MDTIC

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

"IDENTIDAD DIGITAL Y FIRMA ELECTRÓNICA COMO PILARES DE LA TRANSFORMACIÓN DIGITAL"

PROPUESTA DE INTERVENCIÓN
Que para obtener el grado de MAESTRO EN DERECHO DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Presenta:

Marco Antonio Vega Servín

Asesor:

Mtro. Ernesto Ibarra Sánchez

Ciudad de México, mayo 2021.

CONACYT

INFOTEC POSGRADOS

INFOTEC
POSGRADOS

AUTORIZACIÓN DE IMPRESIÓN Y NO ADEUDO EN BIBLIOTECA

MAESTRÍA EN DERECHO DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Ciudad de México, 19 de octubre de 2021
INFOTEC-DAIC-GCH-SE-0338/2021.

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

IDENTIDAD DIGITAL Y FIRMA ELECTRÓNICA COMO PILARES DE LA TRANSFORMACIÓN DIGITAL

Desarrollado por el alumno **Marco Antonio Vega Servín** y bajo la asesoría del **Mtro. Ernesto Ibarra 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.

Lic. Juan Ramón Abarca Damián
Coordinador de Biblioteca

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 mis padres por su apoyo incondicional
y sus consejos en las buenas y en las malas.

A mi familia y hermanos por ser parte del motor que me impulsa a lograr y compartir mis sueños.

A mi Madrina y Padrino por mostrarme que un rico taco y una charla directa y honesta son formas de querer a tú familia.

A Luis Servín por sembrar en mí la semilla del estudio.

A los Ortiz por ser un ejemplo de fortaleza.

A mis abuel@s Reyna, Martha, Ruperto y Hermilo por su humildad, sencillez y enseñarme con su ejemplo que no importan de dónde vienes sino adónde vas.

Tabla de contenido

Introducción ... 1

Capítulo 1. Revolución Industrial ... 6

1.1 Primera revolución industrial ... 7

1.2 Segunda revolución industrial ... 9

1.3 Tercera revolución industrial ... 10

1.4 Cuarta revolución industrial ... 12

1.4.1 Blockchain ... 16

1.4.2 Inteligencia Artificial ... 17

1.4.3 Cómputo en la nube ... 19

1.4.4 Big Data ... 20

1.4.5 Tecnología 5G ... 20

1.4.6 Internet de las cosas ... 21

1.5 Cumbre Mundial de la Sociedad de la Información ... 22

1.6 Objetivos de Desarrollo Sostenible ... 24

1.7 Tratados de libre comercio en la cuarta revolución industrial ... 26

1.7.1 Mercosur ... 27

1.7.2 ALADI ... 27

1.7.3 Alianza del Pacífico ... 28

1.7.4 T-MEC ... 29

1.7.5 Unión Europea ... 29

1.7.6 Foros de cooperación regional en América Latina ... 31

Capítulo 2. Transformación Digital ... 34

2.1 Transformación Digital ... 34

2.2 Índice de Desarrollo de Gobierno Electrónico ... 36

2.2.1 Ranking de países sobre desarrollo de gobierno electrónico -servicios en línea- ... 39

2.2.2 Sudáfrica ... 40

2.2.3 La Isla de Mauricio ... 41

2.2.4 Corea del Sur ... 42

2.2.5 Singapur ... 43

2.2.6 Estonia ... 44

2.2.7 Dinamarca 47
2.2.8 Australia 48
2.2.9 Nueva Zelanda 48
2.2.10 Estados Unidos 49
2.2.11 Uruguay 52
2.2.12 Canadá 55
2.2.13 Argentina 56
2.2.14 Chile 58
2.2.15 Brasil 62
2.2.16 Principales pilares de las estrategias digitales en el contexto internacional 64
Capítulo 3. Identidad digital y firma electrónica 69
3.1 Derecho a la Identidad 70
3.2 Identidad legal 72
3.3 Identidad digital 73
3.3.1 Principios de la identidad digital de la UIT 75
3.4 La firma en la era digital 78
3.4.1 Concepto de firma 78
3.4.2 Firma electrónica simple 80
3.4.3 Firma electrónica avanzada 83
3.4.4 Firma electrónica cualificada 84
3.5 Identidad digital y firma electrónica en el contexto internacional 86
3.5.1 Sudáfrica 86
3.5.2 La Isla Mauricio 87
3.5.3 Corea del Sur 88
3.5.4 Singapur 89
3.5.5 Estonia 91
3.5.6 Dinamarca 92
3.5.7 Australia 93
3.5.8 Estados Unidos 94
3.5.9 Uruguay 96
3.5.10 Canadá 98
3.5.11 Argentina 99
3.5.12 Chile 101

3.5.13 Brasil 103
3.5.14 Comparativo de sistemas de identidad y firma electrónica 104
3.6 Reconocimiento transfronterizo de identidad digital y firma electrónica 108
Capítulo 4. Transformación Digital en México 114
4.1. Regulación de acceso a las TIC e Internet 114
4.1.1 Política de Inclusión Digital Universal 118
4.1.2 Infraestructura 120
4.1.3 Capital Humano 122
4.1.4 Servicios digitales 124
4.1.5 Coordinación institucional para la transformación digital. 125
4.2 El derecho a la identidad en México 129
4.2.1 Identidad RENAPO 130
4.2.2 Identidad fiscal 131
4.2.3 Identidad electoral 132
4.2.4 Identidad pasaporte 132
4.2.5 Identidad militar 133
4.2.6 Identidad cédula profesional 133
4.2.7 Licencia de conducir 134
4.2.8 Identidad digital financiera 135
4.2.8 Hacia un modelo de identidad digital en México 139
4.3 La firma electrónica en México 143
4.3.1 Comercio electrónico 144
4.3.2 Administración Pública Federal 146
4.3.3 Firma electrónica en materia fiscal 149
4.3.4 Firma electrónica en la administración local 150
4.3.5 Firma electrónica en el Poder Judicial Federal y Local 151
4.3.6 Hacia una ley general de firma electrónica avanzada en México 152
Conclusiones 155
Bibliografía 175
ANEXO I. Mecanismos de identidad digital en el contexto internacional 200
ANEXO II. Sistemas internacionales de firma electrónica 204
ANEXO III. Atribuciones institucionales sobre la transformación digital en México 206
ANEXO IV. Legislación en México sobre firma electrónica avanzada 214

Índice de figuras

Figura 1. Agendas Digitales Internacional. Nube de Palabras..... 65

Índice de cuadros

Cuadro 1. Revoluciones industriales y derechos humanos 15
Cuadro 2. Estructura de cuestionario del índice se servicios digitales conforme al EDGI 38
Cuadro 3. Pilares de la agenda digital de Estonia 46
Cuadro 4. Coordinación institucional para la transformación digital de México 128
Cuadro 5. Documentos de identidad en México 137

Siglas y abreviaturas

ALADI	Asociación Latinoamericana de Integración
AGESIC	Agencia de Gobierno electrónico y Sociedad de la Información y del Conocimiento
APF	Administración Pública Federal
BID	Banco Interamericano de Desarrollo
CCN	Número de Control de Tarjeta
CCOM	Código de Comercio
CEDN	Coordinación de la Estrategia Digital Nacional
CFE	Comisión Federal de Electricidad
CFF	Código Fiscal de la Federación
CJF	Consejo de la Judicatura Federal
CMSI	Cumbre Mundial de la Sociedad de la Información
CNUDMI	Comisión de las Naciones Unidas para el Derecho Mercantil Internacional
CONACYT	Consejo Nacional de Ciencia y Tecnología
CONAMER	Comisión Nacional de Mejora Regulatoria
CPEUM	Constitución Política de los Estados Unidos Mexicanos
CSIRT	Centro Nacional de Operación de Ciberseguridad
CURP	Clave Única de Registro Poblacional
DOF	Diario Oficial de la Federación
EDGI	Índice de Desarrollo de Gobierno Electrónico (EGDI, por sus siglas en inglés)
EDN	Estrategia Digital Nacional
IA	Inteligencia Artificial
INEGI	Instituto Nacional de Estadísticas, Geografía e Informática
IFT	Instituto Federal de Telecomunicaciones
INAI	Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales
ITU	*International Telecomunication Union*
ID	Identificación Digital

LFFEA	Ley Federal de Firma Electrónica Avanzada
LFTR	Ley Federal de Telecomunicaciones y Radiodifusión
LGMR	Ley General de Mejora Regulatoria
LGP	Ley General de Población
LOAPF	Ley Orgánica de la Administración Pública Federal
MIT	*Massachusetts Institute of Technology*
MNID	Modelo Nacional de Identidad Nacional
MNIS	Autoridad de Certificación-Isla Mauricio
MERCOSUR	Mercado Común del sur
INE	Instituto Nacional Electoral
OEA	Organización de los Estados Americanos
ODS	Objetivos de Desarrollo Sostenible
ONU	Organización de las Naciones Unidas
PIDU	Política de Inclusión Digital Universal
PJF	Poder Judicial de la Federación
PYMES	Pequeñas y medianas empresas
PFDR	Plataforma de Firma Digital Remota
PND 2018-2020	Plan Nacional de Desarrollo 2018-2024
RED GEALC	Red de Gobierno Electrónico de América. Latina y el Caribe
RENAPO	Registro Nacional de Población
RGPD	Reglamento General de Protección de Datos Personales
SAT	Servicio de Administración Tributaria
SB	Secretaría del Bienestar
SCT	Secretaría de Comunicaciones y Transportes
SE	Secretaría de Economía
SEDENA	Secretaría de la Defensa Nacional
SEP	Secretaría de Educación Pública
SEGOB	Secretaría de Gobernación
SFP	Secretaría de la Función Pública
SRE	Secretaría de Relaciones Exteriores

SSA	Secretaría de Salud
STPS	Secretaría del Trabajo y Previsión Social
SID	Sistema de Identidad Digital
TI	Tecnologías de la Información y Comunicación
TFJA	Tribunal Federal de Justica Administrativa
TLC	Tratados de Libre Comercio
T-MEC	Tratado de Libre Comercio entre México, Estado Unidos y Canadá
TIC	Tecnologías de la Información y Comunicación
UIT	Unión Internacional de Telecomunicaciones, (ITU, por sus siglas en inglés)
UNCITRAL	La Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, CNUDMI (o UNCITRAL por sus siglas en inglés)
UNDESA	Departamento de Asuntos Económicos y Sociales (UNDESA, por sus siglas en inglés)

Introducción

El derecho es cambiante debido a ciertos hechos históricos y sociales, pero lo es también a causa del creciente desarrollo tecnológico. La cuarta revolución digital junto con la crisis sanitaria por COVID-19 constituyen un *hito* de la humanidad como en su momento lo fue el Internet y la segunda guerra mundial. La tecnología se caracteriza por cambiar los modelos sociales, productivos y económicos, pero al mismo tiempo es transformadora de la manera en que se ejercen los derechos humanos.

Además, la tecnología nos ha mostrado ser una medida que también sirve para combatir desafíos globales como lo fue la emergencia sanitaria por COVID-19. No obstante, el uso ante esta emergencia sanitaria también nos mostró brechas sociales y digitales entre aquellas personas que tienen acceso a Internet y a las TIC y aquellos que no. Igualmente, ante el uso masivo de la tecnología observamos que existen riesgos tecnológicos como los ciberataques, los fraudes cibernéticos o el robo de datos que ponen en riegos los derechos humanos en el ciberespacio.

Para afrontar desafíos como el acceso a la infraestructura, el desarrollo de habilidades digitales o contar con un entorno digital seguro, consideramos relevante prestar especial atención en el derecho a la identidad y la validez jurídica de las transacciones electrónicas a través del uso de las TIC.

En un proceso constante de transformación, contar con estrategias armonizadas en aspectos técnicos y normativos nos permitirá reducir las vulneraciones a los derechos humanos. Dentro de las estrategias digitales, la gestión de la identidad digital y el uso de la firma electrónica se han convertido en pilares de la transformación digitales en países que han comprendido que la seguridad de los datos y las transacciones electrónicas debe ser una acción prioritaria para otorgar confianza a sus ciudadanos, a la par de acciones de conectividad, inclusión y habilidades digitales.

En la cuarta revolución industrial contar con una identidad digital no solo permite interrelacionarnos a través de redes sociales, sino también facilita el acceso a servicios públicos, ejercer derechos como la salud, la educación, seguridad social o

el acceso a la justicia, así como también a realizar actos de comercio electrónico que requieren de validez jurídica y en donde la identidad y firma electrónica han cobrada especial importancia para la economía digital y la reactivación económica ante la crisis por COVID-19.

Tanto la identidad digital como la firma electrónica son comunes en transacciones de cualquier naturaleza, sean mercantiles, gubernamentales, financieras, nacionales o internacionales. Los países que no cuenten con un modelo claro en materia de identidad digital y firma electrónica tendrán dos inconvenientes: vulnerar los derechos humanos en la era digital y quedarse rezagados en el desarrollo social y económico.

Así, contar con un marco jurídico y técnico que ofrezca certeza jurídica a las personas y facilite su uso, resulta fundamental para diseñar servicios digitales en beneficio de las personas. La regulación en estas materias debe atender a principios y estándares internacionales como la neutralidad tecnológica y los modelos de gobernanza que permitan la interoperabilidad y seguridad en transacciones nacionales e internacionales.

Si bien existen diferentes modelos de identidad digital y de firma electrónica en el mundo, todos ellos comparten aspectos en común tales como un sólo sistema de identidad digital y una sola ley de firma electrónica que definen las autoridades responsables, las características técnicas, así como la forma en que los prestadores de servicios de certificación colaboran con el gobierno para facilitar a la población estos dos componentes de forma fácil, interoperable y segura.

En México observaremos que en materia de identidad digital y firma electrónica aún no están del todo claro. La identidad de las personas en México se encuentra está administrada por diversas instituciones nacionales y locales, y la firma electrónica cuenta con regulación federal, estatal y por materia. Esto vulnera el principio de seguridad jurídica consagrado en la CPEUM pues como veremos, a diferencia de otros países, México cuenta con una sobrerregulación en materia de firma electrónica que complica la interoperabilidad y reconocimiento de transacciones electrónicas en el ámbito local, federal, comercial, gubernamental y judicial.

De la misma forma, México cuenta con diversas bases de datos que dan

cuenta de la identidad de las personas. Mismas que aún no son interoperables ni seguras en el ámbito digital.

Ante esta problemática, consideramos que en México se necesita una reforma estructural en materia de identidad digital y firma electrónica que permitan el mejor aprovechamiento de servicios públicos, fomente la economía digital y cumpla con los estándares internacionales previstos, incluso, en los TLC que ya regulan aspectos digitales para con la finalidad de facilitar el comercio internacional.

En este contexto, el objetivo del presente trabajo será advertir está problemática a la luz del derecho comparado y propondremos algunas medidas jurídicas que pueden ayudar a resolver la problemática de la identidad digital y firma electrónica en México, con el objeto de sumarnos a los beneficios y desafíos de la cuarta revolución industrial, así como identificar qué modelo de identidad digital se ajusta a las necesidades de nuestro país.

Para ello, observaremos el impacto del desarrollo tecnológico a través de las revoluciones industriales en los derechos humanos. En la cuarta revolución industrial daremos un primer acercamiento a tecnologías como la IA, *blockchain*, internet de las cosas, *big data*, cómputo en la nube, y como el desarrollo tecnológico ha impactado en la generación de nuevos derechos y formas de garantizarlos en medios digitales. Además, en este capítulo será importante advertir el impacto de la cuarta revolución no sólo en las agendas digitales sino también en los tratados de libre comercio en donde se establecen como pilares de la economía digital el reconocimiento transfronterizo de la firma electrónica, ciberseguridad e interoperabilidad de datos, entre otros aspectos.

En el segundo capítulo mostraremos cuáles son los principales temas en que coinciden los países con un mejor índice de desarrollo digital en los cinco continentes, para afrontar los desafíos de la cuarta revolución industrial, en donde además de la ciberseguridad, la gestión de los datos, infraestructura o habilidades digitales, destacan los de interoperabilidad, identidad digital y firma electrónica.

En el tercer capítulo observamos la evolución del derecho a la identidad y la firma electrónica. Además, identificaremos los mecanismos para acreditar la identidad en medios digitales. En cuanto a la firma electrónica conoceremos sus orígenes

y su evolución hasta llegar a la firma electrónica cualificada que tiene por objeto fortalecer la seguridad de las transacciones digitales. En el tema de identidad digital compararemos los diferentes modelos de identidad digital que han adoptado diversos países en su proceso de transformación digital.

Por último, en el cuarto capítulo conoceremos las principales acciones que México ha adoptado en materia de transformación digital, en temas como infraestructura, habilidades y servicios digitales. Destacaremos la importancia de la coordinación institucional. Igualmente conocemos el estado actual del derecho a la identidad en México haciendo especial énfasis en el proyecto de generar el *documento único digital de identificación nacional biometrizado* y la iniciativa sobre la nueva Ley General de Población que contempla la creación de una cédula digital de identidad que sin duda sienta las bases para fortalecer la identidad digital en México.

Aquí será importante analizar los principios para la elaboración de un Modelo Nacional de Identidad Digital a cargo de la Unión Internacional de Telecomunicaciones. Para el caso de México, generamos algunas propuestas de acciones a considerar en el diseño del documento nacional de identidad a cargo de la RENAPO, en donde consideramos estratégica la colaboración e interoperabilidad con el SAT y la CONAMER.

Por último, conoceremos la situación actual de la firma electrónica en México, en donde observaremos la diversa normatividad que existe en la materia y advertiremos la importancia de contar con una ley general de firma electrónica para el sector público que proporcione certeza jurídica en las transacciones gubernamentales, judiciales e internacionales, así como para evitar la duplicidad de esfuerzos regulatorios, administrativo y económicos en su implementación por la Federación, Estados, Municipios, Poder Judicial y organismos constitucionales autónomos.

Lo anterior, nos permitirá poner en contexto los elementos internacionales y nacionales sobre la regulación de la identidad digital y firma electrónica, con el objetivo de proponer determinados elementos regulatorios y de política pública que contribuyan al desarrollo y fortalecimiento del marco normativo en materia de identidad digital y firma electrónica en México.

Capítulo 1
Revolución industrial

Capítulo 1. Revolución Industrial

La tecnología es una herramienta que ha estado presente en el desarrollo y evolución de la humanidad. A través de las diferentes revoluciones industriales hemos sido testigos que el desarrollo tecnológico no sólo impacta en el día a día de las personas sino también en la economía, en las instituciones, en los procesos y en los derechos humanos.

Sucesos como las revoluciones industriales, junto con otros hechos históricos de la humanidad, han sido parte de la motivación y evolución de los derechos humanos. Desde la primera revolución industrial con la máquina de vapor, pasando por la producción en serie en la segunda y la masificación del Internet en la tercera, la cuarta revolución industrial se caracteriza por fusionar el mundo físico con el digital a través de las TIC cuyo proceso se vio acelerado a causa de la pandemia mundial por COVID-19.

Así, en los siguientes párrafos trataremos de responder los siguientes cuestionamientos ¿Qué es una revolución industrial?; ¿Cuáles son las revoluciones industriales?; y ¿Qué impacto tienen las revoluciones industriales en los derechos humanos? Lo anterior, nos permitirá poner en contexto la importancia del derecho para regular las conductas que deriven del uso y aprovechamiento de las TIC.

El concepto de revolución industrial está asociado a la modernización y el desarrollo mundial. Jean-Phillippe, señala que *"la revolución industrial es concebida como un periodo corto y crítico, definida por la irrupción de un paquete de nuevas tecnologías que transformarían velozmente las condiciones tradicionales de producción"*[1]. Por su parte, David S. Landes, señala que "*el término revolución industrial suele referirse al complejo de innovaciones tecnológicas que, al sustituir la habilidad humana por la máquina y la fuerza humana y animal por energía mecánica, provoca*

[1] Peemes, Jean-Philippe, "Revoluciones industriales, modernización y desarrollo", Universidad Católica de Lovaina, Junio 1992, p. 4, Disponible en: https://www.researchgate.net/publication/26498690_Revoluciones_industriales_modernizacion_y_desarrollo. (Fecha de consulta: 7 de octubre de 2019).

desde el paso a la producción artesanal a la fabril, dando así lugar al nacimiento de la economía moderna"[2].

Además del componente tecnológico, en las revoluciones industriales convergen una serie de causas sociales, económicas e industriales que han influido en el desarrollo de las tres generaciones de derechos humanos que hoy conocemos. Cuando se hace referencia al concepto de revolución industrial normalmente se contemplan aspectos relacionados con la producción económica, la mejora de procesos y la sustitución del hombre por las máquinas. Sin embargo, el cambio tecnológico también impacta en el derecho como una ciencia que regula la conducta social a través del tiempo y el espacio.

En seguida, describiremos los *hitos* tecnológicos y sociales previstos en las cuatro revoluciones industriales, los cuales, como veremos, contribuyen a dar forma a la teoría de los derechos humanos, pasando por los derechos civiles y políticos hasta llegar a lo que hoy conocemos como "derechos digitales".

1.1 Primera revolución industrial

La primera revolución industrial se sitúa principalmente en Gran Bretaña entre los años 1750 a 1840 la cual se extendió a gran parte de Europa y Japón. Esta etapa se caracterizó por que la producción pasó de ser manual a industrial. Se generaron inventos como la máquina de vapor, la máquina de coser, el telégrafo, el ferrocarril, la bombilla o el automóvil. En esta etapa surgió un crecimiento económico importante debido a la producción de bienes a través de la existencia de numerosas fábricas y empresas privadas. Fue una etapa en donde se fortaleció la propiedad privada y dio origen a la clase obrera industrial[3].

Dentro del periodo de la primera revolución industrial también encontramos las primeras discusiones globales sobre derechos humanos; principalmente en el ámbito del derecho laboral. Lo anterior, motivado por la sobreexplotación del trabajador en las fábricas y empresas. Así, por ejemplo, es en Gran Bretaña en donde

[2] Landes, D.S. Progreso tecnológico y revolución industrial, Madrid, Tecnos, 1979, p. 15.
[3] Chávez Palacios, Julián, Desarrollo tecnológico en la primera revolución industrial, Universidad de Extremadura, Norba, Revista de Historia, Vol. 17, 2004, p. 93-109, Disponible en: https://dialnet.unirioja.es/descarga/articulo/1158936.pdf. (Fecha de consulta: 7 de octubre de 2019).

nacen los primeros orígenes del desarrollo industrial y, también, de los derechos y libertades de los ingleses a través del "*Bill of Rights"* de 1689[4]. Lo anterior, derivado principalmente por la imposición de multas excesivas y castigos ilegales a las personas. A través del *Bill of Rights* se garantizaron los derechos de libertad, de legalidad y de seguridad jurídica, lo que significó un recorte de los poderes absolutos del monarca.

Al mismo tiempo que en Inglaterra se gestaban los inicios de la revolución industrial y la discusión sobre los derechos civiles y políticos, en Francia también se libraba la llamada "revolución francesa", caracterizada por una marcada división de clases sociales (nobleza; clero; burguesía y campesinos), elevados impuestos y una monarquía absoluta que se sobreponía incluso en la libertad, la vida e igualdad de las personas[5].

Así, en la primera revolución industrial las primeras invenciones como la electricidad, las máquinas de coser y los modelos de producción basados en la fábrica, junto con los abusos del monarca y la marcada distinción de clases sociales, dieron pasó a una generación de derechos humanos que hoy conocemos como la *primera generación de derechos humanos civiles y políticos* que se caracterizan por exigir al Estado una actividad de no intervenir en la vida y libertades de las personas, y de establecer un límite al monarca.

Estos derechos están materializados principalmente a través de la *Declaración de los Derechos del Hombre y del Ciudadano de 1789[6],* en donde se reconocen los derechos a la libertad de propiedad, de seguridad, el debido proceso, de igualdad ante la ley, de asociación política y de protección de la vida privada; entre otros.

---

[4] Bill Of Rights, "Ley que Declara los Derechos y Libertades de los Ingleses y Establece el Orden de Sucesión de la Corona", Inglaterra, 1689, Disponible en https://www.dipublico.org/3664/bill-of-rights-ley-que-declara-los-derechos-y-libertades-de-los-ingleses-y-establece-el-orden-de-sucesion-de-la-corona-inglaterra-1689/. ((Fecha de consulta: 7 de octubre de 2019).

[5] Fernández Lara, Rosa María, "La revolución francesa: bases sociales, ideológicas y proceso de institucionalización", Proyecto CLIO, número 36, s.a., Disponible en: http://clio.rediris.es (Fecha de consulta: 7 de octubre de 2019).

[6] Declaración de los Derechos del Hombre y del Ciudadano de 1789, Disponible en: https://www.conseil-constitutionnel.fr/sites/default/files/as/root/bank_mm/espagnol/es_ddhc.pdf, (Fecha de consulta: 7 de octubre de 2019).

1.2 Segunda revolución industrial

La segunda revolución industrial se sitúa durante todo el siglo XIX hasta la segunda guerra mundial. Siguiendo a Marcos Kaplan, la segunda revolución industrial se caracteriza por descubrimientos físico-naturales y sus aplicaciones técnicas; incrementos de la productividad; luchas por los mercados, y competencias entre grandes empresas[7]. En la primera revolución industrial Gran Bretaña fue una potencia mundial; en la segunda, se unen Francia, Japón, Alemania, Estados Unidos y Rusia[8]. A diferencia de la primera, en la segunda revolución industrial los cambios se dan ante todo en aspectos de las fuentes de energía, los materiales y el tiempo. Es la era del ferrocarril y del barco de vapor, de la producción en serie, de la electricidad, el petróleo, el acero, de los avances en las telecomunicaciones con el telégrafo eléctrico, de la radio y la televisión[9].

El gran crecimiento industrial, económico y de transportes fue el antecedente de la época de la globalización. No obstante, debido a la producción en masa también existió desempleo a causa del uso de la tecnología que reemplazó a los obreros en las fábricas por máquina de producción en serie. Además, es en la segunda revolución industrial en donde se sientan las bases del autoritarismo, el totalitarismo y de una segunda guerra mundial[10].

Estos hechos históricos junto con la innovación y la energía eléctrica potenciaron la producción en serie que cambiaron no sólo la economía de la época, sino también la forma en que las personas, las empresas y el Estado interactuaban. Surgieron de esta forma los denominados *derechos económicos, sociales y culturales*. Al respecto, Carlos Villán Durán señala que estos derechos encuentran parte de sus antecedentes en la revolución industrial, en donde si bien existía un desarrollo industrial, no se reconocían aún el derecho al trabajo, a un salario digno, al descanso,

[7] Kaplan, Marcos, “Estado y globalización”, Instituto de Investigaciones Jurídicas, México, 2002, pp. 149-221, Disponible en: https://archivos.juridicas.unam.mx/www/bjv/libros/1/277/3.pdf (Fecha de consulta: 7 de octubre de 2019).
[8] Idem.
[9] Idem.
[10] Ibídem. p. 220.

a la jubilación, a la educación, a la salud, al sufragio universal de las mujeres, a la libre asociación o el derecho a la libertad sindical[11].

