



MAESTRÍA EN DERECHO DE LAS TECNOLOGÍAS
DE INFORMACIÓN Y COMUNICACIÓN

INFOTEC CENTRO DE INVESTIGACIÓN E
INNOVACIÓN EN TECNOLOGÍAS DE LA
INFORMACIÓN Y COMUNICACIÓN

DIRECCIÓN ADJUNTA DE INNOVACIÓN Y
CONOCIMIENTO
GERENCIA DE CAPITAL HUMANO
POSGRADOS

“Guía para la implementación de trámites en línea en la APF ”

(SOLUCIÓN ESTRATÉGICA)
Que para obtener el grado de MAESTRO EN
DERECHO DE LAS TECNOLOGÍAS DE
INFORMACIÓN Y COMUNICACIÓN

Presenta:

Diana Muñoz Flor

Asesor:

Dr. Mario Anselmo Gómez Sánchez

Ciudad de México, 10 de enero de 2023.



Autorización de impresión



AUTORIZACIÓN DE IMPRESIÓN Y NO ADEUDO EN BIBLIOTECA

Maestría en Derecho de las Tecnologías de Información y Comunicación, MDTIC.

Ciudad de México, 02 de febrero de 2023

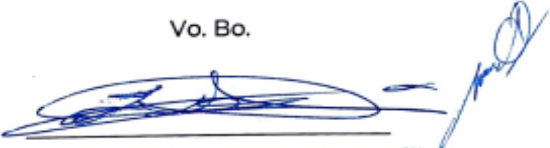
La Gerencia de Capital Humano/Gerencia de Investigación hacen constar que el trabajo de terminal de titulación:

"Guía para la implementación de trámites en línea en la APF".

Desarrollado por la alumna Diana Muñoz Flor, y bajo la asesoría del Dr. Mario Anselmo Gómez Sánchez cumple con el formato de Biblioteca. Por lo cual, se expide la presente autorización para impresión del proyecto terminal al que se ha hecho mención.

Asimismo, se hace constar que no debe material de la biblioteca de INFOTEC.

Vo. Bo.



Mtro. Felipe Alfonso Delgado Castillo
Gerente de Capital Humano

Anexar a la presente autorización al inicio de la versión impresa del trabajo referido que ampara la misma.

C.p.p Servicios Escolares

Agradecimientos

A Joaquín, mi confidente, amigo, compañero, amor de mi vida, gracias por impulsarme siempre, por motivarme a entrar a esta Maestría, por todas las charlas y consejos, por ayudarme a mejorar siempre, por respetar mis procesos y darme tu mano.

A mi mamá, gracias por acompañarme, cuidarme, quererme siempre y haberme enseñado el valor del esfuerzo.

A mi papá, gracias por haberme enseñado el valor de la independencia y la fortaleza

A mi hermana y a mi hermano, gracias por ser un ejemplo, por ayudarme, impulsarme, por estar ahí siempre, por ser mi fortaleza.

A mis sobrinas y sobrino, por ser una de mis fuentes de inspiración.

A mis ángeles de cuatro patas, Yoko, Shaza, Lluvia y Solo, gracias por haberme transformado, por hacerme compañía siempre y amarme tal cual soy.

A Carla, Nitzine, Michel, Esteban, Cinthia y Diego, gracias por acompañarme, apoyarme, escucharme y estar siempre presentes en mi vida.

A INFOTEC, gracias por todos los conocimientos, por recordarme lo maravilloso del conocimiento y todos los caminos para aplicarlo.

A mi asesor, el Dr. Mario Anselmo Gómez Sánchez, por todos sus consejos, paciencia, por compartir sus conocimientos y tiempo y haberme ayudado a lograr este trabajo.

A mis maestros de INFOTEC, gracias por compartirme y contagiarme su amor por el conocimiento y la reflexión.

A Benjamín, gracias por impulsarme y motivarme.

A mis compañeros de la Maestría, gracias por este camino recorrido, especialmente a Mildred, Martha y Miguel gracias por todo lo que me enseñaron y ayudaron, por compartir las preocupaciones, las risas y desveladas.

Tabla de Contenido

Introducción.....	1
Capítulo 1. Aspectos generales del gobierno electrónico y los derechos humanos vinculados.....	3
1.1 Antecedentes del gobierno electrónico.....	3
1.1.1 Etapas	6
1.1.2 Interrelación entre los diversos actores	8
1.1.3 Barreras.....	11
Capítulo 2. Marco jurídico de los trámites en línea en la APF.....	21
2.1 Marco jurídico internacional.....	21
2.1.1 Ley Modelo de la CNUDMI sobre Comercio Electrónico	22
2.1.2 Ley Modelo de la CNUDMI sobre Firmas Electrónicas.....	24
2.1.3 Reglamento (UE) No 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.....	28
2.2. Marco jurídico nacional	30
2.2.1 Ley Federal de Procedimiento Administrativo	30
2.2.2 Ley de Firma Electrónica Avanzada.....	32
2.2.3 Ley Federal de Transparencia y Acceso a la Información Pública	37
2.2.4 Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados	38
2.2.5 Ley General de Mejora Regulatoria.....	39
2.2.6 Ley General de Archivos.....	40
2.2.7 Acuerdo para la adopción y uso por la APF de la Clave Única de Registro de la Población.....	41
2.2.8 Acuerdo por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la APF.....	43
2.2.9 Bases técnicas de Seguridad Informática para las dependencias y entidades de la APF.....	45
2.2.10 Decretos, acuerdos, criterios expedidos por la Unidad de Gobierno Digital ...	45
2.2.10.1 Decreto por el que se establece la Ventanilla Única Nacional para los Trámites e Información del Gobierno.....	45

2.2.10.2 Decreto por el que se establece la regulación en materia de Datos Abiertos	46
2.2.10.3 Disposiciones Generales que establecen los mecanismos de identificación y control de acceso que deberán observar las dependencias y entidades de la APF y las empresas productivas del Estado	46
2.2.10.4 Criterios Técnicos que deberán observar las dependencias y entidades de la APF, así como las empresas productivas del Estado, para la emisión de documentos electrónicos que deriven de un trámite o servicio digital	47
2.3 Marco jurídico nacional aplicable a los particulares con impacto en el sector público.....	48
2.2.1 Código de Comercio	48
2.2.2 Ley Federal de Protección de Datos Personales en Posesión de Particulares. 49	
2.2.3 Norma Oficial Mexicana NOM-151-SCFI-2016, Requisitos que deben observarse para la conservación de mensajes de datos y digitalización de documentos (cancela la NOM-151-SCFI-2002).....	49
2.4. La firma electrónica y los servicios de confianza.....	50
Capítulo 3. Análisis comparativo de gobierno electrónico y la implementación de trámites en línea en los países de Alianza del Pacífico	66
3.1. Colombia.....	66
3.2. Perú	75
3.3. Chile	83
3.4. México	88
Capítulo 4. Guía para implementar trámites en línea en la APF	95
4.1 Introducción	95
4.2 Marco jurídico en México.....	97
4.3 Principios.....	99
4.4 Pasos	101
Conclusiones.....	170
Bibliografía	174

Índice de figuras

Figura 1. Principios y aspectos que se deben considerar durante la implementación de trámites en línea.....	101
Figura 2. Principios de Seguridad de la Información	107
Figura 3. Principios interoperabilidad	113
Figura 4. Pasos para implementar procesos de interoperabilidad	114
Figura 5: Elementos para garantizar la validez de los trámites en línea	122
Figura 6. Niveles de autenticación.....	132
Figura 7. Mecanismos para acreditar la personalidad en línea.....	137
Figura 8. Medios para realizar la notificación electrónica	149
Figura 9. Contenido Aviso de privacidad simplificado	158
Figura 10. Aviso de Privacidad Integral	159
Figura 11. Deberes de protección de datos personales	163
Figura 12. Medios para la difusión de los trámites en línea	168

Índice de cuadros

Cuadro 1. Marco jurídico en Colombia	70
Cuadro 2. Marco jurídico Perú	80
Cuadro 3. Marco jurídico Chile.....	85
Cuadro 4. Marco Jurídico México	99
Cuadro 5. ISOS Seguridad de la información y protección de datos personales	110
Cuadro 6. Principios Datos Personales.....	156

Siglas y abreviaturas

APF	Administración Pública Federal
Acuerdo de Gobierno Digital	Acuerdo por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la APF
CNUDMI	Comisión de las Naciones Unidas para el Derecho Mercantil Internacional
CONAMER	Comisión Nacional de Mejora Regulatoria
CLAD	Centro Latinoamericano de administración para el desarrollo
Criterios Técnicos	Criterios Técnicos que deberán observar las dependencias y entidades de la APF, así como las empresas productivas del Estado, para la emisión de documentos electrónicos que deriven de un trámite o servicio digital
CURP	Clave Única de Registro de Población
ISO	International Organization for Standardization
LFTAIP	Ley Federal de Transparencia y Acceso a la Información Pública
LGPDPSSO	Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados
MIR	Manifestación de Impacto Regulatorio
MinTIC	Marco de Gestión de Seguridad de la Información Ministerio de Tecnologías de la Información y Comunicaciones
NOM 151	Norma Oficial Mexicana NOM- 151.SCFI.2016, Requisitos que deben observarse para la conservación de mensajes de datos y digitalización de documentos
OEA	Organización de los Estados Americanos
OECD	Organisation for Economic Co-operation and Development
PKI	Public Key Infraestructure

PSC	Prestadores de Servicios de Certificación
RENAPO	Registro Nacional de Población
RFC	Request for Comments
RPC	Registro Público de Comercio
RUG	Registro Único de Garantías Mobiliarias
SE	Secretaría de Economía
SAT	Servicio de Administración Tributaria
TSA	Time Stamping Authority
TIC	Tecnologías de la Información y Comunicación
UNCITRAL	United Nations Commission on International Trade Law

Introducción

El Gobierno ha estado evolucionando en los últimos años, a lo que se ha denominado Gobierno Electrónico, el cual implica un cambio de perspectiva y de gestión pública y tiene un impacto directo al interior del gobierno, en los servicios que se prestan a los ciudadanos y en la forma en que éstos participan; por ello, se convierte en una necesidad fundamental el implementar trámites en línea, completamente transaccionales.

Lo anterior, significa mucho más que hacer más eficiente el servicio público, es una forma de hacer políticas públicas donde la ciudadanía participa y forma parte fundamental de éstas, no solo como el centro en el proceso, sino como constructora de las mismas, también permite que las Dependencias dejen de ser entes aislados donde el usuario tiene que ir a tocar diversas puertas para contar con la prestación de un servicio público.

Ahora bien, durante esta implementación se presentan diversos retos, ya que se deben generar mecanismos que contemplen a todos, es decir, considerar la brecha digital, sin dejar de lado la eficacia y eficiencia que se debe garantizar en el servicio público. En el mismo orden de ideas, se deberá considerar la transparencia, los datos abiertos, pero al mismo tiempo garantizar la protección de diversos derechos como es el de datos personales y privacidad.

En este sentido, además de los aspectos antes referidos será fundamental realizar esta implementación con la debida certeza jurídica. En este orden de ideas, agilizar y simplificar los procesos en los trámites no puede significar el sacrificio de esta certeza, por tanto, contar con un marco jurídico adecuado para lo anterior será esencial.

Al respecto, si bien, se puede considerar que en México existe una regulación general para la implementación de medios electrónicos en los trámites y servicios, cuando las Dependencias planean este proceso se enfrentan además de los retos antes señalados a otros relacionados con el marco jurídico, que van desde confusión respecto al que resulta aplicable, hasta los elementos que deben

contemplar para que lo hagan con la validez jurídica que se requiere y los pasos que deben seguir para ello, considerando la forma en que se genera y envía la información a través de mensajes de datos en los cuales se debe mantener la integridad y garantizar la vinculación con el emisor.

Es así, que en el presente trabajo se pretenden abordar en primer término, los aspectos generales del gobierno electrónico, incluyendo sus antecedentes, etapas, interrelaciones, barreras, así como los derechos vinculados, como lo es el derecho a la buena administración; posteriormente, en el segundo capítulo, se analizará el marco jurídico aplicable tanto, referencias internacionales como es la Ley Modelo de la CNUDMI sobre Comercio Electrónico y la Ley Modelo de la CNUDMI sobre Firmas Electrónicas, así como el correspondiente en México, en primer término, las reformas que datan desde el año 2000, año en el que se incluyeron en la legislación modificaciones referentes al comercio electrónico y firma electrónica, así como los servicios de confianza, hasta los Acuerdos más recientes publicados en el marco de la Estrategia Digital Nacional actual. Aunado a ello se desarrollará la firma electrónica y los servicios de confianza como son: los sellos digitales de tiempo y las constancias de conservación de mensajes de datos.

En el tercer capítulo, se desarrollarán las normas jurídicas y aspectos que se han implementado en relación con el gobierno electrónico y en específico con la implementación de trámites en línea en los países de Alianza del Pacífico para con ello, considerar elementos que pudieran ser aplicables también a México.

Por último, en el cuarto capítulo, se propondrá una guía con los pasos que debe seguir la APF para implementar trámites en línea, considerando como elementos clave para la implementación de estos trámites los siguientes:

- Marco jurídico que permita la implementación de estos trámites.
- Elementos que permitan mantener la seguridad y certeza jurídica, como pueden ser la firma electrónica y, en su caso, la incorporación de otros servicios de confianza como el sello digital de tiempo y la constancia de conservación de mensajes de datos.
- Elementos y aspectos que es importante considerar en el diseño de estos trámites.

Capítulo 1.
Aspectos generales del gobierno electrónico y los derechos humanos vinculados



Capítulo 1. Aspectos generales del gobierno electrónico y los derechos humanos vinculados

1.1 Antecedentes del gobierno electrónico

Las TIC son una herramienta fundamental para el gobierno, que en primer término permitieron eficientar los procesos al interior de las organizaciones, y posteriormente un acercamiento directo con el ciudadano. Es así como el concepto de gobierno electrónico ha ido evolucionando desde la década de los noventa como una herramienta de la administración pública para desarrollar y mejorar los servicios a los ciudadanos.¹

Por ello, el concepto de gobierno electrónico ha sido abordado por diversos autores y organismos, al respecto, en todas las definiciones se contempla el uso de las tecnologías de la información y de las comunicaciones, pero incorporando distintas finalidades, que van, desde lograr un mejor gobierno, hasta impactar en los servicios que se prestan a los ciudadanos con mayor transparencia, y finalmente algunas se centran en la generación de información accesible a éstos y su cambio a un rol con participación activa. En este sentido, exploraremos algunas de éstas.

El gobierno electrónico se puede entender como “... el uso de tecnologías de la información y de las comunicaciones, especialmente Internet, como herramienta para lograr un mejor gobierno”.²

Por su parte, la Organización de los Estados Americanos (OEA) señala que “El gobierno electrónico es la aplicación de las tecnologías de la información y la comunicación (TIC) al funcionamiento del sector público, con el objetivo de brindar mejores servicios al ciudadano e incrementar la eficiencia, la transparencia y la participación ciudadana”.³

¹ Madariaga Cardona, Diego Fernando, “El gobierno electrónico. Una herramienta estratégica de toma de decisiones”, *Revista Universidad y Empresa*, Colombia, 2004, vol. 3, núm 3-4-5, p.20.

² OECD e-Government Studies, “The e-Government Imperative”, Francia, 2003, p.11.

³ Organización de los Estados Unidos Americanos, “Mandatos y resoluciones del gobierno digital en las Américas”. (página oficial).

La definición propuesta por la OEA incorpora como elemento fundamental los servicios que se le prestan al ciudadano. Al respecto, las TIC se utilizan como herramienta para mejorar dichos servicios, como es el caso de la implementación de trámites en línea; asimismo, menciona como otro de los objetivos la participación ciudadana.

No obstante, es importante considerar que de conformidad con la Organización de las Naciones Unidas: “El gobierno electrónico no se trata únicamente de la prestación de servicios; también juega un papel en el fortalecimiento de la alfabetización digital (Objetivo 4), la inclusión digital (Objetivos 5, 8 y 10), la conectividad digital (Objetivo 9) e identidad digital”.⁴

En concordancia con lo anterior, la Carta Iberoamericana de Gobierno Electrónico (2007) considera que además de lo anterior el gobierno electrónico debe servir para “orientar la eficacia y eficiencia de la gestión pública”⁵ con ello se incorpora la importancia también al interior del gobierno para generar políticas públicas, orientadas al ciudadano.

De esta manera, con los conceptos antes referidos se puede apreciar que el gobierno electrónico, más allá de la utilización de las TIC para mejorar su gestión interna y externa con los ciudadanos para lograr un mejor gobierno, debe abonar también a otros objetivos, sin los cuales las personas no pueden ser parte de éste –como la inclusión digital–, ya que el gobierno debe buscar implementar trámites y servicios sin excluir a ningún sector de la población.

Asimismo, existen algunos autores que centran el valor del gobierno electrónico en la información, así como en la oportunidad de participación que adquieren los ciudadanos. De ahí que, se menciona que el término gobierno electrónico debería ser reemplazado por “gobierno de la información”, porque ya no se centra sólo en el uso de las TIC como herramientas para la mejora de los servicios; el gobierno de la información se encuentra ligado a los sistemas redes de

⁴ Naciones Unidas, “Encuesta sobre E-Gobierno 2020 Gobierno digital en la década de acción para el desarrollo sostenible”, 2020, New York, p.24

⁵ CLAD, “Carta Iberoamericana de Gobierno Electrónico”, Chile, 2007, p.239

información y centra su importancia en los derechos del individuo, en su participación democrática y en la facilidad de acceso de los ciudadanos a la información.⁶

Esta definición busca tener un alcance mayor al uso de las TIC como herramienta ya que se centra en el valor de la información que se genera, debido a que uno de los objetivos estratégicos del gobierno electrónico está enfocado en “... promover la construcción de una sociedad de información y conocimiento inclusiva, centrada en la persona y orientada al desarrollo”.⁷

Igualmente, se pueden encontrar distintos elementos en un gobierno electrónico, entre los cuales se encuentran: la innovación al interior y exterior del gobierno; el impacto en su función incluyendo el acceso a la información; la presentación de servicios, así como, la realización de trámites y participación ciudadana⁸, todo ello abonando a otros objetivos como la disminución de la brecha digital⁹ y la inclusión digital, con lo cual se pueden aportar mayores elementos para construir valor público.¹⁰

Por consiguiente, el gobierno electrónico comprende más que trámites en línea, permite a la ciudadanía participar en la toma de decisiones y en la construcción de políticas públicas, lo cual también conlleva una responsabilidad para ésta. Por otra parte, garantiza la posibilidad de obtener y explotar información valiosa tanto para el sector privado como para el público en la gestión de sus propios procesos, implementación de políticas públicas y su evaluación.

⁶ Reyes Olmedo Patricia, “La sociedad red y el gobierno de la información”, *Universidad de Valparaíso*, Chile, 2013, p.9.

⁷ CLAD, *op cit.*, p.235.

⁸ Madariaga Cardona, Diego Fernando, *op cit.*, p.26.

⁹ *Ibidem*, p.23.

¹⁰ Prestol Flaquer, Joaquín, “Los Laboratorios de Innovación: como mecanismo para crear Valor Público”, *Revista Centroamericana de Administración Pública*, México, 2020, núm.78, enero-junio 2020, p.173.

1.1.1 Etapas

Si bien no hay un consenso sobre las etapas del gobierno electrónico, se pueden señalar cuatro principalmente, las cuales son:

1) Presencia: en la primera etapa solo se pone información disponible al ciudadano, no implica cambios en los procesos internos; ¹¹

2) Interacción: el ciudadano, puede acceder a información y bajar formatos, asimismo, se puede interactuar con las dependencias de gobierno por medio de correo electrónico;¹²

3) Transacción: se pueden realizar trámites completamente en línea, ello implica una capacidad de respuesta en tiempo real de las dependencias de gobierno; en esta fase, aun no se generan cambios en sus estructuras internas, porque solo se modifica el medio para hacer el trámite, se automatiza y se evita la necesidad de acudir a una ventanilla física, por lo cual, hasta este momento no se crean sinergias entre las instituciones; y¹³

4) Transformación: implica una redefinición de los servicios y de la forma de operar de la administración pública, se crea una integración entre las dependencias de gobierno, el sector privado, las organizaciones no gubernamentales y el ciudadano. En esta fase, es fundamental que las dependencias puedan compartir datos con los que se podrán prestar servicios, es decir, construir el marco jurídico adecuado para ello, lo que permitirá romper barreras entre las dependencias, por lo cual, es la etapa que requiere de una colaboración y reestructura importante.¹⁴ En este contexto, se presenta la fase en que se vuelve fundamental la “interoperabilidad”.¹⁵

¹¹ Madariaga Cardona, Diego Fernando, *op cit.*, p. 28.

¹² *Idem.*

¹³ *Ibidem*, p. 29.

¹⁴ *Idem.*

¹⁵ La interoperabilidad es la capacidad de organizaciones y sistemas, dispares y diversos, para interactuar con objetivos consensuados y comunes, con la finalidad de obtener beneficios mutuos, en donde la interacción implica que las dependencias y entidades compartan infraestructura,

De manera que, se puede considerar que estas etapas están centradas en la implementación de los trámites y servicios a los ciudadanos y han ido evolucionando desde la posibilidad de consultar información, hasta realizar trámites completamente transaccionales donde las dependencias se comunican, relacionan y visualizan como un solo ente al servicio del ciudadano, sin embargo, como se ha observado, el gobierno electrónico también comprende la participación ciudadana.

Es por ello, que aunado a lo anterior se pueden encontrar dos nuevas etapas denominadas Participación y Colaboración, asociadas a la información que se genera, en las cuales se "... recoge la idea de interrelación entre los organismos públicos y entre éstos y la ciudadanía de manera de integrar a la acción gubernamental los requerimientos de participación y colaboración de los receptores de los servicios públicos".¹⁶

Es decir, en las etapas anteriores se integra la idea de participación del ciudadano como un constructor de políticas públicas. El ciudadano ya no solo es el centro del proceso, sino parte de éste, por ello, los servicios son generados de acuerdo con sus expectativas y necesidades y su participación y rol se vuelve activo en la construcción del gobierno.

información y conocimiento mediante el intercambio de datos entre sus respectivos sistemas de tecnología de información y comunicaciones.

Asimismo, señala tres tipos de interoperabilidad:

Interoperabilidad organizacional: a los mecanismos que establecen la forma de colaboración entre las dependencias y entidades para asegurar la coordinación y alineación de los procedimientos administrativos que intervienen en la provisión de los servicios de gobierno digital.

Interoperabilidad semántica: a la capacidad que garantiza el significado preciso de la información para que pueda ser utilizada por cualquier sistema o aplicación.

Interoperabilidad técnica: a las especificaciones técnicas que garantizan que los componentes tecnológicos de los sistemas de información están preparados para interactuar de manera conjunta. ACUERDO por el que se establece el Esquema de Interoperabilidad y de Datos Abiertos de la APF (2011).

¹⁶ Reyes Olmedo Patricia, *op cit.*, p.10

1.1.2 Interrelación entre los diversos actores

El gobierno electrónico presenta relaciones externas e internas para lograr los fines planteados en los conceptos antes señalados, hacia el interior, entre las propias dependencias de gobierno y al exterior hacia el ciudadano y las empresas, a lo que cual se ha denominado, G2G, G2B y G2C, las cuales consisten en lo siguiente:

1) G2C: relaciones entre las dependencias gubernamentales y el ciudadano, con la prestación de servicios y en el acceso a la información; 2) G2B: relaciones entre las dependencias gubernamentales y las empresas con la proveeduría de bienes y servicios y acceso a la información; y 3) G2G: relaciones al interior del gobierno entre dependencias gubernamentales.¹⁷

En la primera (G2C), se encuentra la prestación de servicios eficientes en línea y el acceso a la información que deben tener los ciudadanos. Al respecto, éstos pueden relacionarse electrónicamente con las dependencias para distintos efectos, como son: i) dirigir por vía electrónica escritos, recursos, reclamaciones y quejas; ii) realizar por medios electrónicos pagos; iii) recibir por medios electrónicos notificaciones; iv) acceder por medios electrónicos a la información pública; y v) evitar la presentación de información que ya obra en poder del gobierno, aunque no se trate de la misma dependencia, lo que supone interoperabilidad.¹⁸

Asimismo, se menciona que se debe contar con personal preparado para acceder electrónicamente desde las oficinas públicas, y con la posibilidad de que los ciudadanos puedan acreditar su identidad ante funcionarios públicos habilitados para ello;¹⁹ ello derivado de que como se ha mencionado previamente no puede excluirse a aquellas personas que no estén familiarizadas con las tecnologías la información y comunicaciones.

¹⁷ Madariaga Cardona, Diego Fernando, *op cit.*, p.27.

¹⁸ CLAD, *op cit.*, p. 242.

¹⁹ *Idem.*

Lo anterior, supone un gran reto para las Dependencias, debido a que se enfrentan a diversas barreras, entre las cuales se encuentran, las presupuestales que se mencionarán más adelante, las cuales, les impiden contar con equipo y personal para mantener un servicio con las características antes señaladas, ya que no solo se trata de hacer más eficientes los trámites con todos los elementos jurídicos y tecnológicos que se requieren, sino, además, hacerlo contemplando objetivos como la inclusión digital con los esquemas necesarios para no excluir a ningún sector de la población.

Por su parte, las relaciones con las empresas (G2B), son esenciales para incrementar la competitividad de un país, por ende, estas relaciones también se pueden ver reflejadas en la oferta de servicios en línea que se establecen, desde la apertura de las empresas hasta su continuidad en el tiempo.²⁰ El gobierno desde esta perspectiva debe facilitar y no obstaculizar la vida de las empresas con trámites complejos.

Para efecto de ofrecer mejores servicios a los ciudadanos, en algunos casos, se pueden considerar las Alianzas Público-Privadas, las cuales tienen entre sus ventajas: i) mayor velocidad para la construcción de infraestructura; ii) reducción de costos y tiempos para el diseño y desarrollo de proyectos; iii) distribución eficiente de los riegos; iv) mejor aprovechamiento de los activos públicos a partir de la gestión privada; y v) mejor calidad en la gerencia pública.²¹

Por último, las relaciones G2G son fundamentales para lograr que las dependencias de gobierno compartan información y trabajen coordinadamente, entendiendo un mismo fin y objetivo, esto puede considerarse como uno de los

²⁰ Como ejemplo, en México se encuentra el Registro Público de Comercio que actualmente “funciona en una base de datos nacional, actualizada, en línea y en tiempo real la cual está disponible para el público en general, para las dependencias y entidades del gobierno a través de medios electrónicos”. Puede consultarse en:

<https://rpc.economia.gob.mx/siger2/xhtml/login/login.xhtml>

²¹ Prestol Flaquer, Joaquín, *op cit*, p.176

mayores retos del gobierno, ya que las dependencias actualmente están diseñadas como entes separados con objetivos y facultades específicas.

Por lo anterior, lograr esta unificación, colaboración y coordinación representa retos, jurídicos, presupuestales, tecnológicos y hasta políticos, se requiere una nueva construcción y percepción de gobierno al interior de las propias Dependencias. Además, considerar el marco jurídico necesario para ello, contar con el presupuesto específico y vencer las barreras tecnológicas actuales.

En particular respecto a estas barreras vale la pena considerar que, si las Dependencias trabajan de forma descoordinada, la creación e implementación de sus trámites en línea se realizará a través de diferentes herramientas y sistemas que después no serán compatibles, por lo cual, se complicará la posibilidad de interoperar y ofrecer una sola cara al ciudadano.

Aunado a lo anterior, se pueden encontrar distintos principios que se deben aplicar en la construcción del gobierno electrónico. De acuerdo con la Carta Iberoamericana de Gobierno Electrónico, entre estos principios se encuentran los siguientes²²:

- Principio de igualdad: que en ningún caso esto implique restricciones o limitaciones para los ciudadanos.
- Principio de legalidad: que las garantías previstas en medios tradicionales se respeten en medios electrónicos, y se incluye el derecho a la privacidad.
- Principio de conservación: se debe garantizar que los documentos electrónicos se conserven en las mismas condiciones que por los medios tradicionales.
- Principio de transparencia y accesibilidad: que la información esté en un lenguaje comprensible de acuerdo con el perfil del destinatario.
- Principio de proporcionalidad: de modo que los requerimientos de seguridad sean adecuados a la naturaleza de la relación que se establezca con la Administración.

²² CLAD, *op cit.*, pp. 239, 240, 241.

- Principio de responsabilidad: se refiere a que la administración y el gobierno respondan por sus actos realizados por medios electrónicos de la misma manera que de los realizados por medios tradicionales.
- Principio de adecuación tecnológica: se recomienda el uso de estándares abiertos para que el conocimiento público no sea privatizado.

Además, también señala como un punto fundamental que se deben contemplar cuestiones como la autenticidad e integridad del documento y una regulación sobre la seguridad que debe permitir identificar al emisor y garantizar una comunicación segura con los mismos, como pueden ser sistemas de firma electrónica.²³

Por ello, en la implementación de trámites en línea es fundamental contemplar diversos aspectos como es la equivalencia funcional, la integridad del documento, considerar los medios de autenticación y las medidas de seguridad; por ende, el diseño de los trámites debe ser basado en las necesidades y la experiencia de los ciudadanos, buscar la transparencia de la información pero al mismo tiempo proteger la privacidad y el respeto del derecho de protección datos personales, como se señalará más adelante.

Al respecto, para lograr lo anterior, se requiere contar con un marco jurídico robusto, el cual mencionaremos en el capítulo siguiente.

1.1.3 Barreras

Existen diversas barreras que dificultan la implementación de un gobierno electrónico, las cuales obstaculizan los flujos de información, coordinación, recursos o condiciones técnicas para que los proyectos se puedan implementar de forma exitosa²⁴ entre las cuales, se pueden señalar, las normativas, financieras,

²³ *Ibidem*, pp.244,245.

²⁴ Red de Gobierno Electrónico de América Latina y el Caribe, “De la teoría a la práctica: Cómo implementar con éxito el gobierno electrónico. La experiencia regional y las barreras de la e-innovación”, 2008 p.18.

tecnológicas que incluyen la brecha digital, así como la resistencia al cambio y la renovación de procesos de acuerdo con lo siguiente:

Normativas. – se requiere implementar marcos jurídicos que den un valor equivalente al proceso que se lleva a cabo electrónicamente con el que se realiza en papel, además, en muchos casos los marcos actuales hacen del gobierno una administración rígida y dificultan su colaboración con otras, no tienen flexibilidad y están diseñados para que las Dependencias trabajen como entes separados.²⁵

Financieras. – el costo que implica la implementación de servicios en línea y de los marcos jurídicos para ello.²⁶

Tecnológicas (brecha digital). - diferencias de acceso a las TIC y a Internet, en los que en general los más desfavorecidos son los que tienen los niveles más bajos de acceso, por lo que representa un obstáculo para que accedan a los servicios en línea que ofrece el gobierno²⁷ y por ende para asumir el rol activo que se ha mencionado anteriormente.

Resistencia al cambio. - se pueden encontrar barreras de resistencia al cambio de parte de los propios servidores públicos que dificultan la cooperación para lograr llevar a cabo servicios eficientes e integrados que generen valor al ciudadano y no desde la perspectiva y función de una sola dependencia.²⁸

Además, pueden presentarse dificultades para una adecuada coordinación entre los niveles nacional, regional y local y una falta de apoyo político.²⁹

Renovación de procesos. - se requieren cambios organizacionales donde se modifique el sistema jerárquico de organización, por ejemplo, en la implementación de soluciones globales, los mecanismos tradicionales de compras públicas y contratación de servicios resultan insuficientes.³⁰

²⁵ OECD, *op cit.*, p. 48

²⁶ *Ibidem*, p. 21

²⁷ *Ibidem* p.64

²⁸ Rivera Urrutia, Eugenio, “Concepto y problemas de la construcción del gobierno electrónico. Una revisión de la literatura”, *Gestión y política pública*, México, 2006, vol. 15, núm. 2, pp.268-269.

²⁹ Red de Gobierno Electrónico de América Latina y el Caribe, 2008, *op cit.*, p.19.

³⁰ Rivera Urrutia, Eugenio, *op cit.*, p. 275.

En definitiva, las Dependencias se enfrentan a diversos retos en la implementación de trámites en línea; desde las propias condiciones de acceso a internet y la capacidad de utilizar herramientas tecnológicas de su población, hasta la necesidad de contemplar adecuadamente un marco jurídico para ello. Además de la necesidad considerar el presupuesto requerido y, por último, la propia resistencia al cambio que puede encontrarse en algunos servidores públicos y también en los propios ciudadanos que no confían en los medios electrónicos para llevar a cabo sus trámites.

1.2 Derechos humanos vinculados y el derecho a la buena administración

Del mismo modo, en la construcción del gobierno electrónico y la implementación de los trámites en línea es fundamental el respeto de los derechos humanos. Específicamente, se pueden mencionar algunos que se encuentran estrechamente ligados a ello; desde el propio derecho de acceso a la información y la protección de datos personales, hasta derechos que comprenden los derechos en la red entre los que se incluyen los derechos informáticos³¹ y la inclusión digital, así como, el denominado derecho a la buena administración.

En primer término, al implementar trámites en línea, se transparentan los procesos y la forma en que almacena y se procesa la información es mucho más accesible. En consecuencia, se facilita el acceso a la misma para los ciudadanos, lo cual es fundamental para promover la transparencia e incrementar los mecanismos de participación que mejoren la calidad de vida del ciudadano³² al contar con información oportuna los ciudadanos pueden tomar decisiones y

³¹ López López, Pedro y Samek, Toni, "Inclusión digital: un nuevo derecho humano", *Educación y biblioteca*, Madrid, 2009, núm. 172, p. 6

³² Pérez Romero, Jorge Enrique, "El gobierno digital y los derechos humanos. La normativa costarricense", *Revista de la Facultad de Derecho de México*, México, 2019, vol. 69, núm. 274-2, p. 637

participar en la construcción de políticas públicas, con lo cual, sin duda, su rol se vuelve mucho más activo.

Es importante señalar que lo anterior no implica solo automatizar procesos, es una nueva visión de la administración pública, de la implementación de políticas públicas y de la forma en que se deben relacionar el gobierno con los ciudadanos, así como del propio rol de cada uno, además, lo anterior "...debe contribuir a la transición hacia una Sociedad de la Información, de tal forma que los ciudadanos puedan acceder a la misma y a oportunidades sociales políticas y económicas".³³

Lo antes señalado está plenamente vinculado con lo que se ha denominado "gobierno abierto", el cual responde ya no solo a una necesidad, sino a una exigencia de los ciudadanos que usan las TIC para hacer valer derechos como el de acceso a la información, con lo cual, mejoran o incrementan y transforman su participación política y ciudadana.³⁴

De esta manera, estos derechos están plenamente representados en las etapas Participación y Colaboración que se mencionaron previamente, donde el ciudadano se asume de una forma distinta en el proceso de construcción de gobierno y los derechos tanto de acceso a la información como de privacidad toman un papel fundamental.

Por lo anterior, el artículo 6º de la Constitución Política de los Estados Unidos Mexicanos señala lo siguiente:

"...el derecho a la información será garantizado por el Estado.

[...]

... el Estado garantizará el derecho de acceso a las tecnologías de la información y comunicación, así como a los servicios de radiodifusión y telecomunicaciones, incluido el de banda ancha e internet".³⁵

³³ Ávila Barrios, Delia, "El uso de las TICs en el entorno de la nueva gestión pública mexicana", *Andamios*, México, 2014, vol. 11, núm. 24, p.21

³⁴ Arellano Toledo, Wilma, *et al.*, "Derechos de los ciudadanos en el gobierno abierto: doctrina, legislación y políticas en México", Madrid, 2015, p.110

³⁵ Constitución Política de los Estados Unidos Mexicanos, Artículo 6º, p.12

Es así como este acceso se vuelve un tema trascendental y fundamental para la implementación de este tipo de trámites, ya que la utilización de las tecnologías puede producir una brecha social entre aquellos que tienen acceso y aquellos que no lo tienen.³⁶

De ahí que, el uso de las TIC debe servir para luchar contra la exclusión social y no todo lo contrario, por ello, en la implementación de políticas públicas es fundamental no solo garantizar el acceso, sino desarrollar aquellas que permitan la adopción de las tecnologías por los ciudadanos y fortalezcan sus competencias.³⁷ La implementación de estos trámites en línea debe buscar un mayor acercamiento a los ciudadanos y no por el contrario acrecentar la brecha.

Lo anterior, se encuentra plenamente vinculado con la inclusión digital entendida de la forma siguiente:

“...es un nuevo derecho humano procedente del nuevo entorno tecnológico que ha creado la red. En el esquema propuesto por la profesora Gómez Sánchez tendría cabida en el punto 1 (derecho de acceso a la información de relevancia para la Humanidad y derecho de acceso a los medios técnicos de comunicación públicos y privados), así como en el punto 2 (derechos informáticos). Los avances en información y comunicación deben ser disfrutados por todos los seres humanos, y cabe considerar que en la actualidad exclusión digital equivale a exclusión social”.³⁸

Actualmente, vivir fuera del nuevo entorno creado por las tecnologías de la información, puede implicar de algún modo vivir fuera del mundo, no obstante, el papel del gobierno, no está en acrecentar las brechas sociales, sino todo lo contrario; en consecuencia, debe buscar las condiciones para incluir a todos los sectores, considerando cuestiones que van desde disminuir la brecha digital, hasta

³⁶ Rodríguez Gallardo, Adolfo, “La brecha digital y sus determinantes”, México, 2006, *UNAM, Centro Universitario de Investigaciones Biotecnológicas*, 2006, p. 2

³⁷ Zambrano Acosta, Juan, *et al.*, “Las políticas públicas en TIC. Una oportunidad de cerrar la brecha social”, *Revista Educación, Comunicación, Tecnología*, Colombia, volumen 4, núm.7, 2009, p.14

³⁸ López López, Pedro y Samek, Toni, *op cit.*, p.6.

incluir opciones para aquellos sectores que no utilicen tecnologías de la información, por ello, no puede establecer un solo camino para lograr la prestación de un servicio público o la realización de un trámite.

Por otra parte, en la implementación de trámites en línea, es esencial garantizar el derecho a la protección de los datos personales de los ciudadanos. Al respecto el artículo 6º de la Constitución Política de los Estados Unidos Mexicanos señala lo siguiente:

“...**A.** Para el ejercicio del derecho de acceso a la información, la Federación y las entidades federativas en el ámbito de sus respectivas competencias, se regirán por los siguientes principios y bases:

[...]

...II. La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes”

III. Toda persona, sin necesidad de acreditar interés alguno o justificar su utilización, tendrá acceso gratuito a la información pública, a sus datos personales o a la rectificación de éstos.³⁹

Por su parte, el artículo 16º de la Constitución Política de los Estados Unidos Mexicanos hace referencia a los denominados Derechos ARCO (acceso, rectificación, cancelación u oposición al tratamiento de datos personales) de acuerdo con lo siguiente:

“Artículo 16.

[...]

Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.

[...]”

³⁹ Constitución Política de los Estados Unidos Mexicanos, Artículo 6º, pp.12-13

En este sentido, el derecho de protección de datos personales puede entenderse como:

“El derecho humano que protege a la persona física identificada o identificable frente al tratamiento ilícito de sus datos personales, otorgándole, en la medida de lo posible dado el actual estado de la técnica, la facultad de decidir y controlar de manera libre e informada las condiciones y características del tratamiento de sus datos personales, permitiéndole, además, el ejercicio de determinados derechos y medios de tutela jurídicos para garantía y eficacia práctica de estos últimos”.⁴¹

El derecho de protección de datos personales comprende la garantía de la decisión y control que las personas deben tener sobre su información y el uso de la misma.⁴² Por tanto, lo anterior comprende la protección de los Derechos ARCO y como puede observarse el derecho a la protección de datos personales está ligado con otros como la intimidad, privacidad y autodeterminación informativa.

Es así que los gobiernos deben buscar un equilibrio entre la protección de los derechos del ciudadano y la prestación de servicios eficaces y eficientes.⁴³ Es decir, no es posible que se implementen trámites más eficientes o se busque la obtención de datos para implementar políticas públicas adecuadas y de valor real para los ciudadanos, pero invadiendo la privacidad de las personas.

Por esta razón, el gobierno tiene un gran reto para lograr este equilibrio y por ello, los principios de protección de datos personales toman un papel relevante

⁴⁰ *Ibidem*, p. 17

⁴¹ Davara, Isabel (coord.), *Diccionario de Protección de Datos Personales, Conceptos Fundamentales*, INAI, México, 2019, p. 687.

⁴² Sánchez Gómez, Mario Anselmo Gómez, “La protección de datos personales en México: cambios evolutivos a 10 años de su inclusión a nivel constitucional”, *Revista Mexicana de Ciencias Penales*, 2020, vol. 3, núm 10, p. 49

⁴³ OECD, *op cit.*, p.17.

como es el caso del de la proporcionalidad que permite sólo solicitar la información acorde con la finalidad para la que se requiere.

Además, no resulta conveniente que aludiendo a beneficios en la optimización de los servicios se afecten los derechos de los ciudadanos o no se lleven a cabo los procesos de acuerdo con el marco jurídico correspondiente.⁴⁴

Durante esta época de pandemia, se pudo observar este gran reto y disyuntiva, por ejemplo, a través de las apps por medio de las cuales se debía permitir la ubicación y en caso de que hubiera un resultado positivo, la plataforma accedería a la ubicación del lugar, hora y fecha en la que fue realizado el diagnóstico de posible COVID,-19 con la finalidad de dar seguimiento a las personas que tuvieran un nivel alto de sospecha de haber contraído el virus COVID-19.⁴⁵

Por consiguiente, podría considerarse que estas aplicaciones por un lado buscaban garantizar la salud de las personas y por otro podrían estar invadiendo su privacidad. No obstante, es importante señalar que no siempre se debe visualizar lo anterior como un conflicto entre la preservación de la salud o de la privacidad, ya que el gobierno puede implementar soluciones que permitan un adecuado tratamiento de la salud, pero minimizando el impacto en la privacidad y otros derechos.⁴⁶

Ahora bien, entre las teorías que podemos encontrar, se encuentra la relativa al derecho a la buena administración pública; este derecho implica que se planteen y desarrollen las políticas públicas de acuerdo con la perspectiva del ciudadano.

Es decir, la administración pública debe tener como objetivo el interés general, por tanto, no representa un fin en sí misma, sino un servicio a los ciudadanos, e implica también una mayor participación de éstos. De esta manera, el ciudadano ocupa un papel central y el rol de la Administración Pública es

⁴⁴ Rivera Urrutia, Eugenio, *op cit*, p.26.

