comprende el uso y la prestación de servicios de gobierno y comercio electrónico seguros.

Entiéndase por gobierno electrónico seguro a los servicios públicos, procedimientos administrativos y al ejercicio de la tutela jurisdiccional, prestados por las entidades de la Administración Pública, dentro del marco de la Infraestructura Oficial de Firma Electrónica (IOFE)

Entiéndase por comercio electrónico seguro a la prestación de servicios, la ejecución de procedimientos y la realización de transacciones por parte del sector privado que se desarrollen bajo el marco de la Infraestructura Oficial de Firma Electrónica (IOFE).

Artículo 3.- Del ámbito de aplicación de la Ley

3.1. La presente Ley es de aplicación a todas las entidades de la Administración Pública referidas en el Artículo I del Título Preliminar de la Ley Nº 27444, Ley del Procedimiento Administrativo General.

3.2. La presente Ley se aplica a las relaciones entre las distintas entidades de la Administración Pública, a las relaciones entre personas naturales o personas jurídicas y de aquéllas con las entidades de la Administración Pública.

Artículo 4.- De las definiciones

Para todos los efectos de la presente Ley, las definiciones palabras y términos utilizados se entenderán en el sentido indicado en el Glosario de Términos que como anexo forman parte de la presente Ley.

Artículo 5.- Fines de la Ley

Son fines de la presente Ley:

5.1. Instituir la inclusión digital como un derecho de todas las personas impulsando la puesta a disposición y el aprovechamiento de los servicios de gobierno electrónico seguro.

5.2. Establecer la identidad digital como un derecho de las personas y un deber del Estado para garantizar el ejercicio de la misma en los servicios de gobierno electrónico seguro.

5.3. Establecer las condiciones idóneas para la prestación de servicios de gobierno electrónico seguro determinados en el alcance de la presente Ley.

5.4. Promover la masificación de los servicios y procedimientos administrativos por medios electrónicos seguros mediante el uso de la identidad digital.

5.5. Favorecer el ejercicio del acceso a la tutela jurisdiccional a través del uso de medios electrónicos seguros, contribuyendo al fortalecimiento de los órganos jurisdiccionales.

5.6. Facilitar el ejercicio de derechos y el cumplimiento de deberes de las personas por medios electrónicos seguros.

5.7. Crear las condiciones de confianza en el uso de los medios electrónicos seguros en toda transacción electrónica que se realice con y entre las entidades de la Administración Pública. Estas condiciones deben incluir el cumplimiento de las medidas de seguridad necesarias y la adecuada protección de datos personales en el marco de lo previsto en la normatividad vigente.

5.8. Fomentar la presencia del Estado mediante la provisión de servicios de gobierno electrónico seguro.

5.9. Contribuir a la mejora del funcionamiento interno de todas las entidades de la Administración Pública.

5.10. Simplificar los procedimientos administrativos mejorando la calidad, eficiencia y oportunidad de los servicios que las entidades de la Administración Pública brindan a las personas.

5.11. Implementar el expediente electrónico en las Entidades de la Administración Pública.

5.12. Establecer mecanismos para el intercambio de información entre entidades de la Administración Pública que faciliten el uso y prestación de los servicios de gobierno electrónico seguro.

5.13. Favorecer el empleo por parte de las entidades de la Administración Pública de estándares abiertos así como el uso de software libre y de código abierto.

5.14. Promover el desarrollo del comercio electrónico, propiciando la implementación de servicios de comercio electrónico seguro por parte del sector privado, en el marco de lo dispuesto en la presente Ley.

Artículo 6.- De los principios rectores

6.1. Principio de equivalencia funcional, por el cual el ejercicio de la identidad digital para el uso y prestación de servicios de gobierno y comercio electrónico seguros, confiere y reconoce a las personas las mismas garantías que otorgan los modos tradicionales de relación entre las personas o en la relación con las entidades de la Administración Pública.

6.2. Principio de no discriminación, según el cual en ningún caso el uso de medios electrónicos seguros puede implicar la existencia de restricciones o discriminaciones para las personas que se relacionen con las entidades de la Administración Pública o entre aquellas.

6.3. Principio de protección de datos personales, por el cual se debe garantizar que el uso y prestación de servicios de gobierno y comercio electrónico seguro, respetará las disposiciones contenidas en la normativa de la materia.

6.4. Principio de seguridad de la información, por el cual las entidades de la Administración Pública deben prestar servicios de gobierno electrónico seguro, conforme a las disposiciones contenidas en la presente Ley y en la normatividad vigente sobre la materia.

6.5. Principio del deber de cuidado, por el cual las personas deben observar y tomar las medidas necesarias para la debida salvaguarda en el uso de su identidad digital.

6.6. Principio de simplificación administrativa y sistematización, por medio del cual se busca la mejora y reducción sustancial de tiempo y costos, que permitan la optimización en el uso de recursos, logrando mayor eficiencia y eficacia en la actuación de las entidades de la Administración Pública, que operen a través de medios electrónicos seguros.

6.7. Principio de enfoque por procesos, por el cual las entidades de la Administración Pública deben establecer y configurar sus procesos a fin de prestar servicios de gobierno electrónico seguro.

6.8. Principio de responsabilidad y calidad en la veracidad y autenticidad de la información y dentro de los servicios de gobierno electrónico seguro, ofrecidos por las entidades de la Administración Pública. En todos los casos, las entidades de la Administración Pública responden por los actos realizados por medios electrónicos seguros de la misma manera y con iguales responsabilidades que por los realizados a través de medios tradicionales.

6.9. Principio de usabilidad, según el cual la información de las entidades de la Administración Pública brindada por medios electrónicos, así como, los sistemas y programas usados para la prestación de servicios de gobierno electrónico seguro, deben ser disponibles, accesibles y manejables de manera intuitiva por las personas.

6.10. Principio de conservación, según el cual se garantiza que las comunicaciones y documentos generados a través de medios electrónicos seguros, se conservan en las mismas o mejores condiciones que aquellas utilizadas por los medios tradicionales, de acuerdo a la normatividad de la materia.

6.11. Principio de cooperación en la utilización de medios electrónicos seguros por las entidades de la Administración Pública, según el cual se garantiza tanto la interoperabilidad de los sistemas y soluciones adoptados por cada una de ellas, como en su caso, la prestación conjunta de servicios de gobierno electrónico seguro, a las personas.

6.12. Principio de normalización, según el cual los estándares y patrones establecidos por el Estado, para la prestación de servicios de gobierno electrónico seguro, deberán mantener la mayor correspondencia posible con los estándares internacionales de reconocimiento mundial y regional.

6.13. Principio de proporcionalidad, de modo que los requerimientos de seguridad de los servicios de gobierno electrónico seguro, sean adecuados a la naturaleza de la relación que se establezca con las entidades de la Administración Pública.

6.14. Principio de uso de factores de autenticación, por el cual la identidad digital se verificará mediante un proceso de autenticación digital que utilice factores de autenticación.

TÍTULO PRIMERO
INCLUSIÓN E IDENTIDAD DIGITAL

CAPÍTULO I
DE LA INCLUSIÓN DIGITAL

Artículo 7.- De la inclusión digital

La inclusión digital es el derecho de todas las personas al establecimiento e implementación de las condiciones mínimas necesarias por parte del Estado para hacer uso de servicios de gobierno electrónico seguros; empleando para tales efectos su identidad digital, en el marco de las disposiciones previstas en la presente Ley.

Artículo 8.- De las condiciones necesarias para la inclusión digital

Para la inclusión digital de toda persona, a fin de conseguir la igualdad de oportunidades y aprovechamiento de los servicios de gobierno electrónico seguro, se deberán establecer las medidas que permitan evitar la exclusión digital y la eliminación de barreras existentes para el acceso a dichos servicios.

Corresponde a la Presidencia del Consejo de Ministros (PCM), a través de la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI), en colaboración con el Registro Nacional de Identificación y Estado Civil (RENIEC), y en cooperación con otras entidades de la Administración Pública, la elaboración y aprobación de tales medidas.

Para tal efecto, corresponde a las entidades públicas:

8.1. Disponer las medidas para la obtención del documento credencial electrónico conteniendo la identidad digital que permitirá a las personas el uso de los servicios de gobierno electrónico seguro.

8.2. Implementar las medidas necesarias para la correcta prestación de servicios de gobierno electrónico seguro. Para dicho efecto, se deberá utilizar el documento credencial electrónico a que se refiere el artículo 24° de la presente Ley.

8.3. Implementar medidas para el uso por parte de las personas, de los servicios de gobierno electrónico seguro, utilizando para ello su identidad digital.

8.4. Promover una cultura de uso de servicios de gobierno electrónico seguro. Para tal fin, deberán desarrollarse medios de capacitación adecuada para los distintos niveles y grupos sociales a nivel nacional en el uso de las tecnologías de información y comunicación, con especial atención en los niños, adultos mayores y personas con discapacidad.

8.5. Ampliar el acceso de los sectores populares y zonas rurales, a los servicios de gobierno electrónico seguro. Para ello, las entidades de la Administración Pública podrán suscribir convenios de cooperación con entidades del sector público o privado para la implementación de centros de acceso de conformidad con lo establecido en el Artículo 21º de la presente Ley.

8.6. Impulsar la participación de las micro y pequeñas empresas (MYPES) en las contrataciones públicas a través de medios electrónicos seguros, con la debida transparencia en los procesos respectivos.

8.7. Procurar el desarrollo de habilidades y capacidades de las personas en el uso y aprovechamiento de servicios de gobierno y comercio electrónico seguro.

CAPÍTULO II

DE LA IDENTIDAD DIGITAL

Artículo 9.- Identidad digital

La identidad digital está basada en un documento credencial electrónico, emitido en el marco de la Infraestructura Oficial de Firma Electrónica (IOFE), conforme a las disposiciones legales vigentes.

La identidad digital permite la identificación y autenticación de modo fehaciente en medios electrónicos, para el uso de los servicios de gobierno y comercio electrónico seguros, prestados dentro de la Infraestructura Oficial de Firma Electrónica (IOFE).