Los derechos mencionados se reconocieron internacionalmente el 2 de septiembre de 1945, con base en la *Declaración Universal de Derechos Humanos del 10 de diciembre de 1948*[12], en donde se considera principalmente el derecho a la libertad, la justica, la paz y la dignidad de las personas. Igualmente, el 16 de diciembre de 1966, se publicó el *Pacto Internacional de Derechos Económicos, Sociales y Culturales*[13] el cual, basado en el principio de la dignidad humana, reconoce los derechos al trabajo, a la seguridad social, a una remuneración digna, al salario equitativo entre el hombre y la mujer, a fundar sindicatos, a un nivel adecuado de vida para la persona y su familia, incluyendo la alimentación, el vestido, la vivienda, la salud, la educación, a participar en la vida cultural, entre otros.

De esta forma, observamos que, a diferencia de los derechos de primera generación, en donde se reclamaba un límite al monarca y la no intervención del Estado, en la segunda generación de derechos se demandaba que el Estado proporcionara mayor igualdad económica, social y cultural para las personas frente al desarrollo industrial de la época.

1.3 Tercera revolución industrial

La tercera revolución industrial se sitúa entre los años 1960 y 1990 y se caracteriza por avances en la computación y la creación de Internet. A causa de la segunda guerra mundial, la tercera revolución industrial guardaba un ambiente bélico y de vulneración a los derechos humanos. Por ello no es raro que las invenciones de los próximos años se dieran principalmente en este ámbito.

---

[11] Durán Villán, Carlos, "Historia y descripción general de los derechos económicos, sociales y culturales, en González Monguí, Pablo Elías (coord), Derechos económicos, sociales y culturales, Universidad Libre de Colombia, Colombia, 2009, p.10, Disponible en: http://www.corteidh.or.cr/tablas/26759.pdf (Fecha de consulta: 7 de octubre de 2019).

[12] Declaración Universal de Derechos Humanos, Disponible en: https://www.un.org/es/documents/udhr/UDHR_booklet_SP_web.pdf (Fecha de consulta: 7 de octubre de 2019).

[13] Pacto Internacional de Derechos Económicos, Sociales y Culturales, Disponible en: https://www.ohchr.org/SP/ProfessionalInterest/Pages/CESCR.aspx (Fecha de consulta: 7 de octubre de 2019).

Adrián Estrada recuenta que, ante la posibilidad de un embate nuclear a finales de los sesenta, la Agencia de Proyectos de Investigación Avanzada del Departamento de Defensa de Estados Unidos (DARPA), comisionó en 1967 a la Agencia de Proyectos de Investigación Avanzada (ARPA) la creación de una red para proteger los sistemas estratégicos y de información localizados en los núcleos y ciudades principales[14].

Fue así como lo que hoy conocemos como Internet en sus inicios fue una red tecnológica para fines militares y, para el año 1985, se comenzó a utilizar como una tecnología de apoyo a la comunidad de investigadores y desarrolladores para facilitarles la comunicación y el intercambio de conocimiento a través del correo electrónico[15].

En la tercera revolución industrial observamos que Estados Unidos fue una de las potencias consolidadas que invirtió gran parte de sus recursos en investigación científica y armamento militar. Pasando ya la época militar, Adrián Estrada señala que Internet se convirtió en un instrumento de propagación de la información y un medio de concurrencia entre los individuos para fines académicos y de investigación; igualmente, indica que fue en las universidades en donde se popularizó el correo electrónico a través de los académicos quienes lo adoptaron como una excelente herramienta para colaborar en proyectos de investigación[16].

En este periodo, el desarrollo económico y la innovación científica tuvo como uno de sus pilares el intercambio de información a través de internet, lo que propicio a contar con un mundo más globalizado debido a la facilidad con que las personas de todo el mundo podían comunicarse a vía Internet y el correo electrónico. Esto también permitió un auge en el comercio internacional y en el uso masivo de energías que permitieran la movilidad de personas y mercancías a lo largo del planeta[17].

---

[14] Estrada Corona, Adrián, “Protocolos TCP/IP de Internet”, Revista Digital Universitaria, UNAM, Volumen 5, Número 8, México 2004, p. 2, Disponible en: http://www.revista.unam.mx/vol.5/num8/art51/sep_art51.pdf. (Fecha de consulta: 7 de octubre de 2019).

[15] Leinerp Barry M., kahn Robert E., “Brief History of the Internet 1997”, internetsociety.org, p, 9, Disponible en https://www.internetsociety.org/wp-content/uploads/2017/09/ISOC-History-of-the-Internet_1997.pdf (Fecha de consulta: 21 de julio de 2020).

[16] Estrada Corona, Adrián, op. cit., p. 3.

[17] Nelken-Terner, Antoinette, “Globalización o mundialización ¿Indiscutibles? ¿Incuestionables?”, Política y Cultura, número 10, Universidad Autónoma Metropolitana Unidad Xochimilco, Ciudad de

En materia jurídica estos fenómenos económicos, sociales y políticos también tuvieron impacto en el derecho. Fueron parte de los antecedentes de los llamados derechos de tercera generación que procuran el desarrollo de las naciones, la protección al medio ambiente, a la paz mundial, del derecho a la migración, del comercio internacional, del uso de la tecnología para facilitar el intercambio de mercancías[18]. Además, podemos señalar que, como veremos más adelante, es en la tercera revolución industrial en donde encontramos el antecedente de la firma electrónica que surgió ante el incremento de transacciones electrónicas comerciales a través de internet y el uso de los tratados de libre comercio.

Por otra parte, la tecnológica mostraba ser una herramienta indispensable para el desarrollo de las países, lo que motivó para que en el año 2000, la Asamblea General de la ONU publicara la *Declaración del Milenio*[19], en donde, con base en los valores fundamental a la libertad, la igualdad, la solidaridad, la tolerancia, el respeto a la naturaleza, se propusieron los llamados objetivos del milenio, tales como: *"(i) la paz, la seguridad y el desarme; (ii) el desarrollo y la erradicación de la pobreza; (iii) la protección al medio ambiente; (iv) el respeto a los derechos humanos, a la democracia y al buen gobierno; (v) la protección de las personas vulnerables; (vi) atención a las necesidades especiales de África; y (vii) el fortalecimiento de las Naciones Unidas"*.

1.4 Cuarta revolución industrial

Podemos situar a la cuarta revolución industrial a partir del año 2000 y se caracteriza por el uso masivo de Internet, datos, software, algoritmos y de tecnologías emergentes como la IA, el cómputo en la nube, *blockchain*, el Internet de las Cosas, las ciudades inteligentes, la conducción autónoma, la nanotecnología, la impresión

México, 1998, p. 63, Disponible en: https://www.redalyc.org/pdf/267/26701005.pdf (Fecha de consulta: 7 de octubre de 2019).

[18] Chavero González, Adrián, "La tercera revolución industrial en México: diagnóstico e implicaciones", IIJ-UNAM, México, 1992, pp. 166, 261 y 263, Disponible en http://ru.iiec.unam.mx/1223/1/LaTerceraRevolucion.pdf (Fecha de consulta: 21 de julio de 2020).

[19] Asamblea General de la ONU, Resolución A/RES/55/2, "Declaración del Milenio", Disponible en: https://www.un.org/spanish/milenio/ares552.pdf, (Fecha de consulta: 7 de octubre de 2019).

3D, el aprendizaje de la máquina, y en un uso acelerado de la tecnología a causa de la pandemia mundial del año 2020 por COVID-19. La ONU reconoce que:

> "(…) *cuando hablamos de la cuarta revolución industrial o "industria 4.0, se hace referencia al uso creciente de la automatización y al intercambio de datos para la fabricación de sistemas de producción inteligentes y conectados, a la cual se asocia una mayor digitalización en la producción con base "en la conectividad; el Internet de las Cosas; la recopilación y el análisis de macrodatos; las nuevas formas de interacción entre humanos y máquinas; y las mejoras en el uso de instrucciones digitales gracias a la robótica y la impresión tridimensional (3D)"*[20].

Como en su momento, la energía eléctrica fue pieza clave para potenciar la producción en serie dentro de la segunda revolución industrial, en la cuarta revolución industrial el Internet constituye una herramienta para el desarrollo de innovaciones tecnológicas basadas en tecnologías emergentes como la IA, *blockchain*, 5G o cómputo en la nube.

No obstante, en la cuarta revolución industrial los derechos humanos también tienen un protagonismo importante. Al respecto, la Asamblea General de la ONU reconoció que ante el uso de internet y las nuevas tecnologías se deben salvaguardar los derechos humanos; fomentar el desarrollo sostenible y la alfabetización digital; combatir la brecha digital, y garantizar la seguridad de la información en medios digitales.

Así, la falta de conectividad y acceso a las TIC de grupos vulnerables, el intercambio masivo de datos personales e información a través de Internet, y el surgimiento de sesgos algorítmicos, son algunos de los aspectos de mayor impacto en la forma en que se ejercen y protegen los derechos humanos en la cuarta revolución industrial.

También han surgido nuevos conceptos sobre derechos como, por ejemplo, el derecho a la protección de datos personales, el derecho de acceso a Internet y a

[20] ONU, "Conferencia de las Naciones Unidad sobre Comercio y Desarrollo", TD/B/C.II/43, 02 de septiembre de 2019, p. 4, Disponible en https://unctad.org/system/files/official-document/ciid43_es.pdf (Fecha de consulta: 7 de octubre de 2020).

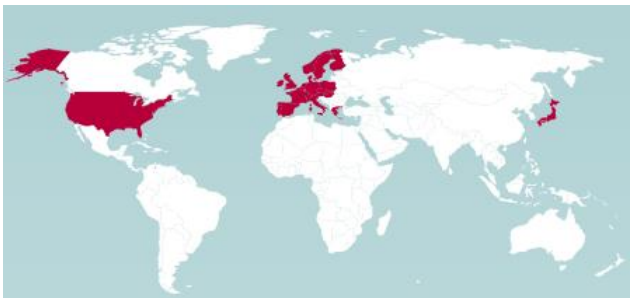
las TIC, el derecho de acceso a la información o el derecho a una ciudadanía digital. Otros derechos ya existentes como la libertad de expresión, la educación, la salud, el trabajo y la privacidad han evolucionado junto con la cuarta revolución industrial motivado por el uso exponencial de Internet y las TIC. También figuras jurídicas clásicas como la responsabilidad civil objetiva, la prueba electrónica, el derecho del consumidor o la propiedad intelectual han sido analizadas desde un punto de vista tecnológico debido al uso de tecnologías como la Inteligencias Artificial, la nube y/o la comisión de delitos cibernético, por mencionar algunos.

Así, en relación con los derechos humanos, hoy en día se habla de una cuarta generación de derechos humanos vinculados al desarrollo tecnológico, en donde encontramos conceptos como derechos a la eliminación de tarifas de interconexión; derecho de acceso a contenidos digitales; a la neutralidad de la red; al teletrabajo; la protección de los menores en Internet.

Además del surgimiento de “nuevos” derechos humanos que no terminan por consolidarse en un solo texto, entorno a la cuarta revolución industrial se han desarrollado una serie de principios y objetivos para el uso de las TIC con respeto a los derechos humanos y en *pro* del desarrollo sostenible. Nos referimos a los principios de la Sociedad de la Información en el marco de la CMSI y a los 17 ODS de la ONU; los cuales analizaremos más adelante.

En resumen, podemos observar que las revoluciones industriales se concentraron en un inicio en algunos cuantos países y posteriormente fueron permeando en el resto. En la cuarta revolución industrial la mayoría de los países del mundo se han visto involucrados casi al mismo tiempo. Se han plasmado principios para garantizar los derechos humanos en relación con la TIC, así como para afrontar desafíos como el acceso a infraestructura digital; la brecha digital; el desarrollo de habilidades digitales; la economía digital, entre otros temas.

Para facilitar esta relación entre las revoluciones industriales y derechos humanos, en el siguiente cuadro identificamos la revolución industrial, los principales inventos, los derechos relacionados y un mapa en donde observamos la creciente evolución tecnológica en el mundo.

Revolución industrial	Inventos	Derechos	Países
Primera **1750 a 1840**	Máquina de coser, de vapor, ferrocarril, electricidad.	Civiles y políticos	
Segunda **1850-1945**	Producción en serie, energías como electricidad, petróleo,	Económicos, sociales y culturales	
Tercera **1945-** **1990**	Internet Computación	Medio ambiente y desarrollo	
Cuarta **2000** **a la fecha**	IA, Blockchain, Cómputo en la nube, Conducción autónoma.	Digitales	

Cuadro 1. *Revoluciones industriales y derechos humanos*
Fuente: elaboración propia.

A diferencia de las otras revoluciones industriales, en donde la innovación tecnológica se centró en la mecanización, en la cuarta revolución industrial las

tecnologías se caracterizan por automatizar los procesos a través del uso de Internet y la explotación de datos a través de tecnologías emergentes, tales como IA, *blockchain*, cómputo en la nube, internet de las cosas, conducción autónoma o el *big data*. En breve, describiremos en qué consisten estas tecnologías propias de la cuarta revolución industrial.

1.4.1 Blockchain

Blockchain o cadena de bloques es la tecnología que creó al *bitcoin* y otras monedas virtuales. Es definida como un libro abierto y distribuido que puede registrar transacciones entre dos partes de manera eficiente y de forma verificable y permanente[21]. A través de la cadena de bloques, distintos actores realizan transacciones dentro de un proceso, las cuales son registradas consecutivamente mediante un *hash*[22]. Lo anterior significa que las transacciones validadas y registradas en la cadena no pueden ser editadas o borradas, y todas las computadoras o servidores conectados a la *blockchain* tendrán una copia de todos los registros.

La tecnología *blockchain* se destaca por ser una herramienta que facilita la transparencia, la descentralización y la eliminación de intermediarios[23]. Algunos de los beneficios que se le reconocen a la cadena de bloques son: (i) la distribución de información en *tiempo casi real*; (ii) todos los participantes pueden *acceder a la* información; (iii) brinda *seguridad en la trazabilidad de la información* ya que no se puede editar ni borrar[24] un bloque sino sólo se puede agregar uno nuevo, y (iv) con

[21] Iansiti, Marco , Karim R. Lakhani, "The Truth About Blockchain", from the january–february 2017 issue, Harvard Business Publishing, Disponible en: https://hbr.org/2017/01/the-truth-about-blockchain (Fecha de consulta: 9 de octubre de 2019).

[22] Un hash constituye un identificador único mediante un código alfanumérico que permite detectar la manipulación de archivos. Para mayor profundidad sobre este tema, sugerimos consultar: Crosby Michael, Nachiappan, Pradhan Pattanayak, Sanjeev Verma Y Kalyanaraman, Vignesh, "Blockchain Technology", Uc Berkeley, San Francisco, California, Octubre, 2015, p. 30, Disponible en: https://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf (Fecha de consulta: 8 de octubre de 2019).

[23] Allende López, Marcos, "Blockchain Cómo desarrollar confianza en entornos complejos para generar valor de impacto social, Banco Interamericano de Desarrollo", Washington, 2018, p. 27, Disponible en: http://governance40.com/wp-content/uploads/2018/11/Blockchain-Como-desarrollar-confianza-en-entornos-complejos-para-generar-valor-de-impacto-social-1.pdf (Fecha de consulta: 8 de octubre de 2019).

[24] Debido a esta característica, uno de los temas que se discute es *blockchain* frente al derecho al olvido, ya que lo que se registra en la cadena de bloques no puede borrarse.

la firma digital y encriptación de información se ofrece mayor seguridad de las transacciones registradas en la cadena de bloques[25].

1.4.2 Inteligencia Artificial

Los primeros antecedentes de la IA los encontramos con Alan Turing quien señaló en su artículo "*Computing Machinery and Intelligence"*, que una máquina podría imitar el comportamiento de la mente humana[26]. Sin embargo, no fue hasta la denominada conferencia de Dartmouth en 1956[27] en donde se acuño por primera vez el concepto de IA, y se estableció como proposición de trabajo que "*todo aspecto de aprendizaje o cualquier otra característica de inteligencia puede ser definido de forma tan precisa que puede construirse una máquina para simularlo"[28].*

A partir de este último antecedente comenzaron a surgir diversas definiciones de IA. El Instituto Tecnológico de Massachussets (MIT, por sus siglas en inglés), ha advertido tres niveles en torno al concepto de IA. El primero constituye a hacer modelos computacionales del *comportamiento* humano; es decir, la su simulación de inteligencia humana por parte de las máquinas. El segundo a hacer modelos computacionales de *procesos de pensamiento humano*; es decir, a construir un programa no sólo que se parezca a los humanos, sino que lo hago como ellos. Y el tercero, a

---

[25] Redl, Christoph, Muente-Kunigami, Arturo, "Blockchain en la Administración Pública ¿Mucho ruido y pocos bloques?", Banco Interamericano de Desarrollo, Washington, Estados Unidos, 2019, p. 84, Disponible en: https://publications.iadb.org/publications/spanish/document/Blockchain_en_la_administraci%C3%B3n_p%C3%BAblica_Mucho_ruido_y_pocos_bloques_es.pdf, (Fecha de consulta: 8 de octubre de 2019).

[26] A. M. Turing, "Computing Machinery And Intelligence", Mind 49: 433-460, Disponible en: https://www.csee.umbc.edu/courses/471/papers/turing.pdf, (Fecha de consulta: 8 de octubre de 2019).

[27] Esta conferencia, denominada en su momento como "Dartmouth Summer Research Conference on Artificial Intelligence", contó entre sus organizadores con mentes de la talla de Marvin L. Minsky y Claude E. Shannon, y en ella participaron, entre otros, Herbert Simon y Allen Newell. Cfr. Villena Román, Julio, Crespo García, Raquel M., García Rueda, José Jesús, "Historia de la Inteligencia Artificial", Universidad Carlos III de Madrid, Madrid, España, s.a., p. 4, Disponible en: http://ocw.uc3m.es/ingenieria-telematica/inteligencia-en-redes-de-comunicaciones/material-de-clase-1/01-historia-de-la-inteligencia-artificial (Fecha de consulta: 8 de octubre de 2019).

[28] Idem.

construir *sistemas computacionales que se comportan inteligentemente*, considerando que podría existir otras formas de ser inteligente además de la forma en que los humanos lo hacen[29].

En este contexto, podemos señalar que la IA es un sistema computacional mediante el cual se pueden llevar a cabo actividades o funciones como las haría una persona. Es por ello por lo que la IA tiene impacto en prácticamente todos los sectores de la sociedad, ya sea en el ámbito laboral, salud, educación, la industria, entre otros. Sin duda la aplicación de esta tecnología tiene gran impacto en los derechos humanos, en donde algunas de sus aplicaciones han demostrado generar actos discriminatorios como lo fue en Estados Unidos el sistema COMPAS (*Correctional Offender Management Profiling for Alternative Sanctions*) utilizado para evaluar la probabilidad de que un acusado se convierta en reincidente, el cual, dado que estaba basado en la recolección de datos históricos sobre las detenciones de afroamericanos, el sistema siempre arrojaba un mayor riesgo para las personas de color[30].

Al tener gran impacto en la sociedad, en torno a la IA, se debaten diversos temas como: sesgos algorítmicos; responsabilidad civil; uso ético de los datos; protección de los datos personales; (v) transparencia y responsabilidad algorítmica; propiedad intelectual; control humano de la tecnología; la responsabilidad profesional, y la promoción de valores humanos[31]. Además de lo anterior, podemos agregar que también deben abordarse temas relacionados con sus elementos habilitadores como la infraestructura digital, los datos; las habilidades digitales, y la creación de entornos de innovación tecnológica.

---

[29] MIT, "What is Artificial Intelligence (AI)?", 6.825 Techniques in Artificial Intelligence, Washington, s.a., pp. 3-7, Disponible en: https://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-825-techniques-in-artificial-intelligence-sma-5504-fall-2002/lecture-notes/Lecture1Final.pdf (Fecha de consulta: 20 de junio de 2020).

[30] ANGWIN, Julia, LARSON, Jeff, MATTU, Surya, and KIRCHNER, Lauren, "Machine Bias, Tehe´s software used across de country to predict future criminals. And it´s biased against blacks", Pro Publica, mayo 23, 2016, https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing (Fecha de consulta: 20 de junio de 2020).

[31] FJELD, Jessica, ACHTEN, Nele, HILLIGOSS, Hannah, CHRISTOPHER, Adam, MADHULIKA SRIKUMAR, Nagy, "Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-based Approaches to Principles for AI", Harvard, Berkman Klein Center, Research Publication No. 2020-1 January 15, Boston, Estados Unidos, 2020, https://cyber.harvard.edu/publication/2020/principled-ai.

1.4.3 Cómputo en la nube

Según la definición del NIST (National Institute of Standard and Technology), el cómputo en la nube *es un modelo tecnológico que permite el acceso ubicuo, adaptado y bajo demanda en red a un conjunto de recursos de computación configurables compartidos (por ejemplo, redes, servidores, equipos de almacenamiento, aplicaciones y servicios) que pueden ser rápidamente aprovisionados y liberados con un esfuerzo de gestión reducido o interacción mínima con el proveedor del servicio"*[32].

Por su parte, el Instituto Nacional de Ciberseguridad en España, señala que el cómputo en la nube es un modelo de computación que permite al proveedor tecnológico ofrecer servicios informáticos a través de internet, es decir, los recursos de hardware, software y los datos se pueden ofrecer bajo demandan del cliente. Se pueden ofrecer un conjunto de servicios como redes, servidores, almacenamiento, aplicaciones y servicios que pueden ser asignados rápidamente por proveedor. Es decir, el cómputo en la nube permite acceder a los servicios y recursos contratados proporcionando flexibilidad y dimensionamiento de acceso[33].

El cómputo en la nube cuenta con gran trascendencia en la era digital. A través de la nube cualquier persona puede acceder a recursos de cómputo, tanto a hardware, software, plataformas y almacenamiento. Sin duda, podemos señalar que el cómputo en la nube puede asimilarse al vehículo automotor que transporta personas y mercancías una maquina industrial en la tercera revolución industrial. En la cuarta revolución industrial, ese vehículo que facilita el transporte de datos y desarrollo de aplicaciones tecnológicas como la IA es la computación en la nube.

---

[32] MELL, Peter, GRANCE, Timothy, "The NIST Definition of Cloud Computing", NIST, Computer Security Division Information Technology Laborator, September 2011, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf, (Fecha de consulta: 20 de junio de 2020).

[33] Instituto Nacional de Ciberseguridad "Cloud computing", guía de aproximación para el empresario, España, s.a., p. 5, Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia-cloud-computing_0.pdf, (Fecha de consulta: 8 de octubre de 2019).

1.4.4 Big Data

El concepto de *Big Data* nace en el año 2000. En un primer momento fue concebido por Viktor Mayer-Schönberger y Kenneth Cukier -en torno a la revolución y almacenamiento de los datos masivos en astronomía y genética-, como el hecho de que el volumen de información había aumentado tanto que la que se examinaba ya no cabía en la memoria que los ordenadores empleaban para procesarla, por lo que los ingenieros necesitaban modernizar las herramientas para poder analizarla[34].

Los datos son la materia prima de la cuarta revolución industrial y cuentan con un valor económico, social y cultural importante para el diseño de políticas públicas o para el emprendimiento de nuevos modelos de negocio. Siguiendo a Gartner, el *big data* lo podemos entender como "*los activos de información de gran volumen, alta velocidad y/o gran variedad que exigen formas innovadoras y rentables de procesamiento de información que permiten una mejor comprensión, toma de decisiones y automatización de procesos"*[35]. Es decir, cuando nos referimos al *big data* es importante considerar las tres "v" que lo caracteriza: volumen, velocidad y variedad. A esto, hay que añadirle los tipos de herramientas que permiten procesar el *big data*, tales como *Hadoop, MongoDB, Elasticsearch, Apache Spark, Apache Storm, Lenguaje R, y Python*[36].

1.4.5 Tecnología 5G

La tecnología 5G tiene que ver con la infraestructura de telecomunicaciones y la gestión del espectro radioeléctrico[37]. A diferencia de sus antecesoras 2G, 3G y 4G, 5G ofrecer mayor capacidad de transmisión de datos a mayor velocidad. La ITU

---

[34] Viktor Mayer-Schönberger y Kenneth Cukier, Big Data, la revolución de los datos masivo, Disponible en: http://catedradatos.com.ar/media/3.-Big-data.-La-revolucion-de-los-datos-masivos-Noema-Spanish-, (Fecha de consulta: 8 de octubre de 2019).

[35] Xiaomeng Su, "Introduction to Big Data", Institutt for informatikk og e-læring ved NTNU, Suecia, s.a., p. 3, Disponible en: https://www.ntnu.no/iie/fag/big/lessons/lesson2.pdf, (Fecha de consulta: 8 de octubre de 2019).

[36] Instituto de Ingeniería del Conocimiento, "7 herramientas del big data para tu empresa", octubre 13, 2016, Disponible en: https://www.iic.uam.es/innovacion/herramientas-big-data-para-empresa/ (Fecha de consulta: 8 de octubre de 2019).

[37] El espectro radioeléctrico es el espacio que permite la propagación, sin guía artificial, de ondas electromagnéticas cuyas bandas de frecuencias se fijan convencionalmente por debajo de los 3,000 gigahertz. Artículo 3, fracción XXI de la LFTR, publicada en el DOF el 11 de junio de 2013, Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFTR_240120.pdf. (Fecha de consulta: 8 de octubre de 2019).

señala que esta tecnología fortalecerá la economía digital a través de la transformación de ciudades inteligentes, ya que permitirá un aumento drástico de las velocidades de datos y una reducción de la latencia comparada con la 3G y 4G, con valores de transmisión de datos inferior a 1ms[38].

Esta tecnología aspira a ofrecer a los usuarios finales nuevas aplicaciones y servicios capaces de alcanzar velocidades de varios *gigabits*, así como aumentar la calidad de funcionamiento, lo que resulta crítico en servicios en donde el tiempo es un factor vital. Podemos concluir que la tecnología 5G está asociada a la conectividad, a mayor volumen y a una mayor velocidad de transmisión de datos en menor tiempo.

1.4.6 Internet de las cosas

Inicialmente, la transmisión de información a través de un mensaje electrónico conectaba a las personas en distintos lugares del mundo. Con el desarrollo tecnológico, y mayor capacidad de infraestructura, así como de la innovación en dispositivos tecnológicos, hoy en día se pueden conectar, a través de Internet, no sólo personas sino también diversos dispositivos digitales. Ahora es posible que un dispositivo conectado a Internet nos proporcione información y nos permita realizar ciertas tareas en nuestro día a día.