⁴⁵ Gobierno de la Ciudad de México, “Términos Y Condiciones De Uso De La “App Covid-19 Cdmx”, México, en: <https://app.covid19.cdmx.gob.mx/terms>.

⁴⁶ Hueso Lorenzo, Cotino, “Inteligencia artificial, big data y aplicaciones contra la COVID-19: privacidad y protección de datos”, *IDP: revista de Internet, derecho y política= revista d'Internet, dret i política*, 2020, núm. 31, p. 3.

permitirlo y facilitarlo.⁴⁷ Es así como el gobierno tiene un papel fundamental en la protección y la búsqueda del bienestar de las personas, garantizado un marco adecuado en una sociedad en común.⁴⁸

El gobierno desde esta perspectiva crea servicios y trámites de acuerdo con las necesidades de los ciudadanos, por lo que, se construyen políticas públicas en conjunto. De ahí que, los roles se modifican, en el caso de los trámites en línea son diseñados para facilitarle el proceso al ciudadano y por ello se busca su perspectiva y validación y no se diseñan desde la facilidad al interior del gobierno y de los servidores públicos.

Así pues, el uso de las TIC en el gobierno electrónico nació como una respuesta casi automática y natural a la propia evolución de la sociedad; en primer término, mejorando su gestión interna y con un enfoque hacia la propia organización, y la eficiencia y mejora de procesos en las propias Dependencias de gobierno; posteriormente, se visualizó el impacto en los servicios que se prestan a los ciudadanos y a las empresas, y se iniciaron diversos esfuerzos tanto de análisis y estudio, como implementaciones en proyectos específicos con esta visión, poniendo al ciudadano en el centro.

En la actualidad, se visualiza como un eje fundamental, el respeto a diversos derechos humanos como lo son: el de acceso a la información, el derecho de protección de datos personales, el de la buena administración, por mencionar algunos, así como la necesidad y trascendencia para el propio gobierno para crear mejores políticas públicas orientadas a crear valor público⁴⁹ donde el ciudadano se convierte en un actor fundamental.

⁴⁷ Muñoz, Jaime Rodríguez-Arana, “El derecho fundamental a la buena administración y la centralidad del ciudadano en el Derecho Administrativo” *El nuevo derecho administrativo*, 2011, pp.4-5.

⁴⁸ Rivera Urrutia, Eugenio, *op cit.*, p. 266.

⁴⁹ “La relación con el desarrollo social, la gobernanza, la garantía de derechos, la satisfacción de necesidades, la prestación de servicios de calidad y el mejoramiento de las condiciones de vida de la sociedad. No sólo es hacer uso de las tecnologías, sino cómo las tecnologías ayudan a resolver problemas reales”. Decreto 088 de 24 de enero de 2022, Colombia, p. 9

Sin duda, conforma una nueva era, donde las dependencias del gobierno requieren reestructurar y asumir las funciones de una forma distinta, coordinada y asumiéndose como un solo ente al servicio del ciudadano, y donde las TIC son utilizadas como una herramienta para lograr lo anterior, desde la perspectiva y necesidades de la ciudadanía.

El gobierno plantea muchos retos que van más allá de la tecnología, pero sin duda, el uso de ésta debe facilitar el proceso, las barreras mencionadas no son sencillas, y como se señaló van desde lo normativo, hasta la propia resistencia al cambio. De manera que, hay muchos temas por revisar y atender, las TIC evolucionan y cambian todos los días, y el gobierno tiene muchos retos que vencer, para continuar también evolucionando y para aportar valor público, donde se encuentren involucrados, ciudadanos, empresas y gobierno.

En conclusión, la implementación de trámites en línea es parte fundamental en la construcción del gobierno electrónico y para ello se requiere contar con todos los elementos necesarios durante su proceso de implementación que permitan mantener la certeza jurídica y abonar a lograr un mejor gobierno.

Capítulo 2.

Marco jurídico de los trámites en línea en la APF



Capítulo 2. Marco jurídico de los trámites en línea en la APF

2.1 Marco jurídico internacional

Como se observó en el capítulo anterior, la implementación de trámites en línea es una parte fundamental en la construcción del gobierno electrónico. En este sentido, en este capítulo se analizarán algunos instrumentos internacionales que han detallado y configurado lineamientos y estándares para el desarrollo en los trámites en línea. Asimismo, se abordará el marco jurídico nacional respectivo y por último, se desarrollarán elementos fundamentales para estos procesos de implementación como son la firma electrónica y los servicios de confianza.

Entre los instrumentos internacionales referentes al desarrollo de transacciones electrónicas, se encuentran diversas leyes modelos emitidas por la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) como son: la Ley Modelo de la CNUDMI sobre Comercio Electrónico; la Ley Modelo de la CNUDMI sobre Firmas Electrónicas y recientemente se puede considerar el Reglamento (UE) N° 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga a Directiva 1999/93/CE.

Al respecto, cabe destacar que las leyes emitidas por la CNUDMI tienen como objetivo armonizar las normas de derecho mercantil internacional, si bien, se trata de normas de carácter de *soft law*, es decir no vinculantes, ofrecen a los países la posibilidad de adaptar principios y mejores prácticas en su legislación nacional ya sea de manera total o parcial.⁵⁰

⁵⁰ Rojas Amadi, Víctor Manuel, "La Ley Modelo de Comercio Electrónico de la Comisión de Naciones Unidas de Derecho Mercantil Internacional y su transformación en el Sistema Jurídico Mexicano", en Sánchez Cordero Jorge (comp.), Centenario de la Constitución de 1917, Reflexiones de Derecho Internacional Privado, México, UNAM, Instituto de Investigaciones Jurídicas, 2017, pp.181 y 182

2.1.1 Ley Modelo de la CNUDMI sobre Comercio Electrónico

Es así como en primer término abordaremos la Ley Modelo de la CNUDMI sobre Comercio Electrónico. Los trabajos de esta Ley Modelo se iniciaron a partir de que, en el 18º período de sesiones de la CNUDMI en 1985, se concluyó que las transacciones comerciales no podían depender de un requisito escrito para que fueran válidas, por lo que en 1988, se consideró la posibilidad de proponer principios para poder llevar a cabo contratos mercantiles a través de medios electrónicos, trabajo que concluyó en 1996 cuando el Grupo de Trabajo aprobó la Ley Modelo.⁵¹

De esta manera, el origen de la Ley Modelo atendió a la necesidad de establecer reglas que dieran certeza y validez a las transacciones llevadas a cabo a través de medios electrónicos, estableciendo un marco legal y prácticas eficientes, además de contemplar un régimen que no obstaculizara el comercio internacional.⁵² Por lo que hace a su estructura, se encuentra dividida en dos partes, la primera dedicada al comercio electrónico en general y la segunda al comercio electrónico en materias específicas, aunque referente a ello, solo se desarrolló el Capítulo I relativo al transporte de mercancías.

Por otra parte, si bien, como se ha comentado el trabajo de la CNUDMI se centra en la armonización de reglas para el derecho mercantil internacional, el ámbito de aplicación de esta ley puede hacerse extensivo a otro tipo de relaciones que no son de carácter comercial como lo son las de los ciudadanos con autoridades debido a los principios que establece.⁵³ Es decir, esta Ley Modelo resulta de aplicación transversal y puede ser aplicada en todos los sectores, aunque su origen sea mercantil.⁵⁴

⁵¹ *Idem*

⁵² CNUDMI, *Guía para la incorporación al derecho interno de la Ley Modelo de la CNUDMI sobre Comercio Electrónico*, Nueva York, Naciones Unidas, 2018, pp. 16-17

⁵³ Rojas Amadi, Victor Manuel, *op cit.*, p.186

⁵⁴ Rincón Cárdenas, Erick y Vergara, Camilo, *Administración pública electrónica: hacia el procedimiento administrativo electrónico*, Colombia, Universidad del Rosario, 2017, p.41

Por ello, resulta primordial mencionar los principales principios que se desarrollan en esta Ley Modelo, que impactarían en la implementación de trámites en línea, los cuales son los siguientes:

Principio de equivalencia funcional: un acto jurídico a través de medios electrónicos tendrá los mismos efectos que aquellos realizados en papel, siempre y cuando cumpla con lo dispuesto en la norma correspondiente,⁵⁵ asimismo, este principio podría estar relacionado con que un mensaje de datos no debe ser objeto de discriminación, es decir, que no debe tener un trato distinto a los documentos en papel.⁵⁶ Al respecto, es importante señalar que la documentación consignada por medios electrónicos en muchas ocasiones puede ofrecer mayor fiabilidad y rapidez que la que se encuentra en papel.⁵⁷

Efectos jurídicos de los mensajes de datos: señala que no se pueden negar efectos jurídicos a la información solo por estar contenida en un mensaje de datos.

Requisito de ley de constar por escrito: se establece que este requisito queda satisfecho si la información es accesible para su ulterior consulta, cabe destacar que de acuerdo con lo desarrollado en la Guía para la incorporación al derecho interno de la Ley Modelo de la CNUDMI sobre Comercio Electrónico, se tuvo especial cuidado de que no se interpretara que cuando se requiere que un documento se presente por escrito necesariamente requiera una firma, por tanto, cuando refiere accesible “se quiere sugerir que la información en forma de datos informatizados debe ser legible e interpretable y que debe conservarse todo programa informático que sea necesario para hacer legible esa información”.⁵⁸

Requisito de originalidad: refiere que en el caso de los mensajes de datos este requisito queda satisfecho si existe garantía de que se ha conservado la integridad de la información a partir del momento en que se generó por primera vez en su forma definitiva como mensaje de datos⁵⁹, y que dicha integridad se considera cuando la información permanece completa e inalterada.

⁵⁵ *Ibidem*, p. 26

⁵⁶ CNUDMI, 2018, *op cit.*, p.33

⁵⁷ *Ibidem*, p.21

⁵⁸ *Ibidem*, p.38

⁵⁹ CNUDMI, *Ley Modelo sobre Comercio Electrónico*, Nueva York, Naciones Unidas, 1999, p.6

Fuerza probatoria de los mensajes de datos: se establece que toda la información contenida en un mensaje de datos goza de fuerza probatoria, y que para ello se debe tener presente la fiabilidad de la forma en que se generó, archivó o comunicó, así como la forma en que como se conservó la integridad de la información, la identificación del emisor, entre otros.

Conservación de los mensajes de datos: se señala que este requisito quedará satisfecho si se cumplen tres condiciones: i) que la información sea accesible para su ulterior consulta; ii) que el mensaje de datos sea conservado en el formato en que se haya generado, enviado o recibido; y iii) que se conserve, todo dato que permita determinar el origen y el destino del mensaje, así como la fecha y la hora en que fue enviado o recibido.⁶⁰

Es en este último punto, donde toman especial relevancia otros servicios relacionados con las firmas electrónicas como son los sellos digitales de tiempo. De manera que, esta ley modelo sienta las bases fundamentales de los principios que se debieran contemplar en las transacciones electrónicas, y por ello fue adoptada por México en su legislación, tal como se detallará más adelante.

2.1.2 Ley Modelo de la CNUDMI sobre Firmas Electrónicas

Ahora bien, una vez que se emitió la Ley Modelo de la CNUDMI sobre Comercio Electrónico, el Grupo de Trabajo comenzó a trabajar en un documento específico de la firma electrónica. En este sentido, la Ley Modelo de la CNUDMI sobre Firmas Electrónicas, fue aprobada el 12 de diciembre de 2001 con la finalidad de lograr una armonización en materia de firmas electrónicas, ya que, si bien en la Ley Modelo de la CNUDMI sobre Comercio Electrónico, ya se había contemplado en el artículo 7 una disposición relativa a la firma electrónica, no se habían

⁶⁰ *Ibidem*, p.7

desarrollado de forma tan específica diversos principios aplicables a la firma electrónica.⁶¹

En el mismo orden de ideas que la Ley Modelo de la CNUDMI sobre Comercio Electrónico, esta Ley Modelo, no solo resulta aplicable a relaciones comerciales y por ello, incluso se establece una propuesta de texto para los Estados que deseen ampliar el ámbito de aplicación de la ley, señalando que en la adopción en el derecho nacional puede establecerse que resulta aplicable a todos los casos donde se utilicen firmas electrónicas, si solo se especifican las excepciones correspondientes.⁶²

En esta ley modelo se resalta la fiabilidad técnica que deben tener las firmas electrónicas en relación con su eficacia jurídica;⁶³ ello en concordancia con las técnicas para la creación de la firma. También se desarrollan diversos principios como: el de la equivalencia funcional y el de neutralidad tecnológica, aunado a ello, se señalan los sujetos que forman parte en un proceso de firma electrónica y sus responsabilidades, igualmente, se hace referencia a la integridad, fiabilidad y al reconocimiento de firmas electrónicas extranjeras. En este sentido, busca otorgar equivalentes funcionales a la firma para contar con un esquema de confianza y seguridad en los medios electrónicos.⁶⁴ Respecto al tipo de firmas electrónicas que regula cabe destacar lo siguiente:

“La CNUDMI ha tratado de elaborar una legislación uniforme que pueda facilitar el empleo tanto de las firmas numéricas como de otras formas de firmas electrónicas. A ese fin, la CNUDMI ha tratado de

⁶¹ Robles Farias, Diego, “El comercio y la firma electrónicos. El modelo mexicano”, en Becerra Ramírez, Manuel (comp.), *Obra en homenaje a Rodolfo Cruz Miramontes*, México, UNAM, Instituto de Investigaciones Jurídicas, 2008, p.15

⁶² CNUDMI, Ley Modelo de la CNUDMI sobre las Firmas Electrónicas, Nueva York, Naciones Unidas, 2002, Nota al pie del artículo 1. Ámbito de aplicación

⁶³ CNUDMI, “*Guía para la incorporación de la incorporación de la Ley Modelo de la CNUDMI para las Firmas Electrónicas* (2001) al derecho interno”, Nueva York, Naciones Unidas, 2002, p. 10

⁶⁴ Rincón Cárdenas, *op cit.*, p.42

abordar las cuestiones jurídicas de las firmas electrónicas a un nivel intermedio entre la gran generalidad de la Ley Modelo de la CNUDMI sobre Comercio Electrónico y la especificidad que podría requerirse al abordar una técnica de firma determinada. En cualquier caso, y siguiendo el criterio de neutralidad respecto de los medios técnicos de la Ley Modelo de la CNUDMI sobre Comercio Electrónico, no debe interpretarse que la Ley Modelo desalienta el empleo de cualquier método de firma electrónica ya existente o que pueda aplicarse en el futuro.”

En este sentido, también resulta fundamental desarrollar los principales aspectos contenidos en esta ley modelo los cuales son los siguientes:

Neutralidad Tecnológica:⁶⁵ se establece que debe existir una igualdad en el tratamiento de las tecnologías de la firma y que las reglas establecidas en la Ley Modelo no pueden aplicarse de forma que excluyan, restrinjan o priven de efecto jurídico a cualquier método para crear una firma. Por ello se puede elegir el sistema de firma que mejor se adapte a la necesidad del usuario.⁶⁶

Equivalencia funcional: este principio refiere a que no se debe hacer diferencia entre la firma electrónica y la firma autógrafa.

Cumplimiento del requisito de firma: al respecto se señala que este requisito queda satisfecho si se utiliza una firma electrónica que sea fiable y resulte apropiada para los fines para los cuales se generó o comunicó.

Fiabilidad: podría considerarse que la fiabilidad es lo que permite que la firma tenga efectos jurídicos, en este sentido, la Guía para la incorporación de la Ley Modelo de la CNUDMI para las firmas electrónicas (2001) menciona que si bien pudiera interpretarse que la determinación de la fiabilidad solo podría ser efectuada *a posteriori*, por un tribunal, el objetivo de esta Ley Modelo era establecer una serie

⁶⁵ Neutralidad tecnológica supone que la legislación debe definir los objetivos a conseguir, sin imponer ni discriminar el uso de cualquier otro tipo de tecnología para conseguir los objetivos fijados. Davara Isabel, *op cit.*, p. 599

⁶⁶ Rincón Cárdenas, *op cit.*, pp.47 y 48

de principios que permitieran contar con una presunción de fondo sobre la misma *a priori*,⁶⁷ por lo cual, refiere cuatro supuestos a partir de los cuales se podrá considerar que la firma es fiable, los cuales son:

a) los datos de creación de la firma, en el contexto que son utilizados corresponden exclusivamente al firmante;

b) los datos de creación de la firma estaban, en el momento de firma, bajo control exclusivo del firmante;

c) es posible detectar cualquier alteración de la firma electrónica hecha después del momento de la firma;

d) cuando sea parte de los objetivos de la firma la integridad de la información a que corresponde también sea posible detectar cualquier alteración de la información hecha después de la firma.⁶⁸

Esta cuestión resulta sumamente relevante porque en este último inciso se hace una clara precisión en relación con la integridad de la información, estableciendo que no necesariamente la firma dará esta integridad a menos de que sea parte de sus objetivos.

Al respecto, si bien la integridad del documento y la integridad de la firma, son dos conceptos que están estrechamente ligados e incluso diversas tecnologías aportan al mismo tiempo la autenticación (referente a la identificación) y la integridad (del documento) se trata de dos conceptos jurídicos diferentes; ya que la integridad del documento no es la función esencial de una firma, y por tanto, basta con demostrar que la firma es suficientemente fiable para satisfacer el requisito legal de la firma, pero no requiere demostrar la integridad del documento.⁶⁹

Aunado a ello para determinar la fiabilidad de los sistemas, procedimientos y recursos humanos utilizados por un PSC se señala que se pueden considerar la calidad de los sistemas de equipo y programas informáticos, los procedimientos para la tramitación del certificado, la disponibilidad de la información para los

⁶⁷ CNUDMI, 2002, *op cit.*, p.59

⁶⁸ CNUDMI, 2002, Ley Modelo *op cit.*, artículo 6

⁶⁹ CNUDMI, 2002, *op cit.*, pp.61 y 62

firmantes, la periodicidad y alcance de la auditoria que debe realizar un órgano independiente, la existencia de un órgano de acreditación.⁷⁰

Partes: Asimismo refiere los tres sujetos principales en un proceso de firma y sus responsabilidades, los cuales son: firmante; PSC y parte que confía en el certificado.

2.1.3 Reglamento (UE) No 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE

Este Reglamento de la Unión Europea tiene como propósito fomentar la confianza en las transacciones electrónicas, logrando el reconocimiento mutuo de la identificación y la autenticación electrónicas para los servicios transfronterizos en línea de los Estados miembros, en este sentido, busca ofrecer un marco general en los servicios de confianza.

Particularmente, el Reglamento regula diversos aspectos relativos a los sistemas de identificación electrónica, considerando medidas de seguridad, condiciones para notificaciones, interoperabilidad, además de detallar aspectos que ya se han mencionado en apartados previos relativos a la firma electrónica pero, en este caso además de la firma electrónica y la firma electrónica avanzada se regula un tipo de firma denominado -firma electrónica cualificada- que es aquella “que se crea mediante un dispositivo cualificado de creación de firmas electrónicas y que se basa en un certificado cualificado de firma electrónica.”⁷¹

Es importante señalar que respecto al uso de la firma electrónica en servicios públicos se refiere que en los servicios en línea que presten los Estados miembros

⁷⁰ CNUDMI, 2002, Ley Modelo *op cit.*, artículo 10

⁷¹ Unión Europea, Reglamento (UE) No. 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por lo que se deroga la Directiva 1999/93/CE, artículo 3 numeral 12.

deberán reconocer tanto las firmas electrónicas avanzadas como las firmas electrónicas cualificadas.

También menciona otros servicios como el de entrega electrónica certificada y el del sello electrónico, estableciendo distintos niveles para éste, que van hasta el sello electrónico cualificado y señala cuestiones relativas a los prestadores de servicios de confianza que también pueden adquirir el carácter de cualificados si cumplen con diversos requisitos establecidos en el propio Reglamento.

Por su parte, los sellos de tiempo, son un servicio de confianza sumamente importante para la prestación de servicios en línea, el Reglamento regula distintos tipos de sellos: i) sello electrónico; ii) sello electrónico avanzado; y iii) sello electrónico cualificado.

Respecto al sello electrónico avanzado, se señalan características similares a las de la firma electrónica avanzada como son: que debe estar vinculado al creador del sello, permitir la identificación del creador del sello, haber sido creado utilizando datos de creación del sello electrónico con un alto nivel de confianza, bajo un control exclusivo y estar vinculado con los datos a que se refiere de todo que se pueda detectar cualquier modificación posterior.⁷²

Por su parte referente al sello cualificado de tiempo electrónico se menciona que tiene una presunción de exactitud de la fecha y hora que indican y de la integridad de los datos a los que están vinculados;⁷³ ello debido a que entre sus características se encuentra la forma en que se vincula el sello con los datos para eliminar la posibilidad de una modificación posterior, así como a que debe basarse en una fuente de información temporal vinculada al Tiempo Universal Coordinado.⁷⁴

De ahí que, al igual que en el caso de la firma electrónica se establece que para el caso de los servicios públicos se reconocerán tanto los sellos electrónicos avanzados como los sellos electrónicos cualificados. Asimismo, contempla el principio ya mencionado en otros instrumentos internacionales referente a la validez de los documentos electrónicos que señala que no se denegarán efectos jurídicos

⁷² *Ibidem*, artículo 36

⁷³ *Ibidem*, artículo 41

⁷⁴ *Ibidem*, artículo 42

ni admisibilidad como prueba en juicio a un documento solo por estar en formato electrónico.

En este sentido, como puede apreciarse este Reglamento a diferencia de las Leyes Modelo analizadas en los apartados previos, regula otras cuestiones relativas a servicios de confianza sumamente importantes en las transacciones en medios electrónicos, y en la implementación de trámites en línea ya que en estos procesos, además de considerar a la firma electrónica resulta fundamental considerar otros elementos como el sello digital de tiempo, los cuales se analizarán en el apartado 3 del presente capítulo.

2.2. Marco jurídico nacional

2.2.1 Ley Federal de Procedimiento Administrativo

Esta ley establece las disposiciones que se aplican a los actos, procedimientos y resoluciones de la Administración Pública Centralizada por lo que es la base fundamental en la emisión actos administrativos; particularmente, señala los elementos y requisitos del acto administrativo, así como sus principios, la forma en que deben presentar los trámites los particulares, las obligaciones de la APF, entre otros, disposiciones que de forma general aplican también en medios electrónicos.

Por lo que hace a los medios electrónicos fue reformada el 30 de mayo del año 2000 adicionando diversas reglas relativas a la posibilidad del uso de éstos en los procedimientos administrativos. En la exposición de motivos se señaló que la reforma tenía por objeto el incremento de la calidad en los servicios que ofrecen las Dependencias para la ciudadanía, evitando desplazamientos, reduciendo costos, así como al interior, para la gestión de los procesos y racionalización de los recursos además de disminuir los actos de corrupción y mejorar la transparencia en la gestión gubernamental.⁷⁵

⁷⁵ Exposición de motivos Ley Federal de Procedimiento Administrativo

De esta manera, en la reforma se incluyó la posibilidad de presentar promociones por medios electrónicos en las etapas que determinaran las propias Dependencias en reglas de carácter general publicadas en el Diario Oficial de la Federación. En relación con ello, se estableció que la vía electrónica sería optativa, asimismo, se incluyó el concepto de equivalencia funcional al especificar que los medios de identificación electrónica producirán los mismos efectos que los firmados autógrafamente y que tienen el mismo valor probatorio.

En este orden de ideas, se mencionó lo relativo a la fecha y hora que se consideraría para los actos que se lleven a cabo por esta vía, especificando que sería responsabilidad de las Dependencias verificar lo anterior en la recepción de dichos actos de conformidad con las disposiciones que debería emitir la Secretaría de la Función Pública, sin embargo, dichas disposiciones no han sido emitidas. Aunado a lo anterior, se señaló que las notificaciones pueden realizarse vía electrónica si así lo acepta expresamente el promovente y se puede comprobar fehacientemente la recepción.

Posteriormente, en una reforma posterior publicada el 2 de mayo de 2017, se estableció que dichas notificaciones se podían llevar a cabo a través de comunicaciones electrónicas certificadas conforme a los requisitos de la Norma Oficial Mexicana NOM- 151.SCFI.2016, Requisitos que deben observarse para la conservación de mensajes de datos y digitalización de documentos (en adelante NOM 151), no obstante, a la fecha solo se ha publicado el proyecto de modificación a la NOM 151 agregando el Apéndice C el cual contempla los requisitos antes referidos a efecto que durante los 60 días naturales siguientes a su publicación los interesados remitieran sus comentarios, por tanto, está pendiente su publicación definitiva.⁷⁶

De acuerdo con lo analizado, el marco jurídico contempla la posibilidad de utilizar medios electrónicos en la presentación de los trámites y en las notificaciones, siempre y cuando esté previsto en las reglas específicas del procedimiento que se lleve a cabo, lo anterior debido a que no se reformó el artículo relativo a los actos

⁷⁶

Puede consultarse en: https://www.dof.gob.mx/nota_detalle.php?codigo=5618010&fecha=11/05/2021#gsc.tab=0

que emiten los servidores públicos ya que de conformidad con el artículo 3 fracción IV de la ley en comento es un requisito del acto administrativo *“Hacerlo contar por escrito y con firma autógrafa, salvo en aquellos casos que la ley autorice otra forma de expedición”*.

2.2.2 Ley de Firma Electrónica Avanzada

La Exposición de Motivos de la Ley de Firma Electrónica Avanzada⁷⁷ refiere el Plan de Acción de Ginebra sobre la Cumbre Mundial de la Sociedad de la Información de 2003, el cual menciona que para maximizar los beneficios sociales, económicos y medioambientales de la Sociedad de la Información, los gobiernos deben crear un entorno jurídico, reglamentario y político fiable, transparente y no discriminatorio, asimismo, se señalan los antecedentes regulatorios en México en diversas leyes en materia civil mercantil, fiscal, administrativa de protección al consumidor, así como que el incluir el uso de la firma electrónica y de medios electrónicos ha abonado a facilitar sus actos correspondientes.

Igualmente, se resalta que el uso de medios electrónicos en el sector público permite crear un gobierno más transparente ya que permite la reducción de la discrecionalidad y la corrupción. Adicionalmente, se destaca la importancia del uso de la firma electrónica avanzada para disminuir el uso del papel como una medida para cuidar el medio ambiente y mitigar el cambio climático, además de los importantes ahorros económicos tanto para el sector público como el privado; se destaca también que permite realizar trámites más ágiles y transparentes.

Aunado a lo anterior, en la iniciativa de reforma se mencionó que la ley busca ampliar y mejorar el acceso y cobertura a los trámites y servicios gubernamentales y lograr una verdadera administración en línea, con la que se comuniquen los servidores públicos al interior de las Dependencias y con los ciudadanos, evitando desplazamientos de éstos.

⁷⁷ Puede consultarse en: https://www.senado.gob.mx/64/gaceta_del_senado/documento/28987

Es así que el 12 de enero de 2012, se publicó la ley y en ésta se estableció como objeto el regular las comunicaciones, servicios, actos jurídicos y administrativos en los cuales los particulares y los servidores públicos de las dependencias y entidades de la APF, y de las unidades administrativas de la Presidencia de la República que utilicen la firma electrónica avanzada; así como los servicios relacionados con la firma electrónica avanzada y la homologación de la misma.

En el contenido de la ley se pueden encontrar diversas definiciones de elementos fundamentales relacionadas con el uso de medios electrónicos; algunas de éstas se establecieron de la misma forma que en las Leyes Modelo abordadas en el apartado uno de este capítulo, sin embargo, se incluyeron algunos términos que difieren de los conceptos incluidos en estas Leyes Modelo o incluso que no se refieren en dichos instrumentos como el de “documento electrónico”. Respecto a ésta, cabe señalar que puede resultar confuso haber incluido una definición de documento electrónico y otra de mensaje de datos. Por ello, se considera que solo se debió considerar la relativa al mensaje de datos, acorde con los instrumentos internacionales al respecto.

Del mismo modo contempla los principios de la firma electrónica avanzada tales como: la Equivalencia Funcional, Autenticidad, Integridad, Neutralidad Tecnológica, No Repudio y Confidencialidad de una forma muy clara, y se considera que fue acertado incluirlos de una forma expresa con una definición específica. Es así que establece un principio básico en materia de firma electrónica al señalar que ésta tendrá el mismo valor que la firma autógrafa.

Por otra parte, regula cuestiones que no son relativas solo a la firma sino al uso de medios electrónicos en la Administración Pública, al respecto es importante reflexionar si estos aspectos debieron ser regulados en la ley específica de la materia que es la Ley Federal de Procedimiento Administrativo.

Entre los aspectos antes referidos, se puede destacar la mención del Sistema de Trámites Electrónico y de un Tablero Electrónico, en el primer caso se señala que se trata de un sitio desarrollado por las dependencias para el envío y recepción de documentos, notificaciones y comunicaciones, y en el segundo que se trata de

un medio por virtud del cual se ponen a disposición de los particulares las actuaciones electrónicas que emiten las dependencias.

En este aspecto, es importante señalar que diversos trámites que utilizan la firma electrónica avanzada, por su propia naturaleza requieren la generación de un sistema específico donde se desarrollan reglas de negocio particulares que no permiten que las acciones antes referidas se lleven a cabo a través de un solo sistema con características generales; por otra parte, es fundamental considerar que no en todos los casos se requerirá firma electrónica, sin embargo, de acuerdo con la Ley en análisis las reglas antes señaladas solo aplicarían si se utiliza firma electrónica avanzada; es por ello que como se mencionó previamente se considera que hubiera sido más oportuno regular estas cuestiones en la ley específica de la materia, es decir, la Ley Federal de Procedimiento Administrativo.

Aunado a lo anterior respecto a las cuestiones y mecanismos de seguridad de la información que se deben considerar en el sistema de trámites electrónico se establece que la Secretaría de la Función Pública emitirá los lineamientos correspondientes, los cuales aún no han sido emitidos.

Otro aspecto que se incluye en la ley que no tiene relación con la firma electrónica avanzada es el relativo a la conservación de la información, aunque solo se hace referencia a que la conservación de esta información debe ser por los plazos previstos en los ordenamientos correspondientes de acuerdo con la naturaleza de la información. Asimismo, se señala que para la conservación de documentos también se establecerán disposiciones que considerarán los requisitos previstos en la NOM 151.

No obstante, para temas de digitalización no menciona la Norma Oficial antes señalada, ello debido a que la fecha en la que se emitió la Ley es anterior a la fecha en la que se agregó el Apéndice B relativo a la Digitalización en la NOM 151. De esta manera, la Ley señala que la migración de documentos impresos con firma autógrafa a formato electrónico, se podrá llevar a cabo por un servidor público que tenga facultades de certificación; así mismo, refiere diversos aspectos del proceso, uno de ellos es que el documento debe mantenerse íntegro e inalterado a partir de que se generó por primera vez en su forma definitiva y debe ser accesible para su

ulterior consulta, para lo cual, es de destacar que se tendría que integrar una constancia de conservación de mensaje de datos. Por lo anterior, se considera que, aunque para la digitalización señalada no está contemplada la NOM 151 debido a las características que se requieren en este proceso si será fundamental considerar los aspectos que se contemplan en el Apéndice B de la citada Norma.

Posteriormente se establecen cuestiones relativas a la estructura y validez del certificado, a los derechos de los titulares de los certificados, asimismo se incluye un capítulo de las autoridades certificadoras y se otorga este carácter a la Secretaría de la Función Pública, la Secretaría de Economía y al Servicio de Administración Tributaria. Por otra parte, se contempla un supuesto en que otras autoridades, así como los Prestadores de Servicios de Certificación (PSC) pueden adquirir tal carácter, para lo cual, se señalan los requisitos que se requieren y el proceso que se tiene que seguir ante la Secretaría de la Función Pública.

Al respecto, es de resaltar que, pese a que estos PSC ya fueron previamente acreditados por la Secretaría de Economía, se solicita que cumplan con un proceso específico para ser acreditados para efectos de esta Ley. Sin embargo, es de resaltar que debido a que esta ley solo regula a la Firma Electrónica Avanzada se entendería que esta acreditación ante la Secretaría de la Función Pública solo sería para el servicio de emisión de certificados digitales y no para los otros servicios que pueden prestar los PSC en términos del Código de Comercio. Además, como se señaló, la Ley contempla a las constancias de conservación de la NOM 151 como una referencia, sin embargo, para contar con una mayor precisión respecto el ámbito de aplicación de los otros servicios que pueden prestar los PSC en el sector público podría ser recomendable adicionar en la Ley que pueden ser utilizados los servicios de dichos PSC.

Posteriormente, se incluye un apartado relativo al reconocimiento de certificados digitales y la celebración de convenios que se puede llevar a cabo para el reconocimiento de certificados digitales homologados, asimismo, se señala lo relativo al reconocimiento transfronterizo de certificados digitales, de un modo similar al Código de Comercio, ya que se señala que tendrán la misma validez si

cumplen con los requisitos, procedimiento validez y vigencia del certificado de las autoridades certificadoras previamente señaladas.

Aunado a lo anterior, la ley refiere que se emitirán unas disposiciones para el adecuado cumplimiento de la Ley, por lo cual el 21 de marzo de 2014, fue publicado el Reglamento de la Ley de Firma Electrónica Avanzada y el 21 de octubre de 2016 las Disposiciones Generales de la Ley de Firma Electrónica Avanzada.

Por lo que hace a este Reglamento se establecieron diversas reglas que será fundamental considerar en la implementación de trámites en línea, una de ellas es la que señala que no es factible el uso de Firma Electrónica Avanzada cuando se exige la firma autógrafa ya sea del servidor público o del ciudadano en alguna disposición legal. Al respecto, es importante considerar que el artículo 3 de la Ley Federal de Procedimiento Administrativo establece en su fracción IV que el acto administrativo debe constar por escrito y con la firma autógrafa de la autoridad que lo expide, salvo los casos en que se autorice otra forma de expedición.

Adicionalmente, el Reglamento antes señalado establece que las Dependencias deben incorporar en sus sistemas informáticos las herramientas tecnológicas o aplicaciones que permitan utilizar la Firma Electrónica Avanzada. Ahora bien, en relación con la aceptación que debe realizar el particular para el uso de medios electrónicos establece que debe realizarse preferentemente por medios electrónicos y utilizando la Firma Electrónica Avanzada, en el Sistema de Trámites Electrónicos.

Respecto a los Acuses de Recibo Electrónico se señala que deben contener un sello digital que permita dar plena certeza sobre la fecha y hora de recepción, así como del registro de los Documentos Electrónicos asociados al mismo Acuse, y si bien se contempla que la Secretaría de la Función Pública emitiría unos lineamientos donde se determinarían las especificaciones técnicas que debe contener dicho sello así como los medios para que la ciudadanía verificara la autenticidad de los Acuses de Recibo Electrónico, éstos no han sido emitidos. Aunado a lo anterior se contempla que la impresión de los documentos electrónicos suscritos con la Firma Electrónica Avanzada debe contener una cadena de caracteres asociados al documento original.

Por lo que hace a las Disposiciones Generales de la Ley de Firma Electrónica Avanzada, en materia de conservación de mensajes de datos, si bien en la ley de la materia se había señalado que en éstas se establecerían los requisitos necesarios para ello considerando aquellos previstos en la NOM 151, en éstas se estableció ya la aplicación directa de esta norma, por tanto, se debe contemplar el uso de una constancia de conservación de mensajes de datos en los términos de la norma oficial antes referida, asimismo, se señala que se deberá considerar la naturaleza de la documentación de acuerdo con la legislación aplicable pero asegurando siempre su integridad y ulterior consulta.

En suma, la Ley de Firma Electrónica Avanzada, así como su Reglamento y Disposiciones regularon cuestiones relativas al uso de medios electrónicos en los trámites en línea, más allá de la propia firma electrónica avanzada. No obstante, si bien se considera que hay aspectos que debieron ser regulados en la ley específica de la materia, es decir, la Ley Federal de Procedimiento Administrativo, sí otorga un marco jurídico robusto que permite contar con principios que coadyuvan a fortalecer la posibilidad de utilizar medios electrónicos en el sector público cuando se utiliza este tipo de firma.

2.2.3 Ley Federal de Transparencia y Acceso a la Información Pública

Esta ley protege el derecho humano de acceso a la información y lo regula respecto a aquella que se encuentra en posesión de las autoridades, para con ello transparentar la gestión pública, favorecer la rendición de cuentas y la participación ciudadana en la toma de decisiones públicas. De acuerdo con la misma, este derecho comprende el solicitar investigar, difundir y recibir información. En este orden de ideas, toda persona tiene derecho de acceso a la información sin discriminación alguna y por ello, se debe considerar que como principio general toda la información en posesión de los sujetos obligados es pública salvo las excepciones previstas en la propia ley, en específico, si bien como regla general se establece que para permitir el acceso a la información confidencial se requiere el consentimiento de los particulares, se refieren ciertas excepciones como es el caso

de cuando se transmite entre sujetos obligados siempre y cuando la información se utilice para el ejercicio de las facultades de los mismos.

Por lo que, un principio fundamental que se debe considerar es el de máxima publicidad, asimismo, se señala que se debe promover la generación, documentación y publicación de la información en formatos abiertos y accesibles, garantizando que la generación, publicación y entrega de información sea accesible, confiable, verificable, veraz y oportuna, en concordancia, se señala que se debe buscar que la información generada tenga un lenguaje sencillo para cualquier persona.

2.2.4 Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados

El derecho a la protección de datos personales ha seguido un camino a través de distintas reformas, en principio se contempló en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (hoy abrogada). Sin embargo, su alcance era solo como un límite al derecho a la libertad de expresión, a la transparencia y no era concebido aún como este derecho humano ligado a la autodeterminación informativa, privacidad e intimidad.⁷⁸

En este sentido fue en la reforma de 2009 a los artículos 16 y 73 fracción XXIX-O de la Constitución Política de los Estados Unidos Mexicanos donde ya se contempló este derecho a la protección de datos personales como un derecho humano, y en la cual se reconocen los denominados Derechos ARCO ⁷⁹, es así como en 2014, se publicó la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPO), la cual aplica de manera directa a la Federación y se trata de un marco de referencia para las entidades federativas.

Al respecto, en esta ley se contemplan los principios que rigen la protección de datos personales, los derechos que tienen los titulares de los mismos entre los

⁷⁸ Solange Maqueo María (coord.) Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, COMENTADA. INAI, p.9

⁷⁹ Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, p. 11

cuales se contempla además de los Derechos ARCO, otros aspectos novedosos como la portabilidad de los datos, asimismo, se señalan las medidas de seguridad que deben considerar los sujetos obligados en el tratamiento de datos personales.

Entre los aspectos que destacan que deben ser considerados por los sujetos obligados, se encuentra el Aviso de Privacidad que se debe poner a disposición de los titulares, tanto el simplificado como el integral, así como el de la implementación de un Sistema de Gestión de Seguridad y un documento de seguridad de conformidad con los artículos del 31 al 42 de esta misma Ley.

Posteriormente en 2018, se publicó en el Diario Oficial de la Federación el Acuerdo mediante el cual se aprueban los Lineamientos Generales de Protección de Datos Personales para el Sector Público, en los cuales se desarrollan las disposiciones previstas en la Ley General que nos ocupa por lo que hace al ámbito federal, por ende, se pueden encontrar reglas muy detalladas respecto al cumplimiento de los requisitos y deberes, así como en relación con el aviso de privacidad, Derechos ARCO y recursos.

2.2.5 Ley General de Mejora Regulatoria

Esta ley se publicó en el Diario Oficial de la Federación el 18 de mayo de 2018, en su exposición de motivos⁸⁰ se refiere que se tenía la necesidad de instrumentar un modelo de mejora regulatoria que permitiera la simplificación nacional de trámites. De manera que señaló como objeto el establecer los principios y las bases a las que deben sujetarse los órdenes de gobierno en materia regulatoria; en específico dentro de sus objetivos se encuentra establecer la obligación de las dependencias en todos los órdenes de gobierno de implementar políticas de mejora regulatoria.

Uno de los aspectos que se puede destacar relacionado con el objetivo del presente proyecto es la implementación del Expediente para Trámites y Servicios que es definido en la misma “como el conjunto de documentos electrónicos emitidos

⁸⁰ Larios Córdova Héctor, Iniciativa con proyecto de Decreto por el que se expide la Ley General de Mejora Regulatoria, p. 7

por los Sujetos Obligados asociados a personas físicas o morales, que pueden ser utilizados por cualquier autoridad competente, para resolver trámites y servicios”.⁸¹

Es decir, lo que se busca es que no se solicite información a los ciudadanos que ya obra en poder de las dependencias a efecto de resolver trámites y servicios. Al respecto, se señalan los efectos que tienen los documentos electrónicos, así como el proceso de migración que se debe llevar a cabo de un documento físico a uno electrónico.

Referente a este punto se puede observar que se incluyen regulaciones y reglas relativas a la digitalización de documentos en distintas leyes que no siempre son coincidentes, aunque si bien el ámbito de aplicación de cada una puede variar, se considera que las reglas deben ser homologas y sin duda contemplar aspectos fundamentales que ya se han señalado en diversos instrumentos internacionales y que se encuentran en el propio marco jurídico nacional como es el caso de la NOM 151.

2.2.6 Ley General de Archivos

La nueva Ley General de Archivos se publicó en el Diario Oficial de la Federación el 15 de junio de 2018, en su exposición de motivos estableció la necesidad de lograr una administración eficiente de los archivos públicos ya que con ello se permite una mejor toma de decisiones, transparencia y rendición de cuentas, no obstante, se resaltó que las condiciones actuales archivísticas en México no garantizan lo anterior, ni el pleno acceso a la información; por ello, surge la necesidad establecer reglas homogéneas para la administración y organización del archivo tanto en el ámbito federal, local y municipal.⁸²

Ahora bien, por lo que hace a los documentos electrónicos, en la Ley publicada se agrega el Capítulo IX que se relaciona específicamente con ello, en el cual se establece que los sujetos obligados deben incorporar en su programa anual

⁸¹ Ley General de Mejora Regulatoria, artículo 3 fracción IX, p.2

⁸² Diaz Salazar Cristina y Hernández Rojas Laura, et. al., Iniciativa con proyecto de Decreto por el que se expide la Ley General de Archivos publicada el 7 de noviembre de 2016, p. 1 y 2

los procedimientos para la generación, administración, uso, control y migración de formatos electrónicos, así como, planes de preservación y conservación y para ello menciona que se apoyará en disposiciones del Consejo Nacional de Archivos, que al igual que las mencionadas en la Ley de Firma Electrónica Avanzada no han sido emitidas.