Artículo 10.- Identidad digital nacional

Entiéndase por identidad digital nacional a aquella identidad digital que es reconocida a las personas naturales nacionales y contenida en su Documento Nacional de Identidad electrónico (DNIe), emitido por el Registro Nacional de Identificación y Estado Civil (RENIEC).

Artículo 11 .- Identificación digital

La identificación digital es el proceso a través del cual una persona ejerce su identidad digital en medios electrónicos seguros.

Artículo 12 .- Autenticación digital

La autenticación digital es el proceso por el cual se confirma la identidad digital de una persona, permitiéndosele el uso de servicios de gobierno y comercio electrónico seguros.

Para verificar la identidad digital de una persona en servicios ofrecidos por canales electrónicos, el proceso de autenticación digital utilizará como mínimo dos (2) de los factores de autenticación siguientes:

a) Tarjetas o dispositivos criptográficos, tabletas, teléfonos móviles, u otros, los cuales deberán cumplir con las especificaciones técnicas para el almacenamiento de las claves privadas de entidad final –usuarios– establecidas por la Autoridad Administrativa Competente.

b) Contraseña de acceso a la clave privada de los Certificados Digitales.

c) Características biométricas.

Tratándose de servicios prestados vía canales electrónicos no presenciales, uno de los factores de autenticación será necesariamente el indicado en el inciso b) del presente artículo.

Entiéndase por no presenciales aquellas comunicaciones y/o transacciones efectuadas en línea en que las personas no se hayan una en presencia de la otra.

Cuando el proceso de autenticación digital incluya características biométricas, pueden utilizarse sistemas biométricos tales como la verificación de huellas digitales, del iris del ojo, del perfil genético, de la voz, del rostro y otros similares, en la medida que estén respaldados por plataformas tecnológicas seguras basados en estándares internacionalmente aceptados.

CAPÍTULO III

DOCUMENTO NACIONAL DE IDENTIDAD ELECTRÓNICO

Artículo 13.- Del Documento Nacional de Identidad electrónico (DNIe)

El Documento Nacional de Identidad electrónico (DNIe), es el Documento Nacional de Identidad emitido por el Registro Nacional de Identificación y Estado Civil (RENIEC), que acredita presencial y no presencialmente la identidad de su titular, permitiendo en este último caso reconocer a las personas naturales nacionales su identidad digital nacional.

El Documento Nacional de Identidad electrónico (DNIe), almacena dos (2) certificados digitales: el de autenticación y el de firma digital emitidos por el Registro Nacional de Identificación y Estado Civil (RENIEC), lo cual permite a su titular autenticar su identidad digital nacional en un medio electrónico y firmar digitalmente documentos electrónicos o mensajes de datos.

Asimismo, el Documento Nacional de Identidad electrónico (DNIe), permite a su titular el uso de servicios de gobierno y comercio electrónico seguro y el ejercicio del derecho al voto electrónico presencial y no presencial en los procesos electorales de conformidad con las disposiciones vigentes sobre la materia.

El Documento Nacional de Identidad electrónico (DNIe) es reconocido como documento de viaje dentro del territorio nacional, así como en aquellos países con los cuales el Perú cuente o suscriba acuerdos o convenios para dicho fin.

El Documento Nacional de Identidad electrónico (DNIe), a solicitud expresa del usuario podrá almacenar información para usos financieros, bancarios y no bancarios.

El empleo del Documento Nacional de Identidad electrónico (DNIe), se encuentra sujeto a lo dispuesto en Ley N° 26497, Ley Orgánica del Registro Nacional de Identificación y Estado Civil y demás normas complementarias, quedando prohibido, bajo ninguna circunstancia, que sea requisado o retenido, bajo responsabilidad.

El RENIEC puede determinar las características técnicas y contenido del circuito integrado o solución tecnológica del Documento Nacional de Identidad electrónico (DNIe).

Artículo 14.- Código Único de Identificación de la Persona Natural con Base Genética.

El Código Único de Identificación (CUI) contenido en el Documento Nacional de Identidad (DNI), se efectúa utilizando el código que resulte de la conversión de la cadena genética de cada persona natural, utilizando el análisis genético de la persona que deberá efectuarse en su nacimiento, utilizando tecnologías informáticas y genéticas seguras.

En el procedimiento señalado, se garantiza la identificación única de la persona natural. El reglamento de la presente Ley establece las acciones y medidas necesarias para evitar duplicidad de los códigos generados con base genética y los existentes antes de su implementación.

CAPÍTULO IV

DE LOS DERECHOS Y DEBERES DE LAS PERSONAS

Artículo 15.- Derecho al reconocimiento de la Identidad Digital en medios electrónicos seguros

15.1 Las personas tienen derecho al uso de servicios de gobierno electrónico seguro, prestados en el marco de la Infraestructura Oficial de Firma Electrónica (IOFE).

15.2 Las personas naturales nacionales pueden relacionarse con las entidades de la Administración Pública a través de medios electrónicos seguros, haciendo uso de su Documento Nacional de Identidad electrónico (DNIe). Con el objeto de garantizar este derecho, constituye obligación de las entidades de la Administración Pública poner a disposición de las personas los servicios de gobierno electrónico seguro a través de mecanismos que se encuentren debidamente acreditados y operando dentro de la Infraestructura Oficial de Firma Electrónica (IOFE), conforme a la normativa de la materia.

15.3 Son derechos conexos relacionados al uso de los servicios de gobierno electrónico seguro, los siguientes

15.3.1 Relacionarse con las entidades de la Administración Pública para el ejercicio de sus derechos y el cumplimiento de sus obligaciones, empleando su identidad digital.

15.3.2 Conocer por medios electrónicos seguros el plazo y los requisitos necesarios para el inicio de cualquier procedimiento o solicitud de servicios ante una entidad de la Administración Pública.

15.3.3 A conocer por medios electrónicos seguros el estado en el que se encuentran los procedimientos administrativos y de solicitar la emisión de constancias electrónicas. no resulta aplicable para los casos que pudieran afectar la intimidad personal, o las vinculadas a la seguridad nacional a que se refiere el Texto Único Ordenado de la Ley 27806 – Ley de Transparencia y Acceso a la Información Pública.

15.3.4 Presentar solicitudes, escritos y/o comunicaciones a través de medios electrónicos seguros todos los días del año, las veinticuatro (24) horas del día.

15.3.5 Realizar todo tipo de pagos, presentar declaraciones de impuestos y cualquier otra clase de obligaciones, por medios electrónicos seguros.

15.3.6 Recibir notificaciones en sus domicilios electrónicos a través de medios electrónicos seguros.

Artículo 16.- Formas de representación de las personas

Las personas podrán otorgar la facultad de representación a otras con el objeto de poder acceder a la prestación de servicios de gobierno electrónico seguro. Para tales efectos, las entidades de la Administración Pública podrán requerir, en cualquier momento, la acreditación del documento en el que de manera fehaciente conste el alcance expreso de dicha representación y su vigencia.

Artículo 17.- Deberes de las personas

Para efectos de la presente ley, las personas tienen los deberes siguientes:

17.1. Salvaguardar el dispositivo que almacena el documento credencial electrónico que contiene su identidad digital, así como mantener la debida reserva de su clave privada, bajo responsabilidad.

17.2 No afectar la disponibilidad de los servicios de gobierno electrónico seguro provistos por las entidades de la Administración Pública, ni alterarlos, ni hacer uso no autorizado o indebido de los mismos, en el marco de las disposiciones legales vigentes.

17.3 Preservar la integridad y confidencialidad de la información gestionada por las entidades de la Administración Pública a través de medios electrónicos seguros. Esto incluye no acceder ni hacer uso indebido de la información o de las bases de datos de las entidades de la Administración Pública.

17.4 La persona es responsable de la veracidad de la información provista a las entidades de la Administración Pública a través de medios electrónicos seguros.

17.5. No facilitar a otras personas su documento credencial electrónico, ni permitir su uso por terceros.

TÍTULO SEGUNDO

DEL RÉGIMEN JURÍDICO DEL GOBIERNO ELECTRÓNICO

CAPÍTULO I

OBLIGACIONES Y GARANTÍAS DE LAS ENTIDADES DE LA ADMINISTRACIÓN PÚBLICA Y ÁMBITO JURISDICCIONAL

Artículo 18.- Obligaciones de las entidades de la Administración Pública para la prestación de servicios de gobierno electrónico seguro

Las entidades de la Administración Pública brindan los servicios de gobierno electrónico seguro, basados en el uso de la identidad digital de las personas. Para ello, deben emplear certificados digitales, software de firma digital y/o servicios de valor añadido, acorde a lo dispuesto por la normativa de la materia, y deben ser provistos a través de canales seguros para la transmisión o intercambio electrónico de datos.

Para ello, la Administración Pública tiene las siguientes obligaciones:

18.1. Prestar servicios de gobierno electrónico seguro, cuya implementación deberá de manera progresiva, habilitando para ello un catálogo de servicios que estará

disponible en su sede electrónica y facilitando los medios necesarios para el adecuado uso de tales servicios.

18.2. Adoptar medidas técnicas y organizativas que garanticen la seguridad de las bases de datos y que eviten su alteración, pérdida, tratamiento o acceso no autorizado, debiéndose asegurar la confidencialidad de los datos personales en el marco de las disposiciones legales vigentes.

18.3. Asegurar de manera progresiva y gradual las condiciones necesarias que permitan el uso de servicios de gobierno electrónico seguro, por parte de todas las personas, sin discriminación de ninguna índole.

18.4. Aceptar documentos electrónicos firmados digitalmente que hayan sido emitidos por las personas naturales, personas jurídicas privadas y/o por otras entidades de la Administración Pública, acorde a lo dispuesto por la normativa sobre la materia.

18.5. No exigir a las personas otros mecanismos de identificación y autenticación que no sean los referidos a su identidad digital conforme a lo establecido en los Capítulos II y III del Título Primero de la presente Ley, para el uso de servicios de gobierno electrónico seguro.