Así, podemos conectar no sólo nuestros celulares a Internet, sino también televisiones, aparatos electrónico o vehículos de conducción autónoma. Por lo general, el término Internet de las Cosas se refiere a escenarios en los que la conectividad de red y la capacidad de cómputo se extienden a los objetos, sensores y artículos de uso diario que habitualmente no se consideran computadoras, permi-

[38] Husenovic, Kemal, “Sentando las bases para la 5G: Oportunidades y desafíos”, ITU, Ginebra, Suiza, 2018, p. 3, Disponible en: https://www.itu.int/dms_pub/itu-d/opb/pref/D-PREF-BB.5G_01-2018-PDF-S.pdf, (Fecha de consulta: 8 de octubre de 2019).

tiendo que estos dispositivos generen, intercambien y consuman datos con una mínima intervención humana[39].Para ello, los datos, la infraestructura, la interoperabilidad, la regulación, la seguridad y la protección de los datos personales son temas importantes a considerar en el Internet de las Cosas[40].

Las tecnologías que hemos estudiado representan actualmente un reto para el derecho las cuales se enmarcan en el contexto de la cuarta revolución industrial. Temas como la protección de los datos personales, la discriminación algorítmica, el robo de identidad, la ciberseguridad, la propiedad intelectual, la validez jurídica de las transacciones electrónicas, o la responsabilidad civil objetiva, son retos que el desarrollo tecnológico ofrece a la ciencia jurídica. Hoy cobra especial importancia el uso ético de la tecnología y los datos, el uso responsable e inclusivo de las TIC y salvaguardar los derechos humanos dentro del contexto cada vez más digital.

1.5 Cumbre Mundial de la Sociedad de la Información

A través de la Resolución 56/183, la Asamblea General de la ONU creó la CMSI[41] para reconocer y atender el intercambio masivo de la información, así como el uso de Internet y las TIC con respeto a los derechos humanos y en *pro* del desarrollo sostenible.

A través de dicha resolución, la ONU reconoció que las TIC son una herramienta indispensable para el desarrollo sostenible e invitó a la ITU para que asumiera la función administrativa principal de la secretaría ejecutiva de la CMSI y su proceso preparatorio. En el marco de la CMSI se desarrolló una serie de *principios*[42]

[39] Rose, Karen, Scott, Lyman Chapin,"Internet de las cosas- una breve reseña, Internet Society, Octubre 2015, p. 5, Disponible en: https://www.internetsociety.org/wp-content/uploads/2017/09/report-InternetOfThings-20160817-es-1.pdf, (Fecha de consulta: 8 de octubre de 2019).
[40] Idem.
[41]ONU, Resolución aprobada por la Asamblea General, 56/183. Cumbre Mundial sobre la Sociedad de la Información, Disponible en: http://www.itu.int/net/wsis/docs/background/resolutions/56_183_unga_2002-es.pdf, (Fecha de consulta: 8 de octubre de 2019).
[42] ONU e ITU, Declaración de Principios CONSTRUIR LA SOCIEDAD DE LA INFORMACIÓN: UN DESAFÍO GLOBAL PARA EL NUEVO MILENIO, Documento WSIS-03/GENEVA/4-S 12 de mayo de 2004, Disponible en: https://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!PDF-S.pdf, (Fecha de consulta: 8 de octubre de 2019).

y un *plan de acción*[43] que orientan a los países que integran la ONU en el desarrollo e implementación de las TIC[44].

Son once los principios de la CMSI relacionados con el uso de las TIC. El **primero** de ellos se refiere a la importancia de la *colaboración de instituciones públicas y privadas* para fomentar servicios centrados en las personas. El **segundo** resalta la necesidad de *infraestructura digital*, a través de la conectividad e infraestructura de red, como habilitador indispensable de la Sociedad de la Información. El **tercero** se refiere a contribuir con el *derecho de acceso a la información*. El **cuarto** a *la creación de capacidad* para que cada persona pueda generar las habilidades que demanda la era digital, en el ámbito laboral, educativo y de innovación. El **quinto** está dirigido a fomentar la *confianza y seguridad* en el uso de las TIC, respetando la privacidad, la protección al consumidor y fomentando una cultura global de ciberseguridad. El **sexto** se enfoca en crear un *entorno propicio* a través de un estado de derecho en el uso de las TIC. El **séptimo** reconoce el *impacto positivo de las TIC en los diversos sectores de la vida cotidiana*, como los servicios gubernamentales, la salud, la educación, el trabajo, la actividad económica, la protección al medio ambiente, y erradicar la pobreza, entre otros. El **octavo** se refiere al *respeto por la diversidad e identidades culturales*, como la lingüística y el contenido local, principalmente velando por las lenguas indígenas y la preservación del patrimonio cultural. El **noveno** se centra en los *medios de comunicación*, para promover los derechos de libertad de prensa y de información. El **décimo** se refiere a un tema cada vez más importante, al *uso ético de los datos* a través de los valores de los valores fundamentales de libertad, igualdad, solidaridad, tolerancia, responsabilidad compartida y respeto a la naturaleza. Y el **onceavo** a fomentar la *cooperación internacional y regional* para atender la brecha digital, así como gestionar eficientemente el espectro radioeléctrico.

[43] ONU e ITU, Plan de Acción, Documento WSIS-03/GENEVA/5-S 12 de mayo de 2004, Disponible en: https://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0005!!PDF-S.pdf, (Fecha de consulta: 8 de octubre de 2019), y Declaración de la CMSI+10 relativa a la aplicación de los resultados de la CMSI, Disponible en: http://www.itu.int/net/wsis/implementation/2014/forum/inc/doc/outcome/362828V2S.pdf, (Fecha de consulta: 8 de octubre de 2019).

Entre los principios se advierte que el uso de las TIC trasciende fronteras y que éstas, así como el Internet, son herramientas que favorecen el desarrollo de los países. La cuarta revolución industrial, al igual que sus sucesoras, ha permeado no sólo en aspectos sociales, económicos o culturales -figurando hoy día conceptos como la educación a distancia, la telemedicina, el teletrabajo o los servicios digitales-, sino también ha impactado en el diseño de políticas públicas, de normas jurídicas y en la discusión sobre el impacto de las TIC en los derechos humanos de primera, segunda y tercera generación, así como en la creación de una cuarta generación de derechos humanos en la era digital.

En el diseño de políticas públicas basadas en el uso y aprovechamiento de las TIC, así como en el desarrollo de soluciones basadas en tecnologías como *blockchain*, IA, 5G, cómputo en la nube o el internet de las cosas, es importante observar los principios de la CMSI para orientar políticas públicas que faciliten la integración y el desarrollo de tecnologías inclusivas, seguras y asequibles.

Además, los principios de la CMSI están vinculados con los 17 ODS de la ONU que también buscan orientar a los países en metas específicas para velar por los derechos humanos, la protección al medio ambiente y un desarrollo económico sostenible e igualitario en la era digital.

1.6 Objetivos de Desarrollo Sostenible

Una política pública reconocida a nivel internacional es la Agenda 2030 para el desarrollo sostenible. Esta agenda, publicada el 21 de octubre de 2015 por la Asamblea General de la ONU[45], contempla 17 ODS[46] relacionados con el respeto a los

[45] Asamblea General de la ONU, Resolución A/RES/70/1, Transformar nuestro mundo: la Agenda 2030 para el Desarrollo Sostenible, 21 de octubre de 2015, Disponible en: https://www.un.org/ga/search/view_doc.asp?symbol=A/RES/70/1&Lang=S. (Fecha de consulta: 8 de octubre de 2019).

[46] Los 17 ODS son: Objetivo 1. Poner fin a la pobreza en todas sus formas y en todo el mundo; Objetivo 2. Poner fin al hambre, lograr la seguridad alimentaria y la mejora de la nutrición y promover la agricultura sostenible; Objetivo 3. Garantizar una vida sana y promover el bienestar de todos a todas las edades; Objetivo 4. Garantizar una educación inclusiva y equitativa de calidad y promover oportunidades de aprendizaje permanente para todos; Objetivo 5. Lograr la igualdad de género y empoderar a todas las mujeres y las niñas; Objetivo 6. Garantizar la disponibilidad y la gestión sostenible del agua y el saneamiento para todos; Objetivo 7. Garantizar el acceso a una energía asequible, fiable, sostenible y moderna para todos; Objetivo 8. Promover el crecimiento económico sostenido, inclusivo y sostenible, el empleo pleno y productivo y el trabajo decente para todos; Objetivo

derechos humanos y el desarrollo sostenible. Mediante este documento, la ONU reconoce la expansión de las TIC y de la interconexión mundial, señalando que la tecnología brinda grandes posibilidades para acelerar el progreso humano, superar la brecha digital y desarrollar sociedades de conocimiento[47].

La ONU y la ITU han creado un vínculo entre los principios de la CMSI y los 17 ODS. Afirman que la tecnología favorece el cumplimiento de las metas internacionales sobre desarrollo sostenible[48]. Por ejemplo, destacan que: (i) el Internet es un nuevo servicio básico y contribuye a reducir la pobreza y crear empleos; (ii) el uso confiable de las TIC es crucial para el desarrollo económico y el desarrollo de aplicaciones seguras y confiables para facilitar las transacciones en línea; (iii) se debe contemplar el componente de seguridad; (iv) las regulaciones predecibles y estables son clave para mantener efectividad en la competencia e impulsar el desarrollo de servicios innovadores de TIC[49].

Igualmente, se reconoce el valor de las TIC en los sectores de la agricultura, la ganadería, el medio ambiente, la educación, el empleo, y contar con mejores instituciones públicas. Los 17 ODS refuerzan las tres generaciones de derechos humanos y constituyen líneas de acción para orientar el diseño e implementación de políticas públicas en los países que integran las Naciones Unidas.

No debemos perder de vista que las innovaciones tecnológicas, presentes en las cuatro revoluciones industriales, son herramientas que han permitido el desarrollo económico, social y cultural de las personas e influido en los derechos humanos.

---

9. Construir infraestructuras resilientes, promover la industrialización inclusiva y sostenible y fomentar la innovación; Objetivo 10. Reducir la desigualdad en los países y entre ellos; Objetivo 11. Lograr que las ciudades y los asentamientos humanos sean inclusivos, seguros, resilientes y sostenibles; Objetivo 12. Garantizar modalidades de consumo y producción sostenibles; Objetivo 13. Adoptar medidas urgentes para combatir el cambio climático y sus efectos; Objetivo 14. Conservar y utilizar sosteniblemente los océanos, los mares y los recursos marinos para el desarrollo sostenible; Objetivo 15. Proteger, restablecer y promover el uso sostenible de los ecosistemas terrestres, gestionar sosteniblemente los bosques, luchar contra la desertificación, detener e invertir la degradación de las tierras y detener la pérdida de biodiversidad; Objetivo 16. Promover sociedades pacíficas e inclusivas para el desarrollo sostenible, facilitar el acceso a la justicia para todos y construir a todos los niveles instituciones eficaces e inclusivas que rindan cuentas; Objetivo 17. Fortalecer los medios de implementación y revitalizar la Alianza Mundial para el Desarrollo Sostenible. Ídem

[47] Ídem.

48 CMSI-ODS Matriz, "Vinculación de las líneas de acción de la CMSI con los Objetivos de Desarrollo Sostenible", Disponible en: https://www.itu.int/net4/wsis/sdg/Content/Documents/wsis-sdg_matrix_document.pdf, (Fecha de consulta: 8 de octubre de 2019).

[49] Idem.

Por lo que, en el uso y aprovechamiento de las TIC, propias de la cuarta revolución industrial, será importante observar tanto los principios de la CMSI como los 17 ODS que sirvan como guía para un desarrollo tecnológico apegado al respeto de los derechos humanos.

1.7 Tratados de libre comercio en la cuarta revolución industrial

Otro rubro en donde observamos el impacto de la cuarta revolución industrial y las TIC es en los TLC, los cuales tienen su punto de partida en el *Acuerdo General sobre Aranceles Aduaneros y Comercio de 1947*, modificado en 1994, (GATT, por sus siglas en inglés)[50]. Los acuerdos comerciales tienen como principal objetivo regular el tránsito de mercancías y de personas entre países, por lo que contemplan principalmente temas como derechos de aduana, impuestos a la importación y exportación y las regulaciones no arancelarias como permisos previos de importación y de exportación.

No obstante, con el uso masivo de las TIC e Internet, observamos que los TLC regulan cada vez más conceptos propios de la cuarta revolución industrial, como, tales como: economía digital; ciberseguridad; autenticación y firma electrónica; infraestructura digital; habilidades digitales; digitalización de certificados de origen; comercio digital, o interoperabilidad. Lo anterior, debido a que dichos temas tienen cada vez mayor impacto en el flujo transfronterizo de mercancías y de personas a través de las TIC; los cuales describiremos en seguida.

[50] Acuerdo General sobre Aranceles Aduaneros y Comercio (GATT de 1947), Disponible en: https://www.wto.org/spanish/docs_s/legal_s/gatt47.pdf (Fecha de consulta: 17 de noviembre de 2019).

1.7.1 Mercosur

En el marco del *Tratado de Asunción para la Constitución de un Mercado Común, del 26 de marzo de 1991*[51], los países miembros del MERCOSUR[52], el 20 de diciembre de 2017, aprobaron la *Agenda Digital del Mercosur*[53]. Esta agenda reconoce los beneficios de la transformación digital en el comercio regional a través de un mercado cada vez más digital.

Mediante la Agenda se creó el "Grupo de Agenda Digital del MERCOSUR" que tiene por objeto diseñar un plan de acción en temas vinculados con la digitalización del comercio regional tales como la infraestructura digital y la conectividad; la seguridad y confianza en el ambiente digital; la economía digital; la habilidades digitales de su población; el gobierno digital, el gobierno abierto y la innovación pública de sus instituciones; así como la regulación y coordinación sobre temas de la agenda digital y de gobernanza de internet[54].

1.7.2 ALADI

En el marco del *Tratado de Montevideo de 1980*, mediante el cual de crea la Asociación Latinoamericana de Integración (ALADI), los países miembros[55] acordaron la integración regional para el desarrollo económico y social, en donde hacen uso de las TIC para facilitar el cumplimiento del acuerdo comercial.

---

[51] Tratado de Asunción para la Constitución de un Mercado Común, del 26 de marzo de 1991, Disponible en: https://www.mercosur.int/documento/tratado-asuncion-constitucion-mercado-comun/, (Fecha de consulta: 17 de noviembre de 2019).

[52] Los miembros del MERCOSUR son Argentina, Brasil, Paraguay, Uruguay.

[53] Agenda Digital del Mercosur, Disponible en: http://www.sice.oas.org/Trade/MRCSRS/Decisions/DEC_027_2017_s.pdf, (Fecha de consulta: 17 de noviembre de 2019).

[54] Entre las iniciativas de la Agenda Digital del MERCOSUR destacan Acciones integradas con vistas al desarrollo de las infraestructuras de telecomunicaciones a su interconexión, con enfoque central en las regiones desasistidas; Suscripción de un acuerdo de eliminación de roaming en la región; Coherencia normativa de políticas nacionales de protección de datos personales; Desarrollo de mecanismo integrado online para solución de controversias relacionadas con operaciones de e-commerce; Suscripción de un acuerdo de reconocimiento mutuo de firmas digitales; Elaboración de un marco de referencia común para el desarrollo de habilidades digitales y pensamiento computacional; Desarrollo de sistemas y programas de formación online comunes. Disponible en: https://www.mercosur.int/temas/agenda-digital/ (Fecha de consulta: 17 de noviembre de 2019).

[55] Argentina, Bolivia, Brasil, Chile, Colombia, Cuba, Ecuador, México, Panamá, Paraguay, Perú, Uruguay y Venezuela. Cualquier país de Latinoamérica puede solicitar su adhesión al proceso de integración. *Cfr.* ALADI, Preguntas frecuentes, Disponible en: http://www.aladi.org/sitioaladi/preguntas-frecuentes-2/ (Fecha de consulta: 17 de noviembre de 2019).

Desde el 23 de septiembre de 2004, se generó la *propuesta para la digitalización de certificados de origen en el ámbito de la ALADI*[56] que facilitar el reconocimiento de los beneficios arancelarios entre los países parte del acuerdo comercial. Para ello, se regulan aspectos sobre principios criptográficos y de firma electrónica; acciones en materia de digitalización, de sitios Web, y de modelo genérico de digitalización de certificados de origen; así como los requerimientos de seguridad de los sistemas digitales.

1.7.3 Alianza del Pacífico

El *Acuerdo marco de la Alianza del Pacífico*[57] también contempla una Agenda Digital desde el año 2016, mediante la cual se creó el "Subgrupo de Agenda Digital". Dicho grupo tiene por objeto construir una hoja de ruta que permita a los países miembros[58] implementar, desarrollar y profundizar en temas concretos relacionados con los capítulos de telecomunicaciones y de comercio electrónico.

La agenda digital contempla cuatro ejes: (i) economía digital -mercado digital, industria TIC y emprendimiento digital-; (ii) conectividad digital -IPv6, *roaming* internacional, redes de alta velocidad, acceso a contenidos-; (iii) gobierno digital -datos abiertos, entrega de servicios al ciudadano, servicios compartidos-; y (iv) ecosistema digital -neutralidad de la red, seguridad digital, protección de la privacidad y tratamiento de datos personales, coordinación entre centros de información de red regionales-[59].

[56] Propuesta para la digitalización de certificados de origen en el ámbito de la ALADI, Disponible en http://www2.aladi.org/nsfweb/Documentos/459Rev2.pdf, (Fecha de consulta: 17 de noviembre de 2019).
[57]Acuerdo marco de la Alianza del Pacífico, Disponible en: http://www.sice.oas.org/TPD/Pacific_Alliance/Agreements/Framework_Agreement_Pacific_Alliance_s.pdf (Fecha de consulta: 17 de noviembre de 2019).
[58] Chile, Perú, Colombia y México, + 32 países de observadores.
[59] Alianza del Pacífico, Subgrupo de Agenda Digital, Disponible en: https://alianzapacifico.net/wp-content/uploads/Hoja-de-Ruta-SGAD2016-2017.pdf, (Fecha de consulta: 17 de noviembre de 2019).

1.7.4 T-MEC

El T-MEC entró en vigor el 01 de julio de 2020[60]. Este nuevo tratado contempla un nuevo capítulo: capítulo 19 sobre comercio digital[61]. En este capítulo se regulan temas como: productos digitales; transacciones electrónicas; autenticación electrónica y firmas electrónicas; protección al consumidor en línea; protección de información personal; comercio sin papeles; acceso y uso de Internet para el comercio digital; transferencia fronteriza de información por medios electrónicos; ubicación de instalaciones informáticas; comunicaciones electrónicas comerciales no solicitadas; ciberseguridad; código fuente; servicios Informáticos interactivos, y datos abiertos gubernamentales.

Estos son cada vez más necesarios atender en su regulación secundaria, ya que las TIC cada vez se consolidan más en ser herramientas que facilitan el intercambio no sólo de información sino también de mercancías de forma oportuna, confiable y segura.

1.7.5 Unión Europea

Si bien en América Latina comienzan a desarrollarse aspectos de las TIC en los TLC, en la Unión Europea ésto ya pasaba de forma más integral y armonizada desde el año 2010 con la *Agenda Digital para Europa*[62], en donde, con la finalidad de potenciar el desarrollo económico y social de Europa, se regulaban temas como el mercado único digital; la interoperabilidad y normas; la confianza y seguridad; acceso a Internet; y habilidades e inclusión digitales.

Posteriormente, para 2015 los países de la Unión Europea adoptaron una *Estrategia para el Mercado Único Digital*[63], que contempla generar normas de comercio electrónico transfronterizo; contenidos digitales; bloqueo geográfico; normas

---

[60] T-MEC, publicado en el DOF el 29 de junio de 2020, Disponible en: http://dof.gob.mx/2020/SRE/T_MEC_290620.pdf. (Fecha de consulta: 10 de julio de 2020).
[61] Ídem.
[62] Comisión Europea, Una Agenda Digital para Europa, Bruselas, 19.5.2010 COM(2010)245 final, Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52010DC0245&from=es, (Fecha de consulta: 17 de noviembre de 2019).
[63] Comisión Europea, Una Estrategia para el Mercado Único Digital de Europa, Bruselas, 6.5.2015, COM(2015) 192 final, Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:52015DC0192, (Fecha de consulta: 17 de noviembre de 2019).

sobre telecomunicaciones; plataformas en línea; contenidos ilícitos en Internet; economía de datos; fomentar la competitividad a través de la interoperabilidad y normalización; habilidades digitales; administraciones electrónicas; reforzar confianza y seguridad en servicios digitales y el tratamiento de datos personales.

Sin duda estos aspectos de integración regional y comercial de la Unión Europea, en un ámbito vinculante para los países miembros, ha facilitado y acelerado la armonización de normas y principios para afrontar los desafíos de la cuarta revolución industrial. Incluso, han desarrollo agendas estratégicas sobre ciberseguridad[64], tecnologías emergentes como 5G[65] o la gobernanza de los datos con impacto en la IA[66].

Entro las normas vinculantes que derivan de la Unión Europea podemos destacar el *Reglamento general de protección de datos*[67]; o el *Reglamento relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior*[68], que son dos normas relevantes en el intercambio de información, seguridad, autenticación digital y protección de datos personales en un contexto de economía digital.

La regulación regional europea en materia de tecnología y ciberseguridad tiene como base el desarrollo de la economía digital entre los países europeos, facilitando tantos aspectos técnicos como regulatorios en el uso de las TIC e inter-

[64] Parlamento Europeo, Estrategia de Ciberseguridad de la Unión Europea, 2013, Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52013JC0001, (Fecha de consulta: 17 de noviembre de 2019).
[65] Comisión Europea, Despliegue seguro de la 5G en la EU, Bruselas, Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020DC0050&from=FR, (Fecha de consulta: 17 de noviembre de 2019).
[66] Comisión Europea, Estrategia Europea de Datos, Bruselas, Disponible en: https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf, (Fecha de consulta: 17 de noviembre de 2019).
[67] Diario Oficial de la Unión Europea, Reglamento General de Datos Personales, Disponible en https://www.boe.es/doue/2016/119/L00001-00088.pdf, (Fecha de consulta: 17 de noviembre de 2019).
[68] Diario Oficial de la Unión Europea, Reglamento relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, Disponible en https://www.boe.es/doue/2014/257/L00073-00114.pdf, (Fecha de consulta: 17 de noviembre de 2019).

cambio de datos, mercancías y tránsito de personas. Más adelante veremos la regulación europea sobre el reconocimiento transfronterizo de la identidad digital y firma electrónica.

1.7.6 Foros de cooperación regional en América Latina

En América Latina existen algunos otros foros de cooperación regional no vinculantes en donde se discuten y comparten acciones y avances en materia digital, tales como el *Foro de Cooperación Económica de Asia Pacífico (APEC)*[69]; la Red de gobierno electrónico de América Latina y el Caribe (*RedGealc)*[70], en el marco de la Organización de los Estados Americanos a cargo del Banco Interamericano de Desarrollo, así como el foro de la *Comisión Económica para América Latina y el Caribe (CEPAL)*[71].

[69] APEC: Participan los siguientes países: Australia, Brunei, Canadá, Chile, Corea del Sur, Malasia, Nueva Zelanda, Filipinas, Indonesia, Japón, Singapur, Tailandia, Estados Unidos, República de China (Taiwán), China, Hong Kong, México, Papúa Nueva Guinea, Perú, Rusia y Vietnam. En su Reunión en Da Nang en 2017, se adoptó la Hoja de ruta de la economía digital y de Internet de APEC, en donde se regulan temas como: (1) gestión de riesgos de seguridad digital; (2) estrategias de economía; (3) infraestructura de información crítica resistente; (4) fortalecer la colaboración; (5) empoderar al usuario digital; (6) tecnologías de seguridad digital para la confianza, y (7) seguridad de datos personales. Cfr. Agenda Digital APEC, Disponible en: https://www.apec.org/-/media/APEC/Publications/2019/11/APEC-Framework-for-Securing-the-Digital-Economy/219_TEL_APEC-Framework-for-Securing-the-Digital-Economy.pdf, (Fecha de consulta: 17 de noviembre de 2019).

[70] REDGEALC. Participan los siguientes países: Antigua y Barbuda, Argentina, Bahamas, Barbados, Belice, Bolivia, Brasil, Canadá, Chile, Colombia, Costa Rica, Dominica, Ecuador, El Salvador, Granada, Guatemala, Guyana, Haití, Honduras, Jamaica, México, Nicaragua, Panamá, Paraguay, Perú, República Dominicana, Santa Lucía, San Kitts Nevis, San Vincente Grenadine, Suriname, Trinidad y Tobago, Uruguay, Venezuela. Cuenta con las siguientes líneas de trabajo: Coronavirus, Servicios Transfronterizos, Innovación, Software Público, Tecnología Emergentes, Datos Abiertos, Medición. Disponible en: http://www.redgealc.org/ (Fecha de consulta: 20 de junio de 2020).

[71] CEPAL. Participan los siguientes países: Alemania, Antigua y Barbuda Argentina, Bahamas, Barbados, Belice, Bolivia, Brasil, Canadá, Chile, Colombia, Costa Rica, Cuba, Dominica, Ecuador, El Salvador, España, Estados Unidos de América, Francia, Granada, Guatemala, Guyana, Haití. Honduras, Italia, Jamaica, Japón, México, Nicaragua, Países Bajos, Panamá, Paraguay, Perú, Portugal, Reino Unido de Gran Bretaña e Irlanda del Norte, República de Corea, República DominicanaSaint Kitts y Nevis, SanVicente y Las Granadinas, Santa Lucía, Suriname, Trinidad y Tabago, Uruguay, Venezuela. Desarrollo la Agenda Digital para América Latina y el Caribe(eLAC2020), que contempla los siguientes rubros: (1) Infraestructura digital; (2) Transformación y economía digitales; (3) Mercado digital regional; (4) Gobierno digital; (5) Cultura, inclusión y habilidades digitales; (6) Tecnologías emergentes para el desarrollo sostenible; (7) Gobernanza para la sociedad de la información. Cfr, Agenda Digital CEPAL, Disponible en: https://www.cepal.org/es/elac2020/agenda-digital-2020, (Fecha de consulta: 20 de junio de 2020).

No obstante, consideramos que, si bien la región latinoamericana cuenta con normas comunes sobre el uso de las TIC, lo cierto es que la diversidad y la desarticulación de foros impide que los países puedan avanzar y focalizar acciones sobre la regulación e implementación de la economía digital que incluyen retos sobre la interoperabilidad de identidades y firmas electrónicas.

A través de los TLC -normativa internacional vinculante-, los países de la región latinoamericana tienen una oportunidad para avanzar de forma estandarizada en temas de desarrollo digitales que son comunes para todos, fortaleciendo así el diseño e implementación de las agendas nacionales y el comercio electrónico. Por ejemplo, al ser vinculantes los TLC, las disposiciones que emanen de sus apartados deberán considerarse en el diseño de las estrategias y normas nacionales, en donde la identidad digital y el reconocimiento transfronterizo de firma electrónica son pieza clave para la economía digital.