Aunado a lo anterior, contempla que los documentos electrónicos que tengan valor histórico se deben conservar en sus formatos originales, en el mismo orden de ideas, se establece que cuando la ley así lo prevea, los sujetos obligados deben conservar los documentos de archivo aun cuando hayan sido digitalizados. Por otra parte, se refiere que los sujetos obligados deben implementar sistemas automatizados para la gestión documental y administración y conservación de archivos electrónicos para lo cual deben cumplir con los lineamientos que emita el Consejo Nacional de Archivos refiriendo únicamente condiciones mínimas de seguridad, accesibilidad, conservación, trazabilidad que deben contener estos lineamientos, sin embargo, éstos tampoco han sido emitidos.

En consecuencia, se puede observar que esta ley proporciona un marco muy general respecto al archivo electrónico, pero son fundamentales la emisión de los lineamientos correspondiente para que el sector público pueda dar el tratamiento adecuado a los archivos electrónicos.

No obstante, de la misma forma que se realizó con otras disposiciones en la materia como es el caso de las emitidas por la Coordinación de Estrategia Digital Nacional, en esta ley también se estableció que las disposiciones reglamentarias vigentes en la materia seguirían aplicando mientras no se opongan a la Ley, hasta en tanto no se publiquen las disposiciones reglamentarias correspondientes, por lo cual, podrían resultar aplicables algunas disposiciones de los Lineamientos para la Organización y Conservación de los Archivos que en uno de sus apartados mencionan reglas correspondientes a los archivos electrónicos y políticas de digitalización.

2.2.7 Acuerdo para la adopción y uso por la APF de la Clave Única de Registro de la Población

Este Acuerdo si bien se expidió desde el año 1996 y puede resultar ya rebasado por las condiciones actuales, aún está vigente y por ello es importante mencionarlo, ya que refiere a la acreditación de identidad de las personas a través de una clave única y homogénea como es la Clave Única de Registro de Población (CURP), ya que se menciona que en los registros de personas se asignaban distintas claves que partían de los mismos datos, pero se integraban de distinta forma. De esta manera, en el numeral 12 se establece que la APF debe promover que en todo trámite oficial que requiera el registro o la identificación de personales se asiente la CURP.

Ello resultó muy útil para iniciar a pensar en temas de interoperabilidad, sin embargo, actualmente requerimos ya de una identidad digital. Al respecto, cabe señalar que el 27 de mayo de 2020, se presentó una Iniciativa con proyecto de reforma por la que se expide la Ley General de Población y se abroga la Ley General de Población publicada en el Diario Oficial de la Federación el 7 de enero de 1974, en la cual, se señala el derecho que tienen todas las personas a la identidad de acuerdo con el artículo 4 de la Constitución Política de los Estados Unidos Mexicanos.

En este sentido, la iniciativa refiere que para registrar a una persona se le asignará la Clave Única de Registro de Población en la que se asociarán entre otros datos, los biométricos, asimismo que se le asignará una Cédula de Identidad Digital a todas las personas que contendrá entre otros datos la CURP y los datos biométricos.

Aunado a lo anterior, dispone que en trámites que involucren documentos oficiales de identificación, las dependencias deberán validar los datos personales que recaben con los que se encuentren en el Registro Nacional de Población incluyendo los datos biométricos, para ello, señala que se deben establecer los mecanismos de interoperabilidad correspondientes; para lo cual se plantea la creación del Servicio Nacional de Identificación Personal, el cual será prestado a través de la Secretaría de Gobernación, y está contemplado como el sistema a través del cual con la información contenida en el Registro Nacional de Población,

se consulta, valida, verifica y acredita la identidad de las personas e incluso la validez de las identificaciones oficiales.⁸³

En este orden de ideas, es importante destacar que la identidad digital es un paso fundamental en los trámites en línea y para lograr la interoperabilidad, sin embargo, debemos considerar que diversos entes públicos ya cuentan con información de la ciudadanía incluyendo sus datos biométricos, por lo que, además de la iniciativa se requiere un plan muy específico que contemple todos esos aspectos para lograr una identidad digital.

2.2.8 Acuerdo por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la APF

Este Acuerdo emitido el 06 de septiembre de 2021⁸⁴ por la Coordinación de Estrategia Digital Nacional de la Oficina de la Presidencia de la República derogó el Acuerdo por el que se expide el Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones y en la Seguridad de la Información publicado en el Diario Oficial de la Federación el 08 de mayo de 2014. Asimismo, en su artículo transitorio tercero menciona que quedan sin efecto las disposiciones administrativas que se opongan al Acuerdo y debido al contenido del mismo se podría señalar que una parte del contenido del Acuerdo por el que se establece el Esquema de Interoperabilidad y Datos Abiertos de la APF publicado en el Diario Oficial de la Federación el 06 de septiembre de 2011, queda sin efectos.

Ahora bien, este Acuerdo resulta de observancia obligatoria para la APF, en principio señala algunas definiciones básicas relacionadas con el gobierno digital,

⁸³ Barrera Badillo Rocío, iniciativa con Proyecto de Decreto por el que se expide la Ley General de Población y abroga la Ley General de Población publicada en el Diario Oficial de la Federación el 7 de enero de 1974.

⁸⁴ Acuerdo por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la APF publicado en el Diario Oficial de la Federación el 6 de septiembre de 2021

seguridad de la información y proyectos en materia de TIC. Posteriormente, refiere las políticas y disposiciones que se deben seguir para realizar implementaciones tecnológicas, se detallan también los objetivos que se deben buscar con cada portafolio de proyectos de tecnologías de la información y comunicación, así como el procedimiento que se debe seguir para contar con el visto bueno de la Coordinación de Estrategia Digital Nacional; una vez realizado lo anterior, se especifican los pasos necesarios para realizar contrataciones de tecnologías y seguridad de la información, también se incluyen políticas tecnológicas aplicables a los proyectos de TIC, así como los estándares técnicos que deben cumplir los servicios de internet y redes de datos. Por otra parte, se incluyen reglas relativas al correo electrónico y a los aplicativos de cómputo.

Otro aspecto importante que contempla el Acuerdo, se refiere al Repositorio de software de la APF, que es señalado como un espacio que administra la propia Coordinación de Estrategia Digital Nacional donde se almacena el código fuente de las aplicaciones o programas desarrollados o con titularidad de las instituciones para usar, estudiar y compartir y con ello se busca lograr un ahorro en el gasto público.

Aunado a lo anterior, respecto a las aplicaciones de cómputo, se señalan las condiciones que se deben cumplir para implementar estos aplicativos, así como, cuando se trate de desarrollos basados en software libre. Asimismo, se prevé que en los desarrollos se debe seguir un modelo de arquitectura de software que genere aplicaciones reutilizables e interoperables, así como, que se deben seguir estándares técnicos en materia de datos abiertos. En adición a lo anterior, se pormenorizan los elementos que debe incluir el diseño del aplicativo a desarrollar entre los cuales se encuentran: requerimientos del negocio, mecanismos o esquemas de seguridad de la información, políticas de privacidad y protección de datos personales, alcance de los módulos, perfiles de usuario, matriz de trazabilidad, protocolos de pruebas y mecanismos de autenticación a través de la Firma Electrónica Avanzada (e-firma) cuando resulte aplicable.

Además, se contempla que en los desarrollos de sistemas electrónicos de trámites y servicios se deben priorizar los procesos de digitalización que permitan el desarrollo de trámites simplificados, y se incluyen a los que formen parte del

Expediente de Trámites y Servicios que se contempla en la Ley General de Mejora Regulatoria.⁸⁵ Por último, se detallan todas las reglas relativas a la imagen y estructura a la que se deben apegar los sitios web.

2.2.9 Bases técnicas de Seguridad Informática para las dependencias y entidades de la APF

Las Bases técnicas de Seguridad Informática expedidas el 12 de marzo de 2020, son recomendaciones mínimas de seguridad informática. Al respecto, detallan acciones que deben seguir las dependencias y entidades de la APF en materia de prevención, detección y respuesta ante incidentes.

2.2.10 Decretos, acuerdos, criterios expedidos por la Unidad de Gobierno Digital

Como se comentó previamente el *Acuerdo por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal* (en adelante Acuerdo de Gobierno Digital)⁸⁶, estableció en su artículo transitorio tercero que las disposiciones que se opusieran al Acuerdo quedarían sin efectos, no obstante, durante el período de 2015 a 2018 se emitieron diversos acuerdos respecto a los cuales se pueden rescatar algunos aspectos que debido a la regla anterior aún se podrían considerar como vigentes, los cuales son los siguientes:

2.2.10.1 Decreto por el que se establece la Ventanilla Única Nacional para los Trámites e Información del Gobierno

Este Decreto fue publicado en el Diario Oficial de la Federación el 3 de febrero de 2015 con el objeto de establecer la Ventanilla Única Nacional para los Trámites e Información del Gobierno, como un punto de contacto del gobierno. De

⁸⁵ *Idem*

⁸⁶ *Idem*

acuerdo al mismo a través de dicha ventanilla se propiciaría la interoperabilidad de los sistemas electrónicos de la APF, es decir, su objetivo es que a través de una sola ventanilla la ciudadanía pueda ingresar y realizar los trámites correspondientes, sin embargo, es de destacar que no se establece como se llevaría a cabo la interoperabilidad que se menciona.

2.2.10.2 Decreto por el que se establece la regulación en materia de Datos Abiertos

Fue publicado el 20 de febrero de 2015, en el Diario Oficial de la Federación, y al respecto si bien en el Acuerdo de Gobierno Digital se incluye una definición de datos abiertos y se señala que las instituciones deberán observar en sus procesos de desarrollo y mantenimiento de aplicativos de cómputo, los estándares técnicos en materia de datos abiertos⁸⁷, del Decreto publicado en 2015, se podrían rescatar las características que deben tener los datos para ser considerados como abiertos, entre las cuales se encuentran que deben ser: gratuitos, no discriminatorios, de libre uso, legibles por máquinas, integrales, primarios, oportunos y permanentes características que son acordes con las establecidas en la Ley General de Transparencia y Acceso a la Información Pública.

2.2.10.3 Disposiciones Generales que establecen los mecanismos de identificación y control de acceso que deberán observar las dependencias y entidades de la APF y las empresas productivas del Estado

Se publicaron en el Diario Oficial de la Federación el 10 de mayo de 2018, ahora bien, en el Acuerdo de Gobierno Digital, se proporciona una definición de autenticación electrónica, no obstante, en estas Disposiciones Generales, se señalan distintos niveles de autenticación relativos a los mecanismos de identificación digital, los cuales son:

⁸⁷ Acuerdo de Gobierno Digital, artículo 66

Tipo “A” Usuario anónimo. - no se requiere de autenticación, ya que se considera como una interacción donde el usuario mantiene secreta su identidad.

Tipo “B” Autenticación con contraseña.- requiere de una autenticación básica, la cual consta de un nombre de usuario y contraseña proporcionada por el usuario

Tipo “C” Autenticación con contraseña dinámica.- requiere de una contraseña que funcione mediante una clave dinámica, de un solo uso, con vigencia determinada y que sirve como mecanismo de acceso a los trámites de las dependencias.

Tipo “D” Autenticación con firma electrónica avanzada.- se requiere que se ingresen los archivos correspondientes a la firma.

Tipo “E”.- Autenticación a través de datos biométricos.- en esta se requiere se ingrese la CURP y uno o más datos biométricos para que se verifique la identidad de la persona.

De esta manera, se considera que con estas Disposiciones Generales se puede observar de una forma muy clara la diferencia entre utilizar la firma electrónica como mecanismo de autenticación y como medio de consentimiento, y también se observan los niveles que pueden existir dependiendo de lo que se requiera en el trámite, sin necesidad de que en todos los casos se utilice firma electrónica avanzada.

2.2.10.4 Criterios Técnicos que deberán observar las dependencias y entidades de la APF, así como las empresas productivas del Estado, para la emisión de documentos electrónicos que deriven de un trámite o servicio digital

Estos Criterios fueron publicados en el Diario Oficial de la Federación el 27 de noviembre de 2018, al respecto, una de las cuestiones que se considera aún está vigente ya que no se contrapone ni detalla en el Acuerdo de Gobierno Digital, se refiere a la descripción de los elementos que deben contener los mensajes de datos y sus representaciones gráficas los cuales son: i) identificador electrónico; ii)

servidor público que lo emite; iii) lugar, fecha y hora de emisión; iv) CURP en caso de personas físicas y RFC para personales morales; v) firma electrónica avanzada del servidor público competente; vi) cadena original, que siempre debe contemplar el contenido del documento; vii) sello digital; viii) mecanismos de validación, a través del código bidimensional QR y un sitio de internet; ix) fundamento legal y razones de hecho que se consideren para sustentar el mensaje de datos y su representación gráfica; x) leyenda con el fundamento legal que da validez a la representación gráfica del mensaje de datos.

Asimismo, se señala que lo anterior es sin perjuicio de que se observe lo dispuesto por el artículo 3 de la Ley Federal de Procedimiento Administrativo. Respecto al sello de tiempo, se establece que debe contar con las especificaciones técnicas que se establecen en los numerales A.4.2 y A.6.1 del Apéndice A de la NOM 151.

Respecto a la CURP, es importante señalar que si bien puede ser considerado como un elemento que deben solicitar las dependencias de la APF como un identificador y campo llave, eso no implica que deba ser plasmado en la representación gráfica del mensaje de datos ya que se trata de un dato personal y al ser publicado dependiendo del tipo de trámite podrían estarse vulnerando los derechos de protección de datos personales de distintas personas.

2.3 Marco jurídico nacional aplicable a los particulares con impacto en el sector público

2.2.1 Código de Comercio

Una de las primeras reformas en materia de medios electrónicos fue la publicada en el año 2000 en el Diario Oficial de la Federación, que reformó entre otros ordenamientos al Código de Comercio donde se reguló lo relativo a la emisión y recepción de los mensajes de datos. Posteriormente, en 2003 se publicó una nueva reforma al mismo ordenamiento, donde se modificaron y adicionaron diversos artículos relativos a lo anterior, y con lo cual se alineó más la reforma a la Ley Modelo de la CNUDMI de Comercio Electrónico y se contempló lo dispuesto en la

Ley Modelo de la CNUDMI sobre las Firmas Electrónicas, entre los cambios fundamentales que se llevaron a cabo, se adicionó un capítulo relativo a la firma electrónica, se agregaron diversas definiciones y se incorporó la figura de PSC y por tanto la base para regular otros servicios de confianza relacionados con la firma electrónica, como los sellos digitales de tiempo; posteriormente las constancias de conservación de mensajes de datos y finalmente la digitalización de documentos.

En este sentido, si bien el Código de Comercio es aplicable a los particulares, estableció las bases en materia de la regulación de medios electrónicos por lo que resulta importante considerarlo como referencia.

2.2.2 Ley Federal de Protección de Datos Personales en Posesión de Particulares

Esta ley se publicó el 5 de julio de 2010, es decir, se trata de un ordenamiento mucho más antiguo que la LGPDPSO, en ésta se destacan las medidas fundamentales que deben cumplir los particulares que recaben datos de la ciudadanía con el fin de proteger sus datos personales, garantizar su privacidad y derecho a la autodeterminación informativa.

Es aplicable a los particulares, tanto personas físicas o morales que lleven a cabo el tratamiento de datos personales, excepto por lo que hace a las sociedades de información crediticia y a las personas que llevan a cabo la recolección y almacenamiento de datos personales para uso exclusivamente personal, por tanto, si bien no resulta aplicable al sector público, si a los PSC en los servicios que prestan como son: la emisión de certificados digitales, sellos digitales de tiempo, constancias de conservación de mensajes de datos y digitalización de documentos en soporte físico y por ello la importancia de su mención.

2.2.3 Norma Oficial Mexicana NOM-151-SCFI-2016, Requisitos que deben observarse para la conservación de mensajes de datos y digitalización de documentos (cancela la NOM-151-SCFI-2002).

La NOM 151, fue publicada en el Diario Oficial de la Federación el 30 de marzo de 2017 y en ésta se establecen los requisitos que se deben observar para

la digitalización de documentos y conservación de mensajes de datos cuando éstos sean utilizados por los comerciantes en actos de comercio que estén relacionados con sus negocios.

Por tanto, es importante resaltar que esta norma refiere a servicios que pueden ser prestados por los PSC y es de aplicación obligatoria para los comerciantes que conserven mensajes de datos, así como que lleven a cabo la digitalización de documentación relacionada con sus negocios, respecto al sector público dependerá de lo establecido en la legislación aplicable, que como se observó en el caso del marco jurídico correspondiente a la APF si se señala su aplicación por lo que hace a la conservación de mensajes de datos, ya que, en definitiva se trata de servicios que son fundamentales en la implementación de trámites en línea.

2.4. La firma electrónica y los servicios de confianza

Como se ha observado, dentro del impulso del uso de medios electrónicos para la implementación de trámites y servicios en línea en la APF, la firma electrónica y los servicios de confianza han cobrado un papel relevante en las transacciones realizadas por medios electrónicos, ello porque se requiere contar con elementos que además de agilizar los procesos y mejorar la gestión pública para lograr una mayor participación y acercamiento al ciudadano, permitan garantizar la certeza y validez jurídica de los actos administrativos.

Por ello, en este apartado se abordarán los aspectos relativos a la firma electrónica, tanto su concepto, como su funcionamiento y aplicación; en primer término, resulta fundamental comprender lo que se entiende por firma autógrafa, así como su finalidad y alcance.

Al respecto, la Real Academia de la Lengua Española señala que la firma es:

“1.f. Nombre y apellidos escritos por una persona de su propia mano en un documento, con o sin rúbrica, para darle autenticidad o mostrar la aprobación de su contenido.

2.f. Rasgo o conjunto de rasgos realizados siempre de la misma manera, que identifican a una persona y sustituyen a su nombre y apellidos para aprobar o dar autenticidad a un documento”.⁸⁸

En los conceptos antes referidos se pueden observar dos elementos primordiales que expresa el autor con su firma: por un lado, la aprobación del contenido y por otro incluso la autenticidad del documento. De esta manera, la firma autógrafa puede ser entendida también como “la declaración de la voluntad y consentimiento plasmada mediante signos a puño y letra.”⁸⁹

Es decir son “trazos, letras o signos que un sujeto estampa con su puño y letra en un documento para asegurar de forma expresa y escrita su voluntad o autoría como firmante en el acto jurídico⁹⁰. Es así que se puede señalar que sirve para acreditar el consentimiento o autorización del autor en relación con la información escrita.⁹¹

Como se puede observar la firma autógrafa se expresa a puño y letra y su función primordial es vincular al autor con el contenido de un documento para expresar su consentimiento, y, por tanto, la firma electrónica debe cumplir con estas mismas funciones.

Aunado a lo anterior, de acuerdo con el Doctor Reyes Krafft, se pueden encontrar elementos formales y materiales en la firma, los primeros se refieren a los procedimientos utilizados para firmar, es decir, la concepción de plasmarla de puño y letra que se señaló previamente, así como el elemento intencional de asumir el contenido del documento firmado, lo cual puede ser sustituido por medios electrónicos; por otra parte, los elementos funcionales que se refieren a la función

⁸⁸ Real Academia Española, <https://dle.rae.es/firma?m=form>

⁸⁹ Covarrubias Llamas, Jersain, Perdiendo El Miedo A Las Firmas Electrónicas (Losing the Fear of Electronic Signatures), *Paradigma Judicial Revista Virtual Incluyente*, México, 2020, p.12

⁹⁰ Mena Escobar Gustavo y Portillo Arroyo Julio César, “La Firma Electrónica”, p.27 http://www.fd.uach.mx/noticias/2020/08/10/LJ49_2.pdf

⁹¹ Del Río, Agustín Cernuda, “Firma Electrónica”, *III Jornadas Internacionales sobre comercio electrónico*, Universidad de Oviedo, 2002. p. 1

de identificación que tiene la firma y la autenticación donde el autor expresa su contenido y hace propio el mensaje.⁹²

Los elementos formales y materiales antes señalados pueden ser cubiertos también por medios electrónicos⁹³, por ello, resulta aplicable el principio de equivalencia funcional mencionado en la Ley Modelo de la CNUDMI sobre firmas electrónicas. Aunado a lo anterior, algunos autores consideran que además de los elementos anteriores, la firma electrónica proporciona adicionalmente también el elemento de integridad.⁹⁴ No obstante, es importante considerar que no es su función principal.

Además, no todos los tipos de firma proporcionarían este elemento; en el caso de la Firma Electrónica Avanzada o Fiable sí se incorpora la integridad y autenticidad, ello en razón de la tecnología que utiliza y debido a la intervención de un tercero de confianza, no obstante que en algunos otros tipos firmas electrónicas se debe determinar que se trata de un mecanismo fiable, para que se pueda considerar que cumple con estos principios.⁹⁵

Ahora bien, ¿qué es la firma electrónica? De acuerdo con el artículo 89 del Código de Comercio Electrónico, la firma electrónica es:

“...Firma Electrónica: Los datos de forma electrónica consignados en un Mensaje de Datos, o adjuntados o lógicamente asociados al mismo por cualquier tecnología, que son utilizados para identificar al Firmante en relación con el Mensaje de Datos e indicar que el Firmante aprueba la información contenida en el Mensaje de Datos, y que produce los mismos efectos jurídicos que la firma autógrafa, siendo admisible como prueba en juicio...”

⁹² Reyes Krafft, Alfredo Alejandro, “La firma electrónica y las entidades de certificación”, *Tesis de Doctorado, Universidad Panamericana*, México, 2004, pp. 160 y 161

⁹³ Reyes Krafft, Alfredo Alejandro, “La firma electrónica”, *Razón y palabra*, México, p. 13

⁹⁴ *Ibidem*, p.13

⁹⁵ Rincón Cárdenas, *op cit.*, p.56

El concepto antes referido incorpora diversos principios de los ya analizados en las Leyes Modelos como es el de equivalencia funcional, cuando se establece que produce los mismos efectos jurídicos que la firma autógrafa; el de neutralidad tecnológica, cuando señala que puede ser a través de cualquier tecnología y además se pueden observar las funciones fundamentales: la vinculación del firmante con el mensaje de datos y su aprobación respecto a la información contenida en el mismo.

Es de destacar que en este concepto no se incorporan elementos como el de la integridad⁹⁶ y autenticidad del mensaje de datos, ya que como se mencionó previamente éstos no son funciones propias de la firma. No obstante, si se identifican funciones esenciales en una firma, las cuales son: “identificar a una persona, proporcionar certidumbre en cuanto a su participación personal en el acto que firma; y vincular a esa persona con el contenido de un documento”.⁹⁷

La firma electrónica también es asociada a procesos de autenticación, y al respecto, también es importante señalar que no es lo mismo hablar de autenticación⁹⁸, como mecanismo de identificación en sistemas de información, para lo cual puede ser utilizada la firma electrónica, que de ésta como mecanismo de consentimiento en medios electrónicos.⁹⁹ La primera se encuentra relacionada con el acceso y el perfil que puede tener un usuario en un sistema de información, es decir, se trata de garantizar que el usuario es quien dice ser y que cuenta con los permisos correspondientes para garantizar lo que está solicitando¹⁰⁰ y por otra parte,

⁹⁶ Concepto referente a que la información no fue alterada. Reyes Krafft, Alfredo Alejandro, “, *op cit.*, p.24

⁹⁷ CNUDMI, 2002, *op cit.* p. 23

⁹⁸ La autenticación es un paso dentro del proceso de Identificación-Autenticación en el que se determina si un usuario o entidad puede tener acceso a un sistema o recurso. Rodríguez Valdés, Osviel y Legón, Carlos M, *et al.*, “Seguridad y usabilidad de los esquemas y técnicas de autenticación gráfica” *Revista Cubana de Ciencias Informáticas*, 2018, vol. 12, p. 14

⁹⁹ Rincón Cárdenas, *op cit.*, p.52

¹⁰⁰ Red de Gobierno Electrónico de América Latina y el Caribe, Organización de los Estados Americanos, Banco Interamericano de Desarrollo, Centro de Investigación para el desarrollo Internacional, “e gobierno y autenticación de identidad”, *Boletín e-Gobierno Red GEALC*, 2015, 108 edición, p.2

se encuentra su uso fundamental relacionado con el consentimiento de la persona y su vinculación con el contenido de un documento.

Así pues, se pueden encontrar distintos tipos de firma como son: i) Basadas en sistema de criptografía¹⁰¹ ya sea asimétrica, en las cuales se realiza la asignación de dos claves, una privada y otra pública relacionadas entre sí o simétrica, en cuyo caso, tanto el que codifica como el que descifra usa la misma llave; ii) Basadas en dispositivos biométricos, la identificación se realiza por características físicas; iii) Números de identificación personal; iv) Uso de contraseñas para autenticar mensajes de datos; v) Uso de tarjetas inteligentes.¹⁰²

En este orden de ideas, es muy importante considerar que estos diversos tipos de firma son reconocidos en nuestra legislación y tienen validez jurídica, por lo que para determinar su uso se deberá considerar el nivel de seguridad, características del sistema y alcance que se le pretende dar, es decir, si solo es para expresar el consentimiento o en su caso si también se busca la integridad y la conservación del mensaje de datos, así como, si adicionalmente se requiere como un mecanismo de autenticación en un sistema de información.

Específicamente, en la reforma publicada en el año 2000 al Código de Comercio señalada en el capítulo pasado se incorporaron dos especies de firma: la firma electrónica en los términos que se definió en párrafos anteriores y la firma electrónica avanzada, respecto a la cual el artículo 97 del Código de Comercio establece las características con las que debe contar para ser considerada Avanzada o Fiable las cuales son las siguientes:

“Artículo 97.- Cuando la ley requiera o las partes acuerden la existencia de una Firma en relación con un Mensaje de Datos, se entenderá

¹⁰¹ “La criptografía es la ciencia que se ocupa de transformar mensajes, utilizando algoritmos matemáticos, para cifrar datos con el fin de hacerlos incomprensibles para cualquiera que no posea su clave, que debe ser privada, con la información secreta”. García Barrera, Myrna Elia, “El documento y la firma electrónica, temas centrales de derecho a las nuevas tecnologías”, en Derecho de las Nuevas Tecnologías, UNAM, *Instituto de Investigaciones Jurídicas*, México, 2008, p.137.

¹⁰² Robles Farias, Diego, *op cit.*, pp.559, 560 y 561

satisfecho dicho requerimiento si se utiliza una Firma Electrónica que resulte apropiada para los fines para los cuales se generó o comunicó ese Mensaje de Datos.

La Firma Electrónica se considerará Avanzada o Fiable si cumple por lo menos los siguientes requisitos:

I. Los Datos de Creación de la Firma, en el contexto que son utilizados, corresponden exclusivamente al Firmante;

II. Los Datos de Creación de la Firma estaban, en el momento de la firma, bajo el control exclusivo Firmante;

III. Es posible detectar cualquier alteración de la Firma Electrónica hecha después del momento de la firma, y

IV. Respecto a la integridad de la información de un Mensaje de Datos, es posible detectar cualquier alteración de ésta hecha después del momento de la firma.

Lo dispuesto en el presente artículo se entenderá sin perjuicio de la posibilidad de que cualquier persona demuestre de cualquier otra manera la fiabilidad de una Firma Electrónica; o presente pruebas de que una Firma Electrónica no es fiable”.

Para comprender lo antes señalado resulta fundamental entender el alcance del concepto Datos de Creación de la Firma Electrónica también contemplado en el artículo 89 del Código de Comercio, el cual lo define como “Son los datos únicos, como códigos o claves criptográficas privadas, que el Firmante genera de manera secreta y utiliza para crear su Firma Electrónica, a fin de lograr un vínculo entre dicha Firma Electrónica y el Firmante”.

Es así, que firma electrónica avanzada tiene incorporados dos de los principios ya integrados también en la firma electrónica simple, el de equivalencia funcional al establecer que tiene los mismos efectos que la firma autógrafa, así

como, el de neutralidad tecnológica al referir que puede realizarse a través de cualquier tecnología y que cualquier persona puede demostrar la fiabilidad de una firma electrónica a través de cualquier otro método; adicionalmente se incorporan los principios de *no repudio*, al contemplar que estos datos de creación deben estar en exclusivo control del firmante, y el de *integridad*¹⁰³ cuando se señala que debe ser posible detectar cualquier alteración tanto de la firma como de la información del mensaje de datos.

Por su parte, el artículo 2 fracción XIII de la Ley de Firma Electrónica Avanzada señala que “es el conjunto de datos y caracteres que permite la identificación del firmante, que ha sido creada por medios electrónicos bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos, la cual produce los mismos efectos jurídicos que la firma autógrafa”.

En esta definición menciona la integridad pero referida al mensaje de datos y no a la firma, cuestión que si es contemplada en el caso de la definición que proporciona el Código de Comercio. Es así es que la firma electrónica avanzada es asociada con aquella que se crea usando un sistema de criptografía asimétrica, es decir, con una clave pública y una privada, basada en la infraestructura de llave pública PKI.

“Una PKI (Public Key Infrastructure o Infraestructura de Clave Pública) puede significar métodos, tecnologías y técnicas que juntas proveen de una infraestructura segura”. Por otro lado, puede significar el uso de claves públicas y privadas para autenticarse y verificación de contenido. Una infraestructura de PKI debe ofrecer a los usuarios los siguientes beneficios: - Confirmación de la integridad y calidad de la información enviada y recibida electrónicamente - Confirmación de la fuente y destino de esa información - Seguridad en el tiempo de la información - Confirmación de la privacidad de la información”.¹⁰⁴

De manera que, en el caso de la criptografía asimétrica se generan dos claves asociadas a una persona, una pública y una privada, la primera es conocida

¹⁰³ Davara Isabel, *op cit.*, p.385

¹⁰⁴ Reyes Krafft, Alfredo Alejandro, *op cit.*, p.24

y puede ser verificada por cualquier persona y la segunda solo queda en poder del titular y ambas son relacionadas matemáticamente. Del mismo modo, a través de la llave privada, se encripta la información del mensaje de datos y por ello solo quien cuente con la llave pública puede descifrar el mensaje codificado.¹⁰⁵ Para otorgar estas claves se debe realizar previamente un proceso donde la persona es plenamente identificada, e incluso puede ser realizada una identificación biométrica, que es considerada como el tercer nivel en los métodos de identificación.¹⁰⁶

Al respecto, es conveniente señalar los tres niveles de identificación que pueden distinguirse: i) El primero, es algo que se sabe, es decir, se presume que únicamente la persona identificada lo sabe como es el caso de una contraseña o PIN; ii) algo que se tiene, como una tarjeta de crédito; y iii) algo que es, por tanto, consiste en la verificación de los rasgos físicos de cada persona, como la huella.¹⁰⁷

Por tanto, en un sistema basado en claves, se utiliza generalmente un nivel de identificación de tercer nivel, con lo cual se garantiza la plena identificación del titular al que se le entregan el par de claves, sin embargo, corresponderá al mismo la adecuada custodia de la clave privada¹⁰⁸. Ahora bien, la clave propiamente dicha puede considerarse como algo que se tiene de acuerdo con los niveles previamente revisados y la contraseña o PIN que también se requiere en un proceso de firma, como algo que se sabe, es decir, se combinan dos niveles de identificación.¹⁰⁹ De ahí su nivel de seguridad.

Este proceso de identificación, se lleva a cabo a través de autoridades certificadoras, es decir, una tercera parte de confianza debe realizar la vinculación de la persona debidamente identificada con un par de claves, es así, que durante

¹⁰⁵ García Barrera Myrna Elia, *op cit.*, pp.138 y 139

¹⁰⁶ Muñoz Soro, José Félix, "Identificación y autenticación en la Ley de Administración electrónica", *Fundación Democracia y Gobierno Local*, 12, 2010, p.171.

¹⁰⁷ *Idem*

¹⁰⁸ García Barrera Myrna Elia, *op cit.*, p.167

¹⁰⁹ Muñoz Soro, José Félix, " , *op cit.* pp. 171 y 172

este proceso emite un certificado que liga la clave privada con el sujeto del certificado y confirma que éste es el que tiene dicha clave privada.¹¹⁰

En la legislación federal mexicana se contemplan tres autoridades certificadoras que pueden llevar a cabo este proceso: la Secretaría de Economía, el Servicio de Administración Tributaria y la Secretaría de Función Pública y adicionalmente terceros que son acreditados por la Secretaría de Economía denominados PSC, respecto a éstos últimos el artículo 104 del Código de Comercio establece que deben comprobar la identidad de los solicitantes utilizando cualquiera de los medios admitidos en derecho.

Con el proceso antes referido, la firma cumpliría esencialmente con dos fines: i) la función de identificación del emisor, ya que las claves privadas son irrepetibles y solo la persona a la que le fue generada podría utilizarla; y ii) la función declarativa, que permite la vinculación del emisor con el mensaje de datos.¹¹¹

En consecuencia, lo que el firmante cifra con su clave privada, es un “resumen” del documento a través de un *hash* que permite obtener de los datos totales del documento solo una longitud del mismo la cual constituirá el resumen, lo fundamental de ello, es que el valor del hash se modifica con cualquier cambio por mínimo que ésta sea de los datos totales del documento, por tanto, con ello, puede garantizarse la integridad.¹¹² Por lo que podría decirse que la firma electrónica constituye “el resumen del documento cifrado con la clave del firmante”.¹¹³

Derivado del proceso antes referido se puede observar que una de las diferencias que tiene la firma electrónica avanzada con la firma electrónica simple es que en la primera se realiza un proceso previo de identificación a través del proceso de enrolamiento antes señalado, además de que se garantiza el momento en que fue realizada, ello debido a la integración de un sello digital de tiempo que se detallará más adelante y con ello se logra también la integridad de la firma y del documento. No obstante, si bien a través de este proceso se puede garantizar el

¹¹⁰ García Barrera Myrna Elia, *op cit.*, p.162

¹¹¹ *Ibidem*, p.141

¹¹² Muñoz Soro, José Félix, *op cit.*, p. 174

¹¹³ *Ibidem*, p.175

control que se debe tener en la generación de la firma, elemento que se requiere para que, pueda ser considerada como fiable, también es fundamental que el titular resguarde debidamente los certificados.

En este tipo de proceso de firma participan principalmente tres sujetos: i) el tercero de confianza que sería la autoridad certificadora; ii) el titular del certificado y iii) el usuario o persona que confía en el certificado, el cual es definido por el Código de Comercio como “la persona que, siendo o no el Destinatario, actúa sobre la base de un Certificado o de una Firma Electrónica”, y en este sentido, este último, es responsable de verificar la fiabilidad de la firma electrónica, la vigencia del certificado y considerar cualquier limitación del uso del certificado, como revocación y suspensión, por lo que debe existir plena confianza en la seguridad de la información.¹¹⁴

Por su parte, como se señaló previamente las autoridades de certificación son las encargadas de vincular la clave pública con el firmante y con ello garantizar la asociación de la persona física con su clave pública, por ello la importancia de la fiabilidad del método.¹¹⁵ Es importante señalar que para demostrar que determinado método de firma es fiable no necesariamente se requiere demostrar la integridad de todo el documento.

Visto lo anterior, tanto la firma electrónica como la firma electrónica avanzada tienen validez jurídica y cumplen con el principio de equivalencia funcional, por ello, cuando se utiliza un sistema de firma para probar su autenticidad se requieren revisar distintos elementos: 1) del método de firma utilizado; 2) que permitan probar que ese método es confiable para el tipo de transacción; y 3) que el método es apropiado para el tipo de transacción.¹¹⁶

Si bien, la firma electrónica simple pudiera garantizar ciertas cuestiones de seguridad, es muy importante homologar los procesos en la APF a efecto de lograr la interoperabilidad de los sistemas y con ello poder generar información de valor tanto para el sector público como para el privado que mejore la implementación de

¹¹⁴García Barrera Myrna Elia, *op cit.*, pp.166 y 167

¹¹⁵ Del Río, Agustín Cernuda, *op cit.*, p. 3

¹¹⁶ Rincón Cárdenas, *op cit.*, p.48

políticas públicas, así como para facilitar los trámites que realiza la ciudadanía, sin exigir datos y requisitos que ya han sido presentados al gobierno, independientemente de las facultades y ámbito de actuación de cada dependencia, lo anterior representa importantes retos tanto tecnológicos, como jurídicos y organizacionales para el sector público.

Por lo anterior, en los trámites del gobierno, se ha impulsado el uso de la firma electrónica avanzada, pero vale la pena cuestionarse algunos elementos fundamentales ¿realmente es necesaria en todos los casos?, ¿la firma electrónica simple pudiera dotarnos de las mismas características que se requieren? ¿puede representar una barrera para los ciudadanos que no cuentan con la misma?

Podríamos decir que en la implementación de estos trámites solo deben exigirse las garantías y medidas de seguridad adecuadas a la naturaleza y circunstancias del caso.¹¹⁷ Ello es considerado en un principio que se incorporó en la Ley 11 2007 de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos de España¹¹⁸ actualmente derogada pero que resulta sumamente útil para entender el alcance, que es el de proporcionalidad y busca que no se incorporen medidas de seguridad excesivas que resulten en un costo mayor para la ciudadanía o que puedan incluso segmentar a la población, ya que es fundamental buscar un equilibrio entre mantener la seguridad y los principios de validez y certeza jurídica y la facilidad de uso.¹¹⁹

Aunado a lo anterior, en este tipo de trámites vale la pena mencionar otros elementos que pueden ser considerados como son: los sellos digitales electrónicos y en su caso las constancias de conservación de mensajes de datos. Por otra parte, también se pueden encontrar los códigos de verificación, sobre todo en los actos administrativos que se emiten de forma automatizada, como pueden ser las copias; con éstos se puede corroborar la validez del documento cuando se introduce el código de verificación, lo cual facilita a la ciudadanía este proceso.¹²⁰

¹¹⁷ *Ibidem*, p. 181

¹¹⁸ Puede consultarse en: <https://www.boe.es/buscar/act.php?id=BOE-A-2007-12352>

¹¹⁹ Muñoz Soro, José Félix, “*op cit.*”, p.195

¹²⁰ *Ibidem*, p.187

Por lo que hace a los sellos digitales de tiempo (time stamping), “son documentos electrónicos, firmados, por una autoridad del sellado de tiempo, que vinculan un momento determinado con un documento a través del resumen *hash* del mismo. De esta manera, se incorporan a los acuses de recibo para garantizar el momento en que se produjo la recepción de un documento.”¹²¹

“El sellado digital de tiempo es un mecanismo informático seguro que permite certificar y demostrar que existió cierta información, derivada de un acontecimiento en un instante muy preciso en el tiempo, logrando el “no repudio.

...

En este sentido sería la manera más adecuada de dar certeza de que un mensaje de datos se generó en un momento y espacio precisos”.¹²²

El Código de Comercio, lo define como:

“**Sello digital de tiempo**: el registro que prueba que un dato existía antes de la fecha y hora de emisión del citado Sello, en los términos que se establezca en la norma oficial mexicana sobre digitalización y conservación de mensaje de datos que para efecto emita la Secretaría”.¹²³

Al respecto, se han creado estándares específicos para distintos temas en el desarrollo tecnológico, uno de ellos son los RFC¹²⁴ y específicamente para el caso de sellos digitales de tiempo se encuentra el RFC3161 cuya finalidad es la siguiente.

¹²¹ *Ibidem*, p. 194

¹²² Sierra, Israel Becerril, “El Sello Digital de Tiempo: Optimización de la tecnología aplicada al tiempo”, *Repositorio Universitario de la DGTIC, UNAM*, México, 2013., p. 5

¹²³ Código de Comercio, artículo 89

¹²⁴ Los RFC por sus siglas en inglés *Request for Comments* son resultado de la búsqueda de estandarización y la interoperabilidad y tienen como idea fundamental detallar las especificaciones

“definir un formato que integre evidencias para dar certeza de la existencia de un documento electrónico en un momento preciso, o del momento en el que su firma electrónica existió.

...

este RFC propone, un protocolo estándar de suma importancia porque cuenta con los atributos de certificación y precisión del momento en que sucede un hecho o evento en particular. Se trata de las mejores prácticas que reúnen el conocimiento de expertos para definir las reglas que ayudarán a la gestión del tiempo en la sincronización del mismo haciendo uso de relojes atómicos a fin de obtener medidas de tiempo tan precisas que solo la mala fe, dolo, fraude o violencia podrían alterar.”

Para la generación del sello digital de tiempo de acuerdo con las características del estándar antes referido, se debe llevar a cabo el procedimiento siguiente¹²⁵: i) el sistema cliente debe obtener el “hash” que es el resumen digital del documento electrónico; ii) dicho hash sirve para generar una solicitud de sello digital de tiempo que es enviada al sistema servidor que es la Autoridad de Sello de Tiempo (TSA-por sus siglas en inglés Time Stamping Authority) a la cual le es emitido un certificado para construir el sello digital de tiempo; iii) posteriormente, el sistema servidor recibirá la solicitud de sellos digital de tiempo y la usará para solicitar la hora oficial al reloj atómico; iv) este último devuelve la hora oficial en formato UTC; v) la Autoridad de Sellado de Tiempo generará la estructura conforme al RFC señalado, para lo cual necesitará la información del certificador, el “hash” y la hora oficial que se obtuvo en los pasos previos; vi) por último, la estructura que se obtuvo deberá ser firmada por la Autoridad de Sellado de tiempo, para lo cual se requerirá la clave privada asociada al certificado.

de los protocolos usados en internet de manera abierta y gratuita para su libre adopción, se realizan a través de la IETF *Internet Engineering Task Force* por sus siglas en inglés. *Ibidem*, p. 7

¹²⁵ *Ibidem*, p.5

De esta manera, el sello digital de tiempo cumple una función primordial para determinar que un determinado acto existió en la fecha y hora que se ha generado y por tanto, en conjunto con la firma electrónica logran la integridad del documento. En concordancia con lo anterior, la Ley Modelo de la CNUDMI sobre Firmas Electrónicas señala que “la firma numérica correspondiente a un mensaje, ya sea creada por el tenedor de un par de claves para autenticar un mensaje o por una entidad certificadora para autenticar su certificado, deberá contener por lo general un sello cronológico fiable para que el verificador pueda determinar con certeza si la firma numérica fue creada durante el “período de validez”.¹²⁶

Por su parte, el Código de Comercio, no señala una definición de constancia de conservación de mensajes de datos, sin embargo, las características que debe cumplir se pueden encontrar en la NOM 151.

Al respecto, Norma Oficial Mexicana NOM-151-SCFI-2002, Requisitos que deben observarse para la conservación de mensajes de datos y digitalización de documentos, actualmente ya derogada, se señalaba que su objetivo fundamental era establecer los requisitos para la conservación del contenido de mensajes de datos para los comerciantes y en ésta solo se refería a la Constancia del PSC como “al mensaje de datos representado en formato ASN.1 conforme al Apéndice de la presente Norma Oficial Mexicana”.