18.6. Emplear estándares abiertos o complementariamente aquellos que sean de uso generalizado por las personas, así como hacer uso de software libre y de código abierto, de ser el caso.

18.7 Efectuar notificaciones electrónicas únicamente en los domicilios electrónicos de las personas, de conformidad con lo establecido en el Artículo 29º de la presente Ley.

18.8. Otras que establezca el Reglamento de la presente Ley.

Artículo 19.- Garantías para la prestación de servicios de gobierno electrónico por medios electrónicos seguros

Las entidades de la Administración Pública deben garantizar a las personas el establecimiento y la prestación de servicios de gobierno electrónico seguro, comprendidos en el alcance de la presente Ley, debiendo para tal efecto:

19.1. Reconocer y aceptar el uso de la identidad digital de todas las personas basadas en los medios de identificación señalados en los Artículos 9º y 10º de la presente Ley.

19.2 Adecuar sus servicios, procedimientos administrativos y, en lo que corresponda, al ejercicio de la tutela jurisdiccional, en función a la normatividad vigente, a fin de llevarlos a cabo por medios electrónicos seguros.

Para tal efecto, se debe garantizar en todo momento la disponibilidad del acceso, la integridad, la autenticidad, el no repudio y la confidencialidad de las transacciones realizadas por estos medios, usando para tales fines certificados digitales, software de firma digital y/o servicios de valor añadido acorde a lo dispuesto por la normativa sobre la materia; debiendo ser provistos por medio de canales seguros para la transmisión o intercambio electrónico de datos.

19.3. Asegurar el uso de los servicios de gobierno electrónico seguro, habilitando Fedatarios Institucionales Electrónicos, en el marco de lo previsto en el artículo 21º de la presente Ley.

19.4. Prestar servicios de gobierno electrónico seguro, en el marco de la presente Ley, garantizando la adecuada protección de los datos personales; para ello, cada entidad debe designar un Oficial de Privacidad como responsable. Los requisitos y funciones específicas del Oficial de Privacidad serán establecidos en el Reglamento de la presente Ley.

19.5. Prestar servicios de gobierno electrónico seguro de manera que se garantice su disponibilidad, así como la integridad y confidencialidad de la información. Para dicho efecto, las entidades de la Administración Pública deberán designar un Oficial de Seguridad, como responsable de garantizar la seguridad de la información. Los requisitos y funciones específicas del Oficial de Seguridad serán establecidos en el Reglamento de la presente Ley.

19.6. Capacitar a su personal en el uso correcto de las firmas y certificados digitales, y demás medios electrónicos requeridos en sus actividades propias, así como, en temas de seguridad, y protección de datos personales que les competan según la función o cargo que ocupen.

19.7. Poner a disposición de las personas a través de la sede electrónica el catálogo de servicios, procedimientos administrativos y aquellos relacionados con el ejercicio a la tutela jurisdiccional que estuvieren a su cargo, siempre que hayan sido implementados a través de medios electrónicos seguros.

19.8. Informar a las personas sobre las condiciones tecnológicas necesarias para el uso de su Documento Nacional de Identidad electrónico (DNIe), o de otros dispositivos

que almacenen su documento credencial electrónico y correspondiente clave privada, para el uso de servicios de gobierno electrónico seguro.

19.9. Contar con personal capacitado para brindar información a las personas sobre el manejo y uso de toda la tecnología requerida para el uso de servicios de gobierno electrónico seguro. Esta información podrá ser proporcionada por un medio físico o por medios electrónicos.

19.10. Brindar, a través de su área competente, las garantías necesarias para una comunicación segura, empleando canales cifrados para el intercambio electrónico de datos.

19.11. Las entidades de la Administración Pública deben admitir para el uso de servicios de gobierno electrónico seguro, aquellos documentos a que se refiere el Artículo 30º de la presente Ley.

19.12. Aplicar criterios de usabilidad en el diseño de los servicios de gobierno electrónico seguro.

19.13. Promover el desarrollo de capacidades y habilidades en las personas, para el correcto y adecuado uso de su identidad digital en los servicios de gobierno electrónico seguro.

Artículo 20.- Centros de Acceso

Las entidades de la Administración Pública deben contar con una red de puntos de acceso a nivel nacional a través de Centros de Acceso que, por medio de canales seguros, permitan la interacción con otras entidades de la Administración Pública. Estos Centros de Acceso deben estar dotados de personal capacitado para brindar la información y facilidades necesarias para que las personas puedan acceder a servicios de gobierno electrónico comprendidos en el alcance de la presente Ley, debiendo igualmente contar con un servicio integral de atención de reclamos y solicitudes de información respecto al empleo de los mecanismos necesarios para la interacción con el Estado.

Artículo 21.- Identificación, autenticación de las personas a través del Fedatario Institucional Electrónico

Para garantizar el uso de servicios de gobierno electrónico seguro de aquellas personas que, por situaciones de carácter excepcional, no cuenten con el documento credencial electrónico que acredite su identidad digital, su identificación y autenticación puede

efectuarse mediante un Fedatario Institucional Electrónico, debidamente habilitado para dicho fin por cada entidad de la Administración Pública.

El Reglamento de la presente Ley establece los supuestos de carácter excepcional que permitan la actuación del Fedatario Institucional Electrónico, así como los requisitos para su designación y las funciones a su cargo.

Artículo 22.- Uso de los documentos credenciales electrónicos contenidos en el DNIe por parte de funcionarios y personal al servicio de las entidades de la Administración Pública.

Los funcionarios y personal al servicio de las entidades de la Administración Pública pueden hacer uso de los documentos credenciales electrónicos contenidos en el DNIe para el ejercicio de sus funciones en los servicios de gobierno electrónico seguro implementados por las entidades de la Administración Pública.

Los documentos credenciales electrónicos contenidos en el DNIe sólo otorgan garantía sobre la identificación de la persona natural, más no del cargo, rol, atribuciones o facultades que ostenta el funcionario o personal al servicio de dichas entidades

Es responsabilidad de las entidades de la Administración Pública gestionar las autorizaciones de accesos y las facultades de sus funcionarios y personal a través de sus aplicaciones de gobierno electrónico seguro.

Artículo 23.- Intercambio de información entre entidades de la Administración Pública

Para permitir el eficaz intercambio de información entre entidades de la Administración Pública, cada entidad debe facilitar el acceso a la información requerida por la entidad de la Administración Pública solicitante, sobre los datos de las personas que obren en su poder y se encuentren en soporte electrónico. Las condiciones, protocolos y criterios funcionales o técnicos necesarios para acceder a dichos datos con las máximas garantías de seguridad, integridad, disponibilidad y confidencialidad se establecen en el Título Tercero de la presente Ley.

La disponibilidad de tales datos está limitada estrictamente a aquellos datos que son requeridos para la tramitación y resolución de procedimientos administrativos, procesos judiciales y servicios de competencia de la entidad de la Administración Pública solicitante. El acceso a los datos de carácter personal está condicionado al cumplimiento de la normativa de la materia.

Quedan excluidas del intercambio, la información que pueda afectar la intimidad personal o la vinculada a la seguridad nacional a que se refiere el Texto Único Ordenado de la Ley 27806 – Ley de Transparencia y Acceso a la Información Pública, aprobado por Decreto Supremo 043-2003-PCM o la que expresamente sea excluida por Ley.

Artículo 24.- Implementación de servicios de gobierno electrónico seguro

Las entidades de la Administración Pública deben implementar y prestar servicios de gobierno electrónico seguro comprendidos en el alcance de la presente Ley.

De ser el caso, las entidades de la Administración Pública deben hacer un análisis de rediseño funcional y simplificación de los procedimientos administrativos y mecanismos para el ejercicio de la tutela jurisdiccional, debiendo contemplar los aspectos siguientes:

24.1. La creación y mantenimiento de registros y archivos electrónicos para el almacenamiento y gestión de los documentos electrónicos generados y las notificaciones o comunicaciones enviadas durante la prestación de los servicios de gobierno electrónico seguro; tales como, recepción y envío de solicitudes, escritos y comunicaciones.

24.2. La protección del derecho a la intimidad, la protección de los datos personales y la confidencialidad de las comunicaciones conforme lo establecido por las normas respectivas.

24.3. El empleo del domicilio electrónico para efectos de las notificaciones o comunicaciones electrónicas que se le deban cursar a las personas; las mismas que deben cumplir con lo dispuesto por la normatividad de la materia.

24.4. Atendiendo a la disponibilidad de la tecnología, las entidades de la Administración Pública pueden habilitar diferentes canales para la prestación de los servicios de gobierno electrónico seguro.

CAPÍTULO II

DE LA SEDE, REGISTRO Y NOTIFICACIÓN ELECTRÓNICA

Artículo 25.- Sede electrónica de las entidades de la Administración Pública.

La sede electrónica es aquella dirección electrónica de cada entidad de la Administración Pública, mediante la cual brinda los servicios de gobierno electrónico seguro comprendidos en el alcance de la presente Ley y que se encuentra disponible para las personas como un canal de comunicación único a través de *Internet*.

La sede electrónica pone a disposición de las personas un catálogo de servicios que permitirá la recepción y envío de documentos electrónicos, desde y hacia las entidades de la Administración Pública y las personas.

Corresponde a cada entidad de la Administración Pública la gestión y administración de la sede electrónica, en el ejercicio de sus competencias.

Para la eficacia de la presente disposición, se debe cumplir con lo siguiente:

25.1. La máxima autoridad de la entidad de la Administración Pública o quien haga sus veces es responsable de la integridad, veracidad y actualización de la información y de la disponibilidad de los servicios de gobierno electrónico seguro a los que puedan acceder las personas a través de la sede electrónica.

25.2. Las entidades de la Administración Pública deben garantizar la identificación de la sede electrónica y establecer canales seguros para la transmisión o intercambio electrónico de datos, debiendo para ello disponer del correspondiente certificado de servidor o de dominio. Se debe poder acceder a la sede electrónica a través del Portal Institucional de la entidad.