De esta forma, en el presente capítulo pudimos observar cómo la innovación tecnológica genera nuevos desafíos para las ciencias sociales como el derecho. El desarrollo sostenible se beneficia de la tecnología, pero será necesario que los gobiernos adopten un marco normativo sólido en torno a la protección de los derechos humanos en la era digital. Se requiere un conjunto de estrategias de políticas públicas que en su conjunto atiendan los desafíos en infraestructura digital, habilidades digitales y protección de derechos humanos en la era digital.

Además, observamos el impacto que ha tenido la cuarta revolución industrial en el comercio internacional. El uso de tecnologías como IA, *blockchain*, conducción autónoma o cómputo en la nube, entre otras, nos ha llevado a generar nuevos bienes y servicios a través de una economía digital que podemos ver plasmada en los TLC, en donde se atienden temas ya no solo sobre el tránsito de personas y mercancías, sino también sobre el uso de nuevas tecnologías.

La seguridad jurídica en torno a estos nuevos derechos que emergen en la era digital será un pilar relevante para la transformación digital de la sociedad. De esta forma, en el siguiente apartado observaremos cuáles son las principales acciones que han adoptado a nivel nacional los países en sus agendas digitales para hacer frente a los desafíos de la cuarta revolución industrial.

Capítulo 2
Transformación Digital

Capítulo 2. Transformación Digital

Las revoluciones industriales conllevan retos para los gobiernos en el diseño de políticas públicas. La tecnología ha mostrado ser una herramienta que facilita el desarrollo, innovación y progreso de la población. El derecho ha reflejado los principales desafíos que se han enfrentado a través de las revoluciones industriales. Por ejemplo, el auge del derecho laboral debido a las largas jornadas de trabajo en la fabricas y los procesos de producción en serie, o recientemente el uso masivo de información a través de internet que pone en riesgo los derechos privacidad y de protección de datos personales.

Además de salvaguardar los derechos humanos en los desafíos del uso y aprovechamiento de las TIC, las revoluciones industriales también nos han mostrado que es necesario adoptar políticas públicas que permitan reducir las brechas sociales. El constante cambio tecnológico requiere una constante adaptación de las instituciones y las personas. La adopción de la tecnología no sólo requiere atender aspectos técnicos sino no también medidas con enfoque multidisciplinario para que la sociedad en general esté preparada para asumir los cambios sociales y económicos que implica el desarrollo tecnológico.

Así, en el siguiente apartado analizáramos cuáles son los principales elementos que los gobierno contemplan para afrontar los retos de la cuarta revolución industrial. Actualmente ante la globalización, la digitalización de procesos y el uso masivo de datos, la cuarta revolución industrial presenta temas que son de interés común para los países como el despliegue de infraestructura, habilidades digitales y servicios nuevos servicios públicos. Para ello, tomaremos como referencia el EDGI de la ONU que nos proporciona un marco de referencia sobre el avance y desarrollo tecnológico de los países a nivel internacional.

2.1 Transformación Digital

Tanto instituciones públicas como privadas alrededor de todo el mundo están utilizando la tecnología para proporcionar nuevos servicios digitales. La pandemia de COVID-19 ha venido a acelerar el cambio en la forma en que hoy en día nos

relacionamos. La tecnología y la innovación están siendo utilizadas para transformar los procesos, la manera en que tomamos decisiones y se producen y consumen bienes y servicios.

Sin embargo, la adopción de la tecnología en la cuarta revolución industrial, al igual que las otras revoluciones industriales, va más allá de sólo usar y aprovechar las TIC. Cuando usamos la tecnología lo hacemos con la finalidad de ser más eficientes, económicos y eficaces en la generación y consumo de servicios. Pero para ello se requiere un cambio global no sólo en la adquisición de la más reciente tecnología. Se requiere transformar los procesos, la cultura institucional y generar mayores capacidades humanas. A este proceso en su conjunto se la conoce como transformación digital.

El concepto de transformación digital no sólo se vincula a transformar ni al uso de la tecnología, sino que es un proceso multisectorial y multifactorial. Gerald C. Kane, señala que la transformación digital "*se trata de la capacidad de las organizaciones, de sus líderes y empleados para adaptarse a los rápidos cambios provocados por la evolución de las tecnologías digitales"*[72]. En el sector público, la UIT y la ONU señalan que los gobiernos están utilizando tecnologías digitales para transformar la forma en que operan, comparten información, toman decisiones y prestan servicios, así como para participar y asociarse con personas para resolver desafíos políticos de interés público, y añaden que la creación de capacidades en las instituciones y servidores públicos es importante para la transformación digital del gobierno[73].

Igualmente, la ONU y la UIT establecen nueve pilares clave para la transformación digital del gobierno digital: 1) visión, liderazgo y mentalidad; 2) marco

72 KANE, Gerald C. "'Digital Transformation" Is a Misnomer, It's not about digital or transformation. It's about adaptation", MIT Sloan Management Review, Bostón, Estados Unidos, Agosto, 2017, Disponible en https://sloanreview.mit.edu/article/digital-transformation-is-a-misnomer/#:~:text=At%20its%20most%20fundamental%20level,wrought%20by%20evolving%20digital%20technologies.&text=Digitally%20mature%20organizations%20exhibit%20certain,nothing%20to%20do%20with%20technology. (Fecha de consulta: 18 de junio de 2020)

73 ONU, Department of Economic and Social Affairs, "E-Government Survey 2020, Digital Government in the Decade of Action for Sustainable Development", Nueva York, 2020, p. XXII, Disponible en: https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2020-Survey/2020%20UN%20E-Government%20Survey%20(Full%20Report).pdf, (Fecha de consulta: 18 de junio de 2020).

institucional y regulatorio; 3) configuración y cultura organizacional; 4) pensamiento e integración de sistemas para la formulación de políticas y prestación de servicios; 5) Garantizar la gestión estratégica y profesional de los datos para permitir la formulación de políticas basadas en datos, y acceso a información a través de datos abiertos; 6) infraestructura de TIC, asequibilidad y accesibilidad a la tecnología; 7) movilizar recursos y alinear prioridades, planes y presupuestos, incluso a través de asociaciones público-privado; 8) crear capacidad en el personal de la administración pública, y 9) desarrollar capacidades sociales de inclusión digital y reducir la brecha digital[74].

Como observamos, la transformación digital no es sólo adoptar nuevas y mejores tecnologías, sino que también implica llevar a cabo diferentes acciones que van desde contar con un cambio de visión, liderazgo y mentalidad de las personas e instituciones, hasta atender aspectos técnicos de seguridad para salvaguardar los derechos humanos en medios digitales. Un aspecto relevante para considerar en los procesos de transformación digital es el hecho que, a mayor digitalización, las personas e instituciones migran sus procesos a un mundo digital.

En las siguientes líneas conoceremos cuales son las medidas que los países mejorar evaluados en el EDGI han adoptados para la transformación digital en su población a través de políticas públicas, leyes y agendas digitales. Para ello, conoceremos brevemente como se conforma el EDGI y cuáles son los rubros medibles en materia de desarrollo digital.

2.2 Índice de Desarrollo de Gobierno Electrónico

A través del *Índice de Desarrollo de Gobierno Electrónico* (EGDI, por sus siglas en inglés)[75], la ONU advierte el desarrollo de gobierno electrónico en cada país, destacando que aquellos que cuentan con una sólida estrategia de transformación digital son los países que mejor se posicionan a nivel mundial en el EGDI[76].

La ONU, mediante el Departamento de Asuntos Económicos y Sociales (UNDESA, por sus siglas en inglés), publica cada dos años el EGDI. Éste índice

[74] Ídem.
[75] Ídem.
[76] Ídem.

tiene por **objeto** medir a nivel mundial el desarrollo de gobierno electrónico de 193 países, con base en tres indicadores: (i) índice de **servicios digitales**[77]; (ii) índice de **capital humano**[78], y el (iii) índice de **infraestructura de telecomunicaciones**[79].

Los temas de infraestructura y capital humano son pilares para afrontar los desafíos que demanda la cuarta revolución industrial. No obstante, consideramos que el tema de servicios digitales nos permite conocer más a detalle el proceso de transformación digital de un país, ya que implica una serie de elementos a considerar para ofrecer servicios públicos centrados en las necesidades de las personas. Es decir, además de la infraestructura y capacidad digital en la población, la estrategia en servicios digitales nos permite conocer el conocimiento e importancia que cualquier país dedica a la transformación digital.

El índice de servicios digitales se obtiene con base en un cuestionario de 148 preguntas estructuradas en seis apartados. A través de estas preguntas se analizan elementos que denotan el grado de avance de un país en materia de desarrollo digital. Estos apartados y elementos analizados en materia de servicios digitales son los siguientes:

ESTRUCTURA DE CUESTIONARIO DEL ÍNDICE DE SERVICIOS DIGITALES DEL EDGI		
NO.	**APARTADO ÍNDICE DE SERVICIOS DIGITALES**	**ELEMENTOS ANALIZADOS**
1	**MARCO INSTITUCIONAL**	• Portal nacional de gobierno electrónico • Director de información
2	**ESTRATEGIA E IMPLEMENTACIÓN**	• Estrategia nacional de gobierno electrónico / estrategia de preparación digital • Estrategia de desarrollo nacional que incorpora ODS • Estrategia que haga referencia específica al uso de nuevas tecnologías • Estrategia que esté alineada con los ODS • Estrategia que esté alineada con el plan nacional de desarrollo
3	**MARCO LEGAL**	• Libertad de expresión y protección de datos personales • Datos gubernamentales abiertos • **Identidad digital**

[77] El **índice de servicios digitales** se obtiene de un "cuestionario de servicios en línea" que consta de una lista de 148 preguntas. Cada pregunta requiere una respuesta binaria. Cada respuesta positiva genera una "pregunta más profunda" dentro y a través de los patrones. El resultado es una encuesta cuantitativa mejorada con un rango más amplio de puntos distribuciones que reflejan las diferencias en los niveles de desarrollo del gobierno electrónico entre los Miembro Estados. Ibídem, p. 236.

[78] El **Índice de Capital Humano** consta de cuatro componentes: (i) tasa de alfabetización de adultos; (ii) la tasa bruta de matriculación primaria, secundaria y terciaria combinada; (iii) años esperados de escolaridad; y (iv) años promedio de escolaridad. Ibídem, p. 235.

[79] El **Índice de Infraestructura de Telecomunicaciones** es un promedio aritmético compuesto de cuatro indicadores: (i) usuarios estimados de Internet por cada 100 habitantes; (ii) número de suscriptores móviles por cada 100 habitantes; (iii) suscripción activa de banda ancha móvil; y (iv) número de suscripciones de banda ancha fija por cada 100 habitantes. Ibídem, p. 232.

		• Contratación electrónica • Publicación digital del gasto público • Interoperabilidad de datos
4	**USO DE SERVICIOS EN LÍNEA Y SATISFACCIÓN DEL USUARIO**	• Recopilación de estadísticas de uso de servicios de gobierno electrónico • Medición de la satisfacción de los ciudadanos en los servicios de gobierno electrónico
5	**NUEVAS TECNOLOGÍAS**	• Una estrategia nacional específica sobre una o más de las nuevas tecnologías • Organismo del gobierno nacional que trabaja específicamente en temas relacionados con nuevas tecnologías
6	**COOPERACIÓN INTERNACIONAL Y REGIONAL**	• Ofrecer (o planificar) apoyo a otros países en el gobierno electrónico • Es parte de cualquier cooperación subregional, regional o internacional en gobierno electrónico

Cuadro 2. *Estructura de cuestionario del índice se servicios digitales conforme al EDGI*
Fuente: ONU, EDGI, 2020.

Además de la infraestructura y las capacidades humanas, el EDGI evalúa una serie de elementos relacionados en conocer si el país cuenta o no con elementos específicos como: un portal de gobierno electrónico; una estrategia nacional de gobierno digital; datos abiertos, protección de datos personales; **identidad digital**; contratación electrónicas; interoperabilidad; encuestas de satisfacción de servicios; estrategias sobre el uso de tecnologías emergentes; una autoridad nacional especializadas en temas relacionados con el uso de nuevas tecnologías; cooperación internacional; y su alineación con los ODS.

Hay ciertos elementos que permiten a un país potenciar su transformación digital y contar con un mejor índice de desarrollo de gobierno electrónico. Se trata de un marco institucional a través de una estrategia digital y de regulación sobre identidad digital. Como analizaremos más adelante, la identidad es un derecho humano que se garantiza desde el nacimiento y al mismo tiempo es un habilitador de otros derechos humanos. En la cuarta revolución industrial es justamente el mecanismo para garantizar esos derechos en medios digitales. De ahí la importancia de contar con marcos jurídicos que garanticen el derecho a la identidad en la cuarta revolución industrial.

Al respecto, con base en el EDGI, los países mejor posicionados cuentan con una regulación sobre identidad digital que se refleja en su estrategia digital o marco jurídicos[80]. En algunos países la **identidad digital** se vincula con la **firma**

[80] Ibídem, p. 14.

electrónica de las personas que les permite suscribir actos jurídicos en medios digitales de forma segura y con plena validez legal.

Adicionalmente, el rubro de **interoperabilidad** que permite el intercambio de datos con respeto a los derechos humanos y con base en los principios de seguridad de la información, también ha sido un elemento importante para la ejecución de las estrategias digitales y la prestación de servicios públicos digitales por parte de los gobiernos. Elementos como la identidad digital, ciberseguridad, firma electrónica e interoperabilidad son piezas claves para la transformación digital de un país.

En el presente apartado analizaremos los contenidos de las agendas digitales, resaltando temas sobre identidad digital y firma electrónica. La muestra que estudiaremos se refiere a los países mejor posicionados en el *ranking* de desarrollo de gobierno electrónico, los cuales analizaremos en los capítulos siguiente haciendo especial referencia al caso de México.

2.2.1 Ranking de países sobre desarrollo de gobierno electrónico -servicios en línea-

Para conocer cuáles son los elementos clave para el desarrollo de gobierno electrónico, analizaremos las estrategias digitales de los países mejor posicionados en el EDGI[81]. Este índice se divide en muy alto (por entre 0.75 y 1.00); alto (entre 0.50 y 0.74); medio (entre 0.25 y 0.49), y bajo (menor a 0.25).

Consideramos importante, para los efectos del presente documento, conocer cuáles son los elementos que contemplan las estrategias digitales de los dos países mejor posicionados en cada continente (América, Europa, África, Asia y Oceanía). En el caso de América Latina, además de los dos primeros lugares conoceremos los casos de Canadá, Chile, Argentina y Brasil, quienes para el 2020 presentaron un índice muy alto de desarrollo de gobierno electrónico[82].

81 Según datos de la ITU, en 2019, 168 países cuentan con una agenda o estrategia digital, y se espera que para 2023 sean 193 países en el mundo que cuenten con su propia estrategia, ITU, "Connect 2030 Agenda, access a better world", Goal 1 – Growth, Target 1.4: By 2023, all countries adopt a digital agenda/strategy", Ginebra, 2020, Disponible en: https://itu.foleon.com/itu/connect-2030-agenda/growth/ (Fecha de consulta: 19 de junio 2020).

82 ONU, Department of Economic and Social Affairs, op cit. p. 37-62.

Así, con base en el EDGI 2020, los dos primero lugares en el índice servicios digitales por continente son: (i) en África, Sudáfrica -0.7471- y La Isla de Mauricio -0.7000-; (ii) en Asia, la República de Corea -1.000-[83] y Singapur -0.9647-; (iii) en Europa, Estonia -0.9941- y Dinamarca - 0.9706-; (iv) en Oceanía, Australia - 0.9471- y Nueva Zelanda - 0.9294-; (v) en América, Estados Unidos - 0.9471-, Uruguay - 0.8412-, y Canadá - 0.8412-, seguidos por Argentina - 0.8471-, Chile - 0.8529-, Brasil - 0.8706-, y México - 0.8235-. En los siguientes apartados analizaremos cuál es la estrategia digital de cada país, que institución pública la lidera, su objetivo y principales componentes.

2.2.2 Sudáfrica

La agenda digital de Sudáfrica, denominada *"E-Gov Strategy"*[84]*,* está liderada por el Departamento de Telecomunicaciones y Servicios Postales. Para su elaboración se contó con la participación de instituciones públicas y privadas.

La estrategia de Sudáfrica tiene como objetivo ofrecer servicios públicos desde cualquier lugar a cualquier tiempo; reducir el costo de la administración pública; harmonizar el marco legal para facilitar la transformación digital; establecer mecanismos de coordinación y facilitación de servicios gubernamentales; desarrollo de habilidades; transformar el gobierno interactuando con los ciudadanos; desarrollar casos de uso con tecnologías como internet de las cosas, *big data*, o cómputo en la nube; fomentar la innovación y proveer servicios gubernamentales con los mejores prácticas y estándares sobre interoperabilidad[85].

Sudáfrica establece cinco principios para el desarrollo de servicios digitales: 1) interoperabilidad; 2) ciberseguridad; 3) economía de escala; 4) eliminar la duplicidad, y 5) inclusión digital. La agenda digital de Sudáfrica está alineada a la

[83] Destaca el caso de Corea del Sur ya que es el único país a nivel mundial en alcanzar la puntuación más alta en el índice de servicios digitales. Ibídem, p. 48.
[84] Department of telecomunications and postal services, "National e-Government Strategy and Roadmap, República de Sudáfrica, 2017, Disponible en: https://www.dtps.gov.za/images/phocagallery/Popular_Topic_Pictures/national_e-Gov_Strategy.pdf (Fecha de consulta: 20 de junio de 2020).
[85] Ibídem, p. 15.

National Integrated ICT Policy[86], en donde se establece que para el acceso a servicios digitales establecer un marco común para proporcionar a todos los ciudadanos una **identidad digital** a través de un sistema robusto y seguro para garantizar el derecho a la identidad de cualquier persona.

Para la promoción de transacciones electrónica seguras, Sudáfrica contempla el uso de la firma electrónica a través de su ley *The Electronic Communications and Transactions Act*, [87] la cual busca adaptarse a protocolos internacionales y regionales. En su plan nacional, Sudáfrica destaca que, si bien el gobierno cuenta con diferentes iniciativas de gestión de la información, estas no son necesariamente interoperables y por ello existe la necesidad de coordinación centralizada que garantice la interoperabilidad de los servicios público[88].

2.2.3 La Isla de Mauricio

Su estrategia digital se denomina *Digital Mauritius* 2030[89]. Es liderada por el Ministerio de Tecnología, Comunicación e Innovación, la cual fue elaborada a través de consultas a los sectores público y privado con la finalidad de transformar la economía digital a través de una serie de medidas relacionadas con cinco ejes: (1)

[86] Department telecomunication and postal services, Republic of South Africa, "National Integrated ICT Policy White Paper", 2016, Disponible en: https://www.dtps.gov.za/images/phocagallery/Popular_Topic_Pictures/National_Integrated_ICT_Policy_White.pdf (Fecha de consulta: 20 de junio de 2020).
[87] Ibídem p. 123.
[88] Ibídem, p. 58.
[89] Ministerio de Tecnología, Comunicación e Innovación, "Digital Mauritius 2030", República de Mauricio, 2018, Disponible en: http://mitci.govmu.org/English/Documents/2018/Launching%20Digital%20Transformation%20Strategy%20191218/DM%202030%2017%20December%202018%20at%2012.30hrs.pdf (Fecha de consulta: 20 de junio de 2020).

gobierno digital y fomento del sector empresarial[90]; (2) infraestructura de TIC[91]; (3) innovación[92]; (4) gestión del talento[93], y (5) ciberseguridad[94].

En la estrategia digital de la Isla de Mauricio, se reconoce como una de sus fortalezas para el gobierno digital y el fomento al sector empresarial, **el uso de la firma electrónica, la gestión de la identidad** y el intercambio de datos a través de la plataforma *InfoHighway*[95], así como acciones para armonizar los procesos de flujo de información mediante la interoperabilidad de sistemas y arquitecturas orientadas a servicios[96].

2.2.4 Corea del Sur

Corea del Sur es el segundo lugar mundial en el EDGI, pero el primero en el índice de servicios digitales con la puntuación más alta. Su estrategia digital se caracteriza por contener los siguientes elementos. Cuenta con una estrategia nacional cada cinco años a través del *Korea e-government master plan 2020*[97], el cual cuenta con cinco grandes objetivos: 1) mejorar la experiencia digital de los ciudadanos y rediseñar los servicios gubernamentales; 2) construir un gobierno inteligente y predictivo basado en datos; 3) crear un nuevo ecosistema gubernamental en colaboración con las industrias; 4) contar con infraestructuras seguras y confiables;

---

[90] En el apartado de gobierno digital y fomento del sector empresarial, destacan acciones relacionadas con la adquisición de tecnología innovadora, reutilización de aplicaciones exitosas, acuerdos marco de compras públicas, revisión y actualización del marco normativo para el uso de las TIC, diseño y reingeniería previa al uso de servicio digitales. Ibidem, p. 6-7.

[91] En el apartado de infraestructura de TIC destacan acciones sobre proporcionar Internet de alta velocidad a través de fibra y la red 5G, desarrollo de Internet para atender emergencias. Idem.

[92] En el rubro de innovación destaca acciones como implicación administrativa, eliminación del papel, desarrollar capacidades en todas las áreas de conocimiento, atraer extranjeros estudiantes, mejorar el sistema educativo incluyendo pensamiento computacional, alfabetización de los datos, incorporar tecnologías emergentes como blockchain, la robótica, Internet de las Cosas, Fintech y Big Data. Idem.

[93] En la gestión de talento se propone atender la demanda de nuevas habilidades, aprendizaje para adultos a través de activos del mercado laboral, promover la capacitación en el trabajo, aprovechar el aula virtual y garantizar la alfabetización de los datos. Idem.

[94] Por último, en ciberseguridad proponer crear capacidad institucional en áreas como la darnet, la moneda virtual, y el lavado de dinero en línea, así como desarrollar un marco regulatorio para contrarrestar el uso de monedas virtuales para actividades delictivas. Idem.

[95] Ibidem, p. 25.

[96] Ibidem, p. 35.

[97] Gobierno de Corea del Sur, “Korea e-Government Master Plan 2020”, Korea, 2017, Disponible en: https://www.kdevelopedia.org/resource/view/04201706080147946.do#.Xws4mShKjIU (Fecha de consulta: 20 de junio de 2020).

5) contar con un gobierno digital que permita fortalecer la coordinación y cooperación internacional.

Entre las iniciativas que contemplan los cinco objetivos anteriores podemos destacar las siguientes: servicios totalmente digitales; contar con información integrada inteligentemente; gobierno abierto e innovador para los ciudadanos; crear un marco general para el desarrollo y uso de la IA y datos para la innovación en la administración pública atendiendo las necesidades de las personas -especialmente las de los grupos más vulnerables-; facilitar la economía de datos e IA con el fin de construir una base sólida para el desarrollo de una economía digital sostenible; acelerar el desarrollo de nuevas tecnologías en beneficio de la sociedad y la administración pública; fomentar la participación electrónica, los datos abiertos (data.go.kr), y adquisición electrónica (KONEPS); contar con un marco legal para el gobierno digital basado en la protección de datos, **la seguridad e identidad digitales**, los cuales se regulan a través de **su Ley de Firma Digital** de 2017[98].

2.2.5 Singapur

La estrategia de Singapur se denominada "*Smart Nation*"[99]. Está liderada por la Agencia Gubernamental de Singapur y colaboran instituciones públicas y privadas. Cuenta con tres ejes (1) economía digital; (2) gobierno digital, y (3) sociedad digital. Para cada uno de estos grandes ejes prevé un plan específico de acción. Para la economía digital está el *Marco de Acción para la Economía Digital*[100] en donde destacan acciones para el uso de tecnologías emergentes como *blockchain*, IA, ciudades inteligentes, fomento a la innovación, ciberseguridad, habilidades digitales.

---

[98] Korea Law, "Digital Signature Act, Korea", 2017, Disponible en: https://elaw.klri.re.kr/eng_service/lawView.do?hseq=42625&lang=ENG#:~:text=The%20purpose%20of%20this%20Act,and%20advancing%20social%20benefit%20and (Fecha de consulta: 20 de junio de 2020).

[99] Smart Nation Singapur, "Agenda Digital", Singapur, 2020, Disponible en: https://www.smartnation.gov.sg/ (Fecha de consulta: 21 de junio de 2020).

[100] Gobierno de Singapur, "Marco de Acción para la Economía Digital en Singapur"Singapur, 2018, Disponible en: https://www.imda.gov.sg/-/media/Imda/Files/SG-Digital/SGD-Framework-For-Action.pdf (Fecha de consulta: 21 de junio de 2020).

Para el apartado de gobierno digital contempla el *Plan de Gobierno Digital*, que incluye integrar servicios que atiendan las necesidades de los ciudadanos y empresarios; fortalecer la integración entre política, operaciones y tecnología; hacer lo digital en un tema común basado en plataformas de datos; trabajar con sistemas confiables y seguros; incrementar las habilidades digitales, y co-crear con los ciudadanos y empresas facilitando la adopción de la tecnología.

Igualmente, en materia de sociedad digital, Singapur contempla el *Plan de planeación digital*[101] en el que prevé acciones desde proporcionar computadoras y tabletas a sus ciudadanos de bajos ingresos, acceso a internet en zonas vulnerables, inclusión financiera, hasta contar con una **identidad nacional digital**. Además, en este último se busca asegurar que los niños y jóvenes reciban habilidades digitales, se fomente la participación comunitaria, y alienta tanto a instituciones públicas y privadas a contar con diseño de servicios en lenguas nativas.

Para llevar a cabo los anteriores planes de acción, Singapur considera proyectos estratégicos en los que se encuentran la identidad digital nacional; permitir un gobierno ágil e interoperable; contar con pagos electrónicos seguros; agrupar servicios digitales basados en las etapas de vida de las personas; usar sensores y datos para ejecutar ciudades inteligentes, y contar con movilidad urbana inteligente aprovechando las TIC y los datos. Además de los planes descritos, Singapur cuenta con una estrategia de ciberseguridad[102] en donde se reconoce que la seguridad y los datos son habilitadores claves para una nación inteligente, resaltando la importancia de la protección de los datos personales.

2.2.6 Estonia

La estrategia digital de Estonia se basa en crear una sociedad digital. La transformación digital de Estonia cuenta con ocho objetivos: **1) identidad digital**; 2)

[101] Ministry of Communications and Information, “Plan de planeación digital de Singapur”, Singapur, 2020, Disponible en: https://www.mci.gov.sg/en/portfolios/digital-readiness/digital-readiness-blueprint (Fecha de consulta: 21 de junio de 2020).
[102] Smart Nation Singapur, “Estrategia de Ciberseguridad de Singapur”, Singapur, 2020, Disponible en: https://www.smartnation.gov.sg/why-Smart-Nation/secure-smart-nation (Fecha de consulta: 22 de junio de 2020).

interoperabilidad de servicios; 3) seguridad y protección; 4) cuidado de la salud; 5) gobierno electrónico; 6) servicios de movilidad; 7) negocios y finanzas, y 8) educación e investigación. Cada uno de estos objetivos tiene a su vez diversas acciones que funcionan e interoperan a través de un *software* de código abierto denominado X-ROAD -considerado por el propio gobierno estoniano, junto con la identidad digital del 99% de sus ciudadanos-, como la espina dorsal de la sociedad digital[103].