Por su parte en la MIR de alto impacto con análisis de riesgo y análisis de impacto en la competencia¹²⁷ referente al Anteproyecto de Norma Oficial Mexicana NOM-151-SCFI-2002, Requisitos que deben observarse para la conservación de mensajes de datos y digitalización de documentos, se señaló que ésta debía ser observada por todos los comerciantes que conservaran mensajes de datos o digitalizaran documentos, además dentro de la justificación para su expedición, se argumentó que se requería expedir para contar con los elementos de seguridad que deben ser utilizados en los mensajes de datos que se deben conservar por períodos prolongados de tiempo para garantizar su integridad y autenticidad y se señaló que

¹²⁶ CNUDMI, 2002, *op cit.*, 32

¹²⁷ Puede consultarse en: <https://cofemersimir.gob.mx/mirs/41426/pdf>

específicamente derivaba del caso de los documentos que deben conservar los comerciantes por un período mínimo de diez años.

Asimismo, refirió diversos estándares respecto a la regulación en otros países, a propósito cabe destacar que en éstos se resalta el uso autoridades de sellado de tiempo y firma electrónica.¹²⁸ Posteriormente, el 30 de marzo de 2017, se publicó en el Diario Oficial de la Federación la NOM 151; en la cual se detallaron los elementos técnicos que debería tener la constancias de conservación y específicamente se refirió que la solicitud y la formación de la solicitud de la constancia se debería efectuar conforme a la especificación descrita en el RFC 3161 y seguir el formato ASN.1

Por otra parte, para que puedan materializarse los trámites en línea es importante contar con un “Sistema de Información”, el cual es definido en la Ley Modelo de la CNUDMI sobre Comercio Electrónico como “todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna otra forma mensajes de datos”.¹²⁹

Derivado de lo que se ha observado en el presente capítulo este sistema, el envío de mensajes y los propios mensajes de datos deben cubrir y garantizar diversas características, como lo es la integridad, la originalidad, accesibilidad, fiabilidad, y en su caso garantizar el consentimiento del contenido de la información contenida en los mensajes de datos, lo cual permitirá a su vez el no repudio y con ello lograr la equivalencia funcional de los trámites realizados en medios electrónicos a los realizados en papel.

Al respecto, cabe destacar lo que se ha referido de la Ley Modelo de la CNUDMI sobre Comercio Electrónico que menciona que se entenderá que cumple con el requisito de la originalidad cuando existe alguna garantía de que se ha conservado la integridad de la información a partir del momento en que se generó por primera vez.¹³⁰

¹²⁸ Manifestación de Impacto Regulatorio. NOM 151 2017. <https://cofemersimir.gob.mx/mirs/53491>

¹²⁹ CNUDMI, Ley Modelo de la CNUDMI sobre Comercio Electrónico, Nueva York, Naciones Unidas, 1999, p. 4

¹³⁰ CNUDMI, 1999, *op. cit.*, p.5

Aunado a lo anterior, se debe considerar que la información se ha mantenido íntegra si ha permanecido completa e inalterable, es decir, que no ha sufrido ninguna modificación.¹³¹ Por su parte, la misma Ley Modelo señala las características que deben considerarse para la conservación de mensajes de datos las cuales ya fueron descritas en el apartado correspondiente.

Otro principio fundamental es el “No repudio” el cual permite “identificar y vincular a las personas que han aceptado o expresado su consentimiento para obligarse al contenido del mensaje de datos, sin que puedan repudiar su consentimiento ni el propio contenido de mensaje de datos”.¹³²

Aunado a lo anterior, se encuentra la fiabilidad, la cual indica que todo el proceso desde que se generó el mensaje de datos fue fiable¹³³. Por último, se puede hablar de la “accesibilidad /disponibilidad que es aquella característica que ratifica que la información puede ser localizada, presentada y mostrada ante las autoridades o ante quienes tengan derecho a ello en el momento que se requiera”.¹³⁴

Además, será fundamental considerar en todo momento los principios de seguridad de la información que son la confidencialidad, integridad y disponibilidad y que serán desarrollados en el apartado Seguridad de la Información del capítulo 4.

Finalmente, como se puso observar en el presente capítulo, se cuenta con un marco jurídico tanto internacional como nacional para implementar trámites en línea con la validez jurídica necesaria; en el marco jurídico nacional si bien hay elementos que pudieran mejorarse, se considera que otorgan un marco general adecuado y suficiente para lograr esta implementación de forma adecuada considerando los distintos elementos que se detallaron previamente.

¹³¹ Gamboa Montejano, Claudia, “Firma Electrónica Avanzada, Análisis de la Iniciativa presentada por el Ejecutivo Federal, Derecho Comparado y Opiniones Especializadas del tema”, Dirección de Servicios de Investigación y Análisis de la Cámara de Diputados, México, 2011, p.9

¹³² Davara Isabel., *op cit.*, p. 741

¹³³ *Ibidem* p.740

¹³⁴ *Ibidem* p.739

Capítulo 3.

Análisis comparativo de gobierno electrónico y la implementación de trámites en línea en los países de Alianza del Pacífico



Capítulo 3. Análisis comparativo de gobierno electrónico y la implementación de trámites en línea en los países de Alianza del Pacífico

La Alianza del Pacífico es una iniciativa regional y económica entre cuatro países: México, Perú, Chile y Colombia, en la cual, se conforman grupos relacionados en temas como facilitación del comercio, cooperación aduanera, pymes, reconocimiento transfronterizo de firma electrónica, entre otros.¹³⁵

Los países integrantes de esta Alianza han presentado avances importantes en materia de gobierno electrónico, aunque aún tienen retos comunes, por ello, en este capítulo se analizará el estatus actual de su marco jurídico y las herramientas que cada uno ha desarrollado para poder implementar trámites en línea, para con ello, considerar los aspectos necesarios para la Guía que se desarrollará en el Capítulo 4 para México.

3.1. Colombia

Colombia ha tenido una gran evolución en materia de gobierno electrónico y en la implementación de trámites en línea. Desde 1995, ha emitido diversas leyes, decretos, planes, guías y estrategias, encaminadas a lograr la eficiencia y eficacia en el gobierno, tanto al interior del mismo como en los servicios para la ciudadanía.

Estas estrategias han ido encaminadas a mejorar los servicios a través de la simplificación administrativa, la estandarización de servicios y la interoperabilidad. Respecto a los trámites, en un primer momento empezó por establecer el envío y recepción de información por medios electrónicos para posteriormente lograr trámites completamente transaccionales. Asimismo, se ha buscado mejorar la conectividad, disminuir la brecha digital y por supuesto también lograr un gobierno abierto. Si bien se han emitido diversos documentos, la estrategia ha mantenido una

¹³⁵ Alianza del Pacífico, ¿Qué es la Alianza del Pacífico? <https://alianzapacifico.net/que-es-la-alianza/>

línea y ha permitido que las entidades públicas trabajen de forma coordinada, con un camino trazado. En este sentido, se mencionarán los principales documentos e instrumentos que se han emitido desde el año 1995 a continuación.¹³⁶

Año	Instrumento	Objeto
1995	Ley 2150	Incluye la obligación del gobierno de implementar un sistema para el envío y recepción de información para trámites. ¹³⁷
1999	Ley 527	Acorde con los cambios internacionales que se estaban realizando como es la Ley Modelo de la CNUDMI sobre Comercio Electrónico, se agrega en el marco jurídico el uso de mensajes de datos, emisión de certificados digitales y conservación de mensajes de datos.
2000	CONPES 3072	Se buscaba promover aún más la oferta de servicios públicos en línea y es en este mismo año que se crea el primer Manual de Gobierno en línea, con el cual además se empieza una estandarización de contenidos en los portales de las entidades públicas ¹³⁸ por lo que se puede considerar el punto de partida para la interoperabilidad, ya que conlleva necesariamente también el inicio de la estandarización de datos y procesos.

¹³⁶ Cardona, Diego, *et al.*, “Gobierno Electrónico en Colombia: Marco Normativo y Desempeño De Tres Índices Estratégicos (Electronic Government in Colombia: Regulatory Framework and Evaluation of Three Strategic Indexes)”, Venezuela, *Revista venezolana de Gerencia*, 2015, vol. 19, núm. 69, pp.14-19

¹³⁷ *Ibidem*, p.14

¹³⁸ *Idem*

2003	Decreto 3816	<p>A partir de éste se crea la Comisión Intersectorial de Políticas y Gestión de la Información para la Administración Pública a través de la cual se buscaba alinear las estrategias y programas de producción de información.</p> <p>De esta manera, se crea la base el Proyecto de Racionalización y Automatización de Trámites a través del cual se buscaba la estandarización, racionalización y automatización de los trámites.</p>
2005	Ley 962	<p>En esta Ley se señala que todos los trámites debían estar autorizados por el Sistema Único de Información de Trámites y se contemplaba la obligación de usar el Portal del Estado Colombiano (PEC) a través del cual se unificaba el acceso e información de los trámites y servicios del gobierno.</p>
2008	Decreto 1151	<p>Se definió una estrategia de Gobierno en Línea encabezada por el Ministerio de Comunicaciones, dicha estrategia incluía diversas fases como la de información, interacción, transacción, transformación y e-Democracia. Asimismo, estableció la elaboración de un Manual que debía facilitar a las entidades la implementación de esta estrategia, es decir, debería contener el proceso para implementar</p>

		trámites en línea y proveer trámites y servicios del Estado. ¹³⁹
2009	Ley de TIC	A través de ésta se buscaba incrementar aún más los servicios en línea a los ciudadanos. En este sentido, en 2010 se publicó el CONPES 3650 a través del cual se instauró nuevamente una estrategia de gobierno en línea que buscaba proporcionar acompañamiento para ejecutar las fases de Interacción y Transacción.
	Plan Vive Digital	Estaba enfocado a lograr la conectividad de la población y a disminuir la brecha digital.
2011	Ley 1450	Estableció la obligación a las entidades de gobierno de poner a disposición de la ciudadanía la información con la que cuentan.
	Ley 1437	Se expidió el Código de Procedimientos Administrativo y de lo Contencioso Administrativo por virtud del cual se faculta al Gobierno nacional para definir los estándares que debían cumplir las autoridades para implementar medios electrónicos en sus trámites administrativos. ¹⁴⁰
2012	Normas relacionadas con la simplificación administrativas	Se emitieron diversas normas orientadas a la eficiencia y eficacia en los servicios que se prestan a los ciudadanos.
2015	Decreto 1083	Se expidió el Decreto Único Reglamentario del Sector de Función Pública en el cual se señala

¹³⁹ Zea Hernández, Germán, “Estado del arte del gobierno electrónico en Colombia para revisar la implementación del gobierno en línea” Tesis Doctoral. Universidad de Cartagena, Colombia, 2015, p.42

¹⁴⁰ Gobierno de Colombia, Función Pública, Decreto 767 de 16 de mayo de 2022, p.1.

		que la Política de Gobierno Digital es una Política de Gestión y Desempeño Institucional, asimismo dispuso que el MinTIC debía contemplar lineamientos y estándares para lograr la integración de trámites al Portal Único del Estado Colombiano. ¹⁴¹
2018	Decreto 1008	Estableció la obligación por parte de todas las entidades públicas de implementar la Política de Gobierno Digital, así como los pasos para aplicar el Manual de Gobierno Digital. ¹⁴²
2019	Decreto 2106	Se incluyeron las normas y lineamientos para simplificar trámites administrativos ¹⁴³
2020	Ley 2052	Se establecieron disposiciones transversales para la digitalización y automatización de trámites ¹⁴⁴
2021	Resolución 500	Se crearon los lineamientos y estándares para la estrategia de seguridad digital y la adopción del modelo de seguridad y privacidad. ¹⁴⁵
2022	Resolución 460	Se expidió el Plan Nacional de Infraestructura de Datos estableciendo los lineamientos generales para su implementación. ¹⁴⁶

Cuadro 1. Marco jurídico en Colombia

Fuente: Elaboración propia con información de Cardona Diego, *op cit.*, pp.14-19, Zea Hernández, *op cit.*, p.42 y Gobierno de Colombia, *op cit.*, p. 1

¹⁴¹ *Ibidem*, p. 2

¹⁴² *Idem*

¹⁴³ *Ibidem*, p.3

¹⁴⁴ *Idem*

¹⁴⁵ *Ibidem*, p.4

¹⁴⁶ *Idem*

Ahora bien, en virtud del Decreto 1008 de 2018¹⁴⁷ antes referido, por virtud del cual se establecen los lineamientos generales de la Política de Gobierno Digital, el MinTIC desarrolló un Manual de Gobierno Digital¹⁴⁸, en el cual se resaltan los retos a los que tienen que enfrentarse las entidades, relacionados por un parte, con lograr la satisfacción real de necesidades y al mismo tiempo con garantizar la protección de los derechos humanos de la ciudadanía.

Asimismo, se menciona algo sumamente trascendente acerca de que el gobierno electrónico ya no trata solo de automatizar procesos y de atender la provisión de trámites y servicios a la ciudadanía, sino de generar valor público, por tanto, en la visión de gestión pública desde esta perspectiva el Estado ya no diseña los servicios para el ciudadano, sino que éstos participan en el diseño.¹⁴⁹

En este orden de ideas, el Manual plantea como se debe implementar la Política de Gobierno Digital, la cual busca una profunda interacción y participación de los ciudadanos, desde el enfoque donde se genere valor público por todos los actores incluyendo la ciudadanía.¹⁵⁰

Ahora bien, el Manual refiere que uno de los primeros pasos que las entidades públicas deben seguir en la implementación de proyectos con el uso de TICs, es el definir la necesidad asegurando la generación de valor para los usuarios, para ello establece los pasos siguientes:

1. **Se debe identificar el problema o necesidad y los actores relacionados con el proyecto:** en este paso se señala que la entidad debe cuestionarse diversos aspectos como son: ¿cuál es la necesidad o problemática concreta que se quiere resolver? ¿cómo el uso de la

¹⁴⁷ Puede consultarse en:

<https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=86902#:~:text=Lineamientos%20y%20est%C3%A1ndares%20de%20la,la%20Pol%C3%ADtica%20de%20Gobierno%20Digital.>

¹⁴⁸ Puede consultarse en: <https://gobiernodigital.mintic.gov.co/portal/Politica-de-Gobierno-Digital/Manual-de-Gobierno-Digital/>

¹⁴⁹ Gobierno de Colombia. Ministerio de Tecnologías de la Información y las Comunicaciones. Viceministerio de Economía Digital Dirección de Gobierno Digital, 2018, Manual de Gobierno Digital, p.10

¹⁵⁰ Puede consultarse en: <https://gobiernodigital.mintic.gov.co/portal/Politica-de-Gobierno-Digital/>

tecnología apoya o provee la solución a la problemática o necesidad identificada? ¿quiénes son los actores relevantes que están relacionados con el proyecto o iniciativa planteada? ¿cuáles son sus características, intereses, necesidades, posibilidades y limitaciones?

Además, realiza sugerencias específicas respecto a las técnicas que se podrían emplear para identificar a los actores relevantes como son: entrevistas individuales, grupos focales, encuestas, paneles de expertos, reuniones con grupos de interés.

2. **Identificar y analizar información y datos proactivamente:** señala como consideraciones indispensables el recolectar datos e información relevante para el diseño y desarrollo de productos o servicios, con el objetivo de identificar previamente las necesidades e intereses de los ciudadanos.
3. **Evaluar la aplicación de metodologías de innovación:** se enfatiza la necesidad de identificar cuando una solución ha sido usada tradicionalmente y no ha logrado resolver la problemática
4. **Aplicar directrices de inversión inteligente:** se resaltan los criterios que se deben seguir considerando el costo/beneficio, utilidad, calidad, necesidad de modernización tecnológica y evaluación.

Como siguiente paso, señala la importancia de contar con la participación de todos, asegurando el respaldo de la alta dirección, posteriormente, refiere la importancia de diseñar integralmente el proyecto, para lo cual será fundamental incorporar a los usuarios en el desarrollo de todas sus etapas desde el diseño hasta la ejecución del proyecto.

Aunado a ello, se resalta la importancia de garantizar el cumplimiento de los requisitos de interoperabilidad, seguridad y privacidad de la información, accesibilidad y usabilidad, apertura (relativo a la necesidad de contar con sistemas de información que permitan la generación de datos abiertos de manera automática para su publicación, uso y reutilización), acceso a través de diferentes dispositivos y un esquema de conocimientos, uso y apropiación para un óptimo funcionamiento

digital, en este aspecto también se incluye la importancia de garantizar que el proyecto sea ambientalmente sostenible.

Por último, se señala que la entidad debe llevar a cabo las acciones necesarias para permitir una adecuada ejecución, seguimiento y retroalimentación del proyecto para evaluar si realmente satisface las necesidades que se identificaron en la etapa inicial.

Respecto a sus anexos uno que resulta fundamental ya que sus aspectos serían plenamente aplicables a los trámites en línea es el denominado “servicios ciudadanos digitales” con este se busca proporcionar herramientas y capacidades a las entidades para facultar el acceso a los ciudadanos a los servicios ofrecidos por la administración pública por medios electrónicos y básicamente se señalan los siguientes:¹⁵¹

- **Servicio de interoperabilidad:** lo que busca es que haya sistemas unificados que permitan la interacción y comunicación entre los sistemas de las entidades, a través de éste se le dan recomendaciones, principios y directrices a las entidades para que adquieran las capacidades para lograr esta comunicación.
- **Servicios de autenticación electrónica:** proporciona mecanismos para la validación electrónica y además para poder utilizar la firma electrónica, dentro de los pasos que deben seguir las dependencias uno que consideramos sumamente interesante es que las entidades deben avisar a los ciudadanos previo a la implementación de los servicios, para que éstos puedan estar preparados en el momento en que se inicien a utilizar estos mecanismos en los trámites o servicios.
- **Servicios de carpeta ciudadana:** a través de ésta se pueden almacenar y conservar los mensajes de datos en la nube, asimismo proporciona una plataforma para realizar las notificaciones electrónicas, la cual cabe destacar es de uso obligatorio.

¹⁵¹ *Ibidem* p.61-67

En 2022, Colombia expidió el Decreto 767 de 16 de mayo de 2022, donde renueva su Política de Gobierno Digital, en esta resalta la importancia de promover el valor público a través de la transformación digital del Estado. En este sentido se establecen diversos principios, habilitadores y líneas de acción. Asimismo, se contempla la obligación del MinTIC de publicar lineamientos, guías y estándares para facilitar la comprensión e implementación de esta Política; en particular se señala que todo lo anterior debe estar contenido en el Manual de Gobierno Digital¹⁵², el cual a diferencia de su versión anterior debe ser interactivo, además se establece que éste debe tener una Caja de Transformación Institucional Digital con herramientas prácticas para facilitar la aplicación de las guías, lineamientos y estándares.

En el mismo año, expidió el Decreto 088 del 24 de enero de 2022, en el cual se reglamentan las disposiciones de la Ley 2052 de 2020, por lo que contempla conceptos, lineamientos y plazos para la digitalización y automatización de los trámites, por lo que se busca que durante el proceso de automatización de trámites se dé un tratamiento archivístico adecuado conforme a los principios del Archivo General de la Nación. En adición a ello, este Decreto contiene en uno de sus anexos la Guía de digitalización y automatización de trámites donde se desarrollan diversos aspectos que se deben considerar durante estos procesos, en específico refiere los principios que se deben aplicar durante el diseño de un trámite.

Ahora bien, por lo que hace a las guías contenidas en el Manual de Gobierno Digital se pueden destacar las siguientes: guía de cómputo en la nube, marco de interoperabilidad, guía de herramientas de analítica para la explotación de datos, manual de sinergias de gobierno, controles de seguridad y privacidad de la información, guía de mejora continua, guía de referencia sobre gestión documental, guía de lineamientos de los servicios ciudadanos digitales, guía de caracterización de ciudadanos, usuarios y grupos de interés, lineamientos para la integración al portal único del Estado GOV.CO.

¹⁵² Puede consultarse en: <https://gobiernodigital.mintic.gov.co/portal/Politica-de-Gobierno-Digital/>

En suma, como se puede observar Colombia cuenta con un marco jurídico sólido que le permite la implementación de los trámites en línea, además su Política de Gobierno Digital tiene objetivos muy claros que van más allá de eficientar trámites y servicios; busca llegar a una nueva faceta del gobierno donde se transforme también el modo de entender e interactuar con la ciudadanía, además ha desarrollado instrumentos específicos y plataformas a los cuales pueden acceder todas las dependencias, para realizar la implementación de estos proyectos de forma homologada y transparente con una misma estructura. Por tanto, Colombia está construyendo la cara de ese nuevo gobierno donde se encuentra plenamente integrado con la ciudadanía y se van eliminando fronteras y barreras entre las dependencias para ser una nueva y sola cara en el proceso de transformación de gestión pública.

3.2. Perú

Perú de la misma forma que Colombia ha apostado por un desarrollo importante de instrumentos y guías en materia de gobierno electrónico, partiendo desde una óptica en donde el ciudadano era el centro de los procesos hasta donde ya es parte de la construcción de políticas públicas y su participación se vuelve fundamental; una gestión pública orientada cada vez más hacia la generación de verdadero valor público. En este sentido, a continuación, se analizarán los instrumentos, guías, políticas que se han emitido al respecto.¹⁵³

Año	Instrumento	Objeto
2001	Lineamientos de políticas generales para la masificación	Se plantea la necesidad de utilizar las Tecnologías de la Información y Comunicación como medio para mejorar y transparentar la gestión del Estado.

¹⁵³ Presidencia del Consejo de Ministros del Perú, “Una mirada al Gobierno electrónico en el Perú”, *Oficina Nacional de Gobierno Electrónico e Informática*, Perú, 2013, pp.31-37.

	de internet en el Perú	
	Portal del Estado Peruano	Se buscaba que este portal fuera el único punto de acceso a toda la información, servicios y procedimientos de la Administración Pública.
2002	Ley de Transparencia y Acceso a la Información Pública	Se fortalece el principio de transparencia al señalar que toda la información de interés público debe estar disponible en los portales de los Estados.
	Lineamientos de Políticas Generales del Desarrollo del Sistema Electrónico de Adquisiciones y Contrataciones del Estado	Su objetivo es mejorar la transparencia en las contrataciones públicas y compras de gobierno, a través de la implementación de mecanismos electrónicos.
2003	Decreto Supremo No. 067-2003-PCM	Se crea la Oficina Nacional de Gobierno Electrónico e Informática, la cual es responsable de dirigir y supervisar las Políticas de Gobierno Electrónico.
2005	Ley de Promoción del Acceso a Personas con Discapacidad	Entre otros aspectos buscaba la adecuación de los portales y páginas web.

	Plan de Desarrollo de la Sociedad de la Información y la Agenda Digital Peruana	Su objetivo era darle continuidad y seguimiento a las políticas de Sociedad de la Información.
2006	Estrategia Digital de Gobierno Electrónico	De acuerdo con la Agenda Digital se estableció la primera estrategia en la materia, con el establecimiento de portales web para proporcionar servicios a la ciudadanía y a las empresas.
	Portal de Servicios al ciudadano	Se creó un único portal donde se pueden encontrar los procedimientos, requisitos y derechos relacionados con los trámites de la Administración Pública.
	Ventanilla Única de Comercio Exterior.	A través de esta ventanilla se realizan trámites relacionados con la importación y exportación de mercancías, como la obtención de permisos, licencias y certificaciones.
2007	Se crea el Portal de Servicios al Ciudadano y Empresas, el Sistema de Ventanilla única y el Sistema Integrado de Servicios Públicos Virtuales	Permiten la integración de los distintos trámites relacionados con diversas dependencias para la constitución de empresas

2008	Lineamientos y mecanismos para la interconexión de equipos de procesamiento electrónico de información entre las entidades del Estado	Con ello se establecen las bases en materia de interoperabilidad.
2009	Plan Maestro de Gobierno Electrónico	Se determina una hoja de ruta para temas como: firma digital, sistema de información judicial, sistema de intercambio de información.
2010		Se establece una política nacional de cumplimiento para que el país cuente con una Red Dorsal Nacional de Fibra Óptica.
2011	Plan Nacional de Desarrollo de la Sociedad de la Información- Agenda Digital 2.0	Se consolida la hoja de ruta para la Sociedad de la Información. La Agenda tenía entre otros objetivos los siguientes: <ul style="list-style-type: none"> • Asegurar el acceso inclusivo y participativo de la población en áreas urbanas, así como el desarrollo de competencias para el acceso y participación de la ciudadanía en la Sociedad de la Información. • Asegurar la inclusión social y el acceso a servicios sociales que permitan el pleno ejercicio de la ciudadanía. • Promover una Administración pública de calidad orientada a la ciudadanía, para ello,

		<p>se establecieron estrategias relacionadas con lo siguiente: la interoperabilidad; la necesidad de proporcionar trámites y servicios accesibles para todos; asegurar los mecanismos para garantizar una participación ciudadana; mejorar las capacidades de los servidores públicos y de la ciudadanía para hacer un adecuado uso de los servicios del Gobierno Electrónico; así como adecuar la normativa necesaria para lo anterior.</p>
2012	<p>Política y Plan Nacional de Gobierno Electrónico (2013-2017) y se consolidaron proyectos de entidades públicas relacionados con Gobierno Electrónico.</p>	<p>Entre los objetivos de la Política, entre los cuales se encuentran:</p> <ul style="list-style-type: none"> • Fortalecer el Gobierno Electrónico, garantizando su interoperabilidad • Acercar el Estado a los ciudadanos • Garantizar la integridad, confidencialidad y disponibilidad de la Administración Pública • Fomentar la inclusión digital de todos los ciudadanos • Promover la transformación de la sociedad en una Sociedad de la Información garantizando la participación activa de las Entidades y la ciudadanía con la finalidad de garantizar que sea íntegra, democrática, abierta e inclusiva. <p>Uno de los proyectos destacables se refiere a la entrega de certificados a entidades públicas para que se impulsara su uso en los procedimientos</p>

		administrativos y en los servicios ofrecidos por medios electrónicos.
	Modificación del Decreto Supremo No. 052-2008-PCM	Su objeto fue acelerar los procesos de adopción de la firma digital.
2013	Norma Técnica Peruana NTP ISO/IEC 27001:2008 EDI. Tecnología de la Información. Técnicas de seguridad. Sistemas de Seguridad de la Información.	Se aprueba como obligatoria esta norma en materia de seguridad de la información
	Decreto Supremo No.083-2011-PCM	Permite la implementación de servicios públicos por medios electrónicos seguros y el intercambio electrónico de datos entre entidades del Estado.

Cuadro 2. Marco jurídico Perú

Fuente: Elaboración propia con información de Presidencia del Consejo de Ministros del Perú, *op cit.*, pp.31-37.

En suma, como se puede apreciar, desde el año 2000, Perú ha emitido una serie de regulaciones, políticas y planes para fortalecer la implementación de gobierno electrónico, en años más recientes es de destacar el Decreto Legislativo

No.1412 a través del cual se publicó la Ley de Gobierno Digital en septiembre de 2018.

Al respecto, la Ley de Gobierno Digital menciona que tiene por objeto establecer el marco necesario para garantizar diversos aspectos relacionados con la gobernanza digital, como es la identidad digital, interoperabilidad, seguridad digital y datos, así como establecer el marco jurídico aplicable al uso de tecnologías en materia de digitalización y prestación de servicios digitales por parte de las entidades de la Administración Pública.¹⁵⁴

Asimismo, es importante resaltar que dentro del concepto de Gobierno Digital se señala la importancia de la creación de valor público, aunado a ello regula todo lo relativo a la identidad digital y al respecto se señala que esta puede entenderse como *“aquel conjunto de atributos que individualiza y permite identificar a una persona en entornos digitales”*.¹⁵⁵

En este sentido, se contempla la creación de una credencial de identidad digital, así como un documento nacional de identidad electrónico, el cual puede ser utilizado por funcionarios y servidores públicos, aunado a ello, se señala la necesidad de que en la prestación de servicios las dependencias realicen un proceso de identificación digital, así como el de autenticación digital. Por otra parte, se establecen diversos aspectos que deben garantizar las dependencias en la prestación de los servicios tales como los siguientes:

- Reconocer y aceptar el uso de identidad digital
- Garantizar la disponibilidad, integridad y confidencialidad de la información
- Capacitar en temas de firma electrónica, protección de datos personales, interoperabilidad, seguridad digital, datos abiertos
- Facilitar el acceso a la información a otras entidades de la Administración Pública en el ámbito de sus competencias
- Considerar pagos electrónicos en los servicios en línea

¹⁵⁴ Ley de Gobierno Digital de Perú, p.5

¹⁵⁵ *Ibidem*, p.6

- Garantizar la información a las personas sobre el tratamiento de sus datos personales
- Garantizar las comunicaciones y documentos generados a través de canales digitales, así como que el diseño y configuración de los servicios se adopten a las medidas técnicas, organizativas y legales.

Además, refiere que para la conservación de documentos deben utilizarse sellos digitales de tiempo, así como el marco aplicable a la gobernanza de datos, interoperabilidad y seguridad digital, también se señala la obligación que tienen las dependencias de utilizar software público peruano bajo licencias libres o abiertas.

En consecuencia de lo anterior, como puede apreciarse la Ley de Gobierno Digital establece de forma general diversos aspectos que deben ser considerados en la implementación de servicios y trámites en línea que podrá ir detallando ya en otros instrumentos como Reglamentos, Lineamientos y Guías específicas, no obstante, consideramos que contempla aspectos sumamente trascendentes en la prestación de los servicios en línea, enfocado ello sobre todo a generar valor público.

De esta manera, en el año 2021 también se emitió un documento sumamente útil en la materia y en la implementación de trámites en línea denominado “Directiva que establece los Lineamientos para la Conversión Integral de Procedimientos Administrativos a Plataformas o Servicios Digitales” el cual refiere los pasos y aspectos que deben considerar las dependencias para poder transformar sus procedimientos físicos a digitales, refiriendo de forma muy detallada como se llevaría a cabo un proceso de digitalización.

Aunado a ello se señala que los diseños de las plataformas para prestar servicios digitales deben ser empáticas, simples, intuitivos, inclusivos y accesibles, considerando la necesidad de los usuarios, sus roles, los desafíos y características específicas de los servicios, también que las entidades deben implementar infraestructura flexible preferentemente en la nube, así como garantizar la disponibilidad de estos servicios las 24 horas, los, 365 días del año.

Además de lo anterior, se han emitido una serie de Lineamientos y Guías específicas no solo para el proceso de digitalización antes referido sino en general

relacionados con el gobierno electrónico, las cuales más allá de los aspectos jurídicos contemplan cuestiones específicas incluso relacionadas con la experiencia de usuario. Por lo que hace a los Lineamientos, resaltan los denominados “Lineamientos generales y consideraciones para diseñar” y entre las guías se pueden señalar las siguientes: guía de estilos; guía de accesibilidad y diseño inclusivo; guía para conocer el problema y las necesidades de los usuarios; guía de desarrollo ágil para servicios digitales.

Así pues, como se pudo observar Perú cuenta con un marco jurídico sólido en materia de gobierno electrónico que se ha desarrollado desde el año 2000, al igual que Colombia ha optado por tener una autoridad central sólida que establece además de políticas, instrumentas y guías, herramientas de apoyo muy específicas para las entidades del sector público que contemplan desde los aspectos jurídicos hasta los de operación considerando siempre el objetivo central de crear valor público para la ciudadanía.

3.3. Chile

Chile de la misma forma que Perú y Colombia empezó un proceso de transformación a principios de la década de los 2000, a través de la promulgación de diversas leyes en la materia, agendas y planes específicos, este proceso se vio acelerado con la pandemia ocasionada por COVID-19 ya que recientemente se publicó una Ley en la materia que se abordará más adelante. Por lo que a continuación, se detallarán los instrumentos planes y programas que han sido aprobados durante estas décadas.¹⁵⁶

Año	Instrumento	Objeto
-----	-------------	--------

¹⁵⁶ Roberts M. Raimundo, “Sobre la digitalización del Estado de Chile: Políticas en curso”, Biblioteca del Congreso Nacional de Chile/BCN, Chile, 2020, pp. 5-7

2002	Agenda de Gobierno Electrónico	Fue uno de los primeros instrumentos de política pública en la materia.
	Ley de Documento, Firma y Certificación Digital	A través de ésta se reconoció el mismo valor a la firma electrónica que a la autógrafa. ¹⁵⁷
2003	Se creó el Grupo Acción Digital	A través de una entidad público-privada se buscó la implementación de la Agenda Digital 2004-2006 la cual tenía entre otros objetivos el desarrollar el Estado en línea.
	Ley de Procedimientos Administrativos	Estableció que las dependencias no podían solicitar a la ciudadanía información que ya estuviera en su poder. ¹⁵⁸
2004	Decreto Supremo Nro. 77 de Eficiencia de Comunicaciones Electrónicas	Regula la forma en que se deben llevar a cabo las comunicaciones electrónicas entre las dependencias y los ciudadanos.
	Decreto Supremo Nro 81 Interoperabilidad de Documentos Electrónicos	Detalla cuestiones relacionadas con la interoperabilidad. ¹⁵⁹
2007-2012	Estrategia Digital 2007-2012	Esta estrategia entre otros tuvo como objetivo el fomento al Gobierno electrónico.

¹⁵⁷ Gutiérrez, Claudio, et al. Gobierno Electrónico en Chile, "Desafíos, perspectivas y oportunidades" *Revista chilena de ingeniería, anales del instituto de ingeniería de Chile*, 2005, vol. 12, núm. 2, p. 70

¹⁵⁸ *Idem*

¹⁵⁹ *Ibidem* p.71

2011	Plan Estratégico de Gobierno Electrónico 2011-2014	Tenía entre sus objetivos el ofrecer a la ciudadanía un acceso sencillo, rápido, directo con el Estado.
2013	Agenda Digital Imagina Chile 2013-2020	Tenía cinco ejes fundamentales: conectividad e inclusión digital, innovación y emprendimiento, educación y capacitación, servicios y aplicaciones y entorno para el desarrollo digital.
2019	Instructivo Presidencial de Transformación Digital	A través de éste se establecieron cuatro medidas básicas para avanzar hacia la transformación digital del Estado: i) “identidad digital única”, a partir de una ClaveÚnica con la cual se llevaría a cabo la autenticación digital; ii) “política cero fila” la cual busca simplificar y digitalizar los trámites y que no se solicitara la misma información al ciudadano que ya se encontrara en poder del Estado; iii) “política cero papel” con la cual se busca eliminar el uso de papel.
2020	Agenda Digital 2020	Consta de cinco ejes: Derechos para el Desarrollo Digital, Conectividad Digital, Gobierno Digital, Economía Digital y Competencias Digitales. Dispone que la División de Gobierno Digital deberá elaborar las pautas, guías y servicios para el desarrollo del Instructivo Presidencial establecido en 2019.

Cuadro 3. Marco jurídico Chile

Fuente: Elaboración propia con información de Roberts M. Raimundo, *op cit.*, pp. 5-7 y Gutiérrez, Claudio, *op cit.*, p. 70

De esta manera a través del Instructivo Presidencial de Transformación Digital, se señalaron diversas medidas que debían ser implementadas por todas las dependencias como son:

Política de Identidad Digital Única: se dispuso el uso de la Clave Única como instrumento de identificación digital; para ello se especificó que se pondría a disposición de las dependencias una directiva, una guía técnica y un kit de implementación.

Política de Cero Fila: en esta se estableció que se debían digitalizar la mayor cantidad de trámites y además que cuando se acudiera a la Administración a realizar un trámite y ésta ya tuviera en su poder información ya no se tendría que hacer “fila”.

Digitalización de Trámites: referente a la simplificación y digitalización de los trámites, así como la eliminación de aquellos que ya no fueran necesarios.

No petición de antecedentes en poder de la Administración del Estado: se estableció que para cumplir con la obligación de los servidores públicos de no solicitar información que ya se encontrara en poder del Estado se ponía a su disposición la plataforma de interoperabilidad del Estado.

Política Cero Papel: se estableció que se debía eliminar gradualmente el uso de papel y optimizar su gestión documental y de expedientes, para ello también se puso a disposición un set de guías de buenas prácticas para la elaboración de políticas de gestión documental.

Posteriormente, considerando dentro de su marco todas estas medidas en Noviembre de 2019 el Gobierno Chileno aprobó la Ley No. 21.180 relativa a la Transformación Digital, la cual entró en vigor el 9 de junio de 2022, ésta busca que todos los procedimientos administrativos, de principio a fin, se realicen por medios electrónicos y establece un plazo de cinco años para su implementación por lo que determina diversas fases y etapas para llevar a cabo lo anterior. Para ello determina 6 ejes fundamentales: comunicaciones electrónicas, notificaciones electrónicas, procedimientos administrativos, expedientes electrónicos, digitalización de documentos y principio de interoperabilidad¹⁶⁰

¹⁶⁰ Puede consultarse en: <https://digital.gob.cl/transformacion-digital/ley-de-transformacion-digital/>

En consecuencia, se crearon diversas plataformas que podrán usar de forma transversal las dependencias como son: i) DocDigital: permite enviar y recibir las comunicaciones entre las dependencias; ii) Plataforma de Notificaciones del Estado: es una herramienta para poder realizar las notificaciones a los particulares; iii) Simple: es un modelador de procesos que no tienen alta complejidad para que las dependencias puedan digitalizar formularios o documentos similares; iv) FirmaGob: se proporciona una API para poder firmar los documentos y a través de ésta se pueden gestionar las firmas de los servidores públicos; vi) Plataforma de interoperabilidad: permite el intercambio de datos entre las dependencias.

En concordancia con la ley antes referida, en diciembre de 2021, se publicó en el Diario Oficial de la República de Chile el *Reglamento que regula la forma en que los procedimientos administrativos deberán expresarse a través de medios electrónicos en las materias que indica, según lo dispuesto en la Ley No. 2180 sobre Transformación Digital del Estado*, el cual detalla la forma en que se deben presentar los documentos electrónicos así como de cotejar la autenticidad de copias digitalizadas, el proceso para realizar las notificaciones electrónicas y los estándares que deben cumplir las plataformas referidas en el párrafo anterior.

En este sentido, se establece que todos los procedimientos administrativos deben constar en un expediente electrónico y se señala que los documentos que se pondrán incorporar en este expediente serán copias digitalizadas de documentos en soporte papel o documentos electrónicos en su origen, para el primer caso se debe declarar por el interesado la autenticidad y conformidad de la copia digitalizada. Asimismo, se dispone que se debe determinar un domicilio único por las personas para recibir notificaciones electrónicas y se señala que las notificaciones se deben practicar por medios electrónicos y que la información que debe contener la plataforma de comunicaciones oficiales es de uso obligatoria para las dependencias.

Respecto a la interoperabilidad se contempla que cuando una dependencia tenga en su poder documentos o información que sean necesarias para trámites en otra dependencia de acuerdo con sus competencias debe remitirlo, ello de acuerdo con la Norma Técnica de Interoperabilidad. Por lo que hace a la conservación de

los documentos se señala que cada dependencia es responsable de mantener la integridad, disponibilidad y autenticidad de la información de acuerdo con la Norma Técnica de Documentos y Expedientes Electrónicos.

Además, desarrolló una serie de guías y estándares para lograr esta implementación entre las cuales se encuentran: marco conceptual de procedimientos administrativos, guía para la formulación de proyectos TIC, guía de buenas prácticas de adopción digital, guía de desarrollo de software, guía técnica para integración de ClaveÚnica, guía de gestión documental, guía para el diseño de interfaces web institucionales, entre otras.

En definitiva, como puede apreciarse Chile, de la misma forma que Perú y Colombia ha desarrollado una política rectora en materia de gobierno electrónico, incluso publicando una ley específica al respecto, además de desarrollar herramientas, guías y estándares para que sean aplicados de forma homologada por todas las dependencias.

3.4. México

La evolución que ha tenido México en el marco jurídico ya fue explorada en el capítulo 2, no obstante, más allá de la base normativa, se considera primordial resaltar también aspectos relacionados con sus políticas, guías y herramientas que se han desarrollado en materia de gobierno electrónico y que en específico pudieran tener relación con la implementación de trámites en línea.

De esta manera iniciaremos por abordar la Estrategia Digital Nacional de 2013-2018¹⁶¹, la cual se desarrolló persiguiendo cinco grandes objetivos: i) Transformación gubernamental; ii) Economía Digital; iii) Transformación del Modelo Educativo; iv) Salud Universal y Efectiva e; 5) Innovación Cívica y Participación Ciudadana, para ello se definieron 5 habilitadores referentes a la conectividad, inclusión y habilidades digitales, interoperabilidad, marco jurídico y datos abiertos, los cuales de forma transversal tienen impacto en la adopción de trámites en línea.

¹⁶¹

Puede

consultarse

en:

https://www.gob.mx/cms/uploads/attachment/file/17083/Estrategia_Digital_Nacional.pdf

Por lo que hace a la transformación digital, se establecieron como objetivos específicos, el lograr un gobierno abierto, implementar la Ventanilla Única Nacional, así como una política de TIC sustentable para la APF, coordinar una política de gestión del territorio nacional y por último adoptar una comunicación digital centrada en el ciudadano. Aunado a ello, en cada uno de esos objetivos específicos se definieron líneas de acción, entre las cuales pueden destacar para el objetivo del presente trabajo las referentes a la estandarización de los procedimientos y normatividad de los trámites y servicios, a la digitalización de los trámites, la promoción de una identidad digital y de la interoperabilidad de la información en poder del gobierno.

Es así que la entonces Unidad de Gobierno Digital adscrita a la Secretaría de la Función Pública tenía una serie de atribuciones específicas para lograr lo anterior¹⁶² entre ellas, se encontraba la de emitir criterios técnicos, metodologías, guías e instructivos enfocados a la estrategia de gobierno digital y datos abiertos. A la luz de ello se emitieron diversos documentos normativos que fueron ya señalados en el capítulo II del presente trabajo, así como diversas guías en el año 2018, es decir en el último año de la Estrategia en comento. No obstante, es importante destacar que estas guías solo fueron publicadas en la página de gob.mx, sin que dicha publicación haya ido acompañada de una estrategia de difusión y capacitación, para los entes de gobierno, además derivado de los cambios en la Estrategia Digital Nacional que se detallarán en líneas posteriores, algunos de los aspectos contenidos en éstas pueden ya no ser aplicables.