25.3 Las entidades de la Administración Pública, deben asegurar las condiciones para el empleo, calidad, seguridad, disponibilidad, accesibilidad, usabilidad e interoperabilidad de los servicios de la sede electrónica. Las disposiciones referidas a su creación, requisitos, contenidos, difusión y otros, son establecidas en el Reglamento de la presente Ley.

25.4. Sin perjuicio de lo establecido en el numeral precedente, las sedes electrónicas deben ser registradas en el Portal de Servicios al Ciudadano y Empresas (PSCE), adscrito al Portal del Estado Peruano (PEP).

25.5. La sede electrónica debe contar, además, con medios disponibles para la formulación de sugerencias y presentación de reclamos, respecto de la prestación de servicios de gobierno electrónico seguro, de conformidad con lo dispuesto por la Ley No. 29571 - Código de Protección y Defensa al Consumidor y demás normas complementarias y modificatorias.

25.6. El uso de servicios de gobierno electrónico seguro a través de la sede electrónica debe respetar los principios rectores establecidos en el Artículo 6º de la presente Ley.

25.7 Las entidades de la Administración Pública pueden establecer la obligatoriedad del uso de la sede electrónica para aquellas personas, naturales o jurídicas, que en razón de su capacidad económica o técnica, dedicación profesional u otros motivos acreditados tengan garantizado el acceso y disponibilidad de los medios electrónicos seguros de conformidad con lo establecido en la presente ley y operando en el marco de la Infraestructura Oficial de Firma Electrónica (IOFE).

Artículo 26.- Identificación de las entidades de la Administración Pública para la prestación de servicios de gobierno electrónico seguro

Las entidades de la Administración Pública, para la prestación de servicios de gobierno electrónico seguro, emplean certificados digitales emitidos por la Entidad de Certificación Nacional para el Estado Peruano o por una Entidad de Certificación para el Estado Peruano, en cooperación con una entidad de Registro o Verificación para el Estado Peruano, de conformidad con la normativa de la materia. Para la realización masiva de firmas digitales se podrá hacer uso de certificados digitales para agentes automatizados de acuerdo a lo establecido en la Ley No. 27269, de Firmas y Certificados Digitales y su Reglamento vigente.

Para la autenticación y generación de documentos electrónicos por parte de la Administración Pública, el personal a su cargo utiliza firmas y certificados digitales de conformidad con lo dispuesto en el Artículo 22º de la presente Ley.

Artículo 27.- Registros electrónicos

Las sedes electrónicas de las entidades de la Administración Pública cuentan con un sistema de registro electrónico para recibir documentos electrónicos, solicitudes, escritos y comunicaciones dirigidos a dicha entidad.

Para la eficacia de la presente disposición se debe cumplir con lo siguiente:

27.1. Las entidades de la Administración Pública pueden, mediante convenios de colaboración, habilitar sus respectivos registros para la recepción de las solicitudes, escritos y comunicaciones de competencia de otra entidad que se determinen en el correspondiente convenio.

27.2. Los registros electrónicos deben emitir automáticamente un acuse de recibo y la constancia de presentación del documento electrónico, escrito, solicitud o comunicación de que se trate, la que deberá incluir fecha y hora cierta del servicio de sellado de tiempo, así como, número de entrada de registro.

27.3. Para los efectos de lo indicado en el numeral precedente, el servicio de sellado de tiempo del que hagan uso las sedes electrónicas de las entidades de la Administración Pública, debe ser provisto por un Prestador de Servicios de Valor Añadido acreditado ante la Autoridad Administrativa Competente y que se encuentre operando dentro de la Infraestructura Oficial de Firma Electrónica (IOFE).

Artículo 28.- Cómputo de Plazos

A efectos del cómputo de los plazos imputables tanto a las personas como a las entidades de la Administración Pública, los registros electrónicos se deben regir por la fecha y hora cierta del servicio de sellado de tiempo del que haga uso la sede electrónica, a que se refiere el numeral 27.3 del artículo precedente.

Para la eficacia de la presente disposición se debe cumplir con lo siguiente:

28.1. Los registros electrónicos deben permitir la presentación de solicitudes, escritos y comunicaciones todos los días de la semana durante las veinticuatro (24) horas del día.

28.2. Para el cómputo de plazos fijados en días hábiles, las presentaciones efectuadas por las personas en un día inhábil, se deben entender realizadas el primer día hábil siguiente, salvo que mediante norma expresa, se permita la recepción en día inhábil, a partir del cual se computa el inicio del plazo que deben cumplir las entidades de la Administración Pública.

28.3. Cada sede electrónica de una entidad de la Administración Pública en la que esté disponible un registro electrónico debe fijar los días considerados como inhábiles a los efectos de los incisos anteriores, de conformidad con las normas respectivas.

Artículo 29.- Procedimiento de notificación por medios electrónicos seguros

29.1 En el procedimiento de notificación por medios electrónicos seguros, se requiere que la persona haya señalado dicho medio como preferente y/o haya consentido su utilización. Tanto la indicación de dicha preferencia, así como el consentimiento citado anteriormente, pueden emitirse y recabarse, por medios electrónicos seguros.

29.2 El RENIEC proporciona el domicilio electrónico oficial del ciudadano, que se habilita para todo ciudadano que obtenga un DNIe, y al que pueden acceder todas las

entidades de la Administración Pública para propósitos de la notificación electrónica. El acceso al domicilio electrónico Oficial es a través del DNIe.

29.3 Para la eficacia de la presente disposición se debe cumplir con lo siguiente:

29.3.1 El sistema de notificación debe permitir acreditar la fecha y hora cierta en la que se produzca la puesta a disposición de la persona del acto objeto de notificación, momento a partir del cual la notificación surtirá todos sus efectos legales.

29.3.2 La fecha y hora cierta se acredita por medio del servicio de sellado de tiempo del que haga uso la entidad pública, conforme a lo establecido en el numeral 27 .3 del artículo 27º de la presente Ley.

29.3.3 Cualquier notificación cursada a la persona, necesariamente debe ser efectuada en el domicilio electrónico que para tales efectos posea conforme a lo establecido por la Ley de Firmas y Certificados Digitales y su Reglamento.

CAPÍTULO III

DEL VALOR PROBATORIO DE LOS DOCUMENTOS ELECTRÓNICOS Y DEL ARCHIVO ELECTRÓNICO

Artículo 30 .- Valor probatorio de los documentos electrónicos

Los documentos electrónicos firmados digitalmente y que hayan sido generados dentro de la Infraestructura Oficial de Firma Electrónica (IOFE), gozan de validez y eficacia jurídica probatoria para todo servicio de gobierno electrónico seguro, de conformidad con la normatividad de la materia.

Tratándose de documentos provenientes de microformas, gozarán de validez y eficacia jurídica y probatoria para todo servicio, procedimiento administrativo y proceso judicial, siempre que hubiesen sido generados dentro de una línea de producción de microformas acreditadas ante el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI) y cumplan con lo establecido en el Decreto Legislativo Nº 681 y sus normas complementarias y reglamentarias.

Artículo 31.- Verificación de las copias de documentos electrónicos

Para la verificación de las copias en papel de documentos electrónicos a que se refiere el Artículo 30 de la presente Ley, los documentos impresos deben incluir la impresión de un código de verificación generado electrónicamente o un enlace que guarde relación con el documento original.

Artículo 32.- Conservación de los documentos electrónicos firmados digitalmente

Para la conservación de documentos electrónicos y garantizar la fiabilidad y perdurabilidad de la firma digital incorporada en aquellos se debe emplear sellos de tiempo que permitan verificar el estado del certificado digital asociado, así como el de los certificados que conforman la cadena de confianza, aplicando mecanismos basados en estándares internacionalmente aceptados que sean reconocidos dentro de la Infraestructura Oficial de Firma Electrónica.

El archivo de los documentos electrónicos se efectúa de acuerdo a las disposiciones legales de la materia.

CAPÍTULO IV

DEL EXPEDIENTE Y LA GESTIÓN ELECTRÓNICA DE LOS SERVICIOS, PROCEDIMIENTOS ADMINISTRATIVOS Y DE LA TUTELA JURISDICCIONAL

Artículo 33.- Expediente Electrónico

El expediente electrónico se constituye en los trámites, procedimientos administrativos o procesos judiciales en la entidad que agrupa una serie de documentos o anexos identificados como archivos, sobre los cuales interactúan los usuarios internos o externos a la entidad que tengan los perfiles de accesos o permisos autorizados.

El expediente electrónico debe tener un número de identificación único e inalterable que permita a lo largo de la prestación de los servicios de gobierno electrónico seguro su identificación unívoca dentro de la entidad de la administración pública que lo origine. Dicho número permite a su vez su identificación para efectos de un intercambio de información entre entidades o por las partes interesadas, así como para la obtención de copias del mismo cuando corresponda.

Cada documento electrónico incorporado en el expediente electrónico debe ser enumerado correlativamente, de modo que se origine un índice electrónico el cual es firmado digitalmente por el personal responsable de la entidad de la Administración

Pública a fin de garantizar la integridad del expediente electrónico y su recuperación siempre que sea preciso.

La conservación del expediente electrónico se realiza con arreglo a lo dispuesto en el Artículo 32º de la presente Ley y en lo dispuesto en el Reglamento de la presente Ley.

Artículo 34.- Utilización de medios electrónicos

La gestión electrónica para la prestación de servicios de gobierno electrónico seguro debe respetar la titularidad y el ejercicio de las competencias de las entidades de la Administración Pública, y el cumplimiento de los requisitos formales y materiales establecidos en las normas que regulen la correspondiente función.

Artículo 35.- Del uso de medios electrónicos en la gestión pública

El uso de los medios electrónicos en la gestión administrativa de las entidades de la Administración Pública debe estar siempre precedido por la realización de un análisis previo, rediseño y simplificación de procedimientos administrativos, servicios y actividades relacionadas al ejercicio de la tutela jurisdiccional, en concordancia con las normas sobre la materia.