Estos dos elementos junto con la **ley electrónica** y la regulación de *blockchain*, han fortalecido a Estonia en materia de desarrollo digital, priorizando la seguridad de las transacciones con base en una **identidad** y **firma digitales**, interoperabilidad y *blockchain*, a raíz de la experiencia del ciberataque que sufrió en 2007 en donde 58 sitios electrónicos quedaron desconectados[104].

En el siguiente cuadro enlistamos estas acciones las cuales nos parece importante conocer en el entendido que Estonia figura como uno de los principales países referentes en servicios digitales.

PILAR		ACCIÓN
1	**Identidad digital** **(la identidad digital se asocia a través de la firma electrónica)**	• Tarjeta de identificación • Identificación móvil • Residencia electrónica • ID inteligente
2	**Interoperabilidad de servicios**	• X-Road® • Registro de tierras electrónicas • Registro de población
3	**Seguridad y protección**	• KSI *Blockchain* • Ley electrónica • Justicia electrónica • e-Police
4	**Cuidado de la salud**	• Registros de salud electrónica • e-ambulancia • Receta electrónica
5	**Gobierno electrónico**	• Nube de gobierno • Embajada de datos • i-Voting • Gabinete electrónico
6	**Servicios de movilidad**	• Sistemas inteligentes de transporte • Estacionamiento móvil • Gestión de colas fronterizas
7	**Negocios y finanzas**	• Impuesto electrónico • Banca electrónica

[103] Estonia, e-estonia, "Interoperability servicies e-Estonia", Estonia, 2020, Disponible en: https://e-estonia.com/solutions/interoperability-services/x-road/ (Fecha de consulta: 22 de junio de 2020).
[104] Estonia, e-estonia, "How Estonia became a global heavyweight in cyber security", Estonia, 2020, Disponible en: https://e-estonia.com/how-estonia-became-a-global-heavyweight-in-cyber-security/ (Fecha de consulta: 22 de junio de 2020).

		• Registro de comercio electrónico
8	**Educación e investigación**	• Sistema de información de educación de Estonia • eKool y Stuudium • Sistema de información de investigación de Estonia • e-Schoolbag • Otras soluciones de e-school

Cuadro 3. *Pilares de la agenda digital de Estonia*
Fuente: E-Estonia. Bloques de construcción de e-estonia. 2020.

Para garantizar transacciones de forma segura, a través de X-ROAD todos los datos salientes se firman y cifran digitalmente, y todos los datos entrantes se autentican y registran. Este *software* se está desarrollando incluso en otros países como Finlandia, Islandia y Japón[105].

Por su parte, el Registro de Población es la base de datos del Estado para almacenar información básica de cada persona que vive en Estonia. Contiene su nombre, código de identificación, fecha de nacimiento, lugar de residencia, y datos estadísticos como nacionalidad, idioma nativo, educación y profesión, y cada ciudadano puede corregir sus datos en cualquier momento a través del registro de población. El Registro de Población está conectado a otros sistemas a través de X-ROAD, y una variedad de sistemas estatales dependen de sus datos para prestar servicios públicos[106].

Otro elemento a destacar de la estrategia de transformación digital de Estonia es el cómputo en la nube, en donde las instituciones estonianas están migrando sus sistemas a la solución "*Government Cloud*", con base en estándares de seguridad nacionales, en donde se garantiza: (i) cumplimiento de los requisitos de seguridad y calidad; (ii) los datos personales se almacenen y manejan con confidencialidad e integridad; (iii) para la seguridad física de la nube, el gobierno de Estonia implementó el almacenamiento de la información en distintas ubicaciones fuera de la ciudad para permitir la gestión distribuida de la información; (iv) colaboración con instituciones privadas para mantener la seguridad de la nube. Sin duda, la identidad digital, interoperabilidad y seguridad de las transacciones han sido elementos clave para el desarrollo digital de Estonia.

[105] Ibidem.
[106] Gobierno de Estonia, "Population Register", Estonia, 2020, Disponible en: https://www.siseministeerium.ee/en/population-register (Fecha de consulta: 23 de junio de 2020).

2.2.7 Dinamarca

La estrategia digital de Dinamarca 2016-2020[107] se divide en tres grandes objetivos: 1) las soluciones digitales deben ser fáciles de usar, rápida y asegurar la calidad; 2) el gobierno debe proporcionar buenas condiciones de crecimiento, y 3) la seguridad y la confianza deben estar enfocadas en todo momento. Estos tres objetivos agrupan treinta y tres acciones. En el primer objetivo destacan acciones como: gestión de la información; seguridad en todas las autoridades; negocio automático; marco legal claro para administración electrónica; compartición de datos; habilidades digitales para niños y gente joven; datos comunes sobre topografía, clima y agua; mejores datos sobre discapacitados y adultos marginados.

En el segundo objetivo se contemplan acciones como procedimientos de licitación digital y adquisiciones; computación en la nube en el sector público; infraestructura para posicionamiento y datos de navegación; intercambio de datos sobre infraestructura subterránea; arquitectura general de TI para datos sobre residuos sector. Y para el tercer objetivo cuentan con acciones relacionadas con estándares comunes para seguridad; intercambio de información**; Identidad digital** y derechos; infraestructura común; información y ayuda para ciudadanos y empresas.

Para la interoperabilidad y cohesión de servicios digitales, Dinamarca contempla que el vínculo entre la identidad digital y la firma electrónica, con la finalidad de llevar a cabo transacciones electrónicas *seguras*. Así, una vez más observamos que **la identidad digital, la firma electrónica** y la **interoperabilidad** de servicios son pieza clave a considerar en las estrategias digitales de los países con un mayor índice de servicios en línea.

[107] Gobierno de Dinamarca, “Digital Strategy 2016-2020” Dinamarca, 2016, Disponible en: https://en.digst.dk/media/14144/ds_spread_uk_web.pdf (Fecha de consulta: 23 de junio de 2020).

2.2.8 Australia

Australia cuenta con la *Estrategia de Transformación Digital y un panel de control*[108], liderada por la Agenda Transformación Digital. Dicha estrategia tiene tres principios: 1) Un gobierno con el que es fácil tratar; 2) Gobierno informado para el ciudadano; y 3) gobierno apto para la era digital. En el primer principio contempla como líneas de acción desarrollar servicios intuitivos y convenientes para los ciudadanos; servicios integrados; y contar con una **identidad digital** para el acceso fácil y seguro a los servicios digitales.

En el segundo principio prevé líneas de acción relacionadas con servicios inteligentes; generar mayores capacidades para desarrollar mejores servicios; fortalecer la confianza y la transparencia. Y en el tercer principio se contempla ampliar la capacidad digital del gobierno; desarrollar infraestructura moderna, y proporcionar responsabilidad de los servicios en línea[109].

2.2.9 Nueva Zelanda

Nueva Zelanda cuenta con una *Estrategia para un Servicio Público Digital* la cual establece la dirección para modernizar y transformar el servicio público colocando a los ciudadanos y a las empresas en el centro de los servicios gubernamentales[110]. La estrategia de Nueva Zelanda cuenta con cinco pilares. El primero sobre integración de servicios para los ciudadanos y negocios, en el que se desarrollan acciones relacionadas con la integración de servicios digitales; un plan de inclusión digital; y servicios para las empresas como conexión de negocios, innovación y empleo. El segundo sobre liderazgo, personas y cultura, en donde se llevan a cabo acciones como la gobernanza, asociación e implementación de la estrategia digital;

---

[108] Gobierno de Australia, "Digital Transformation Strategy", Australia, 2018, Disponible en: https://dta-www-drupal-20180130215411153400000001.s3.ap-southeast-2.amazonaws.com/s3fs-public/files/digital-transformation-strategy/digital-transformation-strategy.pdf (Fecha de consulta: 24 de junio de 2020).

[109] Ibídem, p. 13.

[110] Gobierno de Nueva Zelanda, "Strategy for a Digital Public Service", Nueva Zelanda, 2020, Disponible en: https://www.digital.govt.nz/assets/Digital-government/Strategy/Strategy-for-a-Digital-Public-Service.pdf (Fecha de consulta: 24 de junio de 2020).

generar talento digital en la administración pública; determinación de necesidades futuras de capacidad digital con el Ministerio de Educación.

El tercer pilar se refiere a contar con los cimientos para el desarrollo digital. Este pilar es relevante, ya que prevé como base de la transformación digital acciones vinculadas con la arquitectura digital para el gobierno, como definir una estrategia de transición para el retiro de sistemas obsoletos; producir un marco de confianza y de nuevos enfoques de identidad digital; comenzar la interoperabilidad del gobierno; asegurar la privacidad, la protección de datos personales y la ciberseguridad; definir prácticas de ciberseguridad; establecer un programa de derechos y ética digital; desarrollar y coordinar la política del cómputo en la nube e IA, y definir un marco normativo de gobierno digital.

El cuarto pilar se refiere a la inversión en TIC, en donde se desarrollan acciones como la administración de datos del gobierno; desarrollar una estrategia de inversión digital y TIC y un plan de largo plazo; definir proceso de inversión para datos digitales; brindas asesoría de inversión a sus agencias públicas; generar modelos de adquisición de TIC; y revisar los modelos de gestión de riesgos. Por último, el quinto pilar se centra en nuevas formas de trabajar, en donde se contemplan acciones como desarrollar estándares digitales como *web* y de arquitectura; definir procesos comerciales comunes para el *back* office, generar innovación digital; administración del fondo de innovación para el desarrollo de capacidades gubernamentales, desarrollar y liderar un programa formal de tecnología emergente, que contemple inteligencia artificia, entre otras tecnologías.

2.2.10 Estados Unidos

La estrategia digital de los Estados Unidos está dirigida a brindar mejores servicios digitales al pueblo estadounidense. Contempla varias iniciativas relacionadas con la racionalización de la prestación de servicios y la mejora del servicio al cliente, así como la entrega de un gobierno eficiente, efectivo y responsable[111]. Entre sus

[111] Gobierno de Estados Unidos, “Digital Government Strategy”, Estados Unidos, 2012, Disponible en: https://www.state.gov/digital-government-strategy/#:~:text=A%20comprehensive%20Digital%20Government%20Strategy,launched%20on%2

componentes se encuentra una *política de datos abiertos*, con la que se busca aumentar la eficiencia operativa a costos reducidos, mejorar los servicios, salvaguardar la información personal, y aumentar el acceso público a la información del gobierno. Para ello, con la política de datos abiertos se generan metadatos disponibles al público que fomentan la transparencia, participación y colaboración de la ciudadanía[112] y además genera una serie de estándares, códigos de apoyo, herramientas y estudios de caso en la generación de los metadatos[113].

Otro componente de la estrategia digital de Estados Unidos es lograr eficiencia, transparencia e innovación a través de software reutilizable y de código abierto, con lo que cuenta con una Política Federal de Código Fuente[114]. El código abierto está disponible para otras agencias gubernamentales y analistas informáticos de todo el mundo. Con base en estos componentes, la estrategia digital de Estados Unidos contempla acciones relacionadas con: asegurar que todos los nuevos sistemas de TIC sigan la política de datos abiertos, contenidos y operación *web*; identificar los principales servicios que consumen los ciudadanos; establecer una gobernanza de toda la agencia gubernamental para desarrollar e integrar servicios digitales; desarrollar un inventario de todos los dispositivos móviles y servicio inalámbricas de las instituciones gubernamentales; evaluar las compras gubernamentales; asegurar que todos los servicios digitales cuenten con la experiencia usuario y pautas de mejora.

Este último aspecto, además de los datos abiertos, es muy relevante en Estados Unidos. A través de la *21st Century Integrated Digital Experience Act*[115], se establece una serie de acciones para mejorar los servicios digitales. La primera de ellas tiene por objeto la modernización de los sitios *web*, en donde se contemplan

0May%2023%2C%202012.&text=U.S.%20Government%20agencies%20are%20asked,services%20to%20the%20American%20people.%E2%80%9D (Fecha de consulta: 25 de junio de 2020).

[112] Gobierno de Estados Unidos, "Open Government Initiative", Estados Unidos, 2020, Disponible en: https://www.state.gov/open-government-initiative/ (Fecha de consulta: 25 de junio de 2020).

[113] Gobierno de Estados Unidos, "Project Open Data", Estados Unidos, 2020, Disponible en: https://project-open-data.cio.gov/ (Fecha de consulta: 25 de junio de 2020).

[114] Gobierno de Estados Unidos, "Open Source Software", Estados Unidos, 2016, Disponible en: https://sourcecode.cio.gov/OSS/. (Fecha de consulta: 25 de junio de 2020).

[115] Congreso de Estados Unidos, "21st Century Integrated Digital Experience Act, 05 de octubre de 2018", Estados Unidos, Disponible en: https://www.congress.gov/bill/115th-congress/house-bill/5759/text (Fecha de consulta: 25 de junio de 2020).

acciones como la accesibilidad *web* para que personas con discapacidades tenga acceso a un sitio con apariencia consistente, que no se duplique con ningún otro, cuente con estándares de seguridad, se funcional y utilizable en móviles.

El segundo se refiere a la digitalización de servicios y formularios del gobierno, en donde prevé acciones como la identificación de servicios públicos no digitales, en papel o presenciales; incluir una solicitud de presupuesto para la digitalización de servicios; los servicios públicos deben estar disponibles digitalmente en un periodo de dos años; los servicios que no puedan digitalizarse se deberá justificar su permanencia en papel; además, las agencias deberán mantener la disponibilidad de los servicios digitales de forma presencial, para garantizar que las personas que no puedan utilizar los servicios digitales no se priven ni se les impida acceder a servicios públicos; cada agencia estatal debe generar un plan para acelerar el uso de normas de **firmas electrónicas** con base en la *Electronic Signatures In Global And National Commerce Act*[116]; mediante ésta se permite identificar a una persona en medios digitales.

El tercer elemento de la estrategia digital es la experiencia usuario de servicios digitales, en donde se prevén acciones como la generación de programas externos para conocer la experiencia el usuario; contar con una estrategia de prestación de servicios digitales y presentar recomendaciones al jefe ejecutivo de la agencia gubernamental; utilizar datos cualitativos y cuantitativos relacionados con la satisfacción de los clientes; identificar las áreas de mejora; y coordinar con otras agencias la estandarización de servicios digitales.

Un cuarto objetivo es la normalización, mediante el cual se prevé el diseño e implementación de estándares gubernamentales; coordinar la implementación de la "*21st Century Integrated Digital Experience Act"*; poner a disposición de la Administración de Servicios Generales de Estados Unidos un Programa Federal de Suministros de los sistemas y servicios digitales; interoperar entre agencias gubernamentales; cumplir con estándares de la industria; adherirse a las mejores prácticas para el diseño, accesibilidad y seguridad de la información.

[116] Public Law, "Electronic Signatures In Global And National Commerce Act", Estados Unidos, 2000, Disponible en: https://www.govinfo.gov/content/pkg/PLAW-106publ229/pdf/PLAW-106publ229.pdf (Fecha de consulta: 25 de junio de 2020).

2.2.11 Uruguay

Después de Estados Unidos, Uruguay ocupa el segundo lugar en América respecto al EDGI. Comparte la segunda posición con Canadá en el índice de Servicios Digitales. La Agenda Digital de Uruguay[117] se basa en una transformación digital equitativa, inclusiva y sostenible. Cuenta con cuatro pilares: 1) políticas sociales e inclusión; 2) desarrollo económico sustentable; 3) gestión de gobierno, y 4) gobernanza para la sociedad de la información.

La Agenda Digital de Uruguay cuenta con nueve objetivos que describen en su conjunto 46 acciones. El primer objetivo es desarrollar habilidades digitales inclusivas, en donde se incluyen acciones relacionadas con Incluir digitalmente al 100% de los jubilados de bajos ingresos mediante la entrega de tabletas con conexión a Internet y capacitación para su uso; desarrollar competencias digitales alcanzando a 60 mil personas, y crear el Centro Nacional de Investigación en Informática[118]. El segundo objetivo es utilizar la innovación para el bienestar, en donde se contemplan acciones como Integrar la información de las trayectorias educativas de los estudiantes en todos los niveles de la educación para la efectiva inserción, apoyo, retención y seguimiento; alcanzar al 100% de los prestadores integrales de salud con la Historia Clínica Electrónica Nacional incorporada en al menos 3 áreas (emergencia, ambulatorio, internación, quirúrgico u otras), el 100% de los servicios oncológicos públicos y privados con historia clínica electrónica oncológica implementada y disponer de los instrumentos normativos y técnicos que habiliten la prescripción médica electrónica; integrar la información laboral actualizada y en tiempo real de los trabajadores[119].

El tercer objetivo se refiere a realizar inversión estratégica en infraestructura, con acciones como llegar al 65% de los hogares del país con cobertura de conexión a Internet por fibra óptica (FTTH), el 90% de los hogares conectados a Internet por

---

[117] AGESIC, “Agenda Digital del Uruguay, Uruguay, 2019, Disponible en: https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/politicas-y-gestion/programas/agenda-digital-del-uruguay (Fecha de consulta el 25 de junio de 2020).
[118] Ídem.
[119] Ídem.

banda ancha, y el 65% de la cobertura de LTE en el territorio nacional; optimizar el uso del espectro radioeléctrico nacional y disponer de nuevas bandas con el fin de facilitar el desarrollo de los servicios de telecomunicaciones; desarrollar infraestructura de conectividad y plataformas de gestión que faciliten el despliegue de aplicaciones basadas en internet de las cosas[120].

El cuarto objetivo contempla crear una economía digital e innovación para la competitividad, con acciones relacionada con alcanzar el 90% de pequeñas, medianas y grandes empresas conectadas a Internet por banda ancha, manteniendo un precio de conexión competitivo; apoyar el desarrollo de 50 proyectos innovadores orientados a la solución de problemas de competitividad en empresas de todos los sectores; fortalecer la oferta nacional en comercio electrónico y diseñar una estrategia nacional para la digitalización de las pequeñas y medianas empresas (PYMES), y profundizar el proceso de inclusión financiera[121].

El quinto objetivo se refiera a la gestión con inteligencia de la información ambiental y de emergencias, para lo cual se prevé desarrollar la Infraestructura Nacional de Datos para la Gestión Ambiental; mapear los niveles de radiaciones no ionizantes de estaciones radioeléctricas; incrementar las capacidades de gestión de emergencias y reducción del riesgo de desastres cuidando a las personas[122].

El sexto objetivo se refiere a la promoción del gobierno de cercanía, para lo cual se incluye disponer del 100% de los trámites de la Administración Central para ser iniciados, seguidos y completados en línea; acercar a la población los servicios e información que brinda la Administración Central a través de la implementación de un nuevo Portal integrado “Gub.uy”; profundizar la cultura del gobierno abierto; fortalecer la cultura de la transparencia; alcanzar el 70% de los usuarios de Internet haciendo uso de servicios en línea del gobierno[123].

El objetivo siete se refiere a fortalecer el gobierno integrado e inteligente, con acciones relacionadas con el desarrollo de la arquitectura de datos y de sistemas de información de la Administración Central y habilitar los **registros federados de**

[120] Ídem.
[121] Ídem.
[122] Ídem.
[123] Ídem.

personas, empresas, servicios públicos y direcciones como metadatos en la plataforma de interoperabilidad; desplegar la infraestructura de datos espaciales con al menos 3 niveles de capas de información geográfica como herramienta que sustente la toma de decisiones a nivel territorial; realizar el monitoreo de la gestión estratégica, la coordinación en la implementación de las políticas públicas y la comunicación de resultados del gobierno con base en soluciones de analítica inteligente; contar en todos los ministerios con la aplicación de modelos con grandes volúmenes de datos, para el análisis descriptivo y predictivo de fenómenos que afecten a la comunidad y el diseño de servicios proactivos, y contar con una estrategia para IA en la Administración Pública[124].

El objetivo ocho se refiere a ofrecer confianza y seguridad en el uso de las tecnologías digitales, con acciones como adecuar y actualizar el marco normativo en protección de datos personales, cibercrimen, e-residuos y protección del e-consumidor; crear el Centro Nacional de Operación de Ciberseguridad (SOC Nac) con la participación público-privada; alcanzar el 30% de la población con mecanismos de identidad electrónica (cédula, móvil, etc.), haciendo uso de ésta para la autenticación y la firma digital de documentos; llegar al 100% de organismos de la Administración Central cumpliendo los requerimientos mínimos de los modelos de madurez de ciberseguridad y de continuidad operativa; fortalecer el desarrollo digital del país en el marco de su política exterior, mediante la designación de un representante digital[125].

Por último, el objetivo nueve se refiere a la producción de estadísticas nacionales relacionadas con las TIC, con acciones como mejorar la capacidad local para la producción de estadísticas nacionales de sociedad de la información, en concordancia con los estándares internacionales conformando un ámbito técnico de diálogo y de colaboración entre las instituciones involucrada, e incorporar una perspectiva sobre diversidad en el tratamiento de la información estadística del sector TIC con el fin de proporcionar datos oportunos en el diseño de políticas públicas equitativas[126].

[124] Ídem.
[125] Ídem.
[126] Ídem.

2.2.12 Canadá

Canadá cuenta con el Plan Estratégico de Gestión de la Información y Tecnología de la Información 2017 a 2021[127], el cual se basa en seis principios rectores: 1) diseño centrado en el cliente; 2) datos abiertos; 3) empresa primero; 4) seguridad; 5) servicios en la nube; 6) habilitar un lugar moderno de trabajo. Adicionalmente, cuenta con cuatro objetivos estratégicos *servicio* -integrados, accesibles y centrados en los ciudadanos-; *valor* -inversiones inteligentes de alto valor, rentables y reutilizables, fortalecer el valor de los datos, su gobernanza y responsabilidades-; *seguridad* –protección de la información y los datos, programas y servicios confiables, y ciberseguridad-; *agilidad* -fuerza laboral ágil, conectada y de alto rendimiento, alfabetización digital-.

Además de los principios rectores, los objetivos estratégicos, el plan digital de Canadá cuenta con cuatro acciones estratégicas. La primera sobre *servicios* que incluye la gestión de Servicios, el cómputo en la nube, la modernización tecnológica; la información e intercambio de datos a través de la interoperabilidad. La segunda sobre *gestión* que contempla la gobernanza de la estrategia; aprovechar economías de escala; ser sostenibles; fortalecer el papel de los directores departamental; pensar en una cultura digital; desarrollar asociaciones empresariales; desarrollar prácticas y procesos de gestión de TIC; establecer una junta asesora digital; introducir principios de gobierno digital; transformar la gestión financiera; documentar los roles y responsabilidad de seguridad de TIC; gobernanza de los datos; estandarizar metadatos; gestión de la información; innovación; sostenibilidad de la infraestructura de las TIC; racionalizar inversiones.

La tercera acción estratégica es seguridad, en donde se prevé implementar un enfoque empresarial para la gestión de vulnerabilidades y parches; gestionar y controlar los privilegios administrativos; soluciones y servicios confiables; proteger las transacciones web hacia y desde sitios web externos; implementar una identidad digital confiable para las personas que acceden a redes y sistemas

[127] Gobierno de Canadá, “Plan Estratégico del Gobierno de Canadá para la Gestión de la Información y la Tecnología de la Información 2017 a 2021”, Canadá, 2016, Disponible en: https://www.canada.ca/en/treasury-board-secretariat/services/information-technology/strategic-plan-2017-2021.html (Fecha de consulta: 26 de junio de 2020).

gubernamentales internos; asegure el perímetro de red del gobierno; implementar perfiles de seguridad de punto final; implemente un servicio mejorado de autenticación cibernética; implementar un servicio de comunicación seguro para la información clasificada; implemente la prevención de pérdida de datos empresariales; permitir una comprensión integral de los dispositivos de punto final; mejorar el conocimiento de la amenaza de ciberseguridad empresarial y el entorno de riesgo.

Por último, la cuarta acción estratégica es sobre *comunidad*, el cual se centra en crear una fuerza laborar de alto rendimiento y garantizar a los empleados del servicio público tengan un lugar de trabajo moderno, desarrollo profesional y las herramientas que necesitan para hacer su trabajo. Así, se busca permitir el desarrollo profesional; mejorar la diversidad del ligar de trabajo; modernizar los dispositivos tecnológicos; apoyar una fuerza laboral móvil; proporcionar acceso wifi; proporcionar videoconferencia; mejorar la colaboración digital; gobierno abierto; modernizar la profesión de gestión de la información y datos; desarrollar capacidades en gestión de información y datos; fortalecer el liderazgo; promover la alfabetización digital y la colaboración.

2.2.13 Argentina

Argentina cuenta con la Agenda Digital[128], la cual se estructura en cinco ejes estratégicos. El primero sobre marco normativo contempla acciones como elaborar un modelo de comunicaciones convergentes; establecer marcos legales para la incorporación de nuevas tecnologías; asegurar la protección de datos personales; asegurar la protección a los consumidores en el comercio electrónico; fortalecer el marco normativo para la protección del ciberespacio y de la información; impulsar la adopción de estándares y buenas prácticas internacionales en materia digital; participar de foros internacionales relacionados con Internet y la Agenda Digital; impulsar el desarrollo del comercio electrónico.

[128] Gobierno de Argentina, “Agenda Digital”, Argentina, 2018, Disponible en: http://servicios.infoleg.gob.ar/infolegInternet/anexos/315000-319999/318677/res138.pdf (Fecha de consulta: 27 de junio de 2020.

El segundo sobre *infraestructura* contempla acciones como articular el despliegue para lograr una conectividad integral; completar la ejecución del Plan Federal de Internet; fomentar la inversión público-privada para la expansión y mejora de los servicios TIC; potenciar la aplicación del servicio universal para posibilitar el acceso de todos los habitantes de nuestro país a los servicios TIC; integrar zonas remotas; propiciar el tendido de fibra óptica en obra pública; elaborar un plan de largo plazo para la asignación del espectro radioeléctrico a fin de alcanzar una mejor calidad de los servicios de comunicaciones; densificar los sitios para celulares; propiciar la instalación de centros de datos; fomentar el despliegue para la salida internacional de Internet; brindar conectividad para escuelas rurales; aportar soluciones estructurales para la gestión digital de municipios; desarrollar un plan de conectividad para los centros de salud; extender la conectividad para zonas agrícolas; gestionar la infraestructura para monitoreo y atención de incidentes a nivel nacional; desarrollar un ecosistema de ciberseguridad; elaborar una plataforma de seguimiento del desarrollo de las redes de comunicación públicas y privadas; establecer una continuidad operativa ante eventos catastróficos[129].