Sin embargo, para efectos de este análisis se señalarán los documentos principales. Para comenzar, una de las guías primordiales para la implementación de trámites en línea es la Guía de Digitalización de Trámites y Servicios Gubernamentales, la cual, está compuesta por diversas guías que tienen como objetivo orientar a las dependencias en los procesos que deben llevar a cabo para la digitalización de trámites, entre éstas podemos encontrar las siguientes:

¹⁶² Secretaría de Gobernación, Reglamento Interior de la Secretaría de la Función Pública, 2017, artículo 34

Modelo de tramitación electrónica: con este documento se buscaba identificar los distintos trámites de la APF y su clasificación por proceso, para con ello lograr un catálogo de procesos que pueden tener variables inherentes a una misma categoría del trámite o servicio, esta clasificación se realiza de acuerdo con el tipo de necesidad del solicitante del trámite. De esta manera señala los siguientes: i) autorizaciones, certificados, concesiones, informes, registros y avisos; ii) solicitud de información y asesoramiento; iii) servicios económicos, sociales y de salud; iv) recursos, denuncias y gestión de conflictos y pago de obligaciones.

Al respecto es importante señalar que, si bien cada trámite tiene sus particularidades, el realizar una clasificación puede ayudar a observar pasos y elementos en común que se debieran considerar en los mismos, no obstante, no se observa que esto se realice en este documento. Asimismo, se señalan algunos componentes que estarán disponibles en el mismo portal, pero tampoco se observa que dichos componentes realmente estén a disposición de las dependencias actualmente.

Guía de procesos de tramitación electrónica: busca definir los esquemas de tramitación en la APF¹⁶³, para ello se hace un análisis de distintos trámites y se señalan ejemplos específicos para con éstos generar modelos estándar en donde las dependencias puedan ubicar sus trámites. Al respecto, cabe destacar que, si bien la guía aporta una clasificación general de los trámites y procesos definidos y para cada uno señala la vía que se tendría que seguir en las distintas etapas para los trámites en línea, esto se aborda de forma muy general sin dar pautas específicas de cómo llevarlo a cabo.

Guía de integración de cadenas de interoperabilidad: en esta guía se señala que las cadenas de interoperabilidad agrupan diferentes procesos de acuerdo con el objetivo general que persigue ese conjunto de trámites y que las primeras que se deben formar son las relacionadas con la identidad ya que sirven de base para las

¹⁶³ “Son una representación gráfica a alto nivel del funcionamiento de un trámite o servicio público, con el objetivo de identificar sus etapas y actividades principales”. Gobierno de México, “Modelo de tramitación electrónica”, *wikiguías*, 2018.

cadena siguientes, para ello, se menciona la necesidad de generar mapas de cadenas. No obstante, no se observa de modo específico un lineamiento para las dependencias de cómo llevar a cabo lo anterior, por lo que parece más un documento descriptivo que una guía específica.

Criterios de digitalización de trámites: en este documento se definen los criterios para clasificar los trámites de acuerdo con sus distintos niveles de digitalización y se proporciona un cuestionario para la evaluación de la madurez tecnológica del trámite; también se señalan iniciativas estándar para los procesos identificados. Al respecto, algunos de los aspectos abordados pudieran ser considerados durante la implementación de trámites en línea, por lo que lo correspondiente será considerado en el capítulo 4.

Estándar de resoluciones electrónicas: se refiere el contenido que deben tener las resoluciones electrónicas, también se refieren algunos componentes para ello, como el relativo a la validación de la integridad de los documentos electrónicos, no obstante, tampoco se observa dicho componente en el sitio correspondiente. Por lo que solo pudieran resultar útiles algunos aspectos como referencia

Guía de implementación de datos abiertos: busca establecer las pautas en las que serán publicados los datos abiertos, así como estándares para ello y las actividades que deben realizar las instituciones para lograr los objetivos correspondientes; cabe destacar que esta guía si fue publicada en el Diario Oficial de la Federación el 18 de junio de 2015.

Por otra parte, si bien se desarrollaron algunas otras guías se considera que las principales para efectos del presente trabajo, son las que se han señalado anteriormente, cabe destacar que solo se considerarán algunos aspectos de éstas en el capítulo 4, ya que debido al cambio de perspectiva en diversos aspectos de la nueva Estrategia Digital Nacional 2021-2024¹⁶⁴ no todos los aspectos desarrollados en las mismas resultarían aplicables.

¹⁶⁴

Puede

consultarse

en:

https://dof.gob.mx/nota_detalle.php?codigo=5628886&fecha=06/09/2021#gsc.tab=0

La Estrategia Digital Nacional actual tiene como uno de sus principales objetivos lograr el uso y desarrollo eficiente, democrático e incluyente de las Tecnologías de la Información y Comunicación y señala como principios los siguientes: austeridad, combate a la corrupción, eficiencia de los procesos digitales, seguridad de la información y soberanía tecnológica, por tanto, si bien se busca un país digitalizado se establece que esto debe ser en el marco de un gobierno austero, honesto y transparente con autonomía e independencia tecnológica.

Respecto a los objetivos específicos para efectos de este proyecto resalta el relativo a “Obtener el máximo aprovechamiento de aplicativos de cómputo e infraestructura mediante el intercambio de información y la colaboración tecnológica” el cual tiene entre sus líneas de acción el promover el intercambio de información entre las instituciones para lograr la simplificación de trámites y servicios, fomentar la digitalización de trámites previamente simplificados, promover el uso de la Firma Electrónica Avanzada como medio de autenticación para trámites y servicios así como la adopción de plataformas que sean amigables para los usuarios y que sean interoperables.¹⁶⁵

En este nuevo entorno, se eliminó la Unidad de Gobierno Digital adscrita a la Secretaría de la Función Pública y sus facultades pasaron a la Coordinación de Estrategia Digital Nacional, las cuales actualmente están establecidas en el artículo 36 del Reglamento de la Oficina de la Presidencia de la República, aunque se encuentran mucho más limitadas que las que tenía la Unidad de Gobierno Digital; asimismo, pareciera que esta reforma no fue suficiente para aclarar lo que corresponde a diversas facultades que se encuentran directamente establecidas para la Secretaría de la Función Pública en leyes específicas como la ya mencionada en el capítulo 2 respecto a la acreditación de autoridades certificadoras para efectos de la Ley de Firma Electrónica Avanzada.

Respecto al trabajo realizado por la Coordinación de Estrategia Digital Nacional, es de destacar que se han emitido pocos instrumentos en materia de gobierno electrónico, los cuales ya fueron mencionados en el capítulo 2 y han sido

¹⁶⁵ Acuerdo por el que se expide la Estrategia Digital Nacional 2021-2024, publicado en el Diario Oficial de la Federación el 6 de septiembre de 2021

mucho más enfocados al tema de seguridad de la información, no obstante, aún quedan más de dos años para el desarrollo de esta Estrategia.

En síntesis, México cuenta con un marco jurídico sólido para la implementación de trámites en línea que se fue desarrollando desde el año 2000, aunque en diversas leyes y en algunos casos aún incompleto como lo relativo a los aspectos del archivo y resguardo de los documentos electrónicos. Asimismo, ha desarrollado estrategias encaminadas a ello, no obstante, se observa que a diferencia de los otros países abordados no cuenta con herramientas específicas, estrategias de capacitación y homologación para que las entidades puedan implementar estos trámites. Las guías que se desarrollaron al final de la Estrategia de 2013-2018 son muy generales y debido al cambio de perspectiva en la Estrategia Digital Nacional, ya no existe claridad respecto a la continuidad de las mismas. Tampoco se observa que la autoridad rectora en la materia actualmente establezca pautas y herramientas claras para lograr una implementación de trámites en línea y con un enfoque específico. Por lo anterior, es que existe una confusión de la forma adecuada para llevar a cabo la implementación de trámites en línea, no obstante, con los elementos e instrumentos con los que se cuenta actualmente es que se realizará la propuesta del capítulo 4.

Es así que a través de las experiencias abordadas en el presente capítulo, pudimos observar que si bien contar con un marco jurídico para la implementación de trámites en línea que va desde las leyes aplicables a los procedimientos administrativos, hasta las correspondientes a gestión documental, también resulta sumamente trascendente contar con una autoridad central que establezca la política rectora en la materia; además es primordial el desarrollo de guías y estándares específicos que apliquen todas las dependencias de forma homologada y transversal, así como, herramientas específicas que utilicen en sus procesos de implementación, ello permite que realmente se homologuen los procesos y se logren de forma coordinada y transversal, eficientando los costos y plazos asociados a ello y permitiendo además la interoperabilidad que es fundamental para lograr un proceso de transformación real en el gobierno donde se establezca una sola cara a la ciudadanía.

Asimismo, Perú, Chile y Colombia tienen en común la evolución que han presentado de los objetivos y la visión del gobierno electrónico donde ya no solo se busca eficientar procesos sino generar valor público, donde todos los actores participen, por lo que la ciudadanía cambia de un rol pasivo y pasa a ser también constructora de políticas públicas. Para ello, además, se establecen estrategias de capacitación y concientización también al interior del gobierno, las cuales son fundamentales para lograr una implementación exitosa. Adicionalmente, se pudo observar que más allá de los aspectos jurídicos, existen muchos otros que considerar relativos a los diseños de los propios trámites, de seguridad de la información, transparencia, etc., y es ahí donde las guías desarrolladas por cada uno de estos países toman un gran valor.

Ahora bien, después de haber dado un recorrido por el marco jurídico y los elementos desarrollados de estos tres países, y considerando los aspectos que pudieran ser aplicables en nuestro país, en el siguiente capítulo se realizará una propuesta de la Guía para implementar trámites en línea en México para la APF con el marco jurídico y los elementos que tenemos actualmente.

Capítulo 4.

Guía para implementar trámites en línea en la APF



Capítulo 4. Guía para implementar trámites en línea en la APF

4.1 Introducción

El desarrollo de trámites en línea es mucho más que efficientar procesos, implica un cambio de gestión pública donde la ciudadanía tiene una participación activa y el gobierno debe estar enfocado en generar verdadero valor público, considerando además que debe proporcionar servicios para toda la ciudadanía sin excluir a nadie.

Aunado a ello, estamos en un momento en el que los datos son fundamentales, por tanto, la forma en que se genera la información y se comparte es esencial para implementar políticas públicas. La información en poder del gobierno debe estar al servicio de todas y todos, tanto para el sector público como privado. En este aspecto es fundamental la estandarización para lograr la interoperabilidad, la cual permitirá que el gobierno se convierta en uno solo para la ciudadanía y no por el contrario que se presente como entes separados con requisitos y políticas diversas.

De ahí que, se tiene un gran reto, ya que además de buscar que esta información se genere en formatos abiertos y accesibles debe cuidar, proteger y garantizar el derecho a la privacidad y protección de datos personales de todas las personas así como la seguridad de la información. Por otra parte, debe hacerlo con el menor costo posible, pero sin comprometer la calidad de los servicios y el cumplimiento de principios fundamentales para la prestación de servicios públicos.

Adicionalmente, se debe garantizar que la implementación de estos trámites se realice con la debida certeza jurídica, en consecuencia, se deben analizar los elementos que se deben incorporar para garantizarla dependiendo del tipo de trámite y sin perder de vista que el objetivo final debe ser que la ciudadanía sea parte de ello y se genere valor público.

Por tanto, implementar trámites en línea, puede tener grandes beneficios tanto hacia el interior de las dependencias como hacia el exterior con la ciudadanía,

creando entornos transparentes que disminuyen la discrecionalidad en los trámites, generando datos para mejorar servicios e implementar políticas públicas y crear un entorno donde las dependencias del gobierno dejen de ser entes separados con distintas caras al exterior; un entorno con una ciudadanía empoderada en la participación y construcción de políticas públicas.

Ahora bien, para la presente guía, se han considerado los elementos que se encuentran en el marco jurídico mexicano, tanto en leyes, reglamentos y lineamientos, así como lo correspondiente a las guías mencionadas en el capítulo anterior de Chile, Colombia y Perú que pudieran ser aplicables. Para ello, se iniciará refiriendo el marco jurídico mexicano correspondiente a estos trámites que fue desarrollado en el capítulo 2; posteriormente, se señalarán los principios que se observan en estos trámites, una vez realizado ello, se abordarán los pasos que se considera se deben seguir para este desarrollo; en primer término, aspectos relacionados con el análisis y diseño del trámite como son: la simplificación, objetivo, interoperabilidad, seguridad de la información y las políticas de contratación; después, se realizará el análisis de los aspectos jurídicos, que incluye apartados como los siguientes: elementos que se deben considerar para garantizar la validez de los trámites en línea, así como aquellos que deben contener las resoluciones que se emitan por medios electrónicos, aceptación del particular para el uso de medios electrónicos, autenticación electrónica, mecanismos de consentimiento y validez de los mensajes de datos, acreditación de facultades del representante legal, y gestión y archivo de información electrónica; por último, se abordarán cuestiones relacionadas con las pruebas y estrategias de difusión y capacitación.

Lo anterior, ya que es muy importante considerar que para el diseño de un trámite en línea, se deben abordar aspectos que van más allá de los jurídicos, ya que además se deben contemplar principios fundamentales de la prestación de servicios públicos.

Asimismo, se incluirán ejemplos específicos y en su caso fuentes de información donde se puede conocer más del tema abordado, con lo anterior, se espera que estos aspectos jurídicos y de operación que están dispersos se compilen y puedan ser explicados y desarrollados, para que la implementación de trámites en

línea en la APF se realice de la forma más homologada posible a efecto de lograr los objetivos que se mencionaron en los primeros párrafos y con la debida certeza jurídica.

4.2 Marco jurídico en México

Como se observó en el capítulo 2, en México, se cuenta con el marco jurídico necesario para implementar trámites en línea, el cual se puede resumir de la forma siguiente:

LEYES	
Ley Federal de Procedimiento Administrativo https://www.diputados.gob.mx/LeyesBiblio/pdf/112_180518.pdf	Regula los actos, procedimientos y resoluciones de la APF.
Ley de Firma Electrónica Avanzada https://www.diputados.gob.mx/LeyesBiblio/pdf/LFEA_200521.pdf	Regula el uso de la firma electrónica avanzada de los particulares y servidores públicos en los actos jurídicos y administrativos, trámites, servicios comunicaciones y procedimientos administrativos de la APF.
Ley General de Mejora Regulatoria https://www.diputados.gob.mx/LeyesBiblio/pdf/LGMR_200521.pdf	Establece los principios y bases en materia de mejora regulatoria para los Sujetos Obligados.
Ley General y Federal de Transparencia y Acceso a la Información Pública https://www.diputados.gob.mx/LeyesBiblio/pdf/LGTAIP_200521.pdf	Tiene por objeto establecer, los procedimientos, bases y principios para garantizar el derecho de acceso a la información en posesión de las autoridades.
Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPSO.pdf	Tiene por objeto establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales, en posesión de sujetos obligados.
Ley General de Archivos https://www.diputados.gob.mx/LeyesBiblio/pdf/LGA.pdf	Tiene por objeto establecer los principios y bases generales para la organización y conservación, administración y preservación homogénea de los archivos en posesión de cualquier autoridad.

REGLAMENTOS, LINEAMIENTOS Y ACUERDOS

Reglamento de la Ley de Firma Electrónica Avanzada

https://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFEA.pdf

Disposiciones Generales de la Ley de Firma Electrónica Avanzada

https://www.dof.gob.mx/nota_detalle.php?codigo=5457756&fecha=21/10/2016#gsc.tab=0

Tiene por objeto establecer las normas reglamentarias para el uso de la Firma Electrónica Avanzada en los actos regulados en la Ley de Firma Electrónica Avanzada.

Además de establecer estándares, requisitos y características que deben tener los certificados digitales y que deben cumplir las autoridades certificadoras para tener tal carácter, regulan algunas otras cuestiones como la manera en que se deben llevar a cabo la conservación de mensajes de datos en documentos que tengan Firma Electrónica Avanzada.

Lineamientos Generales de Protección de Datos Personales para el Sector Público

<http://inicio.inai.org.mx/AcuerdosDelPleno/ACT-PUB-19-12-2017.10.pdf>

Tienen por objeto desarrollar las disposiciones previstas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados en lo relativo al ámbito federal.

Acuerdo para la adopción y uso por la APF de la Clave Única de Registro de la Población

https://www.dof.gob.mx/nota_detalle.php?codigo=4903440&fecha=23/10/1996#gsc.tab=0

Tiene por objeto establecer la obligación de las dependencias de la APF para adoptar el uso de la CURP como elemento de identificación de las personas en los registros a cargo de dichas dependencias.

Acuerdo por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la APF

https://www.dof.gob.mx/nota_detalle.php?codigo=5628885&fecha=06/09/2021#gsc.tab=0

Tiene por objeto emitir las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información, que serán de observancia obligatoria en la APF.

Bases técnicas de Seguridad Informática para las dependencias y entidades de la APF

https://www.gob.mx/cms/uploads/attachment/file/651941/Seguridad_Informatica.pdf

Son recomendaciones mínimas de seguridad informática, que incluyen acciones de prevención, detección y respuesta de incidentes.

<p>Decretos, Acuerdos, Disposiciones y Criterios expedidos por la Unidad de Gobierno Digital que incluyen alguna información que pudiera tener aún impacto en la implementación de trámites en línea</p>	<p>Decreto por el que se establece la Ventanilla Única Nacional para los Trámites e Información del Gobierno https://www.dof.gob.mx/nota_detalle.php?codigo=5380863&fecha=03/02/2015#gsc.tab=0 Decreto por el que se establece la regulación en materia de Datos Abiertos https://www.dof.gob.mx/nota_detalle.php?codigo=5382838&fecha=20/02/2015#gsc.tab=0 Disposiciones Generales que establecen los mecanismos de identificación y control de acceso que deberán observar las dependencias y entidades de la APF y las empresas productivas del Estado https://www.dof.gob.mx/nota_detalle.php?codigo=5522133&fecha=10/05/2018#gsc.tab=0 Criterios Técnicos que deberán observar las dependencias y entidades de la APF, así como las empresas productivas del Estado, para la emisión de documentos electrónicos que deriven de un trámite o servicio digital https://dof.gob.mx/nota_detalle.php?codigo=5544814&fecha=27/11/2018#gsc.tab=0</p>
<p>Norma Oficial Mexicana NOM-151-SCFI-2016, Requisitos que deben observarse para la conservación de mensajes de datos y digitalización de documentos (cancela la NOM-151-SCFI-2002) https://www.dof.gob.mx/normasOficiales/6499/seeco11_C/seeco11_C.html</p>	<p>Tiene por objeto establecer los requisitos que deberán observarse para la digitalización de documentos y conservación de mensajes de datos cuando éstos sean utilizados por los comerciantes en actos de comercio que estén relacionados con sus negocios.</p>

Cuadro 4. Marco Jurídico México

Fuente: Elaboración propia

4.3 Principios

Considerando los aspectos que se han revisado de las guías y estrategias previas tanto de Perú, Chile, Colombia y México se podrían definir como principios centrales que se podrán considerar durante estos procesos de implementación los siguientes:

- Todos y todas deben estar incluidos en el diseño del trámite, siempre se debe buscar la satisfacción del interés general, por tanto, será fundamental considerar cuestiones como la brecha digital, ya que el

gobierno no debe acrecentar esta brecha sino todo lo contrario, por ello siempre se deben garantizar alternativas para realizar el trámite.

- Garantizar la transparencia, el derecho de acceso a la información, pero también la protección del derecho a la privacidad y la protección de los datos personales.
- Considerar el marco jurídico aplicable que soporte de forma adecuada y suficiente el trámite en línea.
- Contemplar los aspectos necesarios para garantizar la certeza jurídica sin excederse en los elementos requeridos.
- Recordar que los aspectos generales que aplican a los trámites, actos y procedimientos administrativos, también resultan aplicables en medios electrónicos, ya que lo anterior solo cambia el canal y la vía por la que se llevan a cabo, pero no todos estos principios previos.
- Considerar los principios aplicables a medios electrónicos, como la integridad, autenticidad, fiabilidad y equivalencia funcional.
- Realizar el diseño del trámite de una forma fácil y accesible para todas las personas que puedan acceder a realizar el trámite.
- Por lo que hace a la conservación de los mensajes de datos y gestión de la información generada por medios electrónicos, se deben contemplar todos los elementos necesarios.
- Buscar la interoperabilidad con todos los trámites del gobierno para que éste logre ser una sola cara a la ciudadanía y generar valor real para el sector público y privado.
- No solicitar a la ciudadanía información que ya esté en poder del gobierno, para lo cual la interoperabilidad será fundamental.
- Considerar en todo momento el principio de neutralidad tecnológica para la implementación de estos sistemas buscando también realizarlo al menor costo posible.
- No olvidar que la simplificación administrativa y mejora regulatoria no necesariamente implican la automatización, por lo que previo a esta última se recomienda llevar a cabo el análisis respectivo.

- Es fundamental garantizar los aspectos de seguridad de la información.



Figura 1. Principios y aspectos que se deben considerar durante la implementación de trámites en línea

Fuente: Elaboración propia

4.4 Pasos

De esta manera iniciaremos por desarrollar los pasos y consideraciones que se pondrían contemplar en las distintas etapas:

I) Análisis y consideraciones de diseño del trámite

Debido a que la automatización no necesariamente implica la simplificación, aunque puede estar estrechamente ligada, en primer término, será importante realizar un análisis referente a ello.

Simplificación: el objetivo de esta simplificación debe ser hacer más sencillos, fáciles y accesibles los trámites administrativos, garantizando la legalidad y seguridad jurídica y sin afectar el fin específico del procedimiento. Por tanto, se

deben identificar y realizar propuestas de mejora, para que los trámites se realicen de forma más ágil con eficiencia y eficacia, pero sin afectar el interés general, la legalidad y la seguridad jurídica.¹⁶⁶

Derivado de lo anterior será importante analizar los pasos que se llevan a cabo, los requisitos que se solicitan, los plazos correspondientes, los órganos que intervienen, así como su población objetivo a la luz del trámite que se está realizando, para ello será sumamente útil contar con un mapa y diagrama del trámite; para lo cual, se podría considerar la clasificación de trámites que se realiza en el Modelo de Tramitación Electrónica,¹⁶⁷ siguiendo algunos principios generales.

Asimismo, se pueden contemplar diversos aspectos que determinarán la base sobre la que se realizará la simplificación, relacionadas con el tipo de información que se genera y acceso, ya que posteriormente ello ayudará a determinar los perfiles y medios de acceso que se requerirán, el tipo de notificación, de resolución, entre otros.

Aunado a lo anterior, el Manual de Simplificación Administrativa y Reducción de Cargas para la Administración General del Estado¹⁶⁸ proporciona un panorama de las fases que se pueden seguir para llevar a cabo esta simplificación e incluso proporciona un checklist para la reducción de cargas y la simplificación procedimental, por lo que es recomendable su consulta para realizar este análisis de simplificación.

De esta manera, por ejemplo, si se trata de un trámite que sea solo de consulta y la naturaleza de la información es pública, no se tendría que solicitar ningún documento que acredite la identidad y si fuera el caso eliminar este requisito sería parte de esta simplificación. Por otra parte, si en el trámite se solicita

¹⁶⁶ Ministerio de Hacienda y Administraciones Públicas, Manual de Simplificación Administrativa y Reducción de cargas para la administración general del Estado, España, 2014. pp.37 y 38

¹⁶⁷ Puede consultarse en: <https://www.gob.mx/wikiguías/articulos/modelo-de-tramitacion-electronica?state=published>

¹⁶⁸ Puede consultarse en: <https://www.mptfp.gob.es/portal/funcionpublica/gobernanza-publica/simplificacion/manual-simplificacion.html>

información que ya se encuentra en poder del gobierno, se debe buscar obtenerlo directamente al interior del mismo y no solicitarla dos veces al ciudadano.

Para saber más puedes consultar...

Manual de Simplificación Administrativa y Reducción de cargas para la administración general del Estado. España. <https://www.mptfp.gob.es/portal/funcionpublica/gobernanza-publica/simplificacion/manual-simplificacion.html>

Objetivo: se debe identificar con claridad el objetivo del trámite y de su automatización, para ello se deberá considerar su contribución a los objetivos institucionales y su utilidad social.

Aspectos que se deben considerar en el diseño:

El diseño debe estar centrado en la ciudadanía, en la población objetivo, se deben priorizar sus necesidades, considerando siempre también el interés general, para ello, se debe analizar la experiencia del usuario e incluirlo en el proceso, contemplando a todos los involucrados.

Realizar desde una visión amplia, considerando el impacto y relación al interior de la propia dependencia, así como con otros trámites e incluso con otras dependencias.

Se deben diseñar para que sean de fácil uso, intuitivos para los usuarios, asimismo deben ser inclusivos y accesibles y con un lenguaje amigable, por ello, será fundamental considerar diferentes perfiles en el equipo que diseñe e implemente estos trámites.

Siempre se deben considerar alternativas para llevar a cabo el trámite considerando la brecha digital.

Por lo que hace a los principios, es importante considerar el marco general que rige a los actos administrativos y a los medios electrónicos, así como los principios que le aplican como son: neutralidad tecnológica, compatibilidad internacional, integridad y equivalencia funcional.

Referente a los sistemas que seleccionarán, considerar la aplicación de Estándares Técnicos de la Coordinación de Estrategia Digital Nacional en materia de arquitectura de desarrollo e interoperabilidad y servicios de hospedaje.¹⁶⁹

Privilegiar la implementación de software libre, siempre que cuente con las características necesarias y represente un beneficio tecnológico con ahorros para el Estado. En concordancia con lo anterior, se debe seguir un modelo de arquitectura de software que genere aplicaciones reutilizables e interoperables al interior de la propia dependencia y con otros entes de gobierno, así como privilegiar el uso de estándares abiertos, para lo cual será importante considerar el Estándar “Desarrollo de software” de la Coordinación de Estrategia Digital Nacional ¹⁷⁰.

Adicionalmente el Acuerdo de Gobierno Digital menciona que en el diseño conceptual del proyecto se debe considerar lo siguiente: i) requerimiento del negocio; ii) mecanismos o esquemas de seguridad de la información; iii) políticas de privacidad y protección de datos personales; iv) alcance de los módulos; v) matriz de trazabilidad; vi) protocolos de pruebas y vii) mecanismos de autenticación a través de la Firma Electrónica Avanzada, cuando resulte aplicable. Éste último punto se abordará a detalle en un apartado posterior.

Documentar las reglas de negocio correspondientes y determinar tanto los requerimientos funcionales como los no funcionales, para este aspecto puede ser útil observar lo que menciona la Guía de

¹⁶⁹ Puede consultarse en: <https://wikiguias.atencion.gob.mx/es/interoperabilidad/interoperabilidad> y en <https://wikiguias.atencion.gob.mx/patrones-de-arquitecturas>

¹⁷⁰ Puede consultarse en: <https://wikiguias.atencion.gob.mx/es/desarrollo-de-software/consideraciones-generales>

Digitalización de Digitalización y automatización de Trámites de Colombia.¹⁷¹

Por lo que hace a la imagen, se debe seguir el Manual de Identidad Gráfica 2018-2024 del Gobierno de México.¹⁷²

Aplicar las mejores prácticas para el desarrollo de plataformas web, para lo cual el Acuerdo de Gobierno Digital menciona los estándares y recomendaciones del Consorcio de la Red Informática Mundial (W3C World Wide Web Consortium)¹⁷³ relativos al uso de lenguaje de mercado, hojas de estilo, accesibilidad web y sus validadores.

Considerar que se tenga compatibilidad con navegadores actuales y de futuras generaciones, así como con sistemas operativos móviles y sus navegadores; asimismo que las páginas sean adaptables a resoluciones de dispositivos móviles.

Incluir funciones de accesibilidad para personas con discapacidad, para ello el Acuerdo de Gobierno Digital menciona que se deben considerar los Estándares Técnicos de la Coordinación de Estrategia Digital Nacional, no obstante, es importante señalar que en los Estándares publicados por la Coordinación de Estrategia Digital Nacional aún no se encuentra alguno al respecto.

Realizar las pruebas correspondientes a los sistemas, en esta etapa también será importante involucrar a los usuarios del trámite para poder contar con su perspectiva y observaciones correspondientes desde el inicio del diseño.

Diseñar una estrategia adecuada de capacitación, difusión y mejora continua.

¹⁷¹ Puede consultarse en: https://mintic.gov.co/portal/715/articles-198550_decreto_88_24_enero_2022.pdf

¹⁷² Puede consultarse en: <https://www.gob.mx/wikiguias/articulos/manual-de-identidad-grafica-2018-2024>

¹⁷³ Puede consultarse en: <https://www.w3.org/WAI/standards-guidelines/es>

Para saber más puedes consultar...

Lineamientos generales y consideraciones para diseñar, Perú.

<https://guias.servicios.gob.pe/creacion-servicios-digitales/lineamiento/index>

Conocer el problema y las necesidades de los usuarios, Perú.

<https://guias.servicios.gob.pe/creacion-servicios-digitales/conocer-problema/index>

Seguridad de la información: “La seguridad de la información se define como el conjunto de reglas (políticas), mecanismos (controles) y acciones (procedimientos) que permiten asegurar la información de una organización sin importar la forma en que esta se represente (escrita, oral, gráfica, electrónica, entre otras).¹⁷⁴ Por tanto, en los trámites en línea será fundamental establecer los mecanismos, controles y acciones necesarios que garantizarán la seguridad de la información. Cabe destacar que tiene principalmente tres aspectos: confidencialidad, integridad y disponibilidad.

La confidencialidad hace referencia al acceso que se tiene a la información, el cual solo debe ser por aquellas personas autorizadas; la integridad, por su parte, atiende a que la información solo puede ser modificada o eliminada por los usuarios autorizados; y por último la disponibilidad se refiere a que la información se encuentre disponible en el momento y forma requerida.¹⁷⁵ En los portales, es muy usual controlar los primeros aspectos a través de la creación de los perfiles, ya que de acuerdo a esto se definirá el tipo de información a la que se puede tener acceso y lo que se puede realizar.

¹⁷⁴ Davara Isabel, *op cit.*, p.793

¹⁷⁵ *Idem*

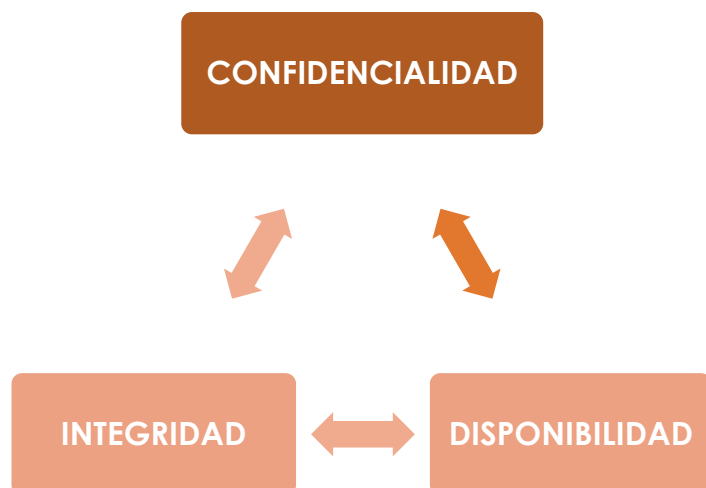


Figura 2. Principios de Seguridad de la Información

Fuente: Elaboración propia

En concordancia con lo anterior, el Acuerdo de Gobierno Digital señala que las instituciones deben contar con un Marco de Gestión de Seguridad de la Información (MGSI) alineado a la política general de SI, en el cual se deberán procurar los máximos niveles de confidencialidad, integridad y disponibilidad de la información. En general la política de seguridad de la información debe estar orientada a garantizar certidumbre en la continuidad de la operación y la permanencia e integridad de la información institucional.¹⁷⁶

Asimismo, en el artículo 76 del citado Acuerdo se señalan los elementos que debe contener el MGSI. Para este efecto será fundamental consultar el Estándar técnico de controles mínimos de seguridad de la información emitido por la Coordinación de Estrategia Digital Nacional.¹⁷⁷

¹⁷⁶ Acuerdo de Gobierno Digital, artículo 75

¹⁷⁷ Puede consultarse en: <https://wikiguias.atencion.gob.mx/es/seguridad-de-la-informacion/estandar-tecnico-de-controles-minimos-de-seguridad-de-la-informacion>

En específico, en relación con las acciones de prevención, detección y respuesta de incidentes se deberán considerar las Bases Técnicas de Seguridad Informática para las dependencias y entidades de la APF.¹⁷⁸

Respecto a la seguridad que deberá proveerse en materia de datos personales, se debe establecer un sistema de gestión de seguridad para el tratamiento de datos personales, el cual de conformidad con el artículo 34 de la LGPDPPSO es el conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales.

“Para adoptar un Sistema de Gestión de Seguridad de Datos Personales (SGSDP), se debe hacer basado en el ciclo PHVA (Planear-Hacer-Verificar-Actuar). Así como también, de estas actividades interrelacionadas para la protección de los datos personales. El responsable debe implementar un sistema de gestión contemplando cuando menos los siguientes aspectos:

- a) Crear políticas internas para la gestión y tratamiento de los datos personales;
- b) Elaborar un inventario de datos personales;
- c) Definir funciones y obligaciones del personal que trate datos personales;
- d) Realizar un análisis de riesgo de los datos personales, el cual deberá considerar amenazas, vulnerabilidades existentes y recursos involucrados en el tratamiento;
- e) Realizar un análisis de brecha. (consistente en comparar las medidas de seguridad existentes contra las medidas de seguridad faltantes;

¹⁷⁸ Puede consultarse en: <https://www.gob.mx/cedn/documentos/bases-tecnicas-de-seguridad-informatica-para-las-dependencias-y-entidades-de-la-administracion-publica-federal>

- f) Elaborar un plan de trabajo para implementar las medidas de seguridad faltantes y el cumplimiento cotidiano de sus políticas de gestión;
- g) Monitorear y revisar de manera periódica las medidas de seguridad implementadas; y
- h) Diseñar y capacitar al personal del responsable”.¹⁷⁹

En este sentido, se debe realizar un análisis detallado de los riesgos y las medidas de seguridad administrativas, físicas, y técnicas, para tal efecto, se recomienda revisar la Guía para cumplir con los principios y deberes de la LGPDPPSO, que detalla cómo se puede realizar lo anterior.

Por otra parte, será fundamental revisar los estándares que existen en esta materia como los emitidos por la Organización Internacional de Normalización (ISO por sus siglas en inglés). Al respecto las principales en materia de seguridad de la información y protección de datos personales son las siguientes:

1 ISO 27000 Vocabulario	2 ISO 27001 Requisitos del SGSI	3 ISO 27002 Guía de buenas prácticas
4 ISO 27003 Guía de implementación de SGSI	5 ISO 27004 Métricas SGSI	6 ISO 27005 Gestión de Riesgo
7 ISO 27007 Directrices de auditoría	8 ISO 27018 Protección de información personal en la nube	9 ISO 27035 Gestión de incidentes de seguridad de la información en la nube
10 ISO 270701	11 ISO 29100 Framework de privacidad	12 ISO 29151

¹⁷⁹ INAI, Guía para cumplir con los principios y deberes de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, pp. 46 y 47.

Sistema de Gestión de Privacidad de la Información		Buenas prácticas de protección de información personal
--	--	--

Cuadro 5. ISOS Seguridad de la información y protección de datos personales

Fuente: Presentación “Privacidad Vs Tecnologías” del Doctor Mario Anselmo Gómez Sánchez

Para saber más puedes consultar...
<p>INAL, Guía para cumplir con los principios y deberes de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPublico/_GuiaPrincipiosDeberes.pdf</p> <p>Lineamientos para la gestión de riesgos de seguridad digital en entidades públicas https://www.funcionpublica.gov.co/documents/418548/34316316/Anexo+4+Lineamientos+para+la+Gestion+del+Riesgo+de++Seguridad+Digital+en+Entidades+P%C3%BAblicas+-+Gu%C3%ADa+riesgos+2018.pdf/1ce5099d-c5e5-8ba2-00bc-58f801d3657b</p>

Interoperabilidad: “Es la capacidad de organizaciones y sistemas dispares y diversos, para interactuar con objetivos consensuados y comunes con la finalidad de obtener beneficios mutuos, en donde la interacción implica que las Instituciones compartan infraestructura, información y conocimiento mediante el intercambio de datos entre sus respectivos sistemas de tecnología de información y comunicación”.¹⁸⁰

De esta manera, la interoperabilidad es un aspecto fundamental para lograr hacer más eficaz y eficiente el servicio público y ser una sola cara al ciudadano. En los trámites es común que la información que se solicita ya sea gestionada por otra dependencia, no obstante, se le solicita al ciudadano, aunque esto signifique para él un doble desplazamiento que implica mayor tiempo, dinero y esfuerzo.¹⁸¹

Ahora bien, la interoperabilidad no es un concepto solo técnico, se requiere contar con un marco jurídico que permita el intercambio de esta información, y después claridad en los estándares que se deberán seguir para lograr este

¹⁸⁰ Acuerdo de Gobierno Digital, artículo 2 fracción XXVIII.

¹⁸¹ Gobierno de Colombia, MINTIC, Marco de Interoperabilidad para el Gobierno Digital, Colombia, p. 19

intercambio, además se contará con un reto mayor cuando ya exista información generada y después se automatice, ya que se deberá contemplar la forma de lograr lo anterior con aquella información que no nació siendo un mensaje de datos.

En este sentido, nuestro marco jurídico contempla ya una normativa que permite este intercambio, en primer término, la Ley Federal de Procedimiento Administrativo refiere que la APF, tiene la obligación de abstenerse de requerir documentos o solicitar información que no sean exigidos por las normas aplicables al procedimiento, o que ya se encuentren en el expediente que se está tramitando, asimismo señala en su artículo 69 C Bis la creación de un expediente electrónico empresarial para evitar duplicidad de información en trámites y crear sinergias entre las diversas bases de datos, las dependencias y organismos descentralizados que estén vinculados en la realización de procedimientos administrativos relacionados con la apertura y operación de empresas. Al respecto, es de destacar que éste se puso en marcha en mayo del año en curso, no obstante, se señaló que actualmente solo tiene información del Registro Público de Comercio y del Módulo Único de Autorizaciones.¹⁸²

En el mismo orden de ideas la Ley General de Mejora Regulatoria menciona la creación de un Expediente de Trámites y Servicios, y al respecto se señala que los Sujetos Obligados no podrán requerir documentación que ya esté integrada en el mismo. Aunado a ello, por lo que hace al derecho de protección de datos personales, la LGPDPSO señala en sus artículos 22 fracción II y 70 fracción II que el responsable no está obligado a recabar el consentimiento del titular para el tratamiento de sus datos personales cuando las transferencias se realicen entre responsables, y sean sobre datos personales que se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos. En este sentido, se podrían compartir datos personales para la resolución de trámites análogos y compatibles, siempre que se cuente con las debidas facultades por parte de las autoridades responsables de dichos trámites.

¹⁸² Puede consultarse en: <https://www.gob.mx/se/prensa/secretaria-de-economia-pone-en-operacion-el-expediente-electronico-empresarial?idiom=es>

Por su parte, el Acuerdo de Gobierno Digital no desarrolla de forma detallada este tema, no obstante, incluye el concepto de interoperabilidad que se mencionó en líneas anteriores y señala que se deberá considerar como campo llave la Clave Única de Registro de Población (CURP) o el RFC al tratarse de personas físicas. Al respecto, se considera que resulta más viable que sea la CURP que es la que tiene cualquier persona y además derivado de la obligatoriedad de solicitarla de acuerdo con lo dispuesto en el Acuerdo para la adopción y uso por la APF de la Clave Única de Registro de la Población.

En el caso de personales morales, se establece que este campo llave será el folio mercantil. Al respecto, es importante destacar que el folio mercantil es único a partir del inicio de operaciones de la nueva plataforma del Registro Público de Comercio, denominada SIGER 2.0 ya que es en esta versión donde las sociedades cuentan con un solo folio mercantil electrónico, la cual inició operaciones en 2015 en 7 entidades federativas.¹⁸³ Por ello, es indispensable considerar que para aquellas personas morales que no cuenten con un folio mercantil único, no sería posible considerar este campo como llave, a pesar de lo descrito por el Acuerdo.