TÍTULO TERCERO

DE LA INTEROPERABILIDAD, REUTILIZACIÓN DE APLICACIONES INFORMÁTICAS Y TRANSFERENCIA DE TECNOLOGÍAS ENTRE ENTIDADES DE LA ADMINISTRACIÓN PÚBLICA

CAPÍTULO I

DE LA INTEROPERABILIDAD

Artículo 36.- La Interoperabilidad de los sistemas de información en la Administración Pública

Las entidades de la Administración Pública deben establecer la interconexión de equipos de procesamiento de datos, a través del uso de estándares que permitan su interoperabilidad, a fin que sus respectivos sistemas y sus componentes puedan intercambiar información, con el objeto de facilitar el cumplimiento de sus respectivas funciones y la prestación de servicios de gobierno electrónico seguro, integrados o brindados en conjunto entre ellas.

Artículo 37.- Sistema de Interoperabilidad del Estado Peruano

El Sistema de Interoperabilidad del Estado Peruano está constituido por políticas, lineamientos, especificaciones, estándares e infraestructura de Tecnologías de la Información, que permitan de manera efectiva la interoperabilidad para la prestación de servicios de gobierno electrónico seguro comprendidos en el alcance de la presente Ley.

Asimismo, permite el intercambio de información o datos entre las distintas entidades de la Administración Pública por medios electrónicos seguros.

Artículo 38.- Gestión del Sistema de Interoperabilidad del Estado Peruano

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

38. 1 Interoperabilidad a nivel organizacional

a. **Ente Rector:** La Oficina Nacional de Gobierno Electrónico e Informática (ONGEI), de la Presidencia del Consejo de Ministros (PCM), es el Ente Rector encargado de establecer las políticas en materia de interoperabilidad y supervisar su cumplimiento.

b. **Comisión Multisectorial:** Encargada de proponer la determinación y actualización de los estándares y aplicaciones de Interoperabilidad para su aplicación en el Estado. Deberá ser creada en el marco de la Ley No. 29158, Ley Orgánica del Poder Ejecutivo y conformada por ONGEI, RENIEC, INDECOPI, SUNAT, SUNARP y otras entidades de mayor desarrollo en temas de interoperabilidad a determinarse por el Ente Rector.

c. **Autoridad de Interoperabilidad Institucional**: Persona de máxima autoridad administrativa o de gestión en las entidades de la Administración Pública.

d. **Las Oficinas de Tecnologías de la Información, sus equivalentes o los órganos que designen las entidades de la Administración Pública:** Órganos responsables de liderar las actividades de interoperabilidad.

e. **Áreas de racionalización o aquellas similares en su función:** Las encargadas de identificar y proponer los procesos relacionados con la implementación de la interoperabilidad en la entidad. El Reglamento de la presente Ley establecerá las funciones y/o responsabilidades a ser asumidas por estas áreas.

38 .2. Interoperabilidad a nivel semántico

En este nivel, se ocupa del significado en el uso de los datos y la información, garantizando que el significado preciso de la información intercambiada pueda ser entendido por cualquier aplicación de otra entidad de la Administración Pública. Dichas entidades deberán adoptar los estándares necesarios para el intercambio de datos.

38.3. Interoperabilidad a nivel técnico

Ejecutado por personal funcional relacionado con los objetivos de la entidad y personal especializado en Tecnologías de la Información y la Comunicación (TIC), de acuerdo a la aplicación de las normas, actividades y desarrollo de proyectos de interoperabilidad.

Artículo39.- Red de comunicaciones de las entidades de la Administración Pública

Las entidades de la Administración Pública deben adoptar las medidas necesarias e incorporarán en sus respectivos ámbitos, las tecnologías precisas para posibilitar la interconexión de sus redes, preferentemente el uso de la banda ancha, con el fin de crear una red de comunicaciones que interconecte los sistemas de información de aquéllas, y permita el intercambio de información electrónica, sobre servicios de gobierno electrónico seguro entre ellas cuando corresponda, así como la interconexión con las redes de otros Estados, en estricta observancia de la legislación de la materia y los convenios y/o acuerdos internacionales que pudiera haber celebrado el Estado Peruano.

Artículo 40.- De las Firmas y Certificados Digitales

El Sistema de Interoperabilidad del Estado Peruano para el uso de firmas y certificados digitales, debe encontrarse operando en el marco de la Infraestructura Oficial de Firma Electrónica (IOFE), aplicando lo establecido en la Ley de Firmas y Certificados Digitales y su Reglamento, así como observando el cumplimiento de estándares, lineamientos y mecanismos para implementar la interconexión de equipos de procesamiento electrónico de información entre entidades de la Administración Pública.

CAPÍTULO II

DE LA REUTILIZACIÓN DE APLICACIONES INFORMÁTICAS Y TRANSFERENCIA DE TECNOLOGÍAS

Artículo 41.- De la reutilización de sistemas y aplicaciones de propiedad de las entidades de la Administración Pública

Las entidades de la Administración Pública que sean titulares de los derechos patrimoniales de aplicaciones, desarrolladas para implementar sus servicios o cuyo desarrollo haya sido objeto de contratación, deben 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.

La puesta a disposición del aplicativo por parte de la entidad cedente, no obliga a esta última a brindar asistencia técnica, mantenimiento ni compensación alguna a la cesionaria en caso de errores de aplicación, quedando eximida de cualquier responsabilidad que pudiera generarse por el posible mal uso del aplicativo por parte de la entidad cesionaria.

Artículo 42.- Del Software Público

La Presidencia del Consejo de Ministros, a través de la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI), implementará un repositorio de software público de las entidades de la Administración Pública, que pueda ser compartido con las entidades que lo requieran, para acelerar los procesos de interoperabilidad, respetando la legislación sobre derechos de autor.

Las entidades de la Administración Pública deben tener en cuenta las soluciones disponibles para la libre reutilización que puedan satisfacer total o parcialmente las necesidades de los nuevos sistemas y servicios o la mejora y actualización de los ya implementados. Las entidades de la Administración Pública procuran la publicación del código de las aplicaciones, sea en desarrollo o finalizadas, en el repositorio de software público para su libre reutilización con el fin de favorecer las actuaciones de compartir, reutilizar y colaborar, en beneficio de una mejor eficiencia.

TÍTULO CUARTO

DEL INCUMPLIMIENTO DE LAS DISPOSICIONES DE LA LEY

CAPÍTULO ÚNICO

Artículo 43.- Del incumplimiento de las entidades de la Administración Pública

Todas las entidades de la Administración Pública quedan obligadas a cumplir lo estipulado en la presente norma sujetándose a lo establecido en el Reglamento.

La máxima autoridad o los funcionarios o servidores públicos designados por ésta como responsables al interior de cada entidad de la Administración Pública, responden administrativamente por el incumplimiento de lo dispuesto en la presente Ley y su Reglamento..

Artículo 44.- Del incumplimiento de las personas

Tratándose de los deberes de las personas, previstos en el artículo 17º de la presente Ley, su incumplimiento es sancionado conforme a las leyes vigentes.

DISPOSICIONES COMPLEMENTARIAS FINALES

PRIMERA.- Sistema de Seguridad de la Información

Todas las entidades de la Administración Pública deben contar con un Sistema de Seguridad de la Información, de acuerdo a las políticas y estándares establecidos por la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) de la Presidencia del Consejo de Ministros (PCM).

SEGUNDA.- Programas de capacitación y difusión

La Presidencia del Consejo de Ministros, a través de la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) y el Registro Nacional de Identificación y Estado Civil (RENIEC), deben coordinar con las entidades competentes, los programas de capacitación y difusión sobre los alcances e impacto de la presente Ley, los que deben ser brindados a las entidades de la Administración Pública.

Asimismo, dichas instituciones deben promover la formación de los servidores de las entidades de la Administración Pública en el uso de medios electrónicos para el desarrollo

de sus actividades y en la formación que les garantice conocimientos actualizados de las condiciones de seguridad correspondientes.

TERCERA.- Clasificador funcional programático

El Ministerio de Economía y Finanzas, dentro del plazo de un año, adecuará las actividades referidas en la presente Ley dentro del clasificador funcional programático, de acuerdo a los procedimientos presupuestales vigentes.

CUARTA.- Reglamentación del Documento Nacional de Identidad electrónico

El Registro Nacional de Identificación y Estado Civil (RENIEC) dictará las medidas reglamentarias referidas al Documento Nacional de Identidad electrónico (DNIe).

QUINTA.- De los servicios mediante el uso del Documento Nacional de Identidad electrónico (DNIe)

Facúltese al Registro Nacional de Identificación y Estado Civil (RENIEC) a implementar un Portal para el acceso a servicios de gobierno electrónico comprendidos en el alcance de la presente Ley que se brinden por medios electrónicos seguros, mediante el uso del Documento Nacional de Identidad electrónico (DNIe), en el marco de la Infraestructura Oficial de Firma Electrónica (IOFE).

SEXTA.- De los Convenios Interinstitucionales

Las Entidades de la Administración Pública podrán celebrar convenios interinstitucionales con los Colegios de Notarios o la Junta de Decanos de los Colegios de Notarios del Perú, a fin que estos les puedan proveer servicios de certificación digital bajo la modalidad de Entidad de Registro o Verificación y/o Prestador de Servicios de Valor Añadido, siempre y cuando el desarrollo de dichas actividades se enmarquen en las disposiciones vigentes sobre la materia y se opere en el marco de la Infraestructura Oficial de Firma Electrónica (IOFE).

SEPTIMA.- Documentos de gestión

Las entidades de la Administración Pública deben adecuar sus documentos de gestión, en lo que resulte necesario, con el objeto de dar cumplimiento a lo dispuesto en la presente Ley.