El tercer eje estratégico se refiere a *educación e inclusión digital* en donde se desarrollan acciones como brindar apoyo a quienes no pueden hacer un uso productivo de Internet; fomentar las sinergias público-privadas en los planes de capacitación digital; reducir la brecha digital, teniendo en especial consideración la brecha de género; fomentar la inclusión de competencias digitales en los planes de estudio; convertir las escuelas en nodos tecnológicos; desarrollar planes de capacitación docente en competencias digitales; integrar habilidades blandas con las tecnológicas aplicadas en los planes educativos; generar herramientas para la inserción o reinserción en el mercado laboral; diseñar políticas para los trabajadores del futuro; promover la interacción entre universidades y empresas del sector TIC[130].

El cuarto eje se refiere a la *economía digital* y se contempla potenciar la producción y el desarrollo de *software* y de contenidos audiovisuales; promover la exportación de servicios del conocimiento; fomentar el desarrollo de servicios

[129] Ídem.
[130] Ídem.

digitales para la industria financiera; digitalizar las PYMES; implementar el uso de certificados de origen digital para el comercio entre países; promover el desarrollo del comercio electrónico; impulsar los negocios basados en datos; y, servicios financieros digitales[131].

El quinto eje se refiere a *gobierno digital* con líneas de acción relacionadas con servicios públicos en línea; ventanilla única del ciudadano; fomentar el uso identidad digital; generalizar el uso de la firma digital; propiciar un gobierno inteligente donde las decisiones se basen en datos; promover que las instituciones públicas soliciten la información sólo una vez a ciudadanos, organizaciones y empresas; fomentar un Estado interoperable; promover plataformas unificadas para todo el Estado Nacional; gobierno colaborativo y participativo; capacitaciones para los empleados públicos en competencias digitales; soluciones digitales para municipios; e incorporación de infraestructura IT en municipios[132].

2.2.14 Chile

Chile cuenta con una Estrategia de Transformación Digital del Estado[133], la cual cuenta con principios estratégicos, principios operacionales y líneas de acción. Como principios estratégicos se contempla los siguientes:

> *"1) Centrado en las personas: analizar siempre las necesidades de las personas y actores involucrados, levantando información, testeando y probando en terreno, para asegurar utilidad y usabilidad de los servicios; 2) Estado digital por diseño: Integrar el uso de las tecnologías digitales en todo el ciclo de políticas públicas, con el objetivo de que todo nuevo producto del Estado sea digital desde su origen, y 3) Abierto y colaborativo por defecto: las herramientas para digitalización y transformación que sean desarrolladas por y/o para el Estado deberán ser de código abierto, uso gratuito y los sistemas deben generar "datos abiertos por defecto" en estándares abiertos y disponibles para su reutilización, 4) Gobierno basado en*

[131] Ídem.
[132] Ídem.
[133] Gobierno de Chile, "Estrategia de Transformación Digital del Estado", Chile, 2019, Disponible en: https://digital.gob.cl/doc/estrategia_de_transformacion_digital_2019_.pdf (Fecha de consulta: 29 de junio de 2020).

datos: políticas públicas basadas en evidencias, uso intensivo de datos e integración con investigación cualitativa para el diseño de servicios de calidad, y 5). Estado proactivo: explorar de manera permanente nuevas soluciones y desarrollo de tecnologías emergentes (…)"[134].

Como principios operacionales, Chile contempla los siguientes:

"(…) 1) Infraestructura de datos para el Estado: se avanzará hacia estándares de infraestructura y arquitecturas de datos comunes en el Estado, que faciliten la integración de servicios, facilite la interoperabilidad, considere el uso de tecnología en la nube, flexible y escalable, sin dejar de lado la ciberseguridad y estándares para entregar garantías de seguridad y privacidad de los datos de los ciudadanos y empresas; 2) Integración de los servicios del Estado, lo que incluye principalmente la interoperabilidad con estándares abiertos y seguros; 3) Ciberseguridad, protección de datos y privacidad; 4) estandarización y digitalización de procesos transversales de administración institucional y gestión documental; 5) Compras inteligentes en TI, y 6) Promoción y atracción de talento para la transformación digital (…)[135].

Por último, agrupa seis tipos de líneas de acción. La primera **sobre identidad digital** que contempla acciones como:

"(…) autenticación única a través de la plataforma del Estado con base en el Registro Único Nacional; que las personas puedan gestionar su identidad con base en la autenticación única; contar con un buzón de notificaciones del Estado para facilitar un trámite o la entrega de un beneficio; uso de la firma electrónica avanzada a través de la nube. En esta línea de acción, Chile destaca que un modelo chileno es uno de los puntos basales de una Estrategia de Transformación Digital que ponga al ciudadano al centro (…)"[136].

134 Ídem.
135 Ídem
136 Ídem.

La segunda línea de acción sobre un *Estado CeroFilas,* contempla:

"(…) un registro nacional de trámites que permita identificar oportunidades de simplificación y eliminación de trámites que nos generen valor a sus usuarios, así como establecer el universo actual de trámites digitalizables para alcanzar el 80% de los trámites disponibles en línea para 2020. Para ello, se contemplan acciones como plataformas compartidas, fomentar la interoperabilidad, estándares de diseño de servicios (…)"[137].

La tercera línea de acción se refiere a *Estado CeroPapel* en donde se busca:

"(…) establecer una oficina de partes virtual, utilizando la firma electrónica, contar con un expediente virtual con base en sistema de gestión de la información, contar con procesos transversales como compras públicas para que en el 2020 Chile es un gobierno cero papeles (…)"[138].

La cuarta línea de acción se denomina *Estado basado en datos* y contempla acciones como:

"(…) definir una Política Nacional de Datos e IA, fomentar el uso de datos; potenciar la optimización de políticas públicas y la automatización de procesos; empoderar a la ciudadanía a través de la disponibilización de información pública y abierta. La línea de acción cinco se refiere a un Estado protegido ante la amenaza de ciberseguridad que contempla acciones como asumir la gestión de riesgos a la ciberseguridad, orientadas a la protección preventiva de infraestructuras tecnológicas y de datos; detección de anomalías e incidentes; respuesta a incidentes; elaboración de una ley de ciberseguridad; mejoramiento y creación de decretos de seguridad de la información, el fortalecimiento del equipo de respuesta o CSIRT ante incidentes de seguridad; modelo de análisis permanente de vulnerabilidades en plataformas críticas; coordinador de ciberseguridad (…)"[139].

[137] Ídem.
[138] Ídem.
[139] Ídem.

Por último, la línea de acción seis se refiere a *un Estado que mira el futuro*, que incluye acciones como:

> *"(…) economía digital; generar instancias de colaboración público privadas para explotar nuevas tecnologías emergentes en el sector público; programa economía del futuro en donde se analizan tecnologías como blockchain, big data, IA y cómputo en la nube. Integrar tecnología en las aulas a través del Ministerio de Educación; y desarrollo de pilotos, público-privados, en colaboración con la División de Gobierno Digital, en tecnologías emergentes como Internet de las Cosas, IA, cómputo en la nube, realidad virtual aumentada*, para la mejora de la gestión y entrega de servicios del Estado *(…)"*[140].

Adicional en su Estrategia de Transformación Digital, Chile cuenta con la *Ley 21280 sobre Transformación Digital del Estado*[141], en donde se regula, entre otros aspectos, lo siguiente:

> *"(i) todo procedimiento administrativo deberá expresarse a través de medios electrónicos; (ii) el procedimiento administrativo y los actos administrativos a los cuales da origen se expresarán por escrito a través de medios electrónicos; (iii) toda comunicación entre órganos de la administración pública se realizará por medios electrónicos; (iv) establece los principios de los procedimientos administrativos por medios electrónicos como neutralidad tecnológica, actualización, equivalencia funcional, fidelidad, interoperabilidad y cooperación; (v) los expedientes electrónicos contendrán un registro actualizado de todas las actuaciones del procedimiento; (vi) los órganos de la Administración estarán obligados a disponer y utilizar adecuadamente plataformas electrónicas para efectos de llevar expedientes electrónicos, los que deberán cumplir con estándares de seguridad, interoperabilidad, interconexión y ciberseguridad; (vii) los documentos electrónicos y los actos de la administración pública deberán cumplir con la ley sobre documentos*

[140] Ídem.
[141] Biblioteca del Congreso Nacional de Chile, "Ley de Transformación Digital del Estado", Chile, 11 de noviembre de 2019, Disponible en: https://www.leychile.cl/Navegar?idNorma=1138479 (Fecha de consulta: 30 de junio de 2020).

electrónicos, firma electrónica y servicios de certificación[142]; (viii) el poder de representación podrá constar en documento suscrito mediante firma electrónica simple o avanzada, aceptándose también la escritura pública o documento privado suscrito ante notario; (ix) las notificaciones se practicarán por medios electrónicos con base en la información contenida en un registro único dependiente del Servicio de Registro Civil e Identificación, sobre el cual se configurarán domicilios digitales únicos, y (x) se definen los pases del archivo digital.

Como observamos, Chile cuenta con una estrategia de transformación digital de forma integral. Por un lado, se enfoca en la modernización del Estado a través de políticas públicas y, por el otro, prioriza la regulación de procedimientos electrónicos en el marco de la Ley de Transformación Digital. Entre las acciones que podemos destacar son la relevancia que otorgan a la identidad digital a través de su registro civil en colaboración con la División de Gobierno Digital para generar una clave única que permite a las personas acceder a servicio digitales del Estado e, incluso, puede ser utilizada en el poder judicial. Otros temas para destacar en Chile son el diseño de servicio centrados en los usuarios, el uso de datos, la ciberseguridad y la estandarización de procesos. No obstante, para poder habilitar los servicios digitales, Chile establece como su primera línea de acción la identidad digital.

2.2.15 Brasil

En la Estrategia Digital de Brasil[143] se contemplan seis objetivos. El primero sobre un gobierno centrado en las personas, con acciones relacionadas con transformar todas la etapas y servicios públicos para 2022; simplificar y agilizar la apertura de empresas en un día; mejorar la satisfacción de los usuarios; y establecer un estándar de calidad para servicios públicos.

---

[142] Biblioteca del Congreso Nacional de Chile, “Ley sobre documentos electrónicos, firma electrónica y servicios de certificación”, Chile, 2002, Disponible en: https://www.leychile.cl/Navegar?idNorma=196640 (Fecha de consulta: 30 de junio de 2020).

[143] Gobierno de Brasil, “DECRETO Nº 10.332, DE 28 DE ABRIL DE 2020”, Brasil, 2020, Disponible en: https://www.redgealc.org/site/assets/files/10577/decreto_n_10_332-_de_28_de_abril_de_2020.pdf (Fecha de consulta: 30 de junio de 2020).

El segundo objetivo se refiere a un *gobierno confiable* que incluye acciones como cumplimiento de la ley de protección de datos personales; plataforma para gestionar a privacidad y el uso de datos personales de los ciudadanos; garantizar que el 99% de las plataformas gubernamentales sean compartidas; monitorear el 80% de los riesgos de seguridad cibernética; definir un estándar mínimo se seguridad cibernética; proporcionar 2 millones de validaciones biométricas mensuales para servicios públicos federales; hacer que la **identidad digital** esté disponible para los ciudadanos; poner a disposición de los ciudadanos mecanismos **de firma digital**; fomentar el uso de firmas digitales; suscripción de códigos abiertos e interoperables.

El tercer objetivo se refiere a un *gobierno integrado* con acciones relacionadas con integrar a todos los Estados a la Red Gov.br para 2022; implementar métodos de pago digital; expandir el uso del portal único gov.br; proporcionar la plataforma de buzón digital del ciudadano; interoperar los sistemas del Gobierno Federal; aumentar el número de atributos en el registro base de ciudadanos; establecer cinco registros de referencia básicos para la interoperabilidad del gobierno federal; establecer un bus de interoperabilidad para los sistemas de gobierno federal para la compartición de datos.

El cuarto objetivo se refiere a contar con un *gobierno transparente y abierto*, con acciones vinculadas a la integración de los portales de transparencia, datos abiertos y defensor del pueblo en el portal único; aumentar las bases de datos abiertos; mejorar la calidad de los datos abiertos; establecer alianzas para construir aplicaciones de control social a través de *datathons* o *hackathons*; mejorar los medios de participación social y proporcionar una nueva plataforma para la participación; poner 20 nuevo servicios interoperables a disposición de empresas y organizaciones; establecer alianzas con la industria de las TIC, la comunicación y la identidad digital con reconocida participación colaborativa.

El quinto objetivo es contar con un *gobierno inteligente* a través de acciones como producir 40 nuevos paneles de evaluación y monitoreo de políticas públicas; catalogar al menos 300 bases de datos principales del Gobierno Federal; poner a disposición el mapa de empresas en Brasil; desarrollo seis proyectos de

investigación, desarrollo e innovación con socios del gobierno federal, instituciones de educación superior y privado. Implementar recursos de IA; disponer de conjuntos de datos a través de soluciones *blockchain*; crear una red interoperable de *blockchain*; laboratorio de tecnología emergentes; servicios públicos personalizados al perfil de los usuarios; y notificación de servicios digitales.

Por último, en el sexto objetivo, sobre *gobierno eficiente*, se contemplan acciones como realizar compras comunes de TIC; intercambiar soluciones de software de estructuración; optimizar la infraestructura de centros de datos gubernamentales; migrar servicios a la nube; capacitar a 10 mil equipos del gobierno federal; cultura digital; y expandir la fuerza laboral dedicada a la transformación digital de la administración pública.

2.2.16 Principales pilares de las estrategias digitales en el contexto internacional

Como observamos, son diversos los elementos que los países mejor posicionados en el EDGI consideran en sus estrategias digitales. Sin embargo, podemos observar que todos ellos coinciden en los siguientes: seguridad; datos; servicios y experiencia usuario; servicios digitales; economía digital; infraestructura; innovación; interoperabilidad; habilidades digitales; identidad; firma electrónica; nube; estándares; inclusión digital, y uso de tecnologías emergentes, tal como observamos en la siguiente imagen:

Figura 1. *Agendas Digitales Internacional. Nube de Palabras*
Fuente: Elaboración propia.

En el análisis algorítmico de las agendas digitales a través de las palabras más recurrente en el mismo, se observó que el top 10 de palabras más recurrente en las agendas son: datos, servicios, seguridad, información, gobierno, ciberseguridad, infraestructura, digitales, estándares y gestión. La gestión de los datos y la ciberseguridad son dos de las principales líneas de trabajo en las agendas digitales a nivel internacional. Además, el despliegue de infraestructura, la generación de estándares técnicos y el uso masivo e intercambio de información son factores que los países consideran para prestar servicios digitales seguros y centrados en las personas.

En los temas de identidad digital y firma electrónica debemos destacar que, si bien no figuran en el top 10 de palabras más utilizadas, son considerados

elementos base de la transformación digital que requieren no sólo del despliegue de infraestructura y estándares técnicos, sino también de un marco normativo que otorgue certeza jurídica en las transacciones digitales. Países como Chile, Nueva Zelanda, Estonia, Singapur, Corea del Sur, Argentina o Uruguay, consideran a la identidad digital y la firma electrónica como pilares clave para su transformación digital. En Estonia, por ejemplo, la identidad digital ha sido clave incluso para llegar a una residencia digital que ya interopera con otros países de la Unión Europea.

En resumen, podemos observar que, para abordar la transformación digital en la cuarta revolución industrial, existen ciertos elementos comunes que los países adoptan para obtener el mejor beneficio de la tecnología y reducir sus riesgos. Estos elementos los describimos en seguida con base en los tres subíndices estructurados en el EDGI:

- *Infraestructura*. El despliegue de infraestructura es un habilitador para reducir la brecha digital en zonas que aún no cuenta con conexión a Internet. En temas de infraestructura, además se consideran aspectos sobre interoperabilidad y adquisición de tecnologías como el cómputo en la nube.
- *Habilidades digitales.* Crear conocimiento en la población para que cuenten con los medios y habilidades para aprovechar tecnología es relevante para impulsar una economía digital y desarrollo social inclusivo. Observamos que incluso en aquellos países considerados con gran desarrollo económico y educativo como Estonia, Dinamarca o Canadá, cuentan con programas para el desarrollo de habilidades digitales para su población. La atención a grupos vulnerables también deberá contar con acciones prioritarias para garantizar un desarrollo social inclusivo.
- *Servicios digitales*. Los países coinciden que la gestión de la información, de los datos, la participación ciudadana, la identidad digital, la firma electrónica, la ciberseguridad y el diseño de servicios centrados en las personas, son elementos clave para prestar servicios públicos sencillos, seguros y asequibles. En este rubro destaca que los países han adoptado acciones como: (i) la privacidad por diseño y seguridad por defecto para salvaguardar el derecho a la protección de datos personales; (ii) gestión de la identidad digital;

(iii) transacciones electrónicas con base en el uso de la firma electrónica y elementos criptográficos; y (iv) estrategias para abordar tecnologías emergentes como la IA, *blockchain*, o Internet de las Cosas.

Ahora bien, para efectos del presente trabajo, abordaremos los rubros de identidad digital y firma electrónica bajo la premisa que han constituido los pilares en la transformación digital en el contexto internacional. Consideramos que elementos como la identidad digital, firma electrónica, interoperabilidad y seguridad de la información, son elementos operacionales para la transformación digital que requieren un marco jurídico y técnico coordinado y articulada entre las entidades públicas y privada, con la finalidad de garantizar el respeto de los derechos humanos en un entorno cada vez más digital.

Capítulo 3
Identidad digital y firma electrónica

Capítulo 3. Identidad digital y firma electrónica

La innovación y el conocimiento tecnológico generan nuevos retos para el derecho ante los conflictos que genera el uso y aprovechamiento de las TIC en los derechos humanos. Si bien existen factores habilitantes como la infraestructura y las capacidades digitales para garantizar el derecho de acceso a las TIC e Internet, existen elementos que deben abordarse desde la óptica del derecho para garantizar un entorno seguro durante el proceso de transformación digital.

Así, por ejemplo, la interacción en medios electrónicos requiere que las personas se identifiquen para con la finalidad de adquirir derechos y obligaciones. Contar con confianza digital es indispensable para usar las TIC en transacciones digitales. Uno de los elementos que otorgan esta confianza es justo acreditar la identidad de las personas en entornos digitales. Igualmente, es importante que cuando se trata de transacciones electrónicas, la expresión de la voluntad esté libre de vicios en el consentimiento. En este último punto, la firma electrónica avanzada es la que otorga certeza jurídica y técnica a la expresión de la voluntad en medios digitales.

En el presente capítulo abordaremos los temas de identidad digital y firma electrónica como elementos operacionales de la transformación digital, en donde conoceremos: (i) los diferentes mecanismos adoptados por los países para garantizar el derecho a la identidad y potencia el desarrollo de servicios digitales, y (ii) el uso de la firma electrónica como herramienta para llevar a cabo actos jurídicos en medio electrónicos.

Estos dos aspectos han cobrado mayor relevancia ante la masificación de medios electrónicos como consecuencia de la crisis sanitaria por COVID-19. Pensemos, por ejemplo, en las acciones que las instituciones de educación adoptaron para reducir los riesgos de contagio mediante clases virtuales; en las citas médicas digitales; o en los trámites gubernamentales que durante la pandemia aún no se encontraban digitalizados.

Los gobiernos han redoblado esfuerzos para diseñar modelos de identidad digital seguros, sencillos y asequibles para atender la creciente demanda de

servicios digitales, así como para otorgar certeza jurídica en los actos jurídicos suscritos digitalmente.

3.1 Derecho a la Identidad

La identidad es un derecho humano que nos permite acceder a otros derechos como a la salud, la educación, el trabajo, o a servicios sociales. También, con nuestra identidad podemos acreditar nuestra personalidad para llevar a cabo actos jurídicos y contraer derechos y obligaciones. Este es uno de los primeros derechos de cualquier ser humano desde el "nacimiento".

El derecho a la identidad se reconoce expresamente a nivel internacional en la *Convención Sobre los Derechos del Niño*, en donde se establece que "*es obligación de los Estados registrar al niño inmediatamente después de su nacimiento, así como respetar su derecho a la identidad y nacionalidad*"[144].

Jorge Fernández Ruíz señala que el derecho a la identidad "*si bien atañe a los atributos de la personalidad como el nombre, el estado civil, el domicilio, la capacidad, el patrimonio y de nacionalidad, también impacta al individuo en su entorno familiar, social, así como en su lenguaje, sus tradiciones, su religión e, incluso, en cuestiones étnicas, biológicas y genéticas*[145]*"*.

Por su parte, Rosa María Álvarez sostiene que "*con el derecho a la identidad existe mayor garantía de acceso a otros derechos políticos y civiles, como el derecho al voto, a la igualdad ante la ley, a la familia, y a los derechos económicos, sociales y culturales, como salud y educación"*[146].

Al respecto, la Corte Interamericana de Derechos Humanos señala que "*el derecho a la identidad está íntimamente asociado al derecho al reconocimiento de*

[144] UNICEF, "Convención sobre los Derechos del Niño", 2006, p. 12, Disponible en: https://www.un.org/es/events/childrenday/pdf/derechos.pdf, (Fecha de consulta: 01 de julio de 2020).
[145] Fernández Ruíz, Jorge, "El Registro del Estado Civil de las Personas", UNAM-IIJ, México, p. 11, Disponible en: https://archivos.juridicas.unam.mx/www/bjv/libros/7/3100/5.pdf, (Fecha de consulta: 01 de julio de 2020)
[146] Álvarez, Rosa María, "Derecho a la identidad", IIJ-UNAM, México, 2002, p. 118, Disponible en: https://archivos.juridicas.unam.mx/www/bjv/libros/9/4242/8.pdf (Fecha de consulta: 01 de julio de 2020)

la personalidad, al derecho a tener un nombre, una nacionalidad y a mantener relaciones familiares"[147].

El derecho a la identidad tiene impacto en prácticamente todos los sectores de nuestra vida. Está asociado a otros derechos humanos y su protección es muy importante desde las primeras etapas del ser humano a través del Registro Civil de cada país. Hoy en día este derecho se ha transformado debido al uso de Internet y las TIC, en donde este el derecho sale del registro civil y se permea en plataformas digitales, redes sociales, acceso a servicios públicos o financieros.

Por otro lado, si bien el derecho a la identidad debe garantizarse desde el nacimiento, existen ciertas condiciones sociales y económicas que lo impiden. Pensemos por ejemplo en la migración o en países en condiciones de pobreza en donde los niños nacen en sus comunidades y no acuden al registro civil. En América Latina, a través del "*Programa interamericano para el registro civil universal y derecho a la identidad*"[148], la Asamblea General de la OEA reconoce la importancia de los registros civiles como las instituciones del Estado que pueden garantizar el reconocimiento de la identidad de las personas y orienta a los Estados americanos a asegurar el registro de todos los nacidos en su territorio nacional independientemente del estatus migratorio de los padres del menor[149].

Igualmente, por la relevancia de este derecho, a través del ODS 16, la ONU ha contemplado como una de sus metas principales el proporcionar acceso a una identidad jurídica para todos, en particular mediante el registro de nacimientos, con la finalidad de que las personas puedan ejercer otros derechos[150].

Para garantizar este derecho, además de los registros civiles, se habla del uso de tecnologías para proporcionar una identidad digital a las personas. Aquí, la

---

[147] Corte Interamericana de Derechos Humanos, "Caso de las Hermanas Serrano Cruz Vs. El Salvador", 2005, p. 71, Disponible en: https://www.corteidh.or.cr/docs/casos/articulos/seriec_120_esp.pdf (Fecha de consulta: 01 de julio de 2020).

[148] OEA, "Programa interamericano para el registro civil universal y "derecho a la identidad", AG/RES. 2362 (XXXVIII-O/08), 2008, Disponible en: http://www.oas.org/sap/docs/puica/RES_2362_ProgramaInteramericano_s.pdf (Fecha de consulta: 02 de julio de 2020)

[149] Ídem.

[150] ONU, ODS 16, Promover sociedades justas, pacíficas e inclusivas, Disponible en https://www.un.org/sustainabledevelopment/es/peace-justice/, (Fecha de consulta: 02 de julio de 2020).

interoperabilidad de plataformas, datos, ciberseguridad y tecnologías emergentes como *blockchain,* cobran mayor relevancia en materia de identidad digital.

Así. en resumen, podemos señalar que la identidad y los registros civiles son fundamentales para que las personas puedan acceder a otros derechos humanos. Es un derecho de gran relevancia a nivel internacional que busca proteger a la persona desde su nacimiento. No obstante, existen retos a nivel mundial para que todas las personas tengan acceso a este derecho tales como la migración, la pobreza, los desplazados y refugiados, en donde las TIC pueden servir como herramientas para proporcionar este derecho a miles de personas.

3.2 Identidad legal

El derecho humano a la identidad, garantizado a través de los registros civiles, que permiten otorgar una nacionalidad y una personalidad jurídica a la persona, ha llevado a regular la identidad legal. Esta es entendida como "*la combinación de los factores que permite a la persona acceder a derechos, beneficios y deberes, o sea el debido registro y documentación de nombre, filiación, fecha de nacimiento e identificación única sea como datos biométricos y/o un número único de identificación*"[151].

Se reconoce a la identidad legal como un derecho que habilita otros derechos, cuya falta de garantía puede plantear situaciones de desigualdad en el acceso a los bienes, servicios y oportunidades sociales en general[152]. Ahora bien, en la era digital una persona normalmente no se identifica con su identidad legal, sino utiliza otros datos personales que no obran normalmente en los registros civiles como lo son una cuenta de correo electrónico o un número de celular, los cuales

[151] Harbitz, Mia, Tamargo, María del Carmen, "El significado de la identidad legal en situaciones de pobreza y exclusión social", Banco Interamericano de Desarrollo, Washington DC, 2010, p. 2, https://publications.iadb.org/publications/spanish/document/El-significado-de-la-identidad-legal-en-situaciones-de-pobreza-y-exclusi%C3%B3n-social-El-subregistro-de-nacimientos-y-la-indocumentaci%C3%B3n-desde-la-perspectiva-de-g%C3%A9nero-y-etnia-en-Bolivia-Ecuador-y-Guatemala.pdf (Fecha de consulta 02 de julio de 2020).

[152] Tamargo, María del Carmen, "Identidad legal, ciudadanía y vulnerabilidad social. Notas para el estudio del subregistro de nacimientos y la indocumentación con perspectiva de género y etnicidad", XXVII Congreso de la Asociación Latinoamericana de Sociología. VIII Jornadas de Sociología de la Universidad de Buenos Aires. Asociación Latinoamericana de Sociología, Buenos Aires, 2009, p. 3, Disponible en http://cdsa.aacademica.org/000-062/655.pdf (Fecha de consulta: 02 de julio 2020).

sirven como mecanismo de interacción y autenticación de nuestra identidad en Internet y aplicativos digitales.