Asimismo, se deberá cumplir con la normativa técnica de domicilios geográficos del Instituto Nacional de Estadística y Geografía (INEGI),¹⁸⁴ la cual permite estandarizar datos para ir logrando la interoperabilidad de conformidad con el Acuerdo de Gobierno Digital

Además de lo anterior, es importante contemplar el Estándar “01 Interoperabilidad”, en el cual se establece que para lograr la interoperabilidad se debe contemplar la actualización de nuevas tecnologías o estándares abiertos que permitan el intercambio de información. Asimismo, se establecen las características del esquema de interoperabilidad, el formato y los medios de distribución.¹⁸⁵

¹⁸³ SE, 2018, “1. Modernización del Registro Público de Comercio: Desarrollo e Implementación del Sistema de Gestión Registral (SIGER 2.0) 2012-2018 Memoria Documental,” pp.23 y 24

¹⁸⁴ Puede consultarse en: puede ser consultada en: https://www.snieg.mx/Documentos/Normatividad/Vigente/Norma_Tecnica_sobre_Domicilios_Geograficos.pdf

¹⁸⁵ Puede consultarse en: puede consultarse en [https://wikiguias.atencion.gob.mx/es/interoperabilidad/interoperabilida,](https://wikiguias.atencion.gob.mx/es/interoperabilidad/interoperabilida)

Por otra parte, se pueden mencionar algunos de los principios que serán aplicables cuando se implementen estos esquemas como son: i) enfoque en el ciudadano, priorizar los servicios de intercambio de información de acuerdo con las necesidades de la ciudadanía; ii) seguridad, protección y preservación de la información, aplicar medidas que aseguren, protejan, preserven y mantengan la privacidad de la información; iii) colaboración y participación, las dependencias deben estimular y participar en los esquemas de interoperabilidad; iv) simplicidad, racionalizar y simplificar trámites; v) neutralidad tecnológica y adaptabilidad, la construcción de servicios en línea debe estar orientada por la funcionalidad y no por la tecnología, no debe haber tecnología exclusiva y limitada a un proveedor; vi) reutilización, aprovechar conocimiento y soluciones tecnológicas previas y con las que ya cuenten otras dependencias; vii) confianza, asegurarse de que se comparte información exacta y confiable y ix) costo efectividad, la inversión debe generar el beneficio que se justifique.¹⁸⁶

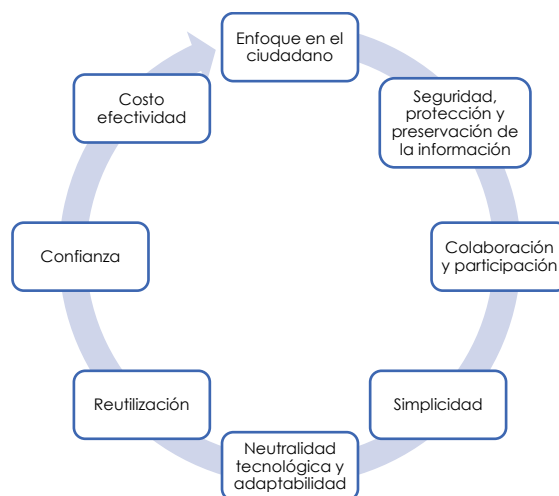


Figura 3. Principios interoperabilidad

Fuente: Elaboración propia con información del Marco de Interoperabilidad para el Gobierno Digital *op cit.*, pp. 28-31

Respecto a los pasos para analizar e implementar estos procesos cumpliendo con la normatividad requerida, el Marco de Interoperabilidad para el

¹⁸⁶ Marco de Interoperabilidad para el Gobierno Digital, *op cit.*, pp. 28-31

Gobierno Digital de Colombia¹⁸⁷, señala una guía muy clara de lo anterior, que puede ser considerada como referencia de acuerdo con lo siguiente:

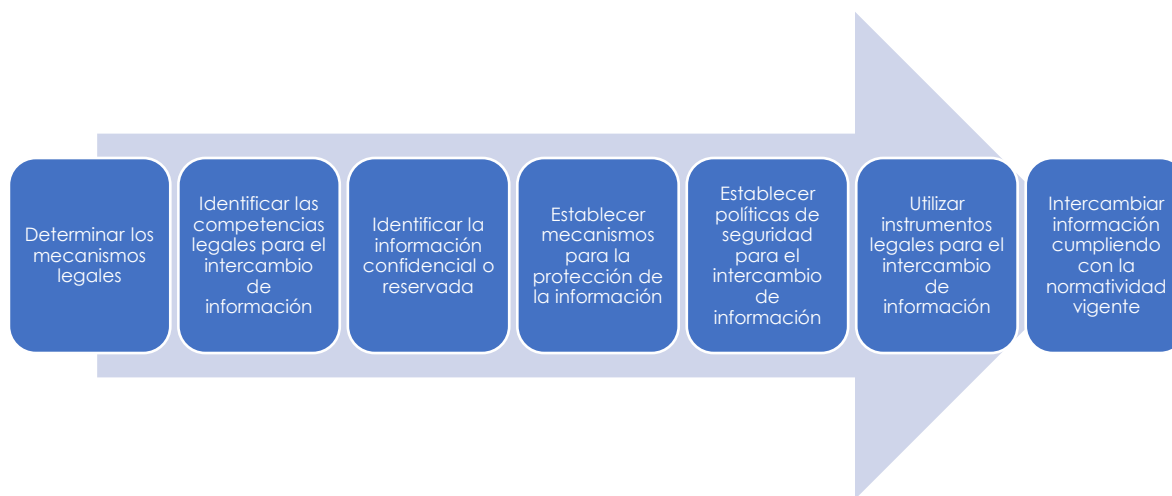


Figura 4. Pasos para implementar procesos de interoperabilidad

Fuente: Elaboración propia con información del Marco de Interoperabilidad para el Gobierno Digital *op cit.*, pp.36 y 37

Para saber más puedes consultar...
CEPAL, Gobernanza Digital e interoperabilidad gubernamental, una guía para su implementación. https://repositorio.cepal.org/bitstream/handle/11362/47018/1/S2100258_es.pdf
Marco de Interoperabilidad para el Gobierno Digital, Colombia, pp.1-94. http://lenguaje.mintic.gov.co/sites/default/files/archivos/marco_de_interoperabilidad_para_gobierno_digital.pdf
Plataforma de Interoperabilidad de Peru https://www.gob.pe/741-presidencia-del-consejo-de-ministros-plataforma-nacional-de-interoperabilidad-del-estado
Interoperabilidad en el gobierno electrónico: aspectos jurídicos a considerar en el desarrollo de plataformas integradas de servicios electrónicos para la Administración Pública. file:///C:/Users/diana/Downloads/Plataforma%20de%20interoperabilidad%20Chile.pdf

Políticas de contratación: además de lo dispuesto en la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, se debe considerar lo que establece

¹⁸⁷ *Ibidem*, pp.36 y 37

el Acuerdo de Gobierno Digital que emitió la Coordinación de Estrategia Digital Nacional donde respecto a este aspecto señala lo siguiente¹⁸⁸:

“Artículo 3.- Para todos los proyectos institucionales que comprendan servicios e implementaciones tecnológicas y de seguridad de la información, la persona titular de la UTIC deberá atender las siguientes políticas y disposiciones generales:

- I. Procurar el ahorro y el uso eficiente de los recursos atendiendo las disposiciones establecidas en la Ley Federal de Austeridad Republicana;
- II. Privilegiar la realización de contratos específicos que deriven de contratos marco vigentes, o la realización de contrataciones consolidadas o licitaciones públicas que garanticen las mejores condiciones para el Estado;
- III. Priorizar el aprovechamiento de los recursos tecnológicos disponibles con que cuentan otras Instituciones, o los registrados en el Inventario de bienes y servicios de TIC de la APF, celebrando los instrumentos de colaboración pertinentes;
- IV. Considerarse entre Instituciones, la celebración de todo tipo de acuerdos que permitan el desarrollo de proyectos conjuntos en materia de TIC.
- V. Privilegiar el alojamiento de la información en territorio nacional y en instalaciones del Estado.
- VI. Observar los Estándares Técnicos emitidos por la CEDN, así como la acreditación de estándares o modelos reconocidos por el sector como las mejores prácticas, y el cumplimiento de normas oficiales;
- VII. Privilegiar el almacenamiento e intercambio de información en formatos basados en estándares abiertos;

¹⁸⁸ Acuerdo de Gobierno Digital, artículo 3

VIII. Atender las disposiciones normativas en materia de protección de datos personales, transparencia y rendición de cuentas;

IX. Sujetarse a la normatividad aplicable en materia de planeación, presupuesto y adquisiciones; y

X. Priorizar los mecanismos que faciliten la participación de los Centros Públicos de Investigación y de las Empresas Productivas del Estado en su desarrollo e implementación; al tratarse de contrataciones de adquisiciones, arrendamientos o servicios de TIC y SI, deberá incluirse la participación de éstos en las investigaciones de mercado que se efectúen, siempre que estén en posibilidades de proveer los bienes o servicios requeridos.”¹⁸⁹

Aunado a lo anterior, se deberá registrar en el registro del Portafolio de Proyectos de Tecnologías de la Información y Comunicación (POTIC).¹⁹⁰

Respecto a ello el Acuerdo de Gobierno Digital establece que cada proyecto debe contener una serie de información para ser presentado, tales como: i) antecedentes; ii) planteamiento del problema; iii) justificación; iv) objetivo; v) impacto; vi) criterios de evaluación; vii) alcance; viii) arquitectura tecnológica; ix) fecha de inicio y cierre del proyecto; x) presupuesto estimado; y xi) cronograma de hitos del proyecto.

Adicionalmente es importante considerar que la Coordinación de Estrategia Digital Nacional deberá emitir un Dictamen Técnico como parte del análisis del proyecto que será indispensable para poder dar inicio al proceso de contratación con la excepción de los supuestos que se mencionan en el mismo Acuerdo.

¹⁸⁹ *Ibidem*

¹⁹⁰ “El POTIC es el conjunto de proyectos estratégicos y operativos en materia de TIC y de SI que las Instituciones planean llevar a cabo en el siguiente ejercicio fiscal”. Acuerdo de Gobierno Digital, artículo 7.

En este orden de ideas es importante resaltar que también se deberá revisar el Inventario de bienes y servicios de la APF, ¹⁹¹ ya que se busca evitar duplicidades aprovechando las que ya existen.

Por lo que hace a la contratación de servicios en la nube, el Acuerdo de Gobierno Digital señala que “en casos específicos, podrá requerirse la contratación de Servicios en la Nube Pública, en este supuesto, deberán aportarse datos que justifiquen la contratación, dentro del Estudio de Factibilidad”. Por su parte la LGPDPPSO, señala que el responsable puede contratar o adherirse a servicios, aplicaciones e infraestructura en el cómputo en la nube y otras materias que impliquen el tratamiento de datos personales siempre que el proveedor garantice políticas de protección de datos personales equivalentes a los principios y deberes establecidos en la misma ley y demás disposiciones aplicables.

Para saber más puedes consultar...

Guía breve para sujetos obligados para la contratación de servicios de cómputo en la nube que impliquen el tratamiento de datos personales https://home.inai.org.mx/wp-content/uploads/Guia_SO_CC.pdf

II) Análisis de los aspectos jurídicos

En primer término, será fundamental analizar el marco jurídico; por lo que hace al que resulta aplicable de forma general a los trámites de la APF se puede considerar lo siguiente:

Elementos que se deben considerar para garantizar la validez de los trámites en línea: la Ley Federal de Procedimiento Administrativo establece las consideraciones generales que aplican a los actos, procesos y procedimientos administrativos, por lo que los **elementos y requisitos del acto administrativo**

¹⁹¹ “El listado que integra los inventarios institucionales de bienes y servicios de TIC, concentrado por la CEDN”, Acuerdo de Gobierno Digital, artículo 2 fracción XXX.

consagrados en el artículo 3 de la Ley, deberán ser integrados en cualquier acto administrativo.

Específicamente respecto a los medios electrónicos, el artículo 69 C de la Ley Federal de Procedimiento Administrativo, establece que se pueden presentar las promociones o solicitudes de los particulares a través de medios de comunicación electrónica en las etapas que las propias dependencias y organismos así lo determinen mediante reglas de carácter general publicadas en el Diario Oficial de la Federación. Asimismo, se señala que en estos casos se emplearán, en sustitución de la firma autógrafa, medios de identificación electrónica.

Aunado a ello, refiere que las dependencias y organismos descentralizados **podrán hacer uso de los medios de comunicación electrónica para realizar notificaciones, citatorios o requerimientos de documentación e información a los particulares.**

Por tanto, **para poder desarrollar un trámite en línea, se deberá establecer en la ley, reglamento o lineamientos aplicables al trámite la forma en que se llevará a cabo, incluyendo pasos, etapas, usuarios, tipos de firmas admitidos tanto para los usuarios como para la autoridad que emite el acto, elementos que deberán contener las resoluciones o documentos que se emitan como resultado del trámite**, es por ello, que si esto no está contemplado en el marco jurídico específico aplicable al trámite deberán realizarse las reformas necesarias.

Asimismo, se deberá garantizar el cumplimiento de los requisitos señalados en el capítulo 2, entre los cuales se encuentran: la integridad, autenticidad y equivalencia funcional de los documentos expedidos electrónicamente, los cuales se deben cumplir para garantizar la validez de éstos cuando se realizan por medios electrónicos.

Al respecto, la Ley Federal de Procedimiento Administrativo, enfatiza que los documentos y promociones presentados electrónicamente, tienen la misma validez que los que se realizan autógrafamente, garantizando con ello el principio de equivalencia funcional.

Ahora bien, por lo que hace a la integridad y la autenticidad de estos documentos en medios electrónicos, además de la firma es importante contemplar otros elementos como son: los sellos digitales de tiempo y las constancias de conservación de mensajes de datos. Al respecto, la Ley Federal de Procedimiento Administrativo menciona que la verificación de la fecha y hora de recepción de las promociones o solicitudes y de la autenticidad de las manifestaciones vertidas en las mismas, deberán hacerse por las dependencias bajo su responsabilidad, y de conformidad con las disposiciones generales que al efecto emita la Secretaría de la Función Pública.¹⁹²

Por su parte el Reglamento de la Ley de Firma Electrónica Avanzada señala que el Acuse de Recibo debe contener un sello digital, no obstante, se considera fundamental contemplarlo no solo en éste, sino también en la resolución respectiva. Al respecto, cabe destacar lo siguiente:

“El sello digital de tiempo permite identificar en que momento se realizó determinado acto, de tal manera que no quede duda de la existencia del mismo. Este sello se encuentra tecnológicamente vinculado con la hora oficial del Centro Nacional de Metrología y Normalización a través de relojes atómicos.”¹⁹³

Es el mismo orden de ideas, en los *Criterios Técnicos que deberán observar las dependencias y entidades de la APF, así como las empresas productivas del Estado, para la emisión de documentos electrónicos que deriven de un trámite o servicio digital* (en adelante “Criterios Técnicos”), se estableció que los mensajes de datos y sus representaciones gráficas deben contener un sello de tiempo y además se refirieron las características que éste debería cumplir, las cuales consisten en las especificaciones técnicas que se establecen en los numerales A.4.2 y A. 6.1 del APENDICE A (NORMATIVO) de la NOM 151,¹⁹⁴ que señalan lo siguiente:

¹⁹² Ley Federal de Procedimiento Administrativo, artículo 69 C

¹⁹³, SE, 2018, “12. Servicios relacionados con Firma Electrónica Avanzada (Sellos de tiempo y NOM-151) Memoria Documental 2012-2018”, p.16

¹⁹⁴ Coordinación de Estrategia Digital Nacional, Criterios Técnicos, 2018, numeral TERCERO inciso g y OCTAVO.

“A.4.2 Cada sello digital de tiempo constará de:

- a) Versión del sello digital de tiempo,
- b) Identificador de Objeto cuyo contenido corresponderá con la versión del documento de las políticas de emisión de sellos digitales de tiempo,
- c) Huella digital electrónica que se obtiene de la solicitud,
- d) Número serial único que identifica al sello digital de tiempo,
- e) Fecha y hora en que se está generando el sello digital de tiempo, y
- f) Extensiones para aquellos casos en que se trate de refrendos de una constancia.

...

A.6 En la presente sección se detallan los procesos y los formatos asociados a la emisión de sello digital de tiempo.

A.6.1 Especificación del sello digital de tiempo:

a) Conforme al RFC 3161, el elemento que trae la información del sello digital de tiempo es la estructura TSTInfo, la cual se define de la siguiente forma:

b) Definición del elemento TSTInfo

TSTInfo ::= SEQUENCE {

version INTEGER {v1(1)},

policy TS

APolicyId,

messageImprint MessageImprint,

MUST have the same value as the similar field in

TimeStampReq

serialNumber INTEGER,

Time-Stamping users MUST be ready to accommodate integers

up to 160 bits.

genTime Generalizedime,

accuracy Accuracy

OPTIONAL,

ordering BOOLEAN DEFAULT FALSE,

nonce INTEGER OPTIONAL,

MUST be present if the similar field was present
in TimeStampReq. In that case it MUST have the same value.

tsa	[0]GeneralName	OPTIONAL,
extensions	[1]IMPLICIT Extensions	OPTIONAL }
...		

En este sentido, entre los servicios que pueden prestar los PSC acreditados por la Secretaría de Economía, se encuentra la emisión de sellos digitales de tiempo. Actualmente existen nueve PSC acreditados para este servicio, mismos que pueden ser consultados en la página de firma digital de la Secretaría de Economía, donde además se pueden consultar sus acreditaciones publicadas en el Diario Oficial de la Federación.¹⁹⁵

Asimismo, debido a que la Secretaría de Economía, tiene una autoridad de sellado de tiempo bajo un esquema de alta disponibilidad¹⁹⁶ y se observa que ha celebrado convenios con algunas dependencias para fomentar la realización de trámites electrónicos¹⁹⁷, se podría tener un acercamiento para consultar la posibilidad de consumir este servicio, atendiendo también al Acuerdo de Gobierno Digital que señala que se debe priorizar el aprovechamiento de los recursos tecnológicos disponibles con que cuentan otras Instituciones, así como los registrados en el Inventario de bienes y servicios de TIC de la APF, para lo cual se deben celebrar los instrumentos de colaboración pertinentes.¹⁹⁸

Aunado a lo anterior, en materia de conservación de mensaje de datos, en las Disposiciones Generales de la Ley de Firma Electrónica Avanzada, **se estableció que se debe observar la NOM 151, a efecto de garantizar la integridad e inalterabilidad del documento y que sea accesible para su ulterior**

¹⁹⁵ La lista de los Prestadores de Servicios de Certificación acreditados puede consultarse en: <http://www.firmadigital.gob.mx/directorio.html>

¹⁹⁶ SE, 12, *op cit.*, p.30

¹⁹⁷ Presidencia de la República, 3 Informe de Gobierno 2020-2021, México, 2021 Informe de gobierno, p.437

¹⁹⁸ Acuerdo de Gobierno Digital, artículo 3, fracción III

consulta, por tanto, se debe contemplar el uso de una **constancia de conservación de mensajes de datos**.¹⁹⁹

Dichas constancias de conservación solo pueden ser emitidas por los PSC autorizados para tal efecto por la Secretaría de Economía de acuerdo a la propia NOM 151. Al respecto, resulta aplicable la lista referida en líneas anteriores respecto a los PSC que pueden prestar este servicio y la página donde se puede consultar lo anterior.



Figura 5: Elementos para garantizar la validez de los trámites en línea

Fuente: Elaboración propia

¹⁹⁹ “Las constancias de conservación de mensajes de datos permiten comprobar que un documento electrónico no ha sido alterado desde su generación”. SE, 12, *op cit.*, p.15.

EJEMPLO DE MARCO JURÍDICO APLICABLE A UN TRÁMITE

Registro Único de Certificados Almacenes y Mercancías

Legislación específica

Ley General de Organizaciones y Actividades Auxiliares del Crédito

Artículo 22 bis 7.- El RUCAM está a cargo de la Secretaría de Economía, será público, se llevará por medios digitales, mediante el programa informático establecido por la propia Secretaría y en una base de datos nacional. Su funcionamiento y operación se regirá por las Reglas de carácter general que para tal efecto emita la Secretaría de Economía.

https://www.diputados.gob.mx/LeyesBiblio/pdf/139_090318.pdf

Reglas de carácter general para el funcionamiento y operación del Registro Único de Certificados, Almacenes y Mercancías

Segunda: Para efectos de las presentes Reglas se entiende por:

...

III. Boleta Electrónica: Documento con firma electrónica y sello digital de tiempo emitido por la Secretaría, el cual cuenta con una cadena única de datos, por medio del cual se hace constar una operación en RUCAM;

IV: Expediente Electrónico: Asiento en el Sistema que, almacena, resguarda e identifica de forma única un Certificado de Depósito y el o los Bono(s) de Prenda asociados a éste, así como la Bodega Propia o Habilitada de un Almacén General de Depósito, y las operaciones que se registren con relación a dicha información.

VII: Sistema: Programa informático establecido por la Secretaría mediante el cual se realiza la captura, envío, almacenamiento, resguardo, consulta y administración de la información registrada en RUCAM;

...

Quinta: El servicio del RUCAM se proporcionará en línea a través del Sistema diseñado para tal fin, el cual contará con la capacidad de recepción, almacenamiento y consulta de la información registrada en el mismo.

Sexta.- Las personas que realicen operaciones en el Sistema para registrar información en los términos señalados en las presentes Reglas, utilizarán su firma electrónica avanzada a través de certificados digitales vigentes que les hayan emitido una Autoridad Certificadora.

Séptima.- La información generada, enviada, recibida, almacenada o archivada en el RUCAM, a través del Sistema, será considerada mensaje de datos en los términos del artículo 89 del Código de Comercio para todos los efectos jurídicos a que haya lugar.

Octava.- Los documentos electrónicos y los mensajes de datos que cuenten con firma electrónica avanzada, producirán los mismos efectos que los presentados con firma autógrafa y, en consecuencia, tendrán el mismo valor probatorio que las disposiciones aplicables les otorgan a éstos, lo anterior en términos de lo dispuesto por el artículo 89, octavo párrafo del Código de Comercio.

Décima.- Los Almacenes Generales de Depósito, a través de su Representante Legal, los Usuarios Autorizados, Fedatarios Públicos, Jueces, Servidores Públicos de la Secretaría y el Público en General deberán autenticarse conforme lo establece el Título Tercero de las presentes Reglas para poder realizar operaciones en el Sistema.

Décima Cuarta.- Las personas señaladas en la Regla Décima Tercera deberán, para su autenticación, proporcionar la información solicitada por el Sistema y

aceptar, mediante su firma electrónica avanzada, los términos y condiciones de uso del Sistema.

El Representante Legal del Almacén General de Depósito adicionalmente a lo establecido en el párrafo anterior, deberá enviar a través del Sistema, el instrumento jurídico por medio del cual acredite la capacidad legal con la que actúa.

Décima Quinta.- Una vez realizada la autenticación, la Secretaría, a través del Sistema, verificará la información proporcionada así como la documentación enviada, y de ser procedente, autorizará a las personas a realizar operaciones en el RUCAM.

Las personas que soliciten su autenticación como Público en General, podrán realizar consultas y solicitar certificaciones sin que requieran autorización de la Secretaría, siempre y cuando se registren en el Sistema con el usuario y contraseña declarado al momento de autenticarse y realicen el pago de derechos cuando así proceda.

Décima Sexta.- El Representante Legal del Almacén General de Depósito, mediante su firma electrónica avanzada y a través del Sistema, podrá autorizar a las personas que estime pertinente para que realicen operaciones a nombre del Almacén General de Depósito, dichas personas tendrán la calidad de Usuario Autorizado.

En todo momento, el Representante Legal del Almacén General de Depósito, mediante su firma electrónica avanzada y a través del Sistema, podrá cancelar la autorización otorgada conforme al párrafo anterior.

Trigésima Primera.- Previa autenticación en el Sistema, y conforme a lo dispuesto en el Título Tercero de las presentes Reglas, se podrá consultar la



Aceptación del particular para el uso de medios electrónicos: la Ley Federal de Procedimiento Administrativo señala que el **uso de medios electrónicos es optativo para cualquier interesado**, por su parte, la Ley de Firma Electrónica Avanzada refiere que se requiere la **manifestación expresa de los particulares** para lo anterior y al respecto el Reglamento de la Ley de Firma Electrónica Avanzada menciona que esta aceptación debe realizarse preferentemente por medios electrónicos en el Sistema de Trámites Electrónicos; no obstante, si este sistema no se ha implementado, se considera que podría realizarse en el sistema que se desarrolle en específico para la implementación del trámite. Por tanto, pudiera contemplarse que esa aceptación se realice al aceptar los Términos y Condiciones del sitio correspondiente.

EJEMPLO

ACEPTACIÓN CONTEMPLADA EN TÉRMINOS Y CONDICIONES

TÉRMINOS Y CONDICIONES DEL SISTEMA ELECTRÓNICO DE PUBLICACIONES DE SOCIEDADES MERCANTILES

La persona que haga uso del “PSM” debe aceptar los presentes Términos y Condiciones por lo que está obligado a analizarlos detenidamente antes de continuar, ya que por el simple uso o acceso a cualquiera de las páginas que integran el “PSM” se entenderá que acepta obligarse en cumplirlos. En caso de no estar de acuerdo en sujetarse a los mismos debe suspender inmediatamente su uso y abstenerse de acceder al “PSM” así como a la información, contenidos o programas que formen parte del mismo.

https://psm.economia.gob.mx/PSM/terminos_condiciones.jsf

Recomendación de redacción

La persona que haga uso del “NOMBRE DEL SISTEMA” acepta realizar “NOMBRE DEL O LOS TRÁMITES” por medios electrónicos desde su inicio hasta su conclusión. En caso de no estar de acuerdo en realizarlos por medios electrónicos debe suspender inmediatamente su uso y abstenerse de acceder al “NOMBRE DEL SISTEMA” así como a la información, contenidos o programas que formen parte del mismo. En dicho caso el trámite podrá llevarse a cabo en “ESPECÍFICAR DIRECCIÓN” de acuerdo con lo señalado en la “FICHA DE TRÁMITE (ESPECÍFICAR HOMOCLEAVE)”

ESPECÍFICACIÓN DE MEDIOS OPTATIVOS

TÉRMINOS Y CONDICIONES DEL REGISTRO PÚBLICO DE COMERCIO

Beneficios y alcances del portal

De conformidad con lo dispuesto en el artículo 20, 20 bis, 30, 30 bis y 30 bis 1 del Código de Comercio, el Gobierno Federal pone a disposición del usuario este Portal, el cual será obligatorio para el personal que opera el SIER 2.0 y **optativo para el fedatario público y ciudadanos ya que en todo momento podrán realizar los trámites de manera presencial** ante las instancias respectivas.

<https://rpc.economia.gob.mx/siger2/xhtml/login/login2.xhtml>

Autenticación electrónica: La acreditación de la identidad es uno de los temas fundamentales para realizar trámites por medios electrónicos, es decir, la verificación de que el usuario es la persona que dice ser y que cuenta con las facultades correspondientes.²⁰⁰ En este sentido, se trata de un proceso que se encuentra plenamente vinculado con el concepto de identidad digital.

²⁰⁰ Red de Gobierno Electrónico de América Latina y el Caribe, 2015, *op cit.*, p. 2

Al respecto, la identidad, puede ser entendida como los atributos y características con las que cuenta una persona que la hace ser única. Por tanto, en el contexto digital los sistemas de identificación implementados por el gobierno, pueden tener varias finalidades: la identificación, paso donde se recolecta información de una persona para determinar su identidad; la autenticación, que permite determinar que una persona es quien dice ser y; la autorización, que es un mecanismo de verificación para determinar si una persona puede o no realizar determinada actividad, o recibir un beneficio.²⁰¹

Ahora bien, en específico la autenticación electrónica puede entenderse como “el procedimiento informático que permite identificar de manera individual e inequívoca los atributos de un usuario, con la finalidad de que pueda acceder a un aplicativo de cómputo o a un servicio electrónico”.²⁰²

Por tanto, este paso también estará íntimamente ligado a los perfiles de usuarios que se generen en un sistema de acuerdo con los privilegios con los que debe contar un usuario, dependiendo del tipo de sistema, facultades requeridas y por tanto de las reglas de negocio establecidas.

Al respecto es importante destacar que debido a la importancia que reviste este proceso, la CNUDMI, ha estado trabajando en el “Grupo de Trabajo IV: Comercio Electrónico” en un “Proyecto de Ley Modelo sobre la utilización y el reconocimiento transfronterizo de la gestión de la identidad y los servicios de confianza”, en el cual se señala que por servicios de gestión de la identidad “se entenderá un proceso utilizado para obtener una garantía suficiente de la vinculación entre una persona y una identidad”.²⁰³

En este sentido, para determinar los atributos y características con las que cuenta una persona se pueden considerar en distintos niveles: i. relacionado con lo

²⁰¹ Cetina Camilo, Capítulo V, Gestión de Riesgos en DIGIntegridad: La transformación digital en la lucha contra la corrupción, Banco de Desarrollo de América Latina (CAF), 2022, p. 157-158

²⁰² Acuerdo de Gobierno Digital, artículo 2 fracción VIII

²⁰³ CNUDMI, Proyecto de Ley Modelo sobre la utilización y el reconocimiento transfronterizo de la gestión de la identidad y los servicios de confianza, 2022, artículo 1 inciso h)

que son las personas (como pudiera ser la biometría); ii) con lo que tienen (como un certificado) y; iii) algo que saben (como una contraseña). En este sentido, los sistemas pueden combinar más de un aspecto dependiendo del nivel de seguridad que requieren.

Es por ello que cuando se ha desarrollado la identidad digital puede resultar mucho más sencillo realizar un proceso de autenticación para realizar trámites en línea, como en el caso de Perú que ya cuenta con un documento de identidad electrónica denominado DNle a través del cual se puede realizar este proceso de autenticación.²⁰⁴

En el caso de México, si bien, como se señaló en el capítulo 2, se presentó una iniciativa al respecto, aún no se cuenta con un documento de identidad digital, por lo que se deberán buscar mecanismos específicos para la autenticación electrónica. Al respecto, el Acuerdo de Gobierno Digital señala que el acceso a las plataformas digitales se debe garantizar mediante mecanismos de autenticación y cifrado a través de certificados digitales. Asimismo, en otro de sus artículos donde aborda el tema de la interoperabilidad señala de forma general que también se pueden utilizar “otros atributos que permitan realizar la autenticación electrónica” y también refiere que en su caso se podrán utilizar mecanismos de autenticación a través de la Firma Electrónica Avanzada (e-firma).

Por tanto, en este Acuerdo el tema de la autenticación electrónica se aborda de forma muy general y como se ha desarrollado a lo largo del presente trabajo, dado que el tipo de autenticación también dependerá del nivel de seguridad requerido no siempre la firma electrónica, será el mecanismo adecuado. Al respecto, las “Disposiciones Generales que establecen los mecanismos de identificación y control de acceso que deberán observar las dependencias y entidades de la APF y las empresas productivas del Estado”, detallan los diferentes niveles de autenticación dependiendo el tipo de usuario de acuerdo con lo siguiente:

²⁰⁴ Puede consultarse en: <https://www.gob.pe/219-sacar-dni-electronico-dnie>

“Tipo “A” Usuario anónimo. - no se requiere de autenticación, ya que se considera como una interacción donde el usuario mantiene secreta su identidad.

Tipo “B” Autenticación con contraseña. - requiere de una autenticación básica, la cual consta de un nombre de usuario y contraseña proporcionada por el usuario

Tipo “C” Autenticación con contraseña dinámica. - requiere de una contraseña que funcione mediante una clave dinámica, de un solo uso, con vigencia determinada y que sirve como mecanismo de acceso a los trámites de las dependencias.

Tipo “D” Autenticación con firma electrónica avanzada. - se requiere que se ingresen los archivos correspondientes a la firma.

Tipo “E” Autenticación a través de datos biométricos. - en esta se requiere se ingrese la CURP y uno o más datos biométricos para que se verifique la identidad de la persona”.²⁰⁵

²⁰⁵ Disposiciones Generales que establecen los mecanismos de identificación y control de acceso que deberán observar las dependencias y entidades de la APF y las empresas productivas del Estado, numeral tercero



Figura 6. Niveles de autenticación

Fuente: Elaboración propia con información del numeral TERCERO de las Disposiciones Generales que establecen los mecanismos de identificación y control de acceso que deberán observar las dependencias y entidades de la APF y las empresas productivas del Estado

Es por lo anterior que para determinar el nivel de autenticación electrónica requerido se deberán analizar los mecanismos de seguridad que correspondan de conformidad con el tipo de trámite y su normativa aplicable, e incluso la etapa en la que se encuentra el usuario dentro del proceso.

EJEMPLOS DE SISTEMAS CON DISTINTOS NIVELES DE AUTENTICACIÓN

NIVEL	DENOMINACIÓN	REGULACIÓN	OPERACIÓN
TIPO A	Consulta de publicaciones de	Acuerdo mediante el cual se establece el	Manual de Usuario del Sistema

	<p>sociedades mercantiles</p> <p>Debido a que sistema nació para realizar las publicaciones que determina la legislación mercantil y que antes se realizaban en periódicos, Diario Oficial, etc., la naturaleza de su consulta es abierta.</p>	<p>Sistema Electrónico de Publicaciones de Sociedades Mercantiles y las disposiciones para su operación</p> <p>Décima Tercera.- Cualquier persona podrá consultar la información en el PSM y descargar las boletas de las publicaciones realizadas.</p> <p>...</p>	<p>Electrónico de Publicaciones de Sociedades Mercantiles</p> <p>4.Operación.</p> <p>I. Consulta publicaciones</p> <p>Cualquier persona podrá consultar información en el PSM y descargar las boletas de publicaciones o rectificaciones, sin necesidad de autenticarse.</p>
--	--	---	---

Consulta Acuerdo en: https://www.dof.gob.mx/nota_detalle.php?codigo=5396538&fecha=12/06/2015#gsc.tab=0

Consulta Manual en: https://psm.economia.gob.mx/PSM/resources/Manual_usuario_PSM.pdf

Consulta Sistema: <https://psm.economia.gob.mx/PSM/index2.jaf>

<p>TIPO B</p>	<p>Consulta en el Registro Único de Garantías Mobiliarias</p> <p>El objetivo de este Registro es que cualquier persona pueda consultar si existen garantías</p>	<p>Reglamento del Registro Público de Comercio</p> <p>ARTÍCULO 34.- Toda persona podrá realizar consultas y solicitar la emisión de certificaciones de Asientos que consten en el RUG.</p>	<p>Lineamientos para la operación del Registro Público de Comercio</p> <p>33. El RUG proporciona servicios en línea de recepción, almacenamiento y consulta de información relativa a</p>
----------------------	--	---	--

	<p>mobiliarias otorgadas a favor de un Acreedor, no obstante, se estableció que si se requiere clave de acceso previo a realizar las consultas correspondientes.</p>	<p>Reglas de carácter general para el funcionamiento y operación del Registro Único de Certificados, Almacenes y Mercancías</p> <p>Trigésima Primera.- Previa autenticación en el Sistema, y conforme a lo dispuesto en el Título Tercero de las presentes Reglas, se podrá consultar la información inscrita en un Expediente Electrónico, así como obtener certificación, previo pago de derechos cuando así corresponda.</p>	<p>las garantías mobiliarias inscritas en él, de conformidad con el Código y el Reglamento. Toda persona que así lo solicite, tendrá acceso al RUG a través del sitio de Internet www.rug.gob.mx, previo registro en dicho sitio.</p>
<p>Consulta Reglamento en: https://rpc.economia.gob.mx/siger2/resources/docs/RRPC.PDF Consulta Lineamientos en: https://rpc.economia.gob.mx/siger2/resources/docs/Lineamientos Op RPC.pdf Consulta las Reglas en: https://www.dof.gob.mx/nota_detalle_popup.php?codigo=5377568 Consulta Sistema: https://www.rug.gob.mx/Rug/homeInicio.do</p>			
TIPO C	<p>No se identifica algún trámite que actualmente utilice este esquema, sin embargo, en el sistema financiero si se utiliza</p>		
TIPO D	<p>Realiza publicaciones</p>	<p>Acuerdo mediante el cual se establece el Sistema Electrónico de</p>	<p>Manual de usuario del sistema de publicaciones de</p>

	de sociedades mercantiles	Publicaciones de Sociedades Mercantiles y las disposiciones para su operación Décima.- ... El Representante Legal deberá ingresar al PSM mediante su firma electrónica avanzada , proporcionar la información solicitada y aceptar los Términos y Condiciones. ...	sociedades mercantiles Se deberá agregar el certificado con terminación .cer, la clave privada con terminación .key y la contraseña de la e.firma, emitida por el SAT, del Representante Legal. Posteriormente se deberá seleccionar la opción de “Ingresar”
Consulta Acuerdo en: https://www.dof.gob.mx/nota_detalle.php?codigo=5396538&fecha=12/06/2015#gsc.tab=0 Consulta Manual en: https://psm.economia.gob.mx/PSM/resources/Manual_Usuario_PSM.pdf Consulta Sistema: https://psm.economia.gob.mx/PSM/			
TIPO E	No se identifica algún trámite que actualmente utilice este esquema, sin embargo, en el sistema financiero si se utiliza		

Es muy importante no establecer mecanismos más complejos y no proporcionales al tipo de trámite, ya que ello implicaría complicar procesos para los usuarios, por lo que será fundamental considerar la proporcionalidad y los principios de economía, eficacia y celeridad administrativa.

En el caso de los trámites específicos antes observados, no es claro porque en el caso del Registro Único de Garantías Mobiliarias se requiere ingresar con claves de acceso a la consulta si es un sistema abierto de consulta pública, por lo que consideramos que no debieran crearse claves de acceso para ello; contrario al caso del Sistema Electrónico de Publicaciones de Sociedades Mercantiles que si

permite la consulta de publicaciones, sin ningún tipo de autenticación, no obstante, cuando se van a realizar publicaciones si requiere la firma electrónica para su ingreso, ello derivado de la vinculación que debe existir con la persona moral para realizar dichas publicaciones, por lo tanto, parece un método proporcional a lo requerido.

Acreditación de facultades del representante legal: el artículo 19 de la Ley Federal de Procedimiento Administrativo señala que en el caso de personas morales deberán acreditarse las facultades del Representante Legal con el instrumento público correspondiente. Ahora bien ¿cómo resolver lo anterior en medios electrónicos? Es decir, como se podría acreditar esta personalidad sin que se tenga que acudir con el instrumento público vía ventanilla. Para ello, pueden existir diversos mecanismos, entre los cuales se pueden señalar los siguientes:

- Que se envíe el instrumento a través del propio sistema digitalizado, así como la identificación necesaria y si existe alguna duda solicitar que se presente para cotejo, no obstante, esta no es la forma más automatizada posible. También se puede considerar que en un sistema esto se realizará idealmente una sola vez, ya que en cuanto se realice el registro de acuerdo con su acreditación, se le asignaría el perfil requerido para ingresar de acuerdo con el método de autenticación correspondiente, por lo que en caso de ser necesario y de acuerdo con la naturaleza y posibilidad del trámite esta sería la forma más básica de llevarlo a cabo.
- Una segunda opción es solicitar que el poder se encuentre inscrito en el Registro Público de Comercio. Actualmente la inscripción de poderes y sus revocaciones es opcional de acuerdo con el artículo 21 fracción VII del Código de Comercio. Por ello, tendría que establecerse como un requisito del trámite que el poder esté inscrito, para efecto de que la autoridad pueda validar directamente esta inscripción en el sistema del Registro Público de Comercio (RPC). <https://rpc.economia.gob.mx/siger2/xhtml/login/login.xhtml>.

Al respecto se observa que en el caso de autoridades se pueden celebrar Convenios de Colaboración con el RPC para efectos de poder consultar su información²⁰⁶.

- Una tercera opción es utilizar el proceso que ya realizó previamente otra autoridad, es decir, la e.firma emitida a la persona moral, ya que para otorgar esta firma el SAT solicita que se presente el poder general para actos de dominio o administración, que acredite la personalidad de la o el representante legal (copia certificada). En este sentido, si el certificado tuviera los datos del nombre del Representante Legal se podría ligar con aquel que presentara el trámite, si por el contrario no tuvieran este dato, no se podría realizar esta vinculación y solo se contaría con la presunción establecida en una ley fiscal, ello podría robustecerse a través de los términos y condiciones que se aceptan, pero aún con lo anterior es importante considerar que esta presunción se encuentra establecida para efectos de lo dispuesto en el Código Fiscal de la Federación. Sin embargo, es de destacar que existen ejemplos de trámites que se llevan a cabo de acuerdo con lo anterior.



Figura 7. Mecanismos para acreditar la personalidad en línea

Fuente: Elaboración propia

²⁰⁶ Presidencia de la República, *op cit.*, p. 437.

Derivado de lo antes señalado, para determinar el método idóneo será fundamental atender a la naturaleza del trámite para determinar el nivel que podría implementarse para cumplir con los niveles requeridos de operación y al mismo tiempo que esté soportado jurídicamente.

EJEMPLO DE DISTINTOS TRÁMITES QUE HAN UTILIZADO LAS FORMAS ANTES REFERIDAS

SOLUCIONES EN DISTINTOS SISTEMAS

EJEMPLO ENVÍO DE PODER POR MEDIO DEL SISTEMA

Registro Único de Certificados Almacenes y Mercancías

Reglas de carácter general para el funcionamiento y operación del Registro Único de Certificados, Almacenes y Mercancías

Décima Cuarta.- Las personas señaladas en la Regla Décima Tercera deberán, para su autenticación, proporcionar la información solicitada por el Sistema y aceptar, mediante su firma electrónica avanzada, los términos y condiciones de uso del Sistema.

El Representante Legal del Almacén General de Depósito adicionalmente a lo establecido en el párrafo anterior, **deberá enviar a través del Sistema, el instrumento jurídico por medio del cual acredite la capacidad legal con la que actúa.**

https://www.dof.gob.mx/nota_detalle_popup.php?codigo=5377568

EJEMPLO A TRAVÉS DE FIRMA DEL SAT (considerando la presunción del Código Fiscal de la Federación)

Lineamientos para la operación del Registro Público de Comercio

35. Los acreedores y entidades financieras en su calidad de acreedores podrán realizar avisos preventivos, inscripciones, modificaciones, transmisiones, rectificaciones por error, cancelaciones, así como renovaciones de vigencia de inscripciones, para **lo cual deberán darse de alta en el sistema como acreedor, utilizando su certificado digital de Firma Electrónica Avanzada emitido por el SAT o por otra Autoridad Certificadora que la Secretaría reconozca** a través del sistema a que se refiere la fracción IX del artículo 1o. del Reglamento. Los acreedores y entidades financieras dados de alta en el sistema podrán autorizar a través del sistema del RUG a cualquier persona para realizar en su nombre Asientos en el RUG. Dichas personas autorizadas podrán tener el carácter de Administradores o Usuarios Autorizados, quienes podrán llevar a cabo las operaciones que los Administradores les hayan previamente autorizado a través del sistema del RUG.

[https://rpc.economia.gob.mx/siger2/resources/docs/Lineamientos Op RP C.pdf](https://rpc.economia.gob.mx/siger2/resources/docs/Lineamientos_Op_RP_C.pdf)

Términos y condiciones del RUG

El usuario que lleva a cabo altas, bajas y cambios en la aplicación de "alta de acreedor" en el RUG, en todo momento en el que realiza dichas operaciones con su firma electrónica, adicionalmente declara lo siguiente:

1. Declaro que cuento con poder general para actos de dominio o administración otorgado por la Persona Física/Moral a la cual represento.
2. **Manifiesto conocer el alcance del artículo 19 A del Código Fiscal de la Federación, que dispone que "se presumirá sin que se admita prueba en**

contrario, que los documentos digitales que contengan firma electrónica avanzada de las personas morales, fueron presentados por el administrador único, el presidente del consejo de administración o la persona o personas, cualquiera que sea el nombre con el que se les designe, que tengan conferida la dirección general, la gerencia general o la administración de la persona moral de que se trate, en el momento en el que se presentaron los documentos digitales."

<https://www.rug.gob.mx/Rug/usuario/add.do>

EJEMPLO A TRAVÉS DE LA FIRMA DEL SAT (DONDE SE SEÑALA QUE LA e.firma DEL REPRESENTANTE LEGAL Y DE LA PERSONA MORAL DEBEN ESTAR ASOCIADAS)

Acuerdo mediante el cual se establece el Sistema Electrónico de Publicaciones de Sociedades Mercantiles y las disposiciones para su operación

Décima.- La autenticación de las personas morales deberá realizarse conforme al siguiente procedimiento y de acuerdo con lo establecido en el manual del programa informático que la Secretaría ponga disposición en el PSM:

El Representante Legal deberá ingresar al PSM mediante su firma electrónica avanzada, proporcionar la información solicitada y aceptar los Términos y Condiciones.