OCTAVA.- Plan Nacional de Identidad Digital y de Implementación de Servicios de Gobierno Electrónico Seguro

Dentro de un plazo que no excederá de 120 (ciento veinte) días hábiles siguientes a la entrada en vigencia del Reglamento de la presente Ley, la Presidencia del Consejo de Ministros (PCM), a través de la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI), en colaboración con el Ministerio de Economía y Finanzas y el Registro Nacional de Identificación y Estado Civil (RENIEC) en su calidad de Entidad de Certificación Nacional para el Estado Peruano elaborará la propuesta de Plan Nacional de Identidad Digital y de Implementación de Servicios de Gobierno Electrónico Seguro, a ser ejecutado por las entidades de la Administración Pública, que contenga las estimaciones de los recursos económicos, técnicos y humanos que se consideren necesarios para la adecuada ejecución de lo previsto en la presente Ley, así como la progresividad y gradualidad de su aplicación.

La propuesta de Plan Nacional de Identidad Digital y de Implementación de Servicios de Gobierno Electrónico Seguro debe incluir las medidas a ser tomadas para la correcta adecuación a la presente Ley, de aquellos servicios y/o procedimientos administrativos que a la fecha son brindados a través de medios electrónicos.

El Poder Judicial, en colaboración con el Ministerio de Economía y Finanzas y, la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI), dentro de un plazo que no exceda de 90 (noventa) días hábiles siguientes a la entrada en vigencia del Reglamento de la presente Ley, debe elaborar un Plan de Implementación del expediente electrónico para el ejercicio de la tutela jurisdiccional a través de medios electrónicos seguros. Este Plan debe contener la progresividad y gradualidad de su aplicación y formará parte del Plan Nacional de Identidad Digital y de Implementación de Servicios de Gobierno Electrónico Seguro.

Corresponde a la Presidencia del Consejo de Ministros (PCM) elevar la propuesta de Plan Nacional de Identidad Digital y de Implementación de Servicios de Gobierno Electrónico Seguro a que se refiere la presente disposición, al Consejo de Ministros, para su aprobación mediante Decreto Supremo.

NOVENA.- Reglamento de la Ley

El Reglamento de la presente Ley será aprobado por Decreto Supremo con refrendo del Presidente del Consejo de Ministros. El Reglamento garantizará de manera especial el derecho de las personas con discapacidad y adultos mayores, que se relacionan con las entidades de la Administración Pública, a fin que puedan acceder a los servicios electrónicos en igualdad de condiciones.

DECIMA.- Modelo de Inclusión Digital

Encárguese al Registro Nacional de Identificación y Estado Civil (RENIEC) la elaboración del modelo de e-inclusión y la metodología de diseño de servicios y procedimientos que, basados en la identidad digital, serán de aplicación para su implementación por las entidades de la Administración Pública. Otórguesele un plazo de noventa (90) días hábiles a partir del día siguiente de la entrada en vigencia de la presente Ley para la presentación del documento correspondiente a la Presidencia del Consejo de Ministros (PCM), para su aprobación y difusión.

DÉCIMO PRIMERA.- De los mecanismos de autenticación electrónicos

Las entidades de la Administración Pública, en la implementación de los servicios de gobierno electrónico, pueden determinar bajo su responsabilidad el uso de modalidades de autenticación electrónica distintas a la identidad digital. El criterio a seguir deberá sustentarse en un proceso de evaluación conforme a las buenas prácticas y estándares de seguridad de la información según se establezca en el Reglamento de la Ley.

DÉCIMO SEGUNDA.- Infraestructura Oficial de Firma Electrónica

Reconózcase a la Infraestructura Oficial de Firma Electrónica (IOFE) como el sistema confiable, acreditado, regulado y supervisado por la Autoridad Administrativa Competente, provisto de instrumentos legales y técnicos que facultan acreditar a Entidades de Certificación, Entidades de Registro o Verificación, Prestadores de Servicios de Valor Añadido y Software para Firmas Digitales, autorizándoles para la emisión de documentos credenciales electrónicos (certificados digitales), así como para la provisión de servicios de valor añadido, lo que posibilita la generación de documentos firmados digitalmente con pleno reconocimiento y valor legal. La Infraestructura Oficial de Firma Electrónica (IOFE) incluye, con los mismos efectos, la Entidad de Certificación Nacional para el Estado Peruano, las Entidades de Certificación para el Estado Peruano, las Entidades de Registro o Verificación para el Estado Peruano y los Prestadores de Servicios de Valor Añadido para el Estado Peruano.

DÉCIMO TERCERA.- Estructura Jerárquica de Certificación del Estado Peruano

El Registro Nacional de Identificación y Estado Civil (RENIEC) es la única Entidad de Certificación Nacional para el Estado Peruano, la misma que ejerce adicionalmente los roles de Entidad de Certificación para el Estado Peruano, Entidad de Registro y Verificación para el Estado Peruano y Prestador de Servicios de Valor Añadido..

DÉCIMO CUARTA.- Registro de Centros de Acceso

La Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) de la Presidencia del Consejo de Ministros (PCM), en un plazo de 90 (noventa) días hábiles computados a partir de la entrada en vigencia del Reglamento de la presente Ley, debe emitir los lineamientos necesarios para la adecuada verificación del cumplimiento de los elementos mínimos de los Centros de Acceso y su respectivo registro en concordancia con lo dispuesto por el Reglamento de la Ley de Firmas y Certificados Digitales.

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

DÉCIMO QUINTA.- De los Portales del Estado Peruano en *Internet*

Facúltese a la Presidencia del Consejo de Ministros (PCM) para que, a través de la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI), revise, actualice y ordene la normatividad en materia del Portal del Estado Peruano (PEP), Portal de Servicios al Ciudadano y Empresas (PSCE), el Sistema Integrado de Servicios Públicos Virtuales (SISEV) de la Ventanilla Única del Estado y Portales Institucionales.

La Oficina Nacional de Gobierno Electrónico (ONGEI) debe establecer las condiciones mínimas que permitan a las Comunidades Nativas y Campesinas acceder a información de su interés a través de los portales institucionales, procurando que dicha información esté disponible en su lengua, así como acceder a servicios prestados a través de un medio electrónico seguro.

DÉCIMO SEXTA.- Modificación del Decreto Legislativo No. 604

Modifíquese los incisos d) y g) del artículo 7° del Decreto Legislativo No. 604, cuyo texto será el siguiente:

> "Artículo 7°.- Los sistemas nacionales de estadística e informática están integrados por:
>
> (…)
>
> d) Las Oficinas de Tecnología de la Información o las que hagan sus veces en las entidades del Poder Ejecutivo.
>
> (…)

g) Las Oficinas de Tecnología de la Información o las que hagan sus veces en los Poderes Públicos y los Organismos a los que la Constitución Política del Perú y las leyes les confiere autonomía."

DÉCIMO SEPTIMA. – Modificación del Texto Único Ordenado de la Ley Nº 27584, Ley que Regula el Proceso Contencioso Administrativo, modificado por el D. Leg. Nº 1067, aprobado por Decreto Supremo Nº 013-2008-JUS.

Modifíquese el numeral 2 del artículo 22º y el artículo 24° del Texto Único Ordenado de la Ley Nº 27584, Ley que Regula el Proceso Contencioso Administrativo, modificado por el D. Leg. Nº 1067, aprobado por Decreto Supremo Nº 013-2008-JUS, conforme a los siguientes textos:

"Artículo 22.- Requisitos especiales de admisibilidad

Sin perjuicio de lo dispuesto por los Artículos 424 y 425 del Código Procesal Civil son requisitos especiales de admisibilidad de la demanda los siguientes:

(…)

2. En el supuesto contemplado en el segundo párrafo del Artículo 13 de la presente Ley, la entidad administrativa que demande la nulidad de sus propios actos deberá acompañar el expediente administrativo contenido en archivo electrónico generado según las normas que rigen la conservación de los documentos electrónicos en la Administración Pública."

"Artículo 24.- Remisión de actuados administrativos

Al admitir a trámite la demanda, el Juez ordenará, de ser el caso, a la Entidad Administrativa, a fin de que el funcionario competente remita copia certificada del expediente administrativo contenido en archivo electrónico generado según las normas que rigen la conservación de los documentos electrónicos en la Administración Pública, con lo relacionado a la actuación impugnada, en un plazo que no podrá exceder de quince días hábiles, con los apremios que el Juez estime necesarios para garantizar el efectivo cumplimiento de lo ordenado, pudiendo imponer a la Entidad multas compulsivas y progresivas en caso de renuencia.

El Juez además de realizar las acciones antes referidas en el párrafo anterior, ante la manifiesta renuencia a cumplir con el mandato, prescindirá del expediente administrativo.

El incumplimiento de lo ordenado a la entidad administrativa no suspende la tramitación del proceso, debiendo el Juez en este caso aplicar lo dispuesto en el Artículo 282 del Código Procesal Civil, al momento de resolver; sin perjuicio que tal negativa pueda ser apreciada por el Juez como reconocimiento de verdad de los hechos alegados".

DECIMO OCTAVA.- De la gestión de las bases de datos de los programas del Estado

El Registro Nacional de Identificación y Estado Civil (RENIEC) queda facultado a brindar asesoría, capacitación, servicios de gestión, infraestructura de soporte, y otros, a las entidades de la Administración Pública para la debida implementación y uso de las aplicaciones de software y estructuras de datos a incorporarse en el Documento Nacional de Identidad electrónico (DNIe) y que se encuentren vinculadas al ejercicio del cumplimiento de las funciones y a las atribuciones que a dichas entidades les competan. Para tal fin, el RENIEC debe suscribir previamente un convenio con la entidad de la Administración Pública correspondiente.

DECIMO NOVENA.- Del archivo de los documentos electrónicos

Encárguese al Archivo General de la Nación (AGN) la administración y archivo final de los documentos electrónicos conservados en microformas emitidos por las entidades de la Administración Pública y que hayan alcanzado un valor permanente, conforme a lo previsto en la presente Ley.

Para dicho efecto, el Archivo General de la Nación deberá determinar las necesidades y condiciones que requiera para ejercer la administración y el archivo previsto en el párrafo precedente, debiendo para ello, elaborar las propuestas normativas que resulten necesarias.