Como veremos más adelante, desde sus orígenes en los años 2000, la firma electrónica prevista en la Ley Modelo de la CNUDMI sobre firma electrónica ya contemplaba la importancia de identificar a una persona en materia de comercio electrónico y garantizar los actos jurídicos derivados del derecho mercantil internacional, en donde el principal medio de intercambio de información era el correo electrónico.

Ante el intercambio masivo de datos, la forma en que hoy puede identificarse a una persona en medios digitales es tan diversa y está motivada por la asociación y vinculación de diversos datos personales. Es así como consideramos relevante que el derecho debe proporcionar seguridad jurídica a través de la regulación de la identidad digital a cargo del Estado. Lo anterior, con la finalidad de prevenir riesgos a los derechos asociados con la identidad legal y la protección de datos personales de una persona en medios físicos y electrónicos.

3.3 Identidad digital

Con la cuarta revolución industrial el derecho a la identidad ha cobrado mayor alcance que el concepto tradicional de la identidad legal. Derivado del uso exponencial de Internet y las TIC, hoy se habla de una identidad digital. Desde 2005 -justo cuando se concluían los principios de la CMSI-, encontramos las primeras definiciones sobre identidad digital. Por ejemplo, Windley, P. J., señala que "*la identidad digital son los datos que describen de manera única a una persona o cosa y contiene información sobre las relaciones del sujeto*", en donde incluye al concepto de identidad digital la importancia de la seguridad y privacidad[153].

Como observamos, el concepto de identidad en medios digitales contempla nuevos conceptos como el de seguridad, privacidad, datos, internet o incluso máquinas, y no hace mención que sea un derecho desde el nacimiento ni que se garantice a través del Registro Civil.

[153] Windley, P. J., "Digital Identity: Unmasking Identity Management Architecture (IMA). O'Reilly Media inc., Estados Unidos de América, 2005, p. 9. Disponible para consulta en: https://www.windley.com/docs/Digital%20Identity.pdf, (Fecha de consulta 02 de julio de 2020).

Sandrasegaran y Li definen a la identidad digital como "*el medio que una entidad (otro ser humano o máquina), puede usar para identificar a un usuario en el mundo digital. El objetivo de la identidad digital es crear el mismo nivel de confianza que se generaría con una transacción cara a cara*"[154]. Por su parte, Valentina Armenta, Adriana Lazzaroni y Laura Abba, señalan que "*la identidad digital son los datos que describen de manera única a una persona o cosa y contiene información sobre las relaciones del sujeto. La identidad social que un usuario de Internet establece a través de identidades digitales en el ciberespacio se conoce como identidad en línea*"[155].

Por su parte la UIT indica que la identidad digital "*es la representación digital de una persona lo suficientemente detallada como para hacerlos distinguible dentro de un contexto digital*"[156]. Igualmente señala que la identidad es un elemento crucial para cada individuo ya que identifica los principales rasgos de cada persona.

La UIT incluye al concepto de identidad digital dos aspectos importantes. El primero, al señalar que la identidad digital permite "identificar los rasgos" de cada persona. El segundo, que dicho concepto contiene "atributos de la persona" sobre información relacionada con: i) su nacimiento, tales como nombre; lugar de nacimiento; fecha de nacimiento; ii) información descriptiva como altura, peso o rasgos físicos; iii) identificadores personales como el número de seguro social; y iv) datos biométricos como la huella digital, el ADN, iris, entre otros[157]. Es decir, vincula la identidad digital con el concepto tradicional de identidad legal.

El Observatorio de *Blockchain* de la Unión Europea, señala que existen un sinnúmero de atributos de la identidad digital, tales como datos biométricos, género, huellas digitales, patrones de voz, la forma en que usamos el teclado o caminamos,

---

[154] Segeran & Li, Sandra, citada en Chaudron, Stephane y Eichinger, Henning, "Eagle-eye on Identities in the digital world", Unión Europea, Publications Office of the European Union, Luxembourg, 2018, p. 19. Disponible para consulta en https://publications.jrc.ec.europa.eu/repository/bitstream/JRC110266/digital_identity_report_final_online_pubsy_1.pdf, (Fecha de consulta: 02 de julio de 2020).
[155] Ídem.
[156] UIT, "Digital identity roadmap guide", 2018, p. 4, Disponible en: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-DIGITAL.01-2018-PDF-E.pdf (Fecha de consulta: 02 de julio de 2020).
[157] Idem.

la identidad social, nombre, fecha de nacimiento, dirección, estado civil, o datos oficiales como nuestro número de identificación nacional[158].

Como observamos, la identidad digital ya no está asociada únicamente a los datos de nuestro registro civil, sino incluye aspectos de otra índole como los datos biométricos, la huella digital[159], datos oficiales o digitales. Así, podemos decir que la identidad digital está vinculada con cualquier "dato personal" que haga identificable a una persona a través de medios electrónicos.

Para gestionar los datos personales que nos permiten identificar a una persona, la CNUDMI, en una resolución sobre el "Panorama general de la gestión de la identidad digital", señala que la gestión de la identidad tiene por objeto responder a dos preguntas sencillas ¿quién es usted? y ¿cómo puede demostrarlo?[160]. Para dar respuesta a estas dos preguntas en medios digitales se han generado ciertos modelos de gestión de identidad digital que buscan ofrecer controles de "identificación", "autenticación" y "autorización" de forma seguridad en medios digitales.

3.3.1 Principios de la identidad digital de la UIT

La UIT reconoce la importancia de la identidad digital para la transformación digital de los países y ha sugerido considerar un MNID destacando los avances que en esta materia tienen países como Canadá, Estonia y Reino Unidos. La UIT señala que la identidad digital atrae beneficios al sector público, tales como la reducción de costos de acceso a servicios, la inclusión ciudadana, la prestación de servicios y la

---

[158] Lyons, Tom, Courcelas, Ludovic, TIMSIT, Ken, "Blockchain and digital identity", EU Blockchain Observatory & Forum, Mayo 2019, p. 12, Disponible en: https://www.eublockchainforum.eu/sites/default/files/report_identity_v0.9.4.pdf. (Fecha de consulta: 02 de julio de 2020).

[159] Las huellas digitales son los registros y rastros que dejamos al utilizar Internet. Las huellas digitales pueden representar un riesgo o un beneficio para cada persona, pero nunca son irrelevantes. Nuestra huella digital puede afectar nuestra reputación en línea e incluso nuestra calificación crediticia. Gracias a nuestra huella digital, puede que no sea necesario iniciar una sesión o ingresar repetidamente nuestros datos personales en un sitio web. Cfr. Biblioteca de la Universidad de Alicante, "La huella digital", Universidad de Alicante, España, p. 2-3, Disponible en: https://rua.ua.es/dspace/bitstream/10045/79601/1/CI2_intermedio_2017-18_Huella-digital.pdf (Fecha de consulta: 02 de julio de 2020).

[160] CNUDMI, "Panorama general de la gestión de la identidad digital", A/CN.9/WG.IV/WP.120, 27 de julio de 2012, p. 5, Disponible en: https://www.uncitral.org/pdf/spanish/workinggroups/wg_iv/46th_WG_IV/wp_120_s.pdf (Fecha de consulta: 02 de julio de 2020).

seguridad de la información[161]. No obstante, para fomentar los beneficios de las herramientas tecnológicas y reducir sus riesgos, la UIT sugiere adoptar una serie de quince principios en el diseño de un MNID. Estos principios son:

1. Definir los objetivos que persigue con la identidad digital;
2. Comprender el contexto global digital y atender el contexto nacional;
3. Considerar el acceso a grupos vulnerables;
4. Fomentar la prosperidad económica y social, y contribuir al desarrollo sostenible y a la inclusión digital;
5. Respetar los derechos humanos;
6. Gestionar los riesgos y garantizar un nivel adecuado de resiliencia;
7. Salvaguardar la privacidad de seguridad de la información para generar confianza entre sus usuarios;
8. Sostenibilidad económica de la plataforma o sistema en que se implemente;
9. Ser flexible y escalable, y permitir actualizarse o modificarse de manera rápida y eficiente;
10. Ser interoperabilidad y garantizar el intercambio de información de los sistemas;
11. Seguir un calendario de despliegue rápido;
12. Fomentar el desarrollo de la identificación digital como plataforma para que los usuarios puedan conectarlo a cualquier dominio y usarlo;
13. Garantizar que las personas tengan acceso a una sola identidad digital;
14. Contar con tecnologías y sistemas robustos que soporten la identidad digital, que sean escalables y estar preparados para el futuro; y
15. Servir como base para otros programas nacionales de importancia, teniendo medidas para garantizar la calidad de los datos en múltiples niveles.

[161] Las huellas digitales son los registros y rastros que dejamos al utilizar Internet. Las huellas digitales pueden representar un riesgo o un beneficio para cada persona pero nunca son irrelevantes. Nuestra huella digital puede afectar nuestra repu-tación en línea e incluso nuestra calificación crediticia. Gracias a nuestra huella digital, puede que no sea necesario iniciar una sesión o ingresar repetidamente nuestros datos personales en un sitio web. Biblioteca de la Universidad de Ali-cante, “La huella digital”, Universidad de Alicante, España, p. 2-3, Disponible en https://rua.ua.es/dspace/bitstream/10045/79601/1/CI2_intermedio_2017-18_Huella-digital.pdf (Fecha de consulta: 02 de julio de 2020).

Estos quince principios nos ofrecen un gran campo de acción para el diseño de políticas públicas en materia de identidad digital. De la misma forma, el Banco Mundial ofrece a los países una serie de diez principios en materia de identidad digital. Estos principios los resumimos en seguida[162]:

1. Garantizar el acceso universal de las personas sin discriminación;
2. Eliminar barreras de acceso y uso;
3. Identidad confiable, única, segura y precisa;
4. Plataforma receptiva e interoperable;
5. Estándares abiertos y evitar las dependencias de proveedores y tecnología;
6. Proteger la privacidad mediante el diseño del sistema;
7. Sostenibilidad financiera y operativa;
8. Protección de datos personales y seguridad cibernética;
9. Mandatos institucionales claros y rendición de cuentas;
10. Cumplir con marcos legales y de confianza con supervisión y atención de quejas.

Parco contar con un modelo de identidad digital, observamos que la UIT y el Banco Mundial coinciden en: considerar el acceso y uso de grupos vulnerables; respetar los derechos humanos, en especial la protección de datos personales y privacidad; contar con seguridad de información; una plataforma única interoperable; identidad digital única; rendición de cuentas; escalabilidad y sostenibilidad.

Estos principios son relevantes ya que a nivel internacional los modelos de identidad digital varían no sólo en su forma sino también en la entidad que lo garantiza. Unos han modernizado sus registros civiles. Otros, utilizan elementos como la firma electrónica en colaboración con unidades de gobierno digital, fiscales o de seguridad pública. Igualmente, debemos resaltar que la adopción de un modelo de identidad digital dependerá de las características legales, técnicas y políticas de

[162] Banco Mundial, “Principios de identificación para el desarrollo sostenible: hacia la era digital”, disponible para su consulta en https://id4d.worldbank.org/principles (Fecha de consulta: 02 de julio de 2020).

cada país, en donde lo importante será garantizar a las personas confianza y seguridad en el uso de sus datos personales en medios digitales.

3.4 La firma en la era digital

Cuando hablamos de firma electrónica es necesario distinguir tres conceptos: firma electrónica simple, firma electrónica avanzada y firma electrónica cualificada. Pero antes de ello, conozcamos que debemos entender por firma.

3.4.1 Concepto de firma

Es interesante observar que al igual que la evolución de los derechos humanos a través de las revoluciones industriales y las formas en que estos se garantizan en cada época, el concepto de firma también ha evolucionado a raíz del uso de las TIC.

Mustapich define a la "firma" como "*el nombre escrito por propia mano en caracteres alfabéticos y de una manera particular, al pie del documento, al efecto de autenticar su contenido*"[163]. Por su parte, Planiol y Ripet, definen este concepto como *"una inscripción manuscrita que indica el nombre de una persona que entiende hacer suyas las declaraciones del acto*"[164]. Por último, Alfredo Baltierra Guerrero señala que la naturaleza jurídica de la "firma autógrafa" es "*la expresión de voluntariedad ya que, al firmarse un documento, el suscriptor se está haciendo responsable de su contenido en lo particular*".[165]

Otro concepto relacionado con la firma es la huella dactilar que normalmente es utilizado en documentos físicos cuando una persona no puede o no sabe firmar autógrafamente. En el ámbito del derecho civil es utilizada para contraer derechos y obligaciones. Anteriormente, este concepto era conocido como huella digital[166];

---

[163] Mustapich, J.M. Tratado de Derecho Notarial, T.1., p 260. Disponible en https://revistas.unlp.edu.ar/RevistaAnalesJursoc/article/download/5083/5453/, (Fecha de consulta: 03 de julio de 2020).

[164] Planiol y Ripet, Traité Practiqué de Droit Civiel Francais, VII, No. 1458. Disponible en https://www.worldcat.org/title/traite-pratique-de-droit-civil-francais-tome-vii-obligations-deuxieme-partie/oclc/490462979, (Fecha de consulta: 03 de julio de 2020).

[165] Baltierra Guerrero, Alfredo, La firma autógrafa en el derecho bancario, UNAM-IIJ, México, Disponible en: https://revistas-colaboracion.juridicas.unam.mx/index.php/rev-facultad-derecho-mx/article/view/30813/27804. (Fecha de consulta: 02 de julio de 2020).

[166] Código Civil Federal: Artículo 1514. "Cuando el testador declare que no sabe o no puede firmar el testamento, uno de los testigos firmará a ruego del testador y éste imprimirá su huella digital, y Artículo 1834.- Cuando se exija la forma escrita para el contrato, los documentos relativos deben ser

ahora, con el uso de las TIC, se distingue entre huella dactilar y huella digital; sin duda, estos cambios conceptuales son motivados por la cuarta revolución industrial.

Antes de la cuarta revolución industrial, el concepto de firma era entendido sólo en un ámbito físico a través de un gráfico manuscrito mediante el cual una persona valida, acepta y "consiente" que el contenido de un documento le es propio. Ahora, en la era digital veremos que las características de la firma han evolucionado. No obstante, es importante señalar que sus elementos de fondo permanecen, tales como el ser un medio de expresión de la voluntad de una persona.

Con la contingencia sanitaria por COVID-19 y, ante el distanciamiento social, contar con mecanismos de validez jurídica en formato digital son cada vez más necesarios. Incluso, en aquellos países en que aún se optaba por la firma autógrafa, se ha comenzado a maximizar el uso de la firma electrónica; esto gracias a una pandemia mundial que aceleró los procesos de transformación digital de los países. No obstante, existen algunos retos para su implementación, tales como la falta de infraestructura digital, el desarrollo de habilidades digitales en la población o contar con estrategias coordinadas en materia digital entre los distintos sectores de la sociedad.

Es importante tener presente que los tipos de firma electrónica en cada país están influenciados por el tipo de sistema jurídico al que pertenecen; romanista o anglosajón. En el sistema anglosajón por regla general los contratos no tienen que ser formalizador por escrito o firmados para que sean válidos y ejecutorios. En cambio, en el sistema romanista se suelen existir algunas formalidades para acreditar la validez jurídica de un documento, como lo podría ser un contrato de compraventa de inmuebles[167].

Con los medios electrónicos y transacciones internacionales, y los costos de tiempo y traslados para la firma entre países, la firma electrónica es una herramienta

---

firmados por todas las personas a las cuales se imponga esa obligación. Si alguna de ellas no puede o no sabe firmar, lo hará otra a su ruego y en el documento se imprimirá la huella digital del interesado que no firmó.

[167] CNUDMI, "Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónicas", ONU, Viene, 2009, p. 3, Disponible en: https://www.uncitral.org/pdf/spanish/texts/electcom/08-55701_Ebook.pdf (Fecha de consulta: 03 de julio de 2020).

que favorece las transacciones comerciales y también el acceso a servicios públicos como presentar una declaración fiscal.

A diferencia de la identidad digital, la firma electrónica cuenta con una base normativa a nivel internacional que orienta su adopción en los países a través de la Ley Modelo de la CNUDMI sobre firma electrónica; tal como veremos en seguida.

3.4.2 Firma electrónica simple

El primer concepto sobre firma electrónica encuentra su principal antecedente en el comercio internacional a través de la Ley Modelo de la CNUDMI sobre Comercio Electrónico[168]. Impulsado por el Internet y el intercambio de información, el comercio internacional tuvo que adaptarse al uso de las TIC ante un acelerado proceso de globalización que incrementó el flujo internacional de mercancías e información por correo electrónico[169] en el marco de los TLC.

Para ofrecer seguridad a las transacciones de derecho mercantil internacional, la CNUDMI publicó dos leyes modelos durante los años 1998 y 2002. La primera sobre comercio electrónico; la segunda sobre firma electrónica.

Con la Ley Modelo sobre Comercio Electrónico la CNUDMI se busca eliminar los obstáculos innecesarios ocasiones al comercio internacional por el uso de mensajes de datos a través de Internet en temas vinculados con el comercio electrónico[170], como lo es, por ejemplo, el transporte de mercancías. La Ley Modelo de la CNUDMI sobre Comercio Electrónico es la primera a nivel internacional aplicable a todo tipo de información en forma de mensaje de datos utilizada en el

---

[168] ONU, “Ley Modelo de la CNUDMI sobre Comercio Electrónico”, 1996, Disponible en: https://www.uncitral.org/pdf/spanish/texts/electcom/05-89453_S_Ebook.pdf. (Fecha de consulta: 03 de julio de 2020).

[169] OEA, “Globalización y su impacto en el comercio mundial y regional”, 1993 Disponible en: https://www.oas.org/dsd/publications/unit/oea33s/ch32.htm (Fecha de consulta: 03 de julio de 2020)

[170] Con base en el numeral 7 de la Guía para la incorporación al derecho interno de la Ley Modelo de la CNUDMI sobre Comercio Electrónico, por comercio electrónico, se entiende una concepción amplia del intercambio electrónico de datos, el cual a su vez se define por el artículo 2, inciso b) de la citada Ley como “la transmisión electrónica de información de una computadora a otra, estando estructurada la información conforme a alguna norma técnica convenida al efecto”. ONU, “Ley Modelo de la CNUDMI sobre Comercio Electrónico”, *op.cit.,* pp. 4, 17 y 18. Op cit.

contexto de actividades comerciales. Regula conceptos como mensaje de datos[171], intercambio electrónico de datos[172] o sistema de información[173].

Si bien en esta ley no se regula la firma electrónica, ya se establecían sus características, tales como (i) identificar a una persona; (ii) dar certeza de la participación en el acto de firmar, y (iii) asociar a esa persona con el contenido del documento[174].

Posteriormente, para otorgar mayor certeza jurídica sobre el uso de la firma en el comercio electrónico, la CNUDMI publicó la Ley Modelo de la CNUDMI sobre Firmas Electrónicas[175]. Esta ley define por primera vez a la firma electrónica como "*los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo, que puedan ser utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el firmante aprueba la información recogida en el mensaje de datos*"[176].

Igualmente, esta ley señala que cuando se exija el requisito de firma en un documento, para el caso de mensaje de datos, se tendrá por acreditado con una firma electrónica que sea fiable, entendiendo por tal que (i) los datos de creación de la firma corresponden exclusivamente con el firmante; (ii) dichos datos estuvieron bajo control exclusivo del firmante al momento de su creación, y (iii) es posible detectar cualquier alteración de la firma electrónica hecha después del momento de

---

[171] Artículo 2, inciso a) de la Ley Modelo de la CNUDMI sobre Comercio Electrónico. Se entenderá por mensaje de datos: la información generada, enviada, recibida o archivada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos (EDI), el correo electrónico, el telegrama, el télex o el telefax. Ibídem, p 4.

[172] Artículo 2, inciso b) de la Ley Modelo de la CNUDMI sobre Comercio Electrónico. Se entenderá intercambio electrónico de datos: la transmisión electrónica de información de una computadora a otra, estando estructurada la información conforme a alguna norma técnica convenida al efecto. Ídem.

[173] Artículo 2, inciso f) de la Ley Modelo de la CNUDMI sobre Comercio Electrónico. Se entenderá por sistema de información: todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna otra forma mensajes de datos. Ídem.

[174] ONU, "Ley Modelo de la CNUDMI sobre Comercio Electrónico", Nueva York, 2002, Disponible en: https://www.uncitral.org/pdf/spanish/texts/electcom/ml-elecsig-s.pdf (Fecha de consulta: 04 de julio de 2020)

[175] Idem.

[176] ONU, "Artículo 2, inciso a) de la Ley Modelo de la CNUDMI sobre Firmas Electrónicas", Nueva York, 2002, Disponible en: https://www.uncitral.org/pdf/spanish/texts/electcom/ml-elecsig-s.pdf (Fecha de consulta: 04 de julio de 2020)

la firma. Bajo estos elementos, se reconoce la validez legal de la firma a nivel internacional[177].

En el marco de la Ley Modelo de la CNUDMI sobre Firmas Electrónicas se contemplan las nuevas características que van dando forma al concepto tradicional de firma en medios digitales, en donde se incluyen elementos como *criptografía*, *clave pública y privada*, *prestadores de servicios de certificación* e *infraestructura de clave pública*. Estos elementos son esenciales cuando hablamos de firma electrónica, los cuales describimos brevemente en los siguientes párrafos.

La criptografía, es una rama de las matemáticas aplicadas que se ocupa para transformar mensajes de datos ininteligibles y devolverlos a su forma original[178] y, hoy en día, es un elemento clave para garantizar la seguridad digital de las transacciones electrónicas. Por su parte, la clave privada se utiliza para que el firmante pueda crear su firma, y la clave pública para que terceros puedan descifrar su mensaje. La infraestructura de clave pública es importante para intercambiar las claves públicas, y normalmente es implementada por una autoridad en los países.

El prestador de servicios de certificación es quien emite un certificado digital que permite asociar la clave pública con el titular de la firma. Un dato relevante es que en la ley modelo de firma electrónica se contempla que los notarios pueden fungir como prestadores de servicios de certificación[179].

Sin embargo, la firma electrónica en sus inicios, y ante la falta de infraestructura que permitiera darle soporte, únicamente se cuidaba que cumpliera con los datos creación y su control en poder del titular, así como la detección de modificaciones futuras. Por ello, se ha entendido que una firma *electrónica es cualquier dato en formato electrónico adjunto o asociado lógicamente con otros datos, el cual es utilizado por el firmante para plasmar su firmar*[180]. A este tipo de

---

[177] Ídem.

[178] DARÍO FLÓREZ, Germán, “La validez jurídica de los documentos electrónicos en Colombia a partir de sus evolución legislativa y jurisprudencial”, Verba Iuris 31, Enero-Junio 2014, Bogotá D.C. Colombia, p. 51. Disponible en https://revistas.unilibre.edu.co/index.php/verbaiuris/article/download/54/48, / (Fecha de consulta 04 de julio de 2020).

[179] Idem.

[180] Diario Oficial de la Unión Europea, “Artículo 3, párrafo 10 del 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

firma, para distinguirla de la avanzada y cualificada, se le ha llamado firma electrónica simple[181] en donde además de firmar un documento digital permite identificar a su firmante.

3.4.3 Firma electrónica avanzada

Con el paso del tiempo, los elementos tecnológicos para el uso de la firma electrónica previstos por la CNUDMI se fortalecieron para otorgar mayor confianza y seguridad en las transacciones electrónicas. Se pudieron implementar los conceptos de criptografía, clave pública, clave privada, infraestructura pública y prestadores de servicios de certificación previstos en la ley modelo.

La firma electrónica avanzada cumple con los mismos elementos de la firma electrónica simple[182]. No obstante, la avanzada se distingue de la simple por la forma en que la firma es creada bajo una serie de medios con control exclusivo del firmante[183]. Es una tecnología de infraestructura de clave pública (PKI, por sus siglas en inglés) que permite intercambiar información y realizar transacciones de manera ágil y sencilla, a través de sistemas en línea y mediante el uso de un certificado digital que cuenta con mecanismos que otorgan certeza y seguridad técnica[184].

De esta forma, la firma electrónica avanzada es considerada una forma más sofisticada y segura para firmar un documento ya que es creada con base en criptografía de clave pública (PKI) e insertada mediante un código en el documento[185], la cual es expedida por un prestador de servicios de certificación que

---

por la que se deroga la Directiva 1999/93/CE", Europa, 2014, Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32014R0910&from=IT (Fecha de consulta 04 de julio de 2020).

[181] Firma electrónica simple. Es el tipo básico de firma electrónica. Es un conjunto de datos electrónicos, unido a un documento electrónico y utilizado cuando un emisor envía un mensaje al receptor, y dicho mensaje va cifrado, de manera que nadie pueda modificarlo ni alterarlo. Su finalidad es, además, identificar al sujeto que la utiliza. Cfr. Barreto Zuñiga, Lizbeth Angélica, "Evolución de la firma autógrafa a la firma electrónica avanzada", Revista Digital Universitaria, 1 de marzo 2011 • Volumen 12 Número 3, p. 5, Disponible en: http://www.revista.unam.mx/vol.12/num3/art34/art34.pdf. (Fecha de consulta 02 de julio de 2020).

[182] Ídem.

[183] Ídem.

[184] Ídem.

[185] Reuters, Thomson, "Electronic signature platforms key contractual issues", PLC Magazine, Reino Unido, January/February 2017, p. 30, Disponible en:

da soporte a esa infraestructura técnica especializada, quien emite un certificado de firma electrónica que constituye una declaración electrónica que vincula los datos de validación de una firma con una persona (nombre o seudónimo de la persona)[186].

La firma electrónica avanzada es utilizada por la mayoría de los países en el mundo con la finalidad de otorgar mayor seguridad en las transacciones digitales. No obstante, algunos otros países, de tradición anglosajona como Estados Unidos, prefieren usar la firma electrónica simple bajo el principio de libertad contractual.

Otros, dada la relevancia que ha adquirido la protección de datos personales y la seguridad de la información, han fortalecido la seguridad de las transacciones electrónicas a través de la criptografía vinculada a la firma electrónica avanzada y, es a esta, a la que se le reconoce "valor probatorio pleno" con los mismos efectos que una firma manuscrita. Además, otros países, han fortalecido aún más la seguridad de la firma electrónica a través de un dispositivo especializado para su creación, surgiendo así el concepto de firma electrónica cualificada.

3.4.4 Firma electrónica cualificada

La firma electrónica cualificada se define en el contexto internacional como una firma electrónica avanzada -es decir, que utiliza infraestructura PKI- pero que además es creada mediante un dispositivo cualificado de creación de firmas electrónicas basado en un certificado cualificado de firma electrónica emitido por un prestador de servicios de certificación[187].

Este tipo de firma, además de cumplir con los requisitos de la firma simple, más los de la firma electrónica avanzada, debe ser generado por un dispositivo cualificado y un certificado -también cualificado- emitido por un prestador de

https://ec.europa.eu/futurium/en/system/files/ged/plc_article_on_e-signature_platforms_final_feb_2017.pdf (Fecha de consulta: 03 de julio de 2020)

[186] DARÍO FLÓREZ, Germán, *op. cit.,* p. 55.