Una vez hecho lo anterior, el Representante Legal deberá dar de alta a la Sociedad en el PSM mediante la firma electrónica avanzada de ésta, ingresando la Denominación o Razón Social y el Registro Federal de Contribuyentes.

https://www.dof.gob.mx/nota_detalle.php?codigo=5396538&fecha=12/06/2015#gsc.tab=0

Manual de Usuario del Sistema Electrónico de Publicaciones de Sociedades Mercantiles

Nota: La e.firma del Representante Legal y persona moral deben estar asociadas https://psm.economia.gob.mx/PSM/resources/Manual_Usuario_PSM.pdf

Mecanismo de consentimiento y vinculación con el mensaje de datos: la Ley Federal de Procedimiento Administrativo señala entre los requisitos que deben contener las promociones que presenten los interesados, que el escrito debe estar firmado. Al respecto cabe destacar que no se especifica que deba ser firma autógrafa, y referente a ello es importante destacar el principio general de derecho “donde la ley no distingue no ha lugar a distinguir”.

No obstante, dado que, en los artículos correspondientes a los medios electrónicos de la misma ley, se refiere que las disposiciones donde se regulen las etapas para la presentación de documentos electrónicos deben establecerse mediante reglas de carácter general publicadas en el Diario Oficial de la Federación, se recomienda que en la regulación específica al trámite se especifique la posibilidad de usar firma electrónica, así como el tipo de firma que se utilizará.

Referente a este último punto, tanto la firma electrónica como la firma electrónica avanzada tienen validez jurídica y equivalencia funcional. Sin embargo, en el caso de los trámites es importante considerar la homologación que se requiere en los procesos a efecto de lograr interoperabilidad y contar con un marco similar, por ello, en los “Criterios Técnicos” se señala que **los mensajes de datos y sus representaciones gráficas deben tener firma electrónica avanzada del servidor público**²⁰⁷, por lo que, en el caso de éste será indispensable usar este tipo de firma y aún en el caso de los usuarios que soliciten el trámite sería recomendable su uso como mecanismo para manifestar el consentimiento, no así su uso necesariamente en el caso de la autenticación tal como se desarrolló previamente. En este sentido, si se utiliza la firma electrónica avanzada, resultarán aplicables las disposiciones de

²⁰⁷ Coordinación de Estrategia Digital Nacional, 2018, *op cit.*, numeral TERCERO, fracción e)

la Ley de Firma Electrónica Avanzada que establecen principios y reglas referentes al uso de medios electrónicos en la implementación de trámites y servicios.

Al respecto, a nivel federal y de acuerdo con la propia Ley antes señalada existen tres autoridades certificadoras: Secretaría de Economía, Servicio de Administración Pública y la Secretaría de la Función Pública. En el caso de la primera si bien, los certificados emitidos por la propia dependencia eran utilizados principalmente para la firma de las inscripciones en el Registro Público de Comercio, actualmente en su nueva plataforma²⁰⁸ se utiliza la Firma Electrónica Avanzada expedida por el Servicio de Administración Tributaria (SAT). Asimismo, es de destacar que es la autoridad raíz a través de la cual se acredita a los PSC.

Por lo que hace a la Secretaría de la Función Pública sus certificados eran utilizados principalmente para llevar a cabo las declaraciones patrimoniales que deben realizar los servidores públicos, no obstante, actualmente también se realizan a través de la Firma Electrónica Avanzada expedida por el Servicio de Administración Tributaria.

En este sentido, pese a que las tres dependencias son consideradas autoridades certificadoras, se observa una política impulsada por parte del Gobierno Federal de utilizar la Firma Electrónica Avanzada expedida por el SAT en todos los trámites de la APF, lo anterior fue reconocido a través de un Convenio de Colaboración que consideró para determinar lo anterior, aspectos como la gratuidad de la firma del SAT, la necesidad de que se eliminaran las múltiples firmas al ciudadano y la capacidad instalada a nivel federal.²⁰⁹

Ahora bien, a diferencia de los otros países, no se cuenta con una aplicación de firma donde se establezca con claridad lo anterior. No obstante, se puede

²⁰⁸

Puede

consultarse

en:

https://rpc.economia.gob.mx/siger2/xhtml/login/login.xhtml;jsessionid=PD0D-fFM96laMr-3ji4ZKqK8VVxE9hiXYPuWagd_hN_XSdXTTy7u!398048140

²⁰⁹ SE, 12, *op. cit.*, p.23

observar que los pasos que han seguido las Dependencias para utilizar la firma electrónica avanzada expedida por el SAT son:²¹⁰:

Reuniones normativas

Firma de Convenio de Colaboración, los convenios que se firmen al respecto deben registrarse en la Secretaría de la Función Pública, por lo cual los mismos pueden consultarse en la liga <https://www.gob.mx/sfp/documentos/convenios-de-firma-electronica-avanzada-por-dependencias?state=published>.

Reuniones técnicas

Las dependencias deben desarrollar la aplicación de la Firma Electrónica Avanzada, asimismo, deben implementar un sello de tiempo ya que la firma electrónica avanzada debe contar con la fecha y hora de su emisión. El SAT proporciona el servicio de consulta del estado de revocación de los certificados “Online Certificate Status Protocol”

Las dependencias deberán verificar ante el SAT la validez y vigencia de los certificados para lo cual el SAT

Para mayor detalle, es importante considerar lo que establecen al respecto las Disposiciones Generales de la Ley de Firma Electrónica Avanza referente a los requerimientos técnicos mínimos y herramientas con los que deben contar las dependencias para el uso de la firma electrónica avanzada:

“QUINTA.- Las dependencias y entidades que requieran utilizar la Firma Electrónica Avanzada, primero deben celebrar un convenio de colaboración o coordinación con la AC que provee el servicio de OCSP y contar con los siguientes requerimientos técnicos mínimos en sus sistemas informáticos, así como en las herramientas tecnológicas o aplicaciones: 1. Contar con la Infraestructura de comunicación

210

Puede

consultarse

en:

http://omawww.sat.gob.mx/ForoTributarioDeServiciosElectronicos2015/Paginas/Documentos/ConveniosColaboracion_FirmaElectronica.pdf

necesaria (equipos de cómputo, conexión a internet). 2. Contar con aplicaciones que empleen el algoritmo de firmado SHA256 con RSA para certificados con una longitud de 1024, 2048 bits o superior. 3. Contar con software capaz de validar los certificados mediante un servicio de consulta basado en el protocolo de comunicación OCSP que permita a los usuarios consultar el estado que guarda un Certificado Digital. 4. Proporcionar a la AC la dirección IP y la URL desde la cual se realizarán las consultas al servicio (considerando la IP del firewall). 5. Configurar sus servicios de comunicación de acuerdo al estándar RFC 6960 – X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP. El procedimiento que deben cumplir las dependencias y entidades, para estar en condiciones de utilizar el protocolo de comunicación OCSP es el siguiente: 1. Verificar que el certificado digital presentado tenga una vigencia válida. 2. Enviar un mensaje para conocer el estado que guarda el certificado digital y suspende la aceptación del certificado digital hasta que la respuesta sea recibida de parte de la AC. 3. Obtener el mensaje de respuesta que envía el servicio de OCSP. 4. Contar con la capacidad de interpretar las respuestas firmadas de las consultas al servicio OCSP utilizando el certificado de la AC para aceptar y en su caso rechazar la solicitud si el certificado ha sido revocado y por lo tanto no es válido a pesar de su vigencia”.

Registro Único de Certificados Almacenes y Mercancías

Reglas de carácter general para el funcionamiento y operación del Registro Único de Certificados, Almacenes y Mercancías

Sexta.- Las personas que realicen operaciones en el Sistema para registrar información en los términos señalados en las presentes Reglas, utilizarán su firma electrónica avanzada a través de certificados digitales vigentes que les hayan emitido una Autoridad Certificadora.

Octava.- Los documentos electrónicos y los mensajes de datos que cuenten con firma electrónica avanzada, producirán los mismos efectos que los presentados con firma autógrafa y, en consecuencia, tendrán el mismo valor probatorio que las disposiciones aplicables les otorgan a éstos, lo anterior en términos de lo dispuesto por el artículo 89, octavo párrafo del Código de Comercio.

https://www.dof.gob.mx/nota_detalle_popup.php?codigo=5377568

Reglamento del Registro Público de Comercio

Registro Único de Garantías Mobiliarias

Artículo 30 bis 1 ...

Los Asientos quedarán realizados en el momento en el que sean firmados electrónicamente por quien los realiza, cuya fecha y hora quedará establecida en el sello digital de tiempo contenido en la boleta que emita el Sistema.

ARTÍCULO 33 Bis 1.- Todo Asiento deberá firmarse electrónicamente en los términos que requiera el Sistema por quien lo realiza, quien será responsable de la existencia y veracidad de la información. Tratándose de instituciones financieras o personas morales que sean acreedores prendarios, fideicomisarios o fiduciarios, éstos serán responsables, independientemente del empleado o funcionario que realiza la inscripción.

La Secretaría podrá reconocer los certificados digitales generados por las autoridades certificadoras a las que se refiere el artículo 23 de la Ley de Firma Electrónica Avanzada, para que los acreedores, entidades financieras en su calidad de Acreedores, personas autorizadas por éstos, jueces, servidores públicos, fedatarios públicos y personas autorizadas por la Secretaría puedan firmar electrónicamente en el Sistema, los Asientos a que se refiere el artículo anterior, siempre y cuando, a su juicio, presenten un grado de confiabilidad y cumplan con las medidas de seguridad suficientes.

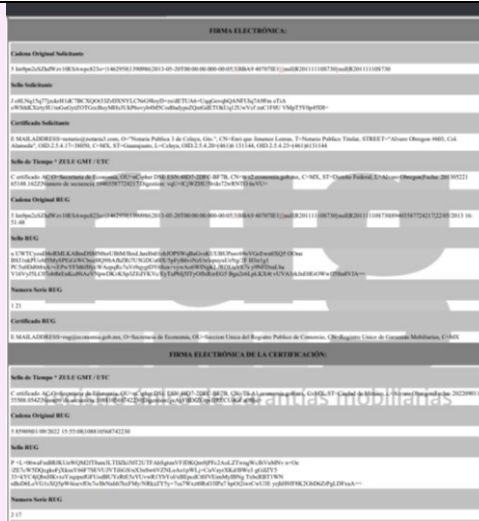
<https://rpc.economia.gob.mx/siger2/resources/docs/RRPC.PDF>

Elementos que deben contener las resoluciones que se emitan por medios electrónicos: en primer término, se debe considerar lo dispuesto en el artículo 3 de la Ley Federal de Procedimiento Administrativo.

Asimismo, contemplar los “Criterios Técnicos” que describen los elementos que deben contener los mensajes de datos y sus representaciones gráficas en el marco de servicios digitales, por lo cual se considera que son aplicables, los cuales son: i) identificador electrónico; ii) servidor público que lo emite; iii) lugar, fecha y hora de emisión; iv) CURP en caso de personas físicas y RFC para personales morales; v) firma electrónica avanzada del servidor público competente; vi) cadena original, que siempre debe contemplar el contenido del documento; vii) sello digital; viii) mecanismos de validación, a través del código bidimensional QR y un sitio de internet; ix) fundamento legal y razones de hecho que se consideren para sustentar el mensaje de datos y su representación gráfica; x) leyenda con el fundamento legal que da validez a la representación gráfica del mensaje de datos.

Respecto a la CURP, es importante señalar que si bien puede ser considerada como un elemento que deben solicitar las Dependencias de la APF como un identificador y campo llave, eso no implica que deba ser plasmado en la representación gráfica del mensaje de datos ya que se trata de un dato personal y al ser publicado dependiendo del tipo de trámite podrían estarse vulnerando los derechos de protección de datos personales de distintas personas.

Los mecanismos de validación son fundamentales para otorgar certeza y confianza en el mensaje de datos y en su representación gráfica, en este sentido y de acuerdo con los Criterios Técnicos la validación de las representaciones gráficas de los documentos electrónicos, **se debe realizar a través de un Código QR y una URL.**



La boleta antes referida se puede validar de la siguiente forma:

2.- Si solo desea dar aviso de una futura garantía mobiliaria de clic en [Aviso Preventivo](#).

3.- Si cuenta con toda la [información necesaria](#) vaya directamente a [Inscribir Garantía Mobiliaria](#).

Validación de Boletas

(Video Tutorial)

Todas las boletas y certificaciones expedidas por el RUG contienen "una cadena única de datos", que podrá ser ingresada al Sistema para verificar su autenticidad. Art 34 RRPC.

Cadena Única de Datos:

Notificaciones electrónicas y acuse de recibo electrónico: la Ley Federal de Procedimiento Administrativo contempla que las notificaciones se pueden realizar por medios electrónicos y que tiene plena validez jurídico; para ello, se pueden considerar las siguientes formas:

Correo electrónico, se recomienda que si se realiza de esta manera, el correo llegue automáticamente del sistema creado para el trámite en línea y que el usuario pueda revisar siempre sus estatus en la plataforma

En el propio sistema donde se implementó el trámite

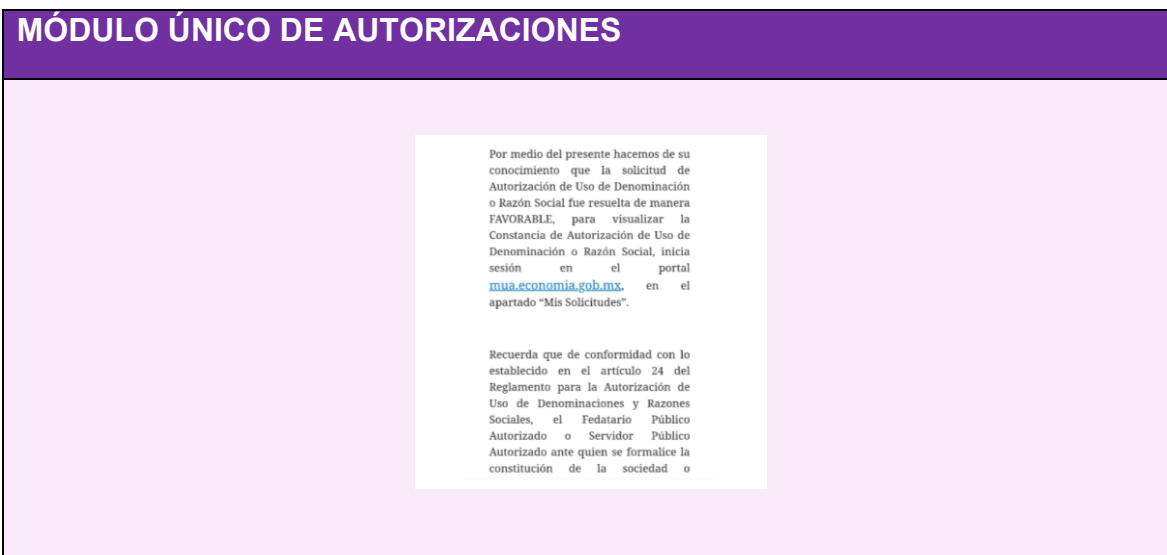
Comunicaciones electrónicas certificadas, no obstante, de acuerdo con el artículo 35 de la Ley Federal de Procedimiento Administrativo, las reglas para éstas deberían contemplarse en la NOM 151 y hasta el momento no han sido publicadas

Figura 8. Medios para realizar la notificación electrónica

Fuente: Elaboración propia

Por su parte, respecto a los Acuses de Recibo Electrónico, el Reglamento de la Ley de Firma Electrónica Avanzada señala que éstos deben contener un sello digital que permita dar plena certeza sobre la fecha y hora de recepción, así como del registro de los Documentos Electrónicos asociados al mismo Acuse. Aunado a lo anterior se contempla que la impresión de los documentos electrónicos suscritos con la Firma Electrónica Avanzada debe contener una cadena de caracteres asociados al documento original; en este sentido, resulta aplicable lo que se señaló respecto al sello digital de tiempo en el apartado Elementos que se deben considerar para garantizar la validez de los trámites en línea y respecto a la validación lo referido en el apartado anterior.

EJEMPLO DE UNA NOTIFICACIÓN POR MEDIO DEL SISTEMA



Transparencia: la transparencia está íntimamente ligada al derecho de acceso a la información, y busca proporcionar a la ciudadanía información accesible, completa y relevante.²¹¹ Por ello, con esta nueva visión, el Estado debe buscar que la información que está en su poder se proporcione de la forma más útil tanto a la ciudadanía para uso particular como a otras dependencias para generar mejores políticas públicas.

Por lo anterior, será fundamental realizar un análisis de la información que se generará con el trámite en línea, considerando este principio y el de máxima publicidad. En este sentido, se deberá observar que la información solo puede ser clasificada como reservada o confidencial bajo ciertos supuestos que se establecen en el artículo 110 y 113 de la LFTAIP respectivamente.

Es por ello que el concepto de dato abierto toma una gran relevancia, el cual se puede considerar desde distintas aristas, desde el lado técnico implica que no se requiera una herramienta especial para su estructura y uso; desde el punto de vista

²¹¹ López Aylon, Sergio, "La transparencia gubernamental" en *Cien ensayos para el centenario. Constitución Política de los Estados Unidos Mexicanos tomo 2: estudios jurídicos*, México, UNAM, 2017, p.282

jurídico implica que el dato sea compartido de forma libre solo citando la fuente.²¹² Es así que el Acuerdo de Gobierno Digital también aborda este concepto señalándolo de la forma siguiente: *“Los datos digitales de carácter público que pueden ser usados, reutilizados y redistribuidos por cualquier interesado”*.²¹³

Asimismo, señala que en el desarrollo de sus aplicativos las instituciones deben considerar los estándares técnicos de datos abiertos²¹⁴. No obstante, los estándares específicos en esta materia no han sido publicados por la Coordinación de Estrategia Digital Nacional. Sin embargo, la Ley General de Transparencia y Acceso a la Información Pública, refiere las características que deben tener los datos abiertos las cuales son las siguientes:

“Artículo 3...

fracción VI...

- a) Accesibles: Los datos están disponibles para la gama más amplia de usuarios, para cualquier propósito;
- b) Integrales: Contienen el tema que describen a detalle y con los metadatos necesarios;
- c) Gratuitos: Se obtienen sin entregar a cambio contraprestación alguna;
- d) No discriminatorios: Los datos están disponibles para cualquier persona, sin necesidad de registro;
- e) Oportunos: Son actualizados, periódicamente, conforme se generen;
- f) Permanentes: Se conservan en el tiempo, para lo cual, las versiones históricas relevantes para uso público se mantendrán disponibles con identificadores adecuados al efecto;
- g) Primarios: Proviene de la fuente de origen con el máximo nivel de desagregación posible;

²¹² Cejudo M Guillermo. Diccionario de Transparencia y Acceso a la Información Pública, INAI, 2019, p.100

²¹³ Acuerdo de Gobierno Digital, artículo 2, fracción XVII

²¹⁴ *Ibidem*, artículo 66

- h) Legibles por máquinas: Deberán estar estructurados, total o parcialmente, para ser procesados e interpretados por equipos electrónicos de manera automática;
- i) En formatos abiertos: Los datos estarán disponibles con el conjunto de características técnicas y de presentación que corresponden a la estructura lógica usada para almacenar datos en un archivo digital, cuyas especificaciones técnicas están disponibles públicamente, que no suponen una dificultad de acceso y que su aplicación y reproducción no estén condicionadas a contraprestación alguna;
- j) De libre uso: Citan la fuente de origen como único requerimiento para ser utilizados libremente;²¹⁵

Por tanto, será fundamental promover que la generación de información que se genere a través de la implementación del trámite en línea cumpla con estos principios.

Para saber más puedes consultar...

Guía de transparencia proactiva emitida por la Secretaría de la Función Pública y el INAI:

https://www.gob.mx/cms/uploads/attachment/file/522552/Gu_a_TransparenciaProactiva2019.pdf

Open Government Standards https://www.access-info.org/wp-content/uploads/Transparency_Standards12072013.pdf

Diccionario de Transparencia y Acceso a la Información Pública (INAI) https://transparencia.guanajuato.gob.mx/bibliotecadigital/normatividad/Diccionario_TyAIP.pdf

<https://datos.gob.mx/>

Datos personales: en la implementación de trámites en línea el gobierno tiene que garantizar el derecho de acceso a la información, pero al mismo tiempo el derecho de protección de datos personales, tal cual fue abordado en el capítulo 1 del presente trabajo. En este sentido, es fundamental garantizar los principios establecidos en la LGPDPPSO, de conformidad con lo siguiente:

²¹⁵ Ley General de Transparencia y Acceso a la Información Pública, Artículo 3, fracción VI

LGDPPSO	Lineamientos Generales de Protección de Datos Personales para el Sector Público
<p>La LGDPPSO puede consultarse en: https://www.diputados.gob.mx/LeyesBiblio/pdf/LGDPPSO.pdf</p> <p>Los Lineamientos pueden consultarse en: https://www.gob.mx/cms/uploads/attachment/file/685007/Lineamientos Generales Protecci n Datos Personales Sectro P blico.pdf</p>	
Licitud	
<p>El tratamiento de datos personales debe estar sujetos a las atribuciones y facultades del responsable.</p>	<p>Ello conforme a su normatividad aplicable, los Lineamientos generales, la legislación mexicana que le resulte aplicable y en su caso el derecho internacional.</p>
Finalidad	
<p>El tratamiento debe tener finalidades concretas, lícitas, explícitas y legítimas.</p> <p>Solo se podrán tratar datos personales para fines distintos a los establecidos en el aviso de privacidad cuando el responsable cuente con atribuciones para ello y cuente con el consentimiento del titular, excepto cuando se trate de una persona desaparecida.</p>	<p>Concretas: cuando el tratamiento atiende a la consecución de fines específicos y determinados</p> <p>Lícitas: cuando las facultades que justifican el tratamiento son acordes con las facultades del responsable.</p> <p>Explícitas: cuando las finalidades se expresan y dan a conocer de manera clara en el aviso de privacidad.</p> <p>Legítimas: cuando las finalidades que motivan el tratamiento de datos personales se encuentran habilitadas por el consentimiento del titular.</p> <p>Observar el artículo 10 de los Lineamientos cuando se trate para fines distintos.</p>

Lealtad	
<p>No se deben obtener datos, por medios engañosos o fraudulentos, se debe proteger la protección de los intereses del titular y la expectativa razonable de privacidad</p>	<p>Por medios engañosos y fraudulentos se entiende aquellos que el responsable utiliza para tratar datos personales con dolo, mala fe o negligencia.</p> <p>Se entiende que privilegia los intereses del titular cuando el tratamiento que realiza no da lugar a discriminación o trato injusto o arbitrario.</p> <p>Por expectativa razonable de privacidad, la confianza que el titular ha depositado en el responsable referente a que sus datos serán tratados conforme al Aviso de Privacidad.</p>
Consentimiento	
<p>Previo al tratamiento de datos personales, el responsable deberá obtener el consentimiento del titular de manera libre, específica e informada.</p>	<p>La solicitud del consentimiento debe ser concisa e inteligible, estar redactada en lenguaje claro y sencillo acorde con el perfil del titular.</p> <p>Por lo que respecta a su modalidad, el consentimiento puede ser de forma expresa o tácita, por regla general es válido el consentimiento tácito, salvo que una ley exija al responsable que sea de forma expresa o cuando se trate de datos personales sensibles.</p> <p>Es tácito, cuando se pone a disposición del titular el aviso de privacidad, éste no manifiesta su voluntad en sentido contrario,</p>

	<p>y es expreso cuando la voluntad del titular se manifieste de forma verbal, por escrito o por medios electrónicos, ópticos, signos inequívocos o por cualquier otra tecnología.</p> <p>Para éste último el responsable debe poner a disposición del titular un medio sencillo y gratuito a través del cual pueda manifestar su voluntad, dentro de esto no se considera: el silencio, las casillas previamente marcadas ni la inacción del titular.</p> <p>En cualquier momento el titular puede ejercer sus derechos ARCO.</p>
Calidad	
<p>El responsable debe adoptar las medidas para mantener exactos, completos, correctos y actualizados los datos personales en su posesión.</p> <p>Se presume que se cumple con la calidad d ellos datos personales cuando éstos son proporcionados directamente por el titular y hasta que éste no manifieste lo contrario.</p>	<p>Exactos y correctos: Cuando los datos personales no presentan errores que pudieran afectar su veracidad.</p> <p>Completos: cuando su integridad permite el cumplimiento de las finalidades que motivaron su tratamiento</p> <p>Actualizados: cuando los datos personales responden fielmente a la situación actual del particular.</p>
Proporcionalidad	
<p>El responsable sólo debe tratar datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento</p>	<p>Esto es cuando son apropiados, indispensables y no excesivos para el cumplimiento de las finalidades que motivaron su obtención.</p>

	<p>Se considerará lo anterior cuando sean:²¹⁶</p> <p>Necesarios: son indispensables conforme a los requisitos que establece la normatividad correspondiente.</p> <p>Adecuados: relacionados con las condiciones, circunstancias y objeto.</p> <p>Relevantes: sean importantes, significativos y no excesivos para el cumplimiento de las finalidades.</p>
Información	
El responsable deberá informar al titular por medio del Aviso de Privacidad la existencia y características principales del tratamiento a la que serán sometidos sus datos personales.	El aviso de privacidad debe ser sencillo, con la información necesaria, expresado en lenguaje claro y comprensible, con una estructura que facilite su entendimiento atendiendo al perfil del titular a quién a dirigido.
Responsabilidad	
Se deben cumplir con diversos mecanismos señalados en el artículo 30 de la LGPDPPSO.	El responsable debe adoptar políticas e implementar mecanismos para asegurar el cumplimiento de los principios, deberes y demás obligaciones establecidas en la Ley General y los Lineamientos Generales.

Cuadro 6. Principios Datos Personales

Fuente: Elaboración propia

De acuerdo con lo anterior, es fundamental que se analicen los datos personales que se solicitarán, para ello se recomienda realizar lo siguiente:

1. Verificar que se encuentre en las facultades y atribuciones, así como fundamentar y motivar adecuadamente el tratamiento. Por tanto, se debe

²¹⁶ INAI, "Recomendaciones para los sujetos obligados respecto a la aplicación del principio de proporcionalidad en el tratamiento de los datos personales recabados" 2021, p.8

realizar un análisis de las facultades de la dependencia en la Ley Orgánica de la APF, en el Reglamento Interno correspondiente, así como del marco jurídico aplicable al trámite ya que los requisitos y datos solicitados deben ser acordes con lo anterior.

2. Buscar mecanismos que permitan que los datos sean exactos y correctos, para ello, cuando sea posible se pueden utilizar bases de datos que permitan corroborar los datos. Por ejemplo, si se solicita la CURP será conveniente no solo realizar una validación de la estructura sino del dato con el Registro Nacional de Población (RENAPO).²¹⁷ Ello permitirá evitar errores en la captura de la información cuando la realiza directamente el usuario.

3. Realizar un análisis de la proporcionalidad en los datos que se están solicitando, por ejemplo, si se realiza el trámite “Inscripción en el Registro Único de Garantías Mobiliarias”, el cual permite inscribir garantías mobiliarias para darles publicidad, prelación y hacerlas oponibles ante terceros²¹⁸, no sería proporcional solicitar el estado civil de las personas. En este sentido, para efecto de cumplir con este principio, se recomiendan revisar las “Recomendaciones para los sujetos obligados respecto a la aplicación del principio de Proporcionalidad en el tratamiento de los datos personales recabados²¹⁹”, la cual contiene un cuestionario que permite contar con una guía sobre el cumplimiento del requisito.

4. Establecer con claridad del Aviso de Privacidad y ponerlo a disposición de los interesados previo al tratamiento de los datos personales.

El Aviso de Privacidad es el “documento a disposición del titular de forma física, electrónica o en cualquier formato generado por el responsable, a partir del

²¹⁷ Puede consultarse en: <https://www.gob.mx/segob/renapo>

²¹⁸ Gobierno de México, Catálogo Nacional de Trámites, servicios, inspecciones y regulaciones de todo México. SE-09-33, Inscripción en el Registro Único de Garantías Mobiliarias (RUG)

²¹⁹ Puede consultarse en: https://home.inai.org.mx/wp-content/uploads/Rec_P_Proporcionalidad.pdf

momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de los mismos”²²⁰.

Este Aviso de acuerdo con la LGPDPPSO debe realizarse en dos modalidades: simplificado e integral. Al respecto, de conformidad con el artículo 27 de la LGPDPPSO el Aviso de Privacidad Simplificado debe contener lo siguiente:

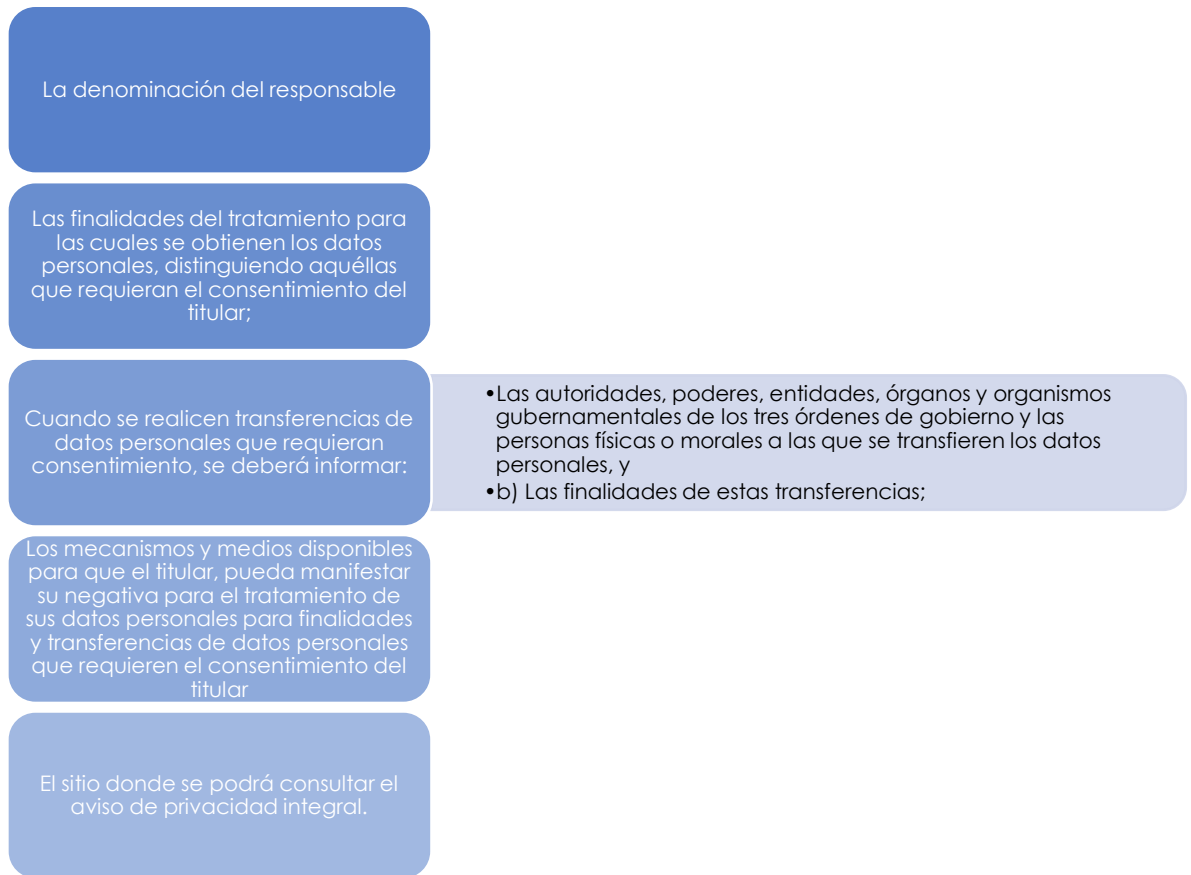


Figura 9. Contenido Aviso de privacidad simplificado

Fuente: Elaboración propia con información del artículo 27 de la LGPDPPSO

Por su parte, el Aviso de Privacidad Integral, además de lo anterior de conformidad con el artículo 28 de la LGPDPPSO debe contener:

²²⁰ Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, artículo 3 fracción II

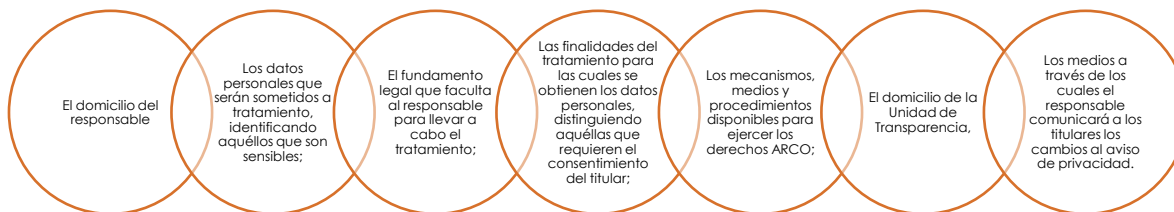


Figura 10. Aviso de Privacidad Integral

Fuente: Elaboración propia con información del artículo 28 de la LGPDPPSO

Para realizar el Aviso de Privacidad puede utilizarse una herramienta del INAI en donde se establece un formato que integra todos los elementos que debe contener cada tipo de Aviso en <http://gapsectorpublico.inai.org.mx/>. Una vez que se ingresa la información que corresponde a cada elemento, se puede obtener el Aviso y realizar en su caso modificaciones si se considera necesario.

Además, se recomienda revisar el “ABC del Aviso de Privacidad” emitido por el INAI donde se puede observar una guía clara sobre la forma de elaborarlo, de ponerlo a disposición de los titulares, de su finalidad, marco normativo, buenas prácticas, así como modelos de cada tipo de aviso. Puede consultarse en: <http://abcavisosprivacidad.ifai.org.mx/PDF/EI%20ABC%20del%20Aviso%20de%20Privacidad.pdf>, así como el Formato de Autoevaluación de Aviso del Sector Público en https://home.inai.org.mx/?page_id=3448 que proporciona un cuestionario donde se detalla cada elemento y de esta manera es posible identificar si se está cumpliendo.

AVISO DE PRIVACIDAD



Aviso de privacidad simplificado:

[https://www.infotec.mx/work/models/Infotec/Resource/743/2/images/Aviso de Privacidad Simplificado-INFOTEC-General.pdf](https://www.infotec.mx/work/models/Infotec/Resource/743/2/images/Aviso_de_Privacidad_Simplificado-INFOTEC-General.pdf)

Aviso de privacidad integral:

[https://www.infotec.mx/work/models/Infotec/Resource/743/2/images/Aviso de Privacidad Integral-INFOTEC-General.pdf](https://www.infotec.mx/work/models/Infotec/Resource/743/2/images/Aviso_de_Privacidad_Integral-INFOTEC-General.pdf)

En el caso del consentimiento, se deberá analizar el tipo de datos que se están solicitando para determinar el tipo de consentimiento que se requiere. Al respecto, la LGPDPSO especifica que puede ser expreso o tácito a menos que la normativa aplicable señale que debe ser expreso o que se trate de datos personales sensibles, lo cual podría realizarse de la forma siguiente:

- Determinar que por el tipo de datos personales que se tratarán puede haber un **consentimiento tácito**, para lo cual se podría poner un mensaje como el siguiente: “En caso de que continúe con el acceso y la navegación de la página se entenderá que consciente el tratamiento de sus datos personales”.
- Solicitar un **consentimiento expreso** para lo cual se podría poner una casilla con el mensaje siguiente: “He leído y acepto el aviso de

privacidad” o en su caso una para seleccionar “Estoy de Acuerdo” o “No estoy de acuerdo”.

- Solicitar un consentimiento expreso y por escrito “Solicitar que se firme electrónicamente la aceptación”.

EJEMPLO DE FORMA DE CONSENTIMIENTO

Usted podrá ejercer los derechos de acceso, rectificación, cancelación u oposición (Derechos ARCO), al tratamiento de sus datos personales, mediante un escrito libre dirigido a la Unidad de Transparencia de la Secretaría de Economía con domicilio en calle Pachuca número 189, Planta Baja, Colonia Condesa, Código Postal 06140, Demarcación Territorial Cuauhtémoc, Ciudad de México, Teléfono 57299100, extensión 11362, correo electrónico: unidaddetransparenciase@economia.gob.mx

¿Dónde puedo consultar el Aviso de privacidad integral de datos personales de la Secretaría de Economía?

Para conocer mayor información sobre los términos y condiciones en que serán tratados sus datos personales, y la forma en que deberá ejercer sus Derechos ARCO, puede consultar el Aviso de Privacidad Integral en la página: <http://www.gob.mx/se/acciones-y-programas/del-aviso-de-privacidad-integral-de-la-secretaria-de-economia?state=published>

Es muy importante que este Aviso de Privacidad se dé a conocer de forma previa al ingreso a un sistema, por lo que podría ponerse en la página inicial del trámite o desplegarse al momento de dar clic para el ingreso o en caso de que se realice un registro de usuario, en la pantalla donde se ingresan los datos para el registro. Ahora bien, debido a que de acuerdo con el artículo 27 fracción IV de la LGPDPSO, se deben poner a disposición de los titulares los mecanismos y medios para manifestar su negativa para el tratamiento de sus datos personales, se recomienda que, aunque sea válido el consentimiento tácito, siempre se ponga una opción para que el titular manifieste su consentimiento o negativa para este tratamiento, como puede ser el mensaje “Estoy de acuerdo” o “No estoy de acuerdo”.

Por otra parte, también se deberán cumplir con los deberes de confidencialidad y seguridad, en el primer caso se refiere a establecer controles o mecanismos que tengan por objeto que todas las personas que intervengan en cualquier fase del tratamiento guarden confidencialidad respecto a los datos personales que tratan, que se evite su divulgación a personas no autorizadas²²¹, es importante considerar que en este caso, las personas que tienen acceso a esta información en su mayoría son servidores públicos a los que les resultará aplicable la Ley General de Responsabilidades Administrativas.

Por su parte respecto al deber de seguridad se deben establecer las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, asimismo se debe garantizar su integridad y disponibilidad, para ello se deberán considerar las actividades mencionadas en el artículo 33 de la LGPDPPSO.

Para ello se deberá contemplar el Sistema de Gestión de Datos Personales que se trató en el apartado de Seguridad respectivo, así como el documento de seguridad el cual de conformidad con el artículo 35 debe contener lo siguiente:

“Artículo 35. De manera particular, el responsable deberá elaborar un documento de seguridad que contenga, al menos, lo siguiente:

I. El inventario de datos personales y de los sistemas de tratamiento;

II. Las funciones y obligaciones de las personas que traten datos personales;

III. El análisis de riesgos;

IV. El análisis de brecha;

V. El plan de trabajo;

VI. Los mecanismos de monitoreo y revisión de las medidas de seguridad, y

VII. El programa general de capacitación.”²²²

²²¹ INAI, Guía para cumplir con los principios y deberes de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, p.45

²²² Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, artículo 35

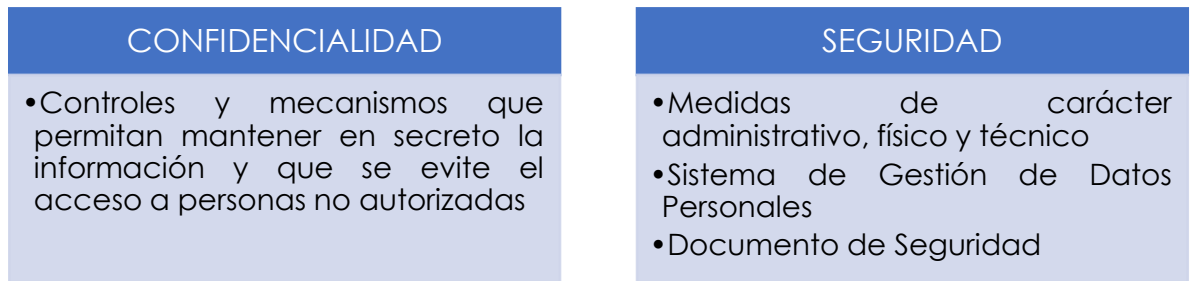


Figura 11. Deberes de protección de datos personales

Fuente: Elaboración propia

Asimismo, será fundamental considerar como se garantizarán los derechos de Acceso, Rectificación, Corrección y Oposición (Derechos ARCO) en el sistema que se implemente para el trámite en línea, por ejemplo, si utilizó un campo como llave, no debería ser a través de un mecanismo en que el usuario pueda tener un error, en este sentido, será importante conectarse con otras bases de datos que puedan ser una fuente de confianza, como pudiera ser RENAPO para la validación de la CURP como se comentó en párrafos previos. De cualquier forma, se deberán garantizar estos derechos y considerar el proceso que se seguirá en el sistema una vez que se solicite alguno de estos derechos.

Para saber más puedes consultar...

El	ABC	del	Aviso	a	la	Privacidad	(INAI)
http://abcavisosprivacidad.ifai.org.mx/PDF/EI%20ABC%20del%20Aviso%20de%20Privacidad.pdf							
Formato de Autoevaluación de Aviso del Sector Público https://home.inai.org.mx/?page_id=3448							
Guía para cumplir con los principios y deberes de la Ley General de Protección de datos personales en	Posesión	de	Sujetos	Obligados	(INAI)	https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPublico/GuiaPrincipiosDeberes.pdf	
Recomendaciones para los sujetos obligados respecto a la aplicación del principio de Proporcionalidad en el	tratamiento	de	los	datos	personales	recabados	(INAI) https://home.inai.org.mx/wp-content/uploads/Rec_P_Proporcionalidad.pdf

Gestión y archivo de información electrónica: la información que se genera por y como parte de estos trámites es de gran valor, aunque en muchas ocasiones en las dependencias se visualiza como un aspecto rutinario, es de destacar que “los documentos y su gestión son reflejo natural de la organización de una institución y es por ello que los procesos de gestión documental, deben necesariamente partir de una profundo cambio de visión de cómo se genera valor y conocimiento dentro de las organizaciones y no en un proceso superficial de cómo clasificar un documento”.²²³

En este sentido, la gestión documental incluye los procesos de toda la gestión del ciclo de una documentación y en el caso de los documentos electrónicos se debe buscar que se garantice su integridad, fiabilidad, autenticidad y disponibilidad.²²⁴

Asimismo, es importante considerar que hay procesos importantes para esta gestión asociados a los propios procesos de la institución como son: i) definir los roles y responsabilidades al interior de la misma; ii) establecer las medidas que deben considerarse sobre la tecnología para el resguardo informático; iii) buscar la estandarización de procesos internos y externos tanto en al interior como a la ciudadanía; iv) realizar una gestión de datos diferenciada, es decir separar la capa de datos de la información general que pueda contener un documento; v)

²²³ Ministerio Secretaría General de la Presidencia, Guía Documental del Estado, Chile, 2019, p.4

²²⁴ *Ibidem*, p.15

estandarizar datos, en donde se deben incluir con claridad las definiciones y formatos en que se guarda la información.²²⁵

Ahora bien, por lo que hace al marco normativo mexicano, se deberá observar lo dispuesto en la Ley General de Archivos que establece algunas reglas generales que deben aplicar a los archivos electrónicos, tales como las siguientes:

Para el caso de aquellos documentos que no nacieron electrónicamente, sino que se están digitalizando²²⁶, se prevé que si tienen un valor histórico se deben conservar en sus formatos originales, así como cuando la ley así lo prevea, aun cuando hayan sido digitalizados, por ejemplo, las inscripciones en un registro público que se realizaba en libros.