VIGÉSIMA.- De la autenticación biométrica de la identidad

Autorícese al RENIEC a promover el uso de la autenticación de la identidad a través de la tecnología biométrica, así como el establecimiento progresivo y gradual del Código Único de Identificación de la Persona Natural con Base Genética.

VIGÉSIMO PRIMERA.- De la implementación de la Ley

La implementación de la presente Ley es gradual, de acuerdo a la disponibilidad presupuestal de las entidades de la Administración Pública, y en concordancia con las políticas, estrategias y planes del Estado,

DISPOSICIÓN COMPLEMENTARIA DEROGATORIA

ÚNICA.- Derogación

Queda derogada la Ley No. 28403 “Ley que dispone la recaudación de un aporte por supervisión y control anual por parte del INDECOPI de las Entidades de Certificación y de Verificación / Registro de Firmas Digitales, acreditadas bajo su ámbito”.

ANEXO 7:

Proyecto de Ley que crea el Sistema Funcional de Identidad Digital, Protección de Datos Personales, Certificación y Registro Digital. (Elaborado por el autor de la presente Tesis).

Articulo 1º. Creacion de Sistema Funcional: Créase el Sistema Funcional de Identidad Digital, Protección de Datos Personales, Certificación y Registro Digital.

Articulo 2º Ente Rector: El Registro Nacional de Identificación y Estado (RENIEC) es el ente Rector del Sistema Funcional de Identidad Digital, Protección de Datos Personales, Certificación y Registro Digital.

Articulo 3º Sustitución del artículo 32º de la Ley 29733: Sustitúyase el artículo 32º de la Ley 29733 por el siguiente:

"Articulo 32º Órgano Competente y régimen Jurídico

El Registro Nacional de Identificación y Estado Civil (RENIEC), es la Autoridad Nacional de Protección de Datos Personales. Para el adecuado desempeño de sus funciones, puede crear y/o reorganizar oficinas en todo el país.

La Autoridad Nacional de Protección de Datos Personales se rige por lo dispuesto en esta Ley, en su reglamento y en los artículos pertinentes del Reglamento de Organización y Funciones del Registro Nacional de Identificación y Estado Civil (RENIEC).

Corresponde a la Autoridad Nacional de Protección de Datos Personales realizar todas las acciones necesarias para el cumplimiento del objeto y demás disposiciones de la presente Ley y de su reglamento. Para tal efecto, goza de potestad sancionadora de conformidad con la Ley 27444, Ley de Procedimiento Administrativo General, o la que haga sus veces, asi como de potestad coactiva, de

conformidad con la Ley 26979, Ley de Procedimiento de Ejecución Coactiva, o la que haga sus veces.

La Autoridad Nacional de Protección de Datos Personales actuará de acuerdo al Plan Nacional de Identidad Digital y Protección de Datos Personales que periódicamente elabore el Ente Rector del Sistema Funcional de Identidad Digital, Protección de Datos Personales y Certificación y Registro Digital; asi como de la correspondiente Política de Estado.

La Autoridad Nacional de Protección de Datos Personales podrá gestionar en coordinación con el Ministerio de Relaciones Exteriores, la celebración de convenios internacionales de reconocimiento y fortalecimiento de la identidad digital, de la protección de datos personales y la certificación y registro digital.

Para el cumplimiento de sus funciones, la Autoridad Nacional de Protección de Datos Personales cuenta con el apoyo y asesoramiento técnico de la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) de la Presidencia del Consejo de Ministros, o la que haga sus veces y de la Dirección General de Derechos Humanos del Ministerio de Justicia y Derechos Humanos, o la que haga sus veces".

Artículo 4: Reglamentación:

El Reglamento regulará las competencias del Sistema Funcional de Identidad Digital, Protección de Datos Personales, Certificación y Registro Digital. Crease una Comisión para su Reglamentación, conformada por:

a) El Jefe Nacional del Registro Nacional de Identificación y Estado Civil (RENIEC) , quien lo presidirá.
b) El Director de la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) de la Presidencia del Consejo de Ministros.
c) El Director General de Derechos Humanos del Ministerio de Justicia y Derechos Humanos.

d) Un representante del Instituto Nacional de Defensa de la Libre Competencia y Protección de la Propiedad Intelectual (INDECOPI).
e) Un representante del Ministerio de Relaciones Exteriores.

El Reglamento será emitido por Decreto Supremo del Poder Ejecutivo y suscrito por el Presidente del Consejo de Ministros, el Ministro de Relaciones Exteriores y el Ministro de Justicia y Derechos Humanos, en un plazo máximo de noventa días calendario contados desde el día siguiente de publicación de la presente ley.

Articulo 5: Derogación

Deróguese las normas que se opongan a la presente Ley.

Lima, Noviembre de 2015.

BIBLIOGRAFIA

- ALAMILLO DOMINGO, Ignacio : "La Identidad en la Red". Investigación y Ciencia. ISSN-0210-136X. Nº 386, 2008. Pàginas 54 a 61

- ALAMILLO DOMINGO, Ignacio y HENAO HOYOS, Erika: "La Gestiòn electrónica de la Identidad y de la firma electrónica en el intercambio electrónico de Datos entre Administraciones Pùblicas" En Revista de Derecho Informàtico, ISSN-e 1681 – 5726 , Nº 121, 2008.

- ALVAREZ-CIENFUEGOS SUAREZ, José María: "Legislación aplicable y jurisdicción competente". En Revista Iberoamericana de Derecho Informático. Nºs. 30,31,32 Ed. Universidad Nacional a Distancia. Centro Regional de Extremadura, Merida, España.. 2000. Páginas 129 a 148.

- BOLAS ALFONSO, Juan: "Seguridad en la Contratación por Internet: Firma Electrónica y Fe Pública". En Revista Iberoamericana de Derecho Informático. Nºs. 30,31,32 Ed. Universidad Nacional a Distancia. Centro Regional de Extremadura, Merida, España.. 2000. Páginas 89 a 105
-
- BONET COMPANY, Jesús: "El Documento Electrónico en el procedimiento administrativo español: ¿Hacia el documento público electrónico?. En Revista Iberoamericana de Derecho Informático. Nºs. 30,31,32 Ed. Universidad Nacional a Distancia. Centro Regional de Extremadura, Merida, España.. 2000. Páginas 207 a 233.

- BUSANICHE, Beatriz: "La Vida de los Otros". En "Habilitando la apertura: el futuro de la sociedad de la información en América Latina y el Caribe". Ed. Fundación Comunica, Montevideo, Uruguay y Coedición: International Development Research Center, Otawa, Canadá. 2013. Páginas 169 a 176.

- CASTELLS, Manuel: "Internet y la Sociedad en Red". Lección Inaugural del programa de doctorado sobre la sociedad de la información y el conocimiento en 2001 en la Universidad Oberta de Cataluña (UOC). En http://tecnologiaedu.us.es/cuestionario/bibliovir/106.pdf Paginas 13. Fecha de consulta 21 de noviembre de 2015.

- COMISION DE NACIONES UNIDAS PARA EL DERECHO MERCANTIL INTERNACIONAL (CNUDMI): "Posible Labor Futura en materia de comercio electrónico: cuestiones jurídicas relacionadas con la gestión de identidad y los servicios de Confianza". Propuesta de Austria, Bélgica,

Francia, Italia y Polonia. A/CN.9/854. 5 de Mayo de 2015. Documentación para el 48º periodo de sesiones en Viena, Austria, de 29 de Junio al 16 de Julio de 2015. Páginas 8. En: http://www.uncitral.org

- CONFERENCIA DE LAS NACIONES UNIDAS SOBRE COMERCIO Y DESARROLLO (UNTACD): "Estudio sobre las perspectivas de la armonización de la ciberlegislación". Ed. Naciones Unidas. Junio de 2008. Página 7.

- CHAVEZ VALDIVIA, Ana Karin: "Identidad Virtual: Implicancias en el Derecho a la Intimidad". Ponencia presentada en el XVIII Congreso Iberoamericano de Derecho e Informática. San José de Costa Rica, el jueves 16 de Octubre de 2014. Página 184. En http://www.juandiegocastro.com Fecha de consulta: 17 de Noviembre de 2014.

- CHECKLAND, Peter: "Pensamiento de sistemas, practica de sistemas". México DF. Grupo Noriega Editores, 1993,

- DAVARA RODRIGUEZ, Miguel Angel: "La Protección de Datos en las Instituciones Sanitarias". En Anuario de Derecho de Tecnologías de la Información y Comunicaciones (TICs) 2006. Ed. Davara &Davara Asesores Jurídicos. Fundación Vodafone España. Madrid, España 2006. Páginas 3 a 69.

- DELPIAZZO, Carlos E. y VIEGA, María José: "Lecciones de Derecho Telemático". Ed. Fundación de Cultura Universitaria. Montevideo, Uruguay. 2004. Página 13

- DE GRACIA, Carlos Gregorio: "¿Está muerta la Privacidad? Algunas Reflexiones a Modo de Respuesta". En "Habilitando la apertura: el futuro de la sociedad de la información en América Latina y el Caribe". Ed. Fundación Comunica, Montevideo, Uruguay y Coedición: International Development Research Center, Otawa, Canadá. 2013. Páginas 147 a 152.

- ESPINOZA, Juan: "Derecho de Personas." Ed. Gaceta Jurídica. Lima, Perú. 2004. Páginas 253 y 254

- FERNANDEZ BURGUEÑO, Pablo: "La Identidad Digital de la Persona Fisica en la Sociedad del Conocimiento. Ponencia XIX Congreso Iberoamericano de Derecho e Informática. 26, 27 y 28 de Agosto de 2015. Medellin, Colombia.

- FERNANDEZ LOPEZ, Juan Manuel: "Flujo Internacional de Datos". En Revista Iberoamericana de Derecho Informático Nºs 30, 31,32. 1999. Ed. Universidad Nacional de Educación A Distancia. Centro Regional de Extremadura- Mérida, España. Página 189.