Asimismo, como se comentó en el capítulo 2 debido a que los lineamientos del Consejo Nacional de Archivos en esta materia no han sido emitidos, se pueden considerar los aspectos de los Lineamientos para la Organización y Conservación de los Archivo que no sean contrarios a la Ley General de Archivos²²⁷, entre los cuales podemos destacar los siguientes:

- En materia de Digitalización, se señala que los documentos digitalizados serán considerados copias simples, si no existe una disposición legal específica que de validez a éstos, por lo que, en caso de que se vaya a realizar este proceso, se debe establecer en el marco jurídico correspondiente ya que de lo contrario aplicaría esta disposición. Además, señala algunas políticas de digitalización que se pondrán seguir en caso de que ésta se lleve a cabo.
- Se deben aplicar los mismos instrumentos de control y consulta que los que corresponden a soporte en papel.

²²⁵ *Ibidem* p.48

²²⁶ La Digitalización es el proceso de convertir documentos impresos o de otro soporte no digital a un formato digital (Ministerio Secretaría General de la Presidencia, *op cit.*, p.26)

²²⁷ En el artículo segundo transitorio de la Ley General de Archivos se señala que a partir de la entrada en vigor de dicha ley, se abroga la Ley Federal de Archivos y todas aquellas disposiciones que contravienen dicha ley.

- Garantizar las características de autenticidad, fiabilidad, integridad y disponibilidad, las cuales fueron abordadas en el apartado *Elementos que se deben considerar para garantizar la validez de los trámites en línea*.
- Para la gestión documental electrónica, se deben contemplar los procesos de incorporación, asignación de acceso y seguridad, almacenamiento, así como uso y trazabilidad.
- Se debe garantizar la recuperación y conservación de los documentos de archivo electrónicos a lo largo del ciclo vital del documento.
- Respecto a la preservación digital, se debe considerar que la información sea: legible en el futuro, entendible, identificable, recuperable, comprensible, auténtica, en este último caso se deben garantizar mecanismos fiables de transferencia y custodia, entorno de almacenamiento y acceso y protección.
- Adoptar las medidas organizativas, técnicas y tecnológicas necesarias para garantizar al recuperación y conservación de los documentos electrónicos de sus bases de datos, es decir, de estos sistemas a través de los cuales se implementaron los trámites en línea.

Ahora bien, un aspecto fundamental que se debe considerar es garantizar la integridad y su ulterior consulta. Al respecto, como se comentó en el apartado *Elementos que se deben considerar para garantizar la validez de los trámites en línea*, será fundamental considerar la integración de una constancia de conservación de mensaje de datos.

Recomendaciones adicionales

- Considerar la destrucción de expedientes físicos solo en caso de que no tengan valor histórico y se realice la Digitalización conforme a la Norma Oficial Mexicana a que se refiere el artículo 49 del Código de Comercio.
- Especificar lo anterior en el marco jurídico que corresponda.

- Integrar la constancia de conservación de mensaje de datos en los mensajes de datos que se generen con motivo de la implementación del trámite en línea.

Para saber más puedes consultar...

Archivo	General	de	la	Nación,	Breviario	de	metadatos
https://www.gob.mx/cms/uploads/attachment/file/228991/InterPARES_4_020617.pdf							
Archivo General de la Nación, Desarrollo de políticas y procedimientos para la preservación digital							
https://www.gob.mx/cms/uploads/attachment/file/228990/InterPARES_2_020617.pdf							
Archivo General de la Nación, Estrategias para lograr el control de los documentos de archivo digitales en							
ambientes		de		red			distribuidos
https://www.gob.mx/cms/uploads/attachment/file/228994/InterPARES_8_020617.pdf							
Archivo General de la Nación, Gestión y preservación de documentos de archivo en ambientes web							
https://www.gob.mx/cms/uploads/attachment/file/228993/InterPARES_7_020617.pdf							
Guía	Documental	del	Estado,	Chile,	pp.	1-49	https://cms-dgd-prod.s3-us-west-2.amazonaws.com/uploads/pdf/Guia_de_Gesti%C3%B3n_Documental.pdf

III) Pruebas y estrategia de capacitación

Por último, es muy importante considerar una etapa de pruebas y de capacitación tanto al interior de las dependencias como con la propia ciudadanía, uno de los grandes retos cuando se implementan este tipo de servicios es la capacidad de adaptarse a los cambios y de realizar mejoras.

De esta manera, uno de los grandes objetivos con la implementación de trámites en línea es lograr la inclusión digital, la cual debe buscar los beneficios de la incorporación de tecnología en los procesos tanto al interior de las dependencias con los propios servidores públicos, como al exterior con la ciudadanía.

En este sentido, se recomienda incluir en el sitio, Guía del Usuario, Preguntas frecuentes, normatividad aplicable, tutoriales, glosario, datos de contacto (con una mesa de ayuda previamente establecida). Esta mesa será fundamental para aclarar todas las dudas jurídicas y de operación y resolver los problemas que se vayan presentando en la plataforma para lo cual se recomienda establecer con claridad los niveles de servicio y las áreas implicadas en dicha atención, por ejemplo,

además de las áreas de negocio y jurídicas correspondientes, siempre deberá estar relacionada el área de tecnologías y comunicación.

Asimismo, se recomienda implementar un Plan de Difusión en el cual será esencial llegar al mayor número de usuarios posible, con la menor cantidad de recursos. En este sentido, es de trascendencia el momento en que se comunicará, los canales de comunicación y el mensaje, así como tener claridad sobre el universo de los usuarios a los que se les quiere hacer llegar la información. Al respecto, una herramienta para lograr lo anterior pueden ser los Mapas de Actores. En la actualidad pueden existir diversos canales para lo anterior como los siguientes:²²⁸



Figura 12. Medios para la difusión de los trámites en línea

Fuente: Elaboración propia con Guía Documental del Estado, Chile, op cit., pp. 47 y 49

Para saber más puedes consultar...

Cómo acercar los servicios digitales a las personas, Chile en <https://innovadorespublicos.cl/documentation/publication/81/>

Medir el éxito del servicio y próximos pasos, Peru. <https://guias.servicios.gob.pe/creacion-servicios-digitales/medir/index>

²²⁸ Guía Documental del Estado, Chile, op cit., pp. 47 y 49

Como se pudo observar la implementación de trámites en línea puede tener un impacto muy importante en la ciudadanía, en la búsqueda de una nueva visión del gobierno y en la construcción de políticas públicas. Por ello, no se deben perder de vista principios fundamentales de la propia prestación de los servicios públicos y los derechos que se deben garantizar de todas las personas, ya que la tarea del gobierno es mucho más que lograr la eficiencia de procesos.

En este sentido, se debe garantizar la certeza jurídica y la validez de los actos que se realizan a través de medios electrónicos, es así, que se deben considerar aspectos que van desde el diseño del trámite y el involucramiento de los usuarios hasta temas relacionados con la forma en que se realizan las contrataciones y se aprovechan los recursos que ya se encuentran disponibles, así como la forma de garantizar la seguridad de la información y los elementos para lograr la interoperabilidad, sin omitir los aspectos jurídicos que darán validez al trámite. Asimismo, se deberán contemplar los mecanismos para la gestión de la información y la protección de derechos, como el de datos personales, al mismo tiempo que se garantiza la transparencia.

Por último, no se debe perder de vista la necesidad de establecer estrategias de difusión, capacitación y evaluación adecuadas, donde se permita una interacción con la ciudadanía, que permita la mejora continua en estos procesos de transformación. En este sentido, respecto a cada uno de los puntos antes señalados, México cuenta con el marco jurídico que se presentó en esta guía y con diversos elementos que se pueden utilizar para lograr los objetivos antes referidos, las experiencias de implementación previas también pueden ser de utilidad para observar ejemplos acerca de lo que ya se ha realizado, para con ello, realizar una implementación adecuada y eficiente de los trámites para lograr una nueva gestión pública.

Conclusiones



Conclusiones

La implementación de trámites en línea, transaccionales de punta a punta e interoperables es hoy en día una necesidad, parte fundamental de lo que se ha denominado Gobierno Electrónico, que observamos en el capítulo 1. Durante este proceso de transformación será fundamental garantizar la transparencia y generar información y datos que sean de utilidad tanto para el sector público como privado; la información que está en poder del gobierno, debe ser abierta y transparente y por ello incluso hay una responsabilidad para que en el diseño de estos trámites se genere información con esa visión, buscando que tenga la mayor utilidad posible.

Además, durante estos procesos de implementación, es una responsabilidad del gobierno, no generar mayores brechas sociales, por lo que será fundamental que se realice con miras a generar valor público, pero sin excluir a nadie, por tanto, se deben contemplar siempre alternativas para realizar los trámites y para generar mayores estrategias de capacitación buscando disminuir la brecha digital. Asimismo, es fundamental que se observe desde una nueva visión de gestión pública, desde la cual, la responsabilidad de una dependencia va mucho más allá de sus propias facultades, debe haber una visión en común donde se integre a toda la ciudadanía en estos procesos y participen en la construcción de políticas públicas. Aunado a ello, resulta esencial considerar que la eficiencia en los procesos no puede afectar en ningún sentido los derechos de la ciudadanía ni la certeza jurídica.

En este sentido, no se debe perder de vista que se requiere de un marco jurídico sólido que soporte la implementación de estos trámites. Al respecto, como se pudo observar en México desde el año 2000, se iniciaron una serie de reformas que garantizaron la validez de operaciones celebradas por medios electrónicos considerando la propia Ley Modelo de la CNUDMI sobre Comercio Electrónico y la de Firmas Electrónicas. Asimismo, se contemplaron diversos aspectos en lo que refiere a los actos y procedimientos administrativos en la Ley Federal de Procedimiento Administrativo. Aunado a ello, en el año 2012, se expidió la Ley de Firma Electrónica Avanzada y posteriormente su Reglamento y Disposiciones que

establecen pautas específicas cuando se realizan trámites en línea utilizando la firma electrónica avanzada.

Además, es a partir de este año donde se observa una Estrategia clara en materia de gobierno electrónico en la Estrategia Digital Nacional 2013-2018, a partir de la cual, la entonces Unidad de Gobierno Digital expidió una serie de Acuerdos, Criterios y Guías relacionados con la materia y estableció la Ventanilla Única Nacional. Asimismo, como se pudo observar, en el año 2018, se expidió la Ley General de Mejora Regulatoria y la Ley General de Archivos que contemplan diversos aspectos que permiten consolidar este marco con aspectos como el establecimiento de un expediente de Trámites y Servicios y regulación sobre los archivos electrónicos, aunque aún falta ponerlos en operación.

Por otra parte, se abordó la publicación de una nueva Estrategia Digital Nacional publicada en 2021, que a diferencia de la anterior, tiene un enfoque dirigido principalmente a la forma de contratación de los servicios, con el objetivo de no depender de proveedores de tecnologías y hacia el aprovechamiento de los recursos públicos de forma eficiente; derivado de ello se han publicado algunos Acuerdos y Estándares.

En este sentido, a diferencia de los otros países analizados en el capítulo 3, no se observan ni durante la Estrategia Digital Nacional de 2013-2018, ni durante la actual, políticas claras a través de las cuales se establezcan directrices para todas las dependencias. Además, no se desarrollaron tampoco guías detalladas que señalen la forma de llevar a cabo estos procesos, ya que si bien, se expidieron algunas fueron muy generales y desde nuestra visión no contemplan políticas transversales con todos los aspectos que se requieren para la implementación de un trámite en línea.

Por otra parte, tampoco se desarrollaron herramientas transversales que pudieran ser utilizadas directamente por las dependencias, a diferencia de Perú, Chile y Colombia que si cuentan con herramientas específicas que utilizan las distintas entidades públicas en sus procesos de implementación y que garantizan la homologación y el seguimiento de una política rectora en la materia y por tanto la interoperabilidad. Aunado a ello, estos países, han implementado estrategias de

difusión y capacitación tanto al interior del gobierno para los propios servidores públicos, como al exterior, buscando el empoderamiento de su ciudadanía, lo cual, nos parece ha sido fundamental para lograr una estrategia coordinada con miras a cumplir objetivos generales.

Pese a ello, con los aspectos normativos con los que se cuenta en el marco jurídico mexicano, es posible llevar a cabo la implementación de estos trámites en línea con la debida certeza jurídica y garantizando los aspectos que se señalaron en los párrafos precedentes, para ello, se deberán considerar principios y aspectos que se pueden encontrar en distintos instrumentos normativos.

En este sentido, en el capítulo 4, se desarrollaron los aspectos que se consideran necesarios, que van desde el diseño del trámite y políticas de contratación, hasta todos los aspectos normativos correspondientes, como son: los elementos del acto administrativo, aspectos de los propios trámites electrónicos, relacionados con la integridad, confidencialidad, seguridad de la información, autenticidad, así como relacionados con la gestión de la información, para lo cual serán fundamentales los servicios relacionados con firmas electrónicas como los sellos digitales de tiempo y las constancias de conservación de mensajes de datos.

Adicionalmente, se deben contemplar formas adecuadas y proporcionales para temas como la autenticación, identificación y expresión del consentimiento, ya que como se pudo observar, la firma electrónica, no es sinónimo de implementación de trámites en línea; así como todos los aspectos necesarios para garantizar el respeto al derecho a la protección de datos personales y privacidad de las personas que proporcionan su información en estos trámites.

Por último, es importante realizar pruebas con los usuarios del trámite para identificar posibles errores y mejoras, así como llevar a cabo una estrategia adecuada de capacitación, tanto para los servidores públicos responsables del trámite, como para los propios usuarios.

No obstante, no se debe perder de vista que será fundamental que se implemente una política rectora en la materia donde se proporcionen directrices y herramientas claras a las dependencias por parte de la autoridad responsable, ya que de lo contrario, los esfuerzos realizados serán aislados y difícilmente se logrará

realizar de forma homologada para con ello alcanzar la interoperabilidad necesaria para proporcionar servicios integrales a la ciudadanía y lograr ser una sola cara donde todos y todas participen en la construcción de políticas públicas.

Bibliografía

- ACUERDO del Consejo Nacional del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, por el que se aprueban los Lineamientos para la Organización y Conservación de los Archivos. https://dof.gob.mx/nota_detalle.php?codigo=5436056&fecha=04/05/2016#gsc.tab=0 el 14 de septiembre de 2022.
- ACUERDO mediante el cual se aprueban los Lineamientos Generales de Protección de Datos personales en el Sector Público. <https://inicio.inai.org.mx/AcuerdosDelPleno/ACT-PUB-19-12-2017.10.pdf> el 20 de septiembre de 2022
- ACUERDO por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la APF. https://dof.gob.mx/nota_detalle.php?codigo=5628885&fecha=06/09/2021#gsc.tab=0 el 20 de septiembre de 2022
- ACUERDO por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la APF. https://www.dof.gob.mx/nota_detalle.php?codigo=5628885&fecha=06/09/2021#gsc.tab=0 el 30 de junio de 2022
- ACUERDO por el que se expide la Estrategia Digital Nacional 2021-2024, publicado en el Diario Oficial de la Federación el 6 de septiembre de 2021. https://dof.gob.mx/nota_detalle.php?codigo=5628886&fecha=06/09/2021#gsc.tab=0 el 14 de febrero de 2022
- ALIANZA DEL PACÍFICO, ¿Qué es la Alianza del Pacífico? <https://alianzapacifico.net/que-es-la-alianza/> el 31 de marzo de 2022

- ARCHIVO GENERAL DE LA NACIÓN, Breviario de metadatos, pp.1-73
https://www.gob.mx/cms/uploads/attachment/file/228991/InterPARES_4_02_0617.pdf
- ARCHIVO GENERAL DE LA NACIÓN, Desarrollo de políticas y procedimientos para la preservación digital, pp. 1-141
https://www.gob.mx/cms/uploads/attachment/file/228990/InterPARES_2_02_0617.pdf el 15 de septiembre de 2022
- ARCHIVO GENERAL DE LA NACIÓN, Estrategias para lograr el control de los documentos de archivo digitales en ambientes de red distribuidos, pp.1-72
https://www.gob.mx/cms/uploads/attachment/file/228994/InterPARES_8_02_0617.pdf
- ARCHIVO General de la Nación, Gestión y preservación de documentos de archivo en ambientes web, pp.1-66
https://www.gob.mx/cms/uploads/attachment/file/228993/InterPARES_7_02_0617.pdf
- ARELLANO TOLEDO, Wilma, *et al.*, “Derechos de los ciudadanos en el gobierno abierto: doctrina, legislación y políticas en México”, Madrid, 2015, pp. 106-127.
<https://infotec.repositorioinstitucional.mx/jspui/bitstream/1027/196/1/DERECHOS%20DE%20LOS%20CIUDADANOS%20EN%20EL%20GOBIERNO%20ABIERTO%20DOCTRINA%2C%20LEGISLACION%20Y%20POLITICAS%20EN%20ME.pdf> el 01 de junio de 2021.
- ÁVILA BARRIOS, Delia, “El uso de las TICs en el entorno de la nueva gestión pública mexicana”, *Andamios*, México, 2014, vol. 11, núm. 24, pp. 263-288.
http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-00632014000100014 el 01 de junio de 2021.
- BARRERA BADILLO Rocío, Iniciativa con Proyecto de Decreto por el que se expide la Ley General de Población y abroga la Ley General de Población publicada en el Diario Oficial de la Federación el 7 de enero de 1974.
http://sil.gobernacion.gob.mx/Librerias/pp_ReporteSeguimiento.php?SID=2

[7e7bf7d48344c00e225e2b2708cb902&Seguimiento=4120781&Asunto=4041872e](https://www.gacetaoficial.gub.ve/verdocumento.aspx?documento=7e7bf7d48344c00e225e2b2708cb902&Seguimiento=4120781&Asunto=4041872e) 03 de junio de 2022

- CARDONA, Diego, *et al.*, “Gobierno Electrónico en Colombia: Marco Normativo y Desempeño De Tres Índices Estratégicos (Electronic Government in Colombia: Regulatory Framework and Evaluation of Three Strategic Indexes)”, Venezuela, *Revista venezolana de Gerencia*, 2015, vol. 19, núm. 69, pp. 11-34.
- CETINA Camilo, “Banco de Desarrollo de América Latina (CAF), Capítulo V, Gestión de Riesgos en DIGIntegridad: La transformación digital en la lucha contra la corrupción”, 2022, pp. 1-209. <https://scioteca.caf.com/handle/123456789/1838>, el 15 de abril de 2022
- CEJUDO M. Guillermo, *Diccionario de Transparencia y Acceso a la Información Pública*, INAI, 2019, pp.1-100. https://transparencia.guanajuato.gob.mx/bibliotecadigital/normatividad/Diccionario_TyAIP.pdf el 10 de marzo de 2022
- CLAD, “Carta Iberoamericana de Gobierno Electrónico”, Chile, 2007, pp.233-256. <https://clad.org/wp-content/uploads/2020/10/7-Carta-Iberoamericana-de-Gobierno-Electr%C3%B3nico-2007-CLAD.pdf> el 10 de octubre de 2021
- Código de Comercio, <https://www.diputados.gob.mx/LeyesBiblio/pdf/CCom.pdf> el 12 de octubre de 2021
- CONAMER, Manifestación de Impacto Regulatorio. NOM 151 2017. <https://cofemersimir.gob.mx/mirs/53491>
- CNUMDI, *Ley Modelo sobre Comercio Electrónico*, Nueva York, Naciones Unidas, 1999, pp. 1-13 https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/es/05-89453_s_ebook.pdf el 08 de abril de 2022
- CNUDMI, *Ley Modelo de la CNUDMI sobre las Firmas Electrónicas*, Nueva York, Naciones Unidas, 2002, pp. 1-7 <https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/es/ml-elecsig-s.pdf> el 08 de abril de 2022

- CNUDMI, *Guía para la incorporación al derecho interno de la Ley Modelo de la CNUDMI sobre Comercio Electrónico*, Nueva York, Naciones Unidas, 2018, pp. 25-82
- CNUDMI, *GUÍA para la incorporación de la Ley Modelo de la CNUDMI para las firmas electrónicas (2001) al derecho interno*, 2001, pp.9-80
- CNUDMI, *Proyecto de Ley Modelo sobre la utilización y el reconocimiento transfronterizo de la gestión de la identidad y los servicios de confianza*, 2022. <https://documents-dds-ny.un.org/doc/UNDOC/GEN/V22/009/41/PDF/V2200941.pdf?OpenElement>, el 03 de septiembre de 2022
- COORDINACIÓN DE ESTRATEGIA DIGITAL NACIONAL, Bases técnicas de Seguridad Informática para las dependencias y entidades de la APF, 2020. https://www.gob.mx/cms/uploads/attachment/file/651941/Seguridad_Informatica.pdf el 20 de junio de 2022
- COORDINACIÓN DE ESTRATEGIA DIGITAL NACIONAL, Criterios Técnicos que deberán observar las dependencias y entidades de la APF, así como las empresas productivas del Estado, para la emisión de documentos electrónicos que deriven de un trámite o servicio digital, 2018. https://dof.gob.mx/nota_detalle.php?codigo=5544814&fecha=27/11/2018#gsc.tab=0 el 20 de noviembre de 2021
- COVARRUBIAS LLAMAS, Jersain, “Perdiendo El Miedo A Las Firmas Electrónicas (Losing the Fear of Electronic Signatures)”, *Paradigma Judicial Revista Virtual Incluyente*, México, 2020, pp.1-33. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3703397 el 05 de marzo de 2022
- DAVARA Isabel (coord.), *Diccionario de Protección de Datos Personales, Conceptos Fundamentales*. México, 2019, pp. 1-89
- DECRETO por el que se establece la Ventanilla Única Nacional para los Trámites e Información del Gobierno. https://www.dof.gob.mx/nota_detalle.php?codigo=5380863&fecha=03/02/2015#gsc.tab=0 el 25 de agosto de 2022.

- DECRETO 1008 de 2018, Colombia. <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=86902#:~:text=Lineamientos%20y%20est%C3%A1ndares%20de%20la,la%20Pol%C3%ADtica%20de%20Gobierno%20Digital> el 10 de agosto de 2022.
- DECRETO 088 de 24 de enero de 2022, Colombia, p. 1-47. https://mintic.gov.co/portal/715/articles-198550_decreto_88_24_enero_2022.pdf el 11 de agosto de 2022
- DEL RÍO, Agustín Cernuda, “Firma Electrónica”, *III Jornadas Internacionales sobre comercio electrónico*, Universidad de Oviedo, 2002. pp.1-6. <http://www.agustincernuda.info/pubs/comercio2002.pdf> el 05 de marzo de 2022
- DIAZ SALAZAR Cristina y Hernández Rojas Laura, et. al., Iniciativa con proyecto de Decreto por el que se expide la Ley General de Archivos publicada el 7 de noviembre de 2016, pp. 1-74 https://infosen.senado.gob.mx/sgsp/gaceta/63/2/2016-11-17-1/assets/documentos/Inic_Ley_General_Archivos_rubricas.pdf, 10 de octubre de 2021
- DIRECTIVA que establece los Lineamientos para la Conversión Integral de Procedimientos Administrativos a Plataformas o Servicios Digitales, Perú. <https://www.gob.pe/institucion/pcm/normas-legales/1976362-001-2021-pcm-sgd> el 06 de agosto de 2022
- DISPOSICIONES GENERALES que establecen los mecanismos de identificación y control de acceso que deberán observar las dependencias y entidades de la APF y las empresas productivas del Estado, 2018. https://www.dof.gob.mx/nota_detalle.php?codigo=5522133&fecha=10/05/2018, el 10 de noviembre de 2021
- Exposición de motivos de la Ley General de Archivos publicada el 7 de noviembre de 2016, pp. 1-75 https://infosen.senado.gob.mx/sgsp/gaceta/63/2/2016-11-17-1/assets/documentos/Inic_Ley_General_Archivos_rubricas.pdf el 16 de mayo de 2022

- Exposición de motivos Ley Federal de Procedimiento Administrativo Consultado en: <https://legislacion.scjn.gob.mx/Buscador/Paginas/wfProcesoLegislativoCompleto.aspx?q=XiHGMGm0tf3DexUGxyTnSDFmqV5vZ3YAMiojSSjNJwl/tS8cYHBG95BXNuFoXDI1my87xTsyujw4/hJ0R3avMQ==> el 04 de junio de 2022.
- GAMBOA MONTEJANO, Claudia, “Firma Electrónica Avanzada, Análisis de la Iniciativa presentada por el Ejecutivo Federal, Derecho Comparado y Opiniones Especializadas del tema”, Dirección de Servicios de Investigación y Análisis de la Cámara de Diputados, México, 2011, pp. 1-66. <https://www.diputados.gob.mx/sedia/sia/spi/SPI-ISS-02-11.pdf> el 05 de marzo de 2022
- GARCÍA BARRERA, Myrna Elia, “El documento y la firma electrónica, temas centrales de derecho a las nuevas tecnologías”, en Derecho de las Nuevas Tecnologías, UNAM, Instituto de Investigaciones Jurídicas, México, 2008, pp.105-168. <http://ru.juridicas.unam.mx/xmlui/handle/123456789/28894> el 08 de abril de 2022
- GOBIERNO DE COLOMBIA, Función Pública, Decreto 767 de 16 de mayo de 2022, pp.1-9. https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=186766 el 30 de marzo de 2022
- GOBIERNO DE COLOMBIA, Ministerio de Tecnologías de la Información y las Comunicaciones. Viceministerio de Economía Digital Dirección de Gobierno Digital, 2018, Manual de Gobierno Digital, pp.1-87. https://gobiernodigital.mintic.gov.co/692/channels-594_manual_gd.pdf el 30 de marzo de 2022
- GOBIERNO DE COLOMBIA, MINTIC, Marco de Interoperabilidad para el Gobierno Digital, Colombia, pp.1-94. http://lenguaje.mintic.gov.co/sites/default/files/archivos/marco_de_interoperabilidad_para_gobierno_digital.pdf el 17 de septiembre de 2022
- GOBIERNO DE MÉXICO, Catálogo Nacional de Trámites, servicios, inspecciones y regulaciones de todo México. SE-09-33, Inscripción en el Registro Único de

<https://catalogonacional.gob.mx/FichaTramite?traHomoclave=SE-09-033>

- GOBIERNO DE MÉXICO, Manual de Identidad Gráfica 2018-2024 del Gobierno de México, <https://www.gob.mx/wikiguias/articulos/manual-de-identidad-grafica-2018-2024> el 31 de agosto de 2022
- GOBIERNO DE MÉXICO, “Modelo de tramitación electrónica”, *wikiguias*, 2018, <https://www.gob.mx/wikiguias/articulos/modelo-de-tramitacion-electronica?state=published>
- GOB DIGITAL CHILE, Cómo acercar los servicios digitales a las personas, Chile, 2021, pp. 1-60. <https://innovadorespublicos.cl/documentation/publication/81/> el 17 de septiembre de 2022
- GOBIERNO DE LA REPÚBLICA, Estrategia Digital Nacional de 2013-2018, México. [https://www.gob.mx/cms/uploads/attachment/file/17083/Estrategia Digital Nacional.pdf](https://www.gob.mx/cms/uploads/attachment/file/17083/Estrategia_Digital_Nacional.pdf) el 26 de agosto de 2022
- GOBIERNO DE LA REPÚBLICA, Estrategia Digital Nacional 2021-2024, México. https://dof.gob.mx/nota_detalle.php?codigo=5628886&fecha=06/09/2021#gs.tab=0 el 26 de agosto de 2022
- GUTIÉRREZ, Claudio, et al. Gobierno Electrónico en Chile, “Desafíos, perspectivas y oportunidades” *Revista chilena de ingeniería, anales del instituto de ingeniería de Chile*, 2005, vol. 12, núm. 2, p. 67-79
- HUESO LORENZO, Cotino, “Inteligencia artificial, big data y aplicaciones contra la COVID-19: privacidad y protección de datos, *IDP: revista de Internet, derecho y política= revista d'Internet, dret i política*, 2020, núm. 31, pp. 1-17
- INAI, El ABC del Aviso a la Privacidad, p. 1-71 <http://abcavisosprivacidad.ifai.org.mx/PDF/EI%20ABC%20del%20Aviso%20de%20Privacidad.pdf> el 13 de septiembre de 2022
- INAI, Guía para cumplir con los principios y deberes de la Ley General de Protección de datos personales en Posesión de Sujetos Obligados, p.1-78 <https://home.inai.org.mx/wp->

- INAI, Recomendaciones para los sujetos obligados respecto a la aplicación del principio de proporcionalidad en el tratamiento de los datos personales recabados, 2021, p.1-11. https://home.inai.org.mx/wp-content/uploads/Rec_P_Proporcionalidad.pdf el 13 de septiembre de 2022
- LARIOS CÓRDOVA Héctor, Iniciativa con proyecto de Decreto por el que se expide la Ley General de Mejora Regulatoria, p. 7 https://www.senado.gob.mx/comisiones/comercio_fomento/docs/mejora_regulatoria/Iniciativa_LGMR.pdf el 20 de septiembre de 2021
- Ley de Gobierno Digital de Perú. <https://cdn.www.gob.pe/uploads/document/file/353216/decreto-legislativo-que-aprueba-la-ley-de-gobierno-digital-decreto-legislativo-n-1412-1691026-1.pdf> el 06 de agosto de 2022
- Ley Federal de Procedimiento Administrativo, https://www.diputados.gob.mx/LeyesBiblio/pdf/112_180518.pdf, el 12 de octubre de 2021
- Ley Federal de Transparencia y Acceso a la Información Pública. https://www.diputados.gob.mx/LeyesBiblio/pdf/LFTAIP_200521.pdf el 25 de agosto de 2022
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. <https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf> el 01 de septiembre de 2021
- Ley General de Mejora Regulatoria, https://www.diputados.gob.mx/LeyesBiblio/pdf/LGMR_200521.pdf el 02 de septiembre de 2021
- Lineamientos generales y consideraciones para diseñar, Perú. <https://guias.servicios.gob.pe/creacion-servicios-digitales/lineamiento/index> el 17 de septiembre de 2022.
- LÓPEZ AYLON, Sergio, “La transparencia gubernamental” en *Cien ensayos para el centenario. Constitución Política de los Estados Unidos Mexicanos tomo 2: estudios jurídicos*, México, UNAM, 2017, pp. 277, 296.

<https://archivos.juridicas.unam.mx/www/bjv/libros/9/4319/19.pdf> el 10 de marzo de 2022

- LÓPEZ LÓPEZ, Pedro y SAMEK, Toni, “Inclusión digital: un nuevo derecho humano”, *Educación y biblioteca*, Madrid, 2009, núm. 172, pp. 1-9. <https://core.ac.uk/download/pdf/11886312.pdf> el 08 de junio de 2021.
- MADARIAGA CARDONA, Diego Fernando, “El gobierno electrónico. Una herramienta estratégica de toma de decisiones”, *Revista Universidad y Empresa*, Colombia, 2004, vol. 3, núm 3-4-5, p. 20-45.
- MENA ESCOBAR Gustavo y Portillo Arroyo Julio César, “La Firma Electrónica”, pp.55. http://www.fd.uach.mx/noticias/2020/08/10/LJ49_2.pdf el 8 de abril de 2022
- MINISTERIO SECRETARÍA GENERAL DE LA PRESIDENCIA, Guía Documental del Estado, Chile, 2019, pp. 1-49 https://cms-dgd-prod.s3-us-west-2.amazonaws.com/uploads/pdf/Guia_de_Gesti%C3%B3n_Documental.pdf
- MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS, Manual de Simplificación Administrativa y Reducción de cargas para la administración general del Estado., España, 2014. pp.1-108. https://www.mptfp.gob.es/dam/es/portal/funcionpublica/gobernanza-publica/simplificacion/doc-referencia/14_Manual_Simplificacion_Administrativa_y_reduccion_de_cargas_AGE.pdf#page=1 el 27 de agosto de 2022
- MUÑOZ, JAIME Rodríguez Arana, “El derecho fundamental a la buena administración y la centralidad del ciudadano en el Derecho Administrativo” *El nuevo derecho administrativo*, 2011. p. 407-427
- MUÑOZ SORO, José Félix, “Identificación y autenticación en la Ley de Administración electrónica”, Fundación Democracia y Gobierno Local, 12, 2010, pp. 169-197. http://repositorio.gobiernolocal.es/xmlui/bitstream/handle/10873/971/claves12_12_munoz.pdf?sequence=1 el 26 de febrero de 2022
- NACIONES UNIDAS, “Encuesta sobre E-Gobierno 2020 Gobierno digital en la década de acción para el desarrollo sostenible”, 2020, New York, pp. 364,

<https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2020>.

- OEA, “Mandatos y resoluciones del gobierno digital en las Américas”. (página oficial). <http://portal.oas.org/Portal/Sector/SAP/DptodeModernizaci%C3%B3ndelEstadoyGobernabilidad/NPA/SobreProgramadeeGobierno/tabid/811/lanquage/es-CO/default.aspx>, el 10 de abril de 2021
- OECD, “e-Government Studies, The e-Government Imperative”, OCDE, 2003, pp.1-199. https://www.oecd-ilibrary.org/governance/the-e-government-imperative_9789264101197-en-el-10/09/2020), el 20 de mayo de 2021
- ORTEGA GARCÍA, Florencio, “La Firma Electrónica en México”, *TecnoTrend, México, Universidad de la Salle Bajío, número 4, 2016, pp. 1-7*
- PÉREZ ROMERO, Jorge Enrique, “El gobierno digital y los derechos humanos. La normativa costarricense”, *Revista de la Facultad de Derecho de México*, México, 2019, vol. 69, núm. 274-2, pp. 627-644. <http://revistas.unam.mx/index.php/rfdm/article/view/70017> el 01 de junio de 2021
- PRESTOL FLAQUER, Joaquín, “Los Laboratorios de Innovación: como mecanismo para crear Valor Público”, *Revista Centroamericana de Administración Pública*, México, 2020, núm.78, enero-junio 2020, pp.162-187.
- PRESIDENCIA DEL CONSEJO DE MINISTROS DEL PERÚ, “Una mirada al Gobierno electrónico en el Perú”, *Oficina Nacional de Gobierno Electrónico e Informática*, Perú, 2013, pp.1-128. [https://www2.congreso.gob.pe/sicr/cendocbib/con4_uibd.nsf/0D6D8CA5D781070305257E9200775428/\\$FILE/3_pdfsam_libro_ongei.pdf](https://www2.congreso.gob.pe/sicr/cendocbib/con4_uibd.nsf/0D6D8CA5D781070305257E9200775428/$FILE/3_pdfsam_libro_ongei.pdf) el 06 de agosto de 2022
- PRESIDENCIA DE LA REPÚBLICA, 3 Informe de Gobierno 2020-2021, México, 2021 <https://framework-gb.cdn.gob.mx/informe/5b8e7a983a893dfcbd02a8e444abfb44.pdf> el 22 de septiembre de 2022

- REAL ACADEMIA ESPAÑOLA, <https://dle.rae.es/firma?m=form>, el 05 de agosto de 2022
- RED DE GOBIERNO ELECTRÓNICO DE AMÉRICA LATINA Y EL CARIBE, “De la teoría a la práctica: Cómo implementar con éxito el gobierno electrónico. La experiencia regional y las barreras de la e-innovación”, 2008, pp.1-65. <https://idl-bnc-idrc.dspacedirect.org/bitstream/handle/10625/46778/133233.pdf?sequence=1> el 19 de octubre de 2021.
- RED DE GOBIERNO ELECTRÓNICO DE AMÉRICA LATINA Y EL CARIBE, Organización de los Estados Americanos, Banco Interamericano de Desarrollo, Centro de Investigación para el desarrollo Internacional, “e gobierno y autenticación de identidad”, *Boletín e-Gobierno Red GEALC*, 2015, 108 edición, pp.2-20. <http://portal.oas.org/LinkClick.aspx?fileticket=8BCLmudUz0k%3D&tabid=1729> el 01 de septiembre de 2022
- Reglamento de la Oficina de la Presidencia de la República (2019). https://www.dof.gob.mx/nota_detalle.php?codigo=5581283&fecha=09%2F12%2F2019#gsc.tab=0 el 26 de agosto de 2022
- Reglamento que regula la forma en que los procedimientos administrativos deberán expresarse a través de medios electrónicos en las materias que indica, según lo dispuesto en la Ley No. 21.80 sobre transformación digital del Estado, Chile, <https://www.bcn.cl/leychile/navegar?idNorma=1169585> el 12 de agosto de 2022
- SECRETARÍA DE GOBERNACIÓN, Reglamento Interior de la Secretaría de la Función Pública, 2017. https://www.dof.gob.mx/nota_detalle.php?codigo=5490821&fecha=19/07/2017#gsc.tab=0 el 26 de agosto de 2022
- REYES KRAFFT, Alfredo Alejandro, “La firma electrónica y las entidades de certificación”, *Tesis de Doctorado, Universidad Panamericana*, 2004, pp.320
- REYES KRAFFT, Alfredo Alejandro, “La firma electrónica”, *Razón y Palabra*, México, pp.48. <http://www.razonypalabra.org.mx/libros/libros/firma.pdf> el 8 de abril de 2022

- REYES OLMEDO, Patricia, “La sociedad red y el gobierno de la información”, *Universidad de Valparaíso*, Chile, 2013.
- RINCÓN CÁRDENAS, Erick y Vergara, Camilo, “Administración pública electrónica: hacia el procedimiento administrativo electrónico”, *Editorial Universidad del Rosario*, Colombia, 2017, pp.292
- RIVERA URRUTIA, Eugenio, “Concepto y problemas de la construcción del gobierno electrónico. Una revisión de la literatura”, *Gestión y política pública*, México, 2006, vol. 15, núm. 2, pp. 259-305.
- ROBERTS M. Raimundo, “Sobre la digitalización del Estado de Chile: Políticas en curso”, *Biblioteca del Congreso Nacional de Chile/BCN*, Chile, 2020, pp. 1-9.
https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/28623/1/BCN_Gobierno_Digital_Chile_2020.pdf el 12 de agosto de 2022
- ROBLES FARIAS, Diego, “El comercio y la firma electrónicos. El modelo mexicano”, en Becerra Ramírez, Manuel (comp.), *Obra en homenaje a Rodolfo Cruz Miramontes*, México, UNAM, Instituto de Investigaciones Jurídicas, 2008, pp.545-579.
<http://ru.juridicas.unam.mx/xmlui/handle/123456789/29065> el 24 de febrero de 2022
- RODRÍGUEZ GALLARDO, Adolfo, “La brecha digital y sus determinantes,” *UNAM, Centro Universitario de Investigaciones Biotecnológicas*, México, 2006, pp. 1-254.
http://ru.iibi.unam.mx/jspui/bitstream/IIBI_UNAM/L100/1/brecha_digital_y_determinantes.pdf el 08 de junio de 2021.
- RODRÍGUEZ VALDÉS, Osviel y Legón, Carlos M, et al ., “Seguridad y usabilidad de los esquemas y técnicas de autenticación gráfica” *Revista Cubana de Ciencias Informáticas*, 2018, vol. 12, p. 13-27.
- ROJAS AMADI, Victor Manuel, “La Ley Modelo de Comercio Electrónico de la Comisión de Naciones Unidas de Derecho Mercantil Internacional y su transformación en el Sistema Jurídico Mexicano”, en Sánchez Cordero Jorge (comp.), *Centenario de la Constitución de 1917, Reflexiones de Derecho*

Internacional Privado, México, UNAM, Instituto de Investigaciones Jurídicas, 2017, pp.179-202.

<https://archivos.juridicas.unam.mx/www/bjv/libros/10/4730/9.pdf> el 24 de febrero de 2022

- SÁNCHEZ GÓMEZ, Mario Anselmo Gómez, “La protección de datos personales en México: cambios evolutivos a 10 años de su inclusión a nivel constitucional”, *Revista Mexicana de Ciencias Penales*, 2020, vol. 3, núm. 10, p. 47-58.
- SE, 2018, “1. Modernización del Registro Público de Comercio: Desarrollo e Implementación del Sistema de Gestión Registral (SIGER 2.0) 2012-2018 Memoria Documental,” pp. pp.41 https://www.gob.mx/cms/uploads/attachment/file/421889/MD_SCN_1_SIGER_2_0.pdf el 22 de septiembre de 2022.
- SE, 2018, “12. Servicios relacionados con Firma Electrónica Avanzada (Sellos de tiempo y NOM-151) Memoria Documental 2012-2018”, pp.1-41. https://www.gob.mx/cms/uploads/attachment/file/421900/MD_SCN_12_FEA.pdf el 22 de septiembre de 2022
- SECRETARÍA DE GOBERNACIÓN, Reglamento Interior de la Secretaría de la Función Pública, 2017, artículo 34. https://www.dof.gob.mx/nota_detalle.php?codigo=5490821&fecha=19/07/2017 el 30 de agosto de 2022
- SIERRA BECERRIL, Israel, *et al.*, “El Sello Digital de Tiempo: Optimización de la tecnología aplicada al tiempo”, *Repositorio Universitario de la DGTIC, UNAM*, México, 2013. pp. 13 <https://www.ru.tic.unam.mx/handle/123456789/2146> el 08 de abril de 2022
- SOLANGE MAQUEO, María (coord.) Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, COMENTADA, INAI, pp. 1-441
- UNIÓN EUROPEA, Reglamento (UE) No. 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado

interior y por lo que se deroga la Directiva 1999/93/CE.
<https://www.boe.es/doue/2014/257/L00073-00114.pdf>

- ZAMBRANO ACOSTA, Juan, *et al.*, “Las políticas públicas en TIC. Una oportunidad de cerrar la brecha social”, *Revista Educación, Comunicación, Tecnología*, Colombia, volumen 4, núm.7, 2009, pp.1-17
- ZEA HERNÁNDEZ, Germán, “*Estado del arte del gobierno electrónico en Colombia para revisar la implementación del gobierno en línea*” Tesis Doctoral. *Universidad de Cartagena, Colombia*, 2015, pp.1-6