- FERNANDEZ SESSAREGO, Carlos: "Derecho a la Identidad Personal". Ed. Astrea. Buenos Aires, Argentina. 1992. 489 p.p.

- FERREYROS SOTO, Carlos: "Ejecutivos, Redes Sociales e Identidad Digital". Blog Derecho y Nuevas Tecnologías, sábado, 29 de Diciembre del 2012. En http://derecho-ntic.blogspot.pe/search?updated-min=2012-01-01T00:00:00-08:00&updated-max=2013-01-01T00:00:00-08:00&max-results=19

- FERREYROS SOTO, Carlos; GONZALES AGUILAR, Audilio; CARRASCOSA LOPEZ, Valentín: "Los Contratos en la Sociedad de la Información". Ed. Fondo Editorial del Pedagógico de San Marcos. Primera Edición en el Perú. Lima, Perú. Octubre del 2004. 524 p.p..

- FINOCCHIARIO, Giusella: "Identità Personalle su Internet: Il diritto alla contestualizzazione dellínformazione". Rivista "Il Diritto dell'informazione e dell ìnformatica . Anno XXVII. Fasc.3. 2012. Milano. Giufrè Editore. Italia.

- FROSINI; Vittorio: "Il giurista nella societá dell'informaziones". Rivista Internazionale INFORMATICA E DIRITTO" .Ediziones Scientifiche Italiane. Napoli. Italia. 2001. Nº2 . Páginas 193 a 207.

- GAETE GONZALES, Eugenio Alberto: "Instrumento Público Electrónico". Editorial Boch. Barcelona, España. 2000. 532 p.p.
-
- IGLESIAS, Lidia Viviana: "Firma Digital. Seguridad en Internet. Certificados. En Memorias del VIII Congreso Iberoamericano de Derecho e Informática. TEC de Monterrey. México. Noviembre 2000. Página 515.

- ITEANU, Olivier: L´identité numerique en question. 10 scenarios pour la amitrise juridique de son identite sur internet"Ed. EYROLLES. Paris, Francia. Abril 2008. Paginas 5 y 6. En ir.nmu.org.ua/bitstream/handie/123456789/1c5018659518F67372c0bf9687170a9d.pdf?sequence=1.

- KNORR; Jolene y SAUMA, Marcelo: "La Protección al Consumidor en el Comercio Electrónico ". Editorial IJSA Investigaciones Jurídicas S.A. San José, Costa Rica. 2001. 282 p.p.

- LESSIG, Lawrence: "El Código y otras Leyes en el Ciberespacio". Ed. Taurus. Madrid, España. 2001. Pàgina 27.

- MARTINEZ FONS, Daniel: "El Uso y Control del Correo Electrónico e Internet en la Empresa: Aspectos Laborales. En Libro "El uso laboral y sindical del Correo Electrónico e Internet en la empresa". Ed. Tirant Lo Blanch. Valencia, España 2007. Página 179.

- MARTIN-MORENO, M y SAEZ VACA F.: "Análisis Preliminar del Comercio Electrónico" En: www.dit.upm.es/~fsaez/intl/proyectos/contenidos/Bloque%20I.**pd**. **Fecha de Consulta: 3 de Enero de 2014.**

- MOLINA MATEOS, José María: "Firma Electrónica y Fe Pública Extrajudicial" En Revista Iberoamericana de Derecho Informático. Nºs. 30,31,32 Ed. Universidad Nacional a Distancia. Centro Regional de Extremadura, Merida, España.. 2000. Página 421.

- MOURON PHILIPE: "Internet et Identité virtuelle des persones". En: http://junon-u-3mrs.fr/u3ired01/Main%20docu/internet/chronp-identitevirtuelle.pdf Fecha de Consulta: 05 de Octubre de 2015.

- Marco para Identificación Electrónica Social Iberoamericana" Aprobado por la XIII Conferencia Iberoamericana de Ministros y Ministras de Administración Pública y Reforma del Estado Asunción, Paraguay, 30 de junio - 1° de julio de 2011

- NUÑEZ PONCE, Julio: "Actos y Contratos Electrónicos en Internet, Derecho Informático y Principio Aplicable". En Revista del Foro. Año MMII, Nº1. Ed, Ilustre Colegio de Abogados de Lima- Lima, Perú. Abril, 2002. Página 125 a 134.

- NUÑEZ PONCE, Julio: "Derecho de Negocios Electrónicos en Internet". En Libro Homenaje a los XXV años de la Facultad de Derecho. Ed. Fondo de Desarrollo Editorial de la Universidad de Lima. Lima, Perù. 2006. Página 424.

- NUÑEZ PONCE, Julio: "El Derecho Informático y la Identificación". En Gaceta Registral. Revista de Jurisprudencia Institucional del RENIEC. Año VIII. Numero 7, 2014. Páginas 30 a 37.

- NUÑEZ PONCE, Julio: "La Contratación Electrónica" . En Tratado de Derecho Mercantil. Tomo III. Contratos Mercantiles y Bancarios. Ed. Gaceta Jurídica S.A. Lima, Perú. Abril, 2008. Páginas 35 a 57.

- ORMAZABAL SANCHEZ, Guillermo: "La prueba documental y los medios e instrumentos idóneos para reproducir imágenes o sonidos o archivar y conocer datos". Editorial La Ley. Madrid, España. 2000. 237 p.p.
-
- PARDINI, Anibal: "Derecho en Internet". Ediciones La Rocca. Buenos Aires, Argentina. 2002. Página 27.

- PEREZ LUÑO, Antonio Enrique: "Manual de Informática y Derecho" Ed. Ariel Derecho. Barcelona, España. 1996. 222 p.p.

- PUIGCERVER ASOR, Carlos: "La Firma Digital y las Autoridades de Certificación: Regulación e Interacción en el proceso Español tras la regulación del Comercio Electrónico". En Revista de Derecho Comercial y de las Obligaciones. Nº 197. Ed. Depalma. Buenos Aires, Argentina. 2000. Páginas 133 a 145.

- RAWLS, Jhon: "Teoria de la Justicia" Ed. The Belknap Press of Harvard University, Cmabirdge, Massachussets. Segunda Edicion en Español, sexta reimpresion. 2006

- RAYPORT, Jeffrey et al: "E-Commerce" Ed. Mc Graw Hill. México D.F. , México. 2003. 493 p.p.

- Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo de 23 de Julio de 2014. Diario Oficial de la Unión Europea del 28.8.2014. L 257/73
.
- RENIEC: "Enciclopedia del Sistema Registral" Ed. Registro Nacional de Identificación y Estado Civil. Lima, Perú. 2010. Página 139.

- RODRIGUEZ TADEO, María Jose: "Impacto de la Protección de Datos Personales en Uruguay". En Memorias del XIV Congreso Iberoamericano de Derecho e Informática. Nuevo León, México del 25 al 30 de Octubre de 2010. Versión Digital. Páginas 725 y 726.

- ROIG, Antonio: "El uso de Internet en la Empresa: Aspectos Constitucionales". En Libro "El uso laboral y sindical del Correo Electrónico e Internet en la empresa". Ed. Tirant Lo Blanch. Valencia, España 2007. Páginas 24 y 25.

- RUIZ, Claudio: "¿Está muerta la pivacidad? Propuestas para una reflexión crítica sobre la protección de la privacidad en la era de internet". En "Habilitando la apertura: el futuro de la sociedad de la información en América Latina y el Caribe". Ed. Fundación Comunica, Montevideo,

Uruguay y Coedición: International Development Research Center, Otawa, Canadá. 2013. Páginas 143 a 145.

- SAARENPAA , Ahti : "Legal Welfare And Legal Planning In The Network Society" . En Memorias del XVI Congreso Iberoamericano de Derecho e Informática . Ed. Ministerio de Justicia, Derechos Humanos y Culto. Imprenta Moreno. Quito, Ecuador. Septiembre 2012. Página 41

- SARRA, Andrea Viviana: "Comercio Electrónico y Derecho" Ed. Astrea. Buenos Aires, Argentina. 2000. 443 p.p.

- SMEDINGHOFF, Thomas: Information Security Law: The Emerging Standard for Corporate Compliance. Ed. IT Governance Publising . United Kingdom. 2008, ISBN 978- 1-905356-66-9

- SUÑE LLINAS, Emilio: "La Ventanilla Única Electrónica". En Memorias del X Congreso Iberoamericano de Derecho e Informática. Celebrado en Santiago de Chile del 6 al 9 de Setiembre de 2004. Ed. Biblioteca del Congreso Nacional de Chile, Facultad de Derecho de la Universidad de Chile. Santiago de Chile, 2004. Chile. Páginas 15 a 42.

- TAYLOR, Charles: "Fuentes del yo : La construcción de la identidad moderna". Ed. Paidos. Barcelona, España. 2006

- URTEAGA, Eguski: "La Teoría de Sistemas de Niklas Luhman".En Contrastes. Revista Internacional de Filosofía. Vol XV (2010).(Pags.301 a 317) Recibido 26-11-2008. Aprobado 22-01-2009. En http://www.uma.es/contrastes/pdfs/015/ContrastesXV-16.pdf

- VON BERTALANFFY, Ludwig: "Teoría General de Sistemas: Fundamentos, desarrollo, aplicaciones". Ed. Fondo de Cultura Económica". México D.F. Primera Edición en español, Séptima Reimpresión, 1989. Páginas 33 y 34.

- YRRIVARREN LAZO, Jorge Luis: "Construyendo nuestra Identidad Digital". En Página de Opinión del Diario Oficial El Peruano. Lima, Jueves, 13 de Setiembre de 2012. Página 12.

- YRIVARREN LAZO, Jorge: "Identidad, Identificación y Persona Humana: Por la institucionalidad de lo diverso". En : RENIEC: "Identidad Digital: La

identificación desde los registros parroquiales al DNI Electrónico". Primera Edición, diciembre 2015. Páginas 21 a 47.

INDICE GENERAL

Capitulo 3: Necesidad de un Sistema Funcional de Identidad Digital que garantice la seguridad y confianza en los procesos electrónicos.