[187] Diario Oficial de la Unión Europea, "Artículo 3 (12), del 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", Europa, 2014, Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32014R0910&from=IT (Fecha de consulta: 03 de julio de 2020)

servicios de certificación registrado en una lista de confianza publicada por la autoridad de cada país competente en la materia[188].

El término “cualificado” se refiere a la formación especializada de algo o alguien, y se utiliza también para referirse a una autoridad[189]. En el caso de la firma electrónica cualificada podemos decir que además de que: (i) los datos de creación de la firma corresponden exclusivamente con el firmante; (ii) los datos de creación estuvieron bajo control exclusivo del firmante al momento de su creación; (iii) es posible detectar cualquier alteración de la firma electrónica hecha después del momento de la firma; (iv) utiliza infraestructura PKI; (v) es expedida por un prestador de servicios de certificación registrado en las listas de confianza de la autoridad nacional, y (vi) es creada además mediante un dispositivo “cualificado”[190].

En el marco de la Unión Europea se contemplan los requisitos que deben cumplir los dispositivos cualificados, tales como (i) garantizar la confidencialidad y seguridad de los datos de creación de la firma, y que el firmante puede protegerlos frente a terceros; (ii) no alterar los datos que deben firmarse ni impedir que dichos datos se muestren al firmante antes de firmar, y (iii) la gestión de los datos de creación de la firma en nombre del firmante sólo deben correr a cargo del prestador cualificado de servicios de confianza[191].

Como observamos la firma en la era digital ha ido evolucionando con la finalidad de otorgar mayor confianza y seguridad en las transacciones electrónicas. Desde sus orígenes guarda elementos necesarios que están asociados con los datos de creación bajo el control exclusivo del firmante y, para reforzar su forma de creación, se han incorporado elementos de infraestructura PKI respaldada por proveedores de servicios de certificación y dispositivos cualificados para su creación.

---

[188] Reuters, Thomson, “Electronic signature platforms key contractual issues”, *op cit*. p. 31.
[189] Real Academia Española, 2020, Disponible en: https://dle.rae.es/cualificado (Fecha de consulta: 04 de julio de 2020).
[190] REGLAMENTO (UE) No 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de julio de 2014, *op.cit.,* p. 50.
[191] Ídem.

3.5 Identidad digital y firma electrónica en el contexto internacional

En las siguientes líneas observaremos brevemente los **modelos de identidad digital y firma electrónica** adoptados por los países mejor ranqueados en el EDGI que revisamos en el segundo capítulo. Lo anterior, nos permitirá conocer cuáles son las estrategias, acciones y mecanismos que dichos países han adoptado en estos dos rubros considerándolos como pilares de la transformación digital.

Esto nos permitirá identificar cuáles son las formas que a nivel internacional los países han adoptado para implementar los sistemas de identidad digital, así como las autoridades que la gestión dicha identidad. Por una parte, observaremos que ya no son sólo los registros civiles, sino que en algunos casos son autoridades fiscales, de seguridad del interior o las recientes unidades de gobierno. Por otro, lado, también podremos observar que los modelos de identidad pueden ser agrupados en cuatro tipos: (i) tarjeta física con chip; (ii) clave y usuario; (iii) certificados digitales, y (iv) sistemas de validación de identidad a través de plataformas digitales mediante el uso de datos biométricos.

En cambio, la firma electrónica avanzada en los países sigue un estándar basado en la Ley Modelo de la CNUDMI sobre firma electrónica, en donde cuentan con una sólo ley a nivel nacional. La diferencia está básicamente en los tipos de firma electrónica regulados en el país: simple, avanzada y cualificada.

3.5.1 Sudáfrica

Sudáfrica cuenta una tarjeta de identificación inteligente a cargo del Departamento del Interior del Gobierno[192] que permite acreditar a los ciudadanos tanto su identidad presencial como su identidad digital. Se trata de una tarjeta física que, además de los datos como nombre, fotografía y número de identidad, contiene datos como la huella biométrica, código de barras, y código QR. Además, Sudáfrica cuenta con verificación de identidad a través de la huella biométrica y un código PIN. La tarjera de identidad contiene un microprocesador que contiene detalles de la identidad de

[192] Gobierno de Sudáfrica, “Conoce la nueva Tarjeta de Identificación Inteligente”, Sudáfrica, 2020, Disponible en: http://www.dha.gov.za/index.php/id-smart-card, (Fecha de consulta el 20 de julio de 2020).

una persona y garantiza que sólo las autoridades autorizadas puedan leer y verificar los datos de la tarjeta utilizando escáneres legibles por máquinas sin contacto.

Como mecanismos de seguridad, la tarjeta de identidad en la parte física cuenta con hologramas, grabados láser y detalles personales que proporcionan una verificación visual de la tarjeta e identifican fácilmente las tarjetas manipuladas. En seguridad técnica, incluye datos biométricos de huellas dactilares y datos biográficos integrados en el chip de la tarjeta física. Entre los objetivos y usos de la identidad digital en Sudáfrica están el asegurar servicios gubernamentales; reducir el fraude y el robo de identidad; proporcionar una identidad única a todos sus ciudadanos; sentar las bases para una plataforma futura que incluya servicios en línea de autenticación y firmas digitales; eliminar la necesidad de llevar múltiples documentos de identificación; mejorar la confianza en la credenciales de identidad oficiales; acelerar los controles de identidad en el cruce de fronteras; y establecer la ciudadanía en el Registro Nacional de la Población para que los ciudadanos puedan ejercer su voto y otras actividades cívicas.

Sudáfrica regula la firma electrónica avanzada a través de su Ley "*Electronic communicatios and transactions Acta 2002*"[193], en donde se establecen los requisitos que deberán cumplir los prestadores de servicios de certificación por parte del gobierno. La firma es admisible para efectos jurisdiccionales, comerciales, y transacciones con organismos públicos, privados, instituciones y entre ciudadanos. La firma electrónica en Sudáfrica, si bien los proveedores de identidad se basan en la tarjeta de identificación inteligente para acreditar la identidad de la persona y expedir un certificado digital, no están vinculadas para suscribir un documento digitalmente como sucede en otros países.

3.5.2 La Isla Mauricio

La Isla Mauricio proporciona una identidad digital a sus ciudadanos a través de la Tarjeta de Identidad Nacional a cargo de la Oficina del Primer Ministro. En la tarjeta física de identidad cuenta con un chip que evita que otras personas alteren o usen

[193] Gaceta Gubernamental, "Electronic communicatios and transactions Acta 2002", Sudáfrica, 2002, Disponible en: https://www.gov.za/sites/default/files/gcis_document/201409/a25-02.pdf (Fecha de consulta: 15 de julio de 2020).

tarjetas perdidas o robadas, así como un código de barras para la lectura de los datos de identidad[194].

Los datos contenidos en la tarjeta se protegen electrónicamente y solo se pueden validar a través de la Autoridad de Certificación MNIS que garantiza la autenticidad de la identidad del individuo. Incluye una serie de características de seguridad visual que incluyen impresión de líneas entrecruzadas, microimpresión, impresión ultravioleta (UV) y utiliza un grabado láser para imprimir en diferentes capas de las tarjetas de identificación. Todas y cada una de las tarjetas Smart ID tienen un Número de Control de Tarjeta (CCN) único. Estas características de seguridad proporcionan el mecanismo para detectar cualquier caso de falsificación[195].

Entre los principales objetivos de la tarjeta de identidad digital es evitar llevar varios documentos a varias organizaciones, como bancos y otras agencias gubernamentales para probar la identidad y el comprobante de domicilio; proporcionar a los ciudadanos un servicio digital de calidad.

En cuanto a la firma electrónica, la Isla Mauricio regula la firma electrónica simple y avanzada a través de su ley "*The electrónic transactions Act 2000*"[196], la cual regula a los prestadores de servicios de certificación autorizado por el gobierno. La firma puede ser utilizada para comercio electrónico, servicios de gobierno, notarios y ante el tribunal de justicia. Por último, el sistema de identidad digital de la Isla Mauricio no se encuentra directamente vinculado a su firma electrónica.

3.5.3 Corea del Sur

Corea del Sur cuenta con una tarjeta de identificación móvil a cargo del Ministerio del Interior y Seguridad, a través de certificados digitales que se guardan en los dispositivos móviles. Corea del Sur está apostando por una identidad digital

[194] Portal de Gobierno de la República de Mauricio, ""Card layout and Design New ID Card", República de Mauricio, 2020, Disponible en: http://mnis.govmu.org/English/ID%20Card/Pages/Card-Design.aspx (Fecha de consulta: 15 de julio de 2020).
[195] Portal de Gobierno de la República de Mauricio, "Assurance", República de Mauricio, 2020, Disponible en: http://mnis.govmu.org/English/ID%20Card/Pages/Assurance.aspx (Fecha de consulta: 15 de julio de 2020).
[196] Parlamento Mauricio, "The electronic transactions Act 2000", República de Mauricio, 2000, Disponible en https://www.icta.mu/docs/laws/eta.pdf (Fecha de consulta: 15 de julio de 2020).

descentralizada a través del uso de *blockchain* para que sean las personas quienes tengan el control de sus datos.[197]. Como mecanismo de seguridad, los ciudadanos obtienen un certificado digital que se utiliza en su teléfono celular y con el cual pueden acceder a servicios digitales. Además, en las transacciones electrónicas se utiliza *blockchain*.

Corea del Sur regula la firma electrónica simple y avanzada a través de su ley "*Framework Act on electronic documents and transactions*"[198] y la "*Electronic Signature Act (ESA)*"[199], mediante el cual se regula a los prestadores de servicios de certificación autorizados por el gobierno. Aunque no está vinculada directamente a la tarjeta de identidad digital, la firma electrónica en Corea del Sur puede ser utilizada para firmar contratos comerciales, contratos de trabajo, contratos de arrendamiento y otros tipos comunes de contratos; procesos judiciales; actos de comercio y servicios gubernamentales[200].

3.5.4 Singapur

Singapur cuenta con una plataforma de identidad digital nacional denominada NDI que permite a los ciudadanos tener una identidad digital única para realizar transacciones en el sector público y privado, la cual fue desarrollada por la Agencia de Tecnología del Gobierno de Singapur. Esta plataforma cuenta con soluciones móviles mediante un token de software basado en criptografía. Los usuarios pueden utilizar su huella digital, reconocimiento facial o una contraseña de 6 dígitos. Su plataforma de identidad interopera con las bases de datos que contienen

---

[197] Ministerio del Interior y Seguridad, "Ampliación del servicio no presencial", 2020, Disponible en: https://www.innogov.go.kr/ucms/main/contents.do?menuNo=300135, Fecha de consulta: 15 de julio de 2020).

[198] Ley Korea, "Framework Act on electronic documents and transactions", 2016, Disponible en: http://www.law.go.kr/lsInfoP.do?lsiSeq=179518&lsId=002000&chrClsCd=010202&urlMode=engLsInfoR&viewCls=engLsInfoR#0000 (Fecha de consulta: 15 de julio de 2020).

[199] Korea La, "Electronic Signature Act (ESA)", Korea, 2017, Disponible en: https://elaw.klri.re.kr/eng_service/lawView.do?hseq=42625&lang=ENG (Fecha de consulta 15 de julio de 2020).

[200] Adobe, "Electronic Signature Laws & Regulations - South Korea", 2020, Disponible en: https://helpx.adobe.com/sign/using/legality-south-korea.html (Fecha de consulta: 19 de julio de 2020).

información sobre el certificado de nacimiento, pasaporte, la licencia de conducir, certificados educativos o incluso registros médicos[201].

Por su parte, la firma electrónica se regula por "*The Electronic Transactions Act* (ETA) (Cap 88)"[202], y la "*Electronic Transactions* (*Certification Authority*) Regulations 2010"[203], que regulan la firma electrónica simple y avanzada. En la primera ley se contempla el concepto de "firma electrónica segura" la cual es equivalente a la firma electrónica simple ya que se define como aquella firma que permite verificar que (i) se generó con datos bajo uso exclusivo de la persona que la usa; (ii) es capaz de identificar a dicha persona, y (iii) está vincula a un registro electrónico con el que pueda observarse si los datos asociados a la firma fueron modificados. No obstante, con base en la segunda norma, Singapur regula a los prestadores de servicios de certificación, quienes deben ser acreditados por la autoridad competente en el país, y generar una firma electrónica utilizando un certificado digital basado en una clave pública, lo que la convierte en una firma electrónica avanzada.

El caso de Singapur la firma electrónica se realiza a través de prestadores de servicios de certificación acreditados por el gobierno[204]. Igualmente, el gobierno de Singapur desarrollo, con base en su sistema de identidad digital, el servicio de firmado de documentos utilizando la plataforma la *National Digital Identity* con sus mecanismos de seguridad a través de un token de software. Esta plataforma cuenta con elementos de seguridad como lo es la criptografía (con el uso de un token) y biometría para acreditar la identidad de las personas. En Singapur, al igual que Dinamarca -como veremos más adelante- observamos una tendencia a contar con

---

[201] Smart Nation Singapur, "National Digital Identity (NDI), Singapur, 2020, Disponible en: https://www.smartnation.gov.sg/what-is-smart-nation/initiatives/Strategic-National-Projects/national-digital-identity-ndi (Fecha de consulta: 19 de julio de 2020).

[202] Smart Nation Singapur, "National Digital Identity (NDI), Singapur, 2020, Disponible en: https://www.signwithgreen.com/pdf/Singapore-Electronic-Transactions-Act.pdf (Fecha de consulta: 19 de julio de 2020).

[203] Singapure Statutes Online, "Electronic Transactions (Certification Authority) Regulations 2010", Singapur, 2010, Disponible en: https://www.imda.gov.sg/-/media/Imda/Files/Regulation-Licensing-and-Consultations/Acts-Regulations/Electronic-Transactions-Certification-Authority.pdf?la=en (Fecha de consulta: 19 de julio de 2020).

[204] Agencia del Gobierno de Singapur, "Conceptos clave", Singapur, 2020, Disponible en: https://www.imda.gov.sg/regulations-and-licensing-listing/electronic-transactions-act-and-regulations/controller-of-certification-authorities/key-concepts, (Fecha de consulta: 19 de julio de 2020).

una sola plataforma de identidad digital que cuente con los elementos criptográficos característicos de la firma electrónica avanzada. Por lo que vemos una tendencia al uso de la identidad digital basada en criptografía frente a la firma electrónica.

3.5.5 Estonia

Estonia cuenta con el sistema de tarjetas de identificación digital más avanzado del mundo. Su tarjeta nacional de identidad proporciona acceso digital a todos los servicios digitales -públicos y privados- de Estonia de forma segura. Su sistema de identidad digital se introdujo en el 2002 y casi el 100% de sus ciudadanos lo usa. En este caso, el proveedor de identidad es el gobierno de Estonia, a través de su registro civil.

En su cédula de identidad los ciudadanos cuentan con un chip cifrado de llave pública que permite probar su identidad digital en medios digitales. En 2007 las autoridades introdujeron una aplicación móvil que permite a los ciudadanos utilizar sus teléfonos como una forma de identidad digital evitando el lector de las tarjetas físicas con chip. Para validar la identidad digital se interopera con los datos asociados a pasaporte o licencia de conducir[205]. Además, Estonia es el primer país en ofrecer una residencia digital a extranjeros que cuentan en sus países una identidad digital a través de la *e-Residency*[206], que interoperar con los servicios de identidad de los países de la Unión Europea.

Estonia vincula la firma electrónica a través de su identidad digital (*ID-card*, *Mobile-ID or Smart-ID*) con la cual las personas pueden generar firmas digitales. A través de la aplicación de la identidad digital, en Estonia algunas empresas ofrecen el servicio de firma electrónica tales como SK ID *Solutions* y *Nortal*. Gracias a su tarjeta de identificación, Estonia tiene uno de los sistemas de firma digital más avanzados el mundo, la cual se trata de una tarjeta de identidad física a la que se

[205] e-Estonia, “we have built a digital society and we can show you how”, Estonia, 2020, Disponible en: https://e-estonia.com/, (Fecha de consulta: 19 de julio 2020)
[206] Republica de Estonia, “Become an e-resident), Estonia, 2020, Disponible en: https://e-resident.gov.ee/become-an-e-resident/ (Fecha de consulta: 19 de julio de 2020).

le integra un chip electrónico para la validación de identidad y generación de firmas electrónicas cualificadas[207].

3.5.6 Dinamarca

Dinamarca cuenta con el servicio *NemID* para proporcionar identidad digital a sus ciudadanos. Esta plataforma, consta de tres elementos: identificación del usuario, contraseña y una tarjeta de códigos para llevar a cabo transacciones de forma segura. Este último componente -tarjeta de códigos- es el que le da el carácter de firma electrónica cualificada.

Su plataforma *NemID*[208] presenta diversas funciones que son aplicables dependiendo las necesidades y requerimientos de los ciudadanos. Así, por ejemplo, además de servicios de identidad digital, cuenta con: (i) *NemID Code App*, mediante el cual se incorpora un código a la identidad digital que puede ser usado en servicios bancarios; (ii) *NemID for all services*[209] el cual constituye una firma digital pública válida por tres años que puede ser usada en sitios web públicos y privados. En Dinamarca sólo existe un proveedor del servicio de firma electrónica el cual está a cargo de una empresa privada llamada *Nets DanID A/S*[210] quien es responsable de la operación y mantenimiento de *NemID* en nombre del Ministerio de Finanzas.

En Dinamarca, desde el 2002 se utilizó la firma electrónica que permite realizar transacciones entre en los sectores público y privado. Posteriormente, en 2007, Dinamarca creó la aplicación *NemID* que funge hoy en día como su plataforma de identidad con la cual se pueden firmar digitalmente cualquier

---

[207] E-Estonia, “e-Identity”, Estonia, 2020, Disponible en: https://e-estonia.com/solutions/e-identity/ (Fecha de consulta: 19 de julio de 2020).

[208] Nemid, “NemID conditions for online banking and public digital signatures, v.7), 2020, Disponible en: https://www.nemid.nu/dk-en/about_nemid/nemid_conditions/NemID-rules-for-online-banking-and-public-digital-signature-version-7.pdf (Fecha de consulta: 20 de julio de 2020).

[209] Nem ID, “Use the same NemID for all services”, Dinamarca, 2020, Disponible en: https://www.nemid.nu/dk-en/help_for_nemid/use_one_nemid/, (Fecha de consulta: el 19 de julio de 2020).

[210] Nem ID, “Sitio web de proveedor de servicios”, Dinamarca, 2020, Disponible en: https://www.medarbejdersignatur.dk/ (Fecha de consulta: el 19 de julio de 2020).

transacción[211]. Con base en la sección 1 de la Ley Danesa de Contratos[212], en Dinamarca no se requiere necesariamente una firma por escrito para que un contrato sea válido. Los contratos son generalmente válidos si las partes, legalmente competentes, llegan a un acuerdo (verbal, electrónico o en papel). No obstante, en el caso de Dinamarca destaca que cuenta con una estrategia armonizada sobre identidad digital y firma electrónica al igual que Estonia[213].

3.5.7 Australia

Australia proporciona el servicio de identidad digital a través de un software descargable "*MyGovID*"[214] en el teléfono móvil de los ciudadanos, la cual está a cargo de la Oficina de Impuestos que tiene por objeto de crear una identidad digital que pueda ser utilizada para iniciar sesión en los servicios gubernamentales en línea y evitar nuevos aumentos en el costo del delito de identidad. Para acreditar la identidad, se necesita descargar la *app* en el teléfono móvil, proporcionar nombre, correo electrónico y fecha de nacimiento para obtener una "identidad básica" y acceder a ciertos tipos de servicios públicos[215]. Para acceder a una identidad "estándar" que permita acceder a todos los servicios gubernamentales, los usuarios deben proporcionar algún documento de identidad (licencia de conducir, pasaporte, certificado de nacimiento, visa, o tarjeta médica)[216].

Igualmente, la identidad digital se puede vincular a la empresa. La gestión de la identidad se realiza con un software que cuenta con estándares de seguridad y principios de privacidad, seguridad e integridad del gobierno australiano tales como: datos personales, acreditación con documentos de identidad física, supervisado por

---

[211] Nem ID, "NemID and Digital Denmark", Dinamarca, 2020, Disponible en: https://studycph.dk/nemid-digital-denmark/ (Fecha de consulta: el 19 de julio de 2020).
[212] Trans-Lex, University of Colage, "Danish Contracts Act", 2020, Disponible en: https://www.trans-lex.org/604900/_/danish-contracts-act/ (Fecha de consulta: el 19 de julio de 2020).
[213] Agency for Digitisation, Ministry of Finance, "National identity and signing", Dinamarca, 2020, Disponible en: https://en.digst.dk/digitisation/eid/ (Fecha de consulta: el 19 de julio de 2020).
[214] Gobierno de Australia, "An easy and secure way to prove who you are online", Australia, 2020, Disponible en: https://www.mygovid.gov.au/, (Fecha de consulta: 20 de julio de 2020).
[215] Gobierno de Australia, "How do I get set up?", Australia, 2020, Disponible en: https://www.mygovid.gov.au/how-do-i-get-set-up, (Fecha de consulta: el 20 de julio de 2020).
[216] Idem.

una autoridad de supervisión a cargo del gobierno y el consentimiento informado del usuario[217].

Australia regula el uso de la firma simple a través de su ley "*Electronic Transactions Regulatiosn 2000*"[218], la cual puede ser utilizada para el sector comercial, procesos judiciales, y transacciones con las empresas y el gobierno, aunque para este último se utiliza principalmente la identidad digital a través de *MyGovID*. Al tratarse de una firma simple no cuenta con proveedores de servicios de certificación y su uso tiene como base jurídico el consentimiento y voluntad de las partes.

3.5.8 Estados Unidos

Estados Unidos no cuenta con un sistema nacional de identidad digital. Sin embargo, cada uno de sus Estados desarrolla sus propios sistemas de gestión de identidad como *MILogin* en el estado de Michigan[219] o OHIID para el estado de Ohio[220], con los cuales los ciudadanos acceden a una identidad digital a través de un nombre de usuario y contraseña.

En Estados Unidos únicamente se regula la firma electrónica simple, en la "*Electronic signatures in global and national commerce Act*", y se define como cualquier "sonido, símbolo o proceso electrónico, adjunto o lógicamente asociado con un contrato u otro registro y ejecutado o adoptado por una persona con la intención de firmar electrónicamente[221].

---

[217] Gobierno de Australia, "myGovID Terms of use – User", Australia, 2019, Disponible en: https://www.mygovid.gov.au/mygovid-terms-of-use-user, (Fecha de consulta: el 20 de julio de 2020).
[218] Gobierno de Australia, "Electronic Transactions Regulations", Australia, 2000, Disponible en: https://www.legislation.gov.au/Details/F2019C00345, (Fecha de consulta: el 20 de julio de 2020).
[219] MILogin, "Sitio web de la solución de identidad del estado de Michigan", Michigan, 2020, Disponible en: https://milogin.michigan.gov/, (Fecha de consulta: 10 de julio de 2020).
[220] OH ID, "Portal de acceso a Ohio ID", Ohio, 2020, Disponible en: https://ohid.ohio.gov/wps/portal/ohid/business/login/!ut/p/z1/fY3BCoJAFEW_Zra-h46l7cYWRZAREenbhMo4iu-bIODW_n1CboLq7czmXCwQZ0FA8WlXYVg9FP3NOi6t_XIttssE0CuMlijQ4iyQ--ZxzuAAB_VEO_C3gjwiEHZDqdfm6E0MZRArlyFoaaby7mevG2nFaMW-TonPOU1qqXXqVvDL9NGj1ZyD5NGLuu3tswfwIviP2a/dz/d5/L2dBISEvZ0FBIS9nQSEh/ (Fecha de consulta: 10 de julio de 2020).
[221] Gobierno de Estados Unidos, Public Law, "Electronic signatures in global and national commerce Act", U.S, 2000, Disponible en: https://www.govinfo.gov/content/pkg/PLAW-106publ229/pdf/PLAW-106publ229.pdf (Fecha de consulta: 10 de julio de 2020).

Debido al sistema anglosajón de Estados Unidos, este no cuenta con una autoridad certificadora y permite el uso de aplicaciones de firma electrónica desarrolladas por particulares; el más emblemático es *DocuSign*[222].

La firma electrónica simple se creó principalmente para facilitar el comercio electrónico, pero también es aplicable para el sector público. Con base en la ley de Estados Unidos, la firma electrónica no puede ser utilizada cuando (i) una ley exija una solemnidad del acto jurídico; (ii) requiera la concurrencia de las partes, y (iii) en el derecho de familia. Respetando estas excepciones, la firma electrónica en Estados Unidos puede utilizarse en cualquier ámbito público, privado o incluso judicial.

En caso de controversia entre las partes, esta firma requiere adminicularse con otras pruebas para acreditar el consentimiento de las partes. También debe cuidarse las excepciones y contar con un registro electrónico que permita su generación y posterior consulta. De lo contrario se la restará valor probatorio. Algunos casos interesantes que podemos observar sobre la firma electrónica en Estados Unidos son: (i) Tribunal de quiebras de los Estados Unidos en California (2016)[223], y (ii) Tribunal de Apelación de California del Norte (2018)[224].

---

[222] Empresa estadounidense con sede en San Francisco, California, que permite a las organizaciones gestionar acuerdos electrónicos. Ofrece una aplicación llamada eSignature, como una forma de firmar electrónicamente en diferentes dispositivos. DocuSign eSignature cumple con la Ley de ESIGN de EE. UU. Y UETA, así como con el Reglamento eIDAS de la UE. Es una firma electrónica simple. No es una firma electrónica avanzada ni cualificada. Docusign, "Sitio web de la solución", Estados Unidos, 2020, Disponible en: https://www.docusign.com/ (Fecha de consulta: 10 de julio de 2020).

[223] Se utilizó DocuSign para solicitudes de quiebras, en donde la ley de la materia exige ciertas formalidades. Se utilizó el software en lugar de firmas originales, y el Tribunal determinó que si bien DocuSign es apropiado en muchos entornos comerciales no constituye un reemplazo de las firmas originales en documentos legales y similares, señalando que las firmas de DocuSign pueden manipularse o falsificarse fácilmente abriendo la puerta a que las personas se declaran en bancarrota para afirmar que no fueron los firmantes, lo que afectaría la integridad del sistema legal. Corte de los Estados Unidos, "Case 16-22134", Estados Unidos, 2016, Disponible en: https://www.govinfo.gov/content/pkg/USCOURTS-caeb-2_16-bk-22134/pdf/USCOURTS-caeb-2_16-bk-22134-0.pdf (Fecha de consulta: 11 de julio de 2020)

[224] En un caso sobre disputa sobre supuestas compras fraudulentas no reconocidas, Moonwalkers (compañía) afirmó que nunca firmó electrónicamente un contrato con Bank of America (institución financiera, quien acreditó, con registros de DocuSign, la fecha y hora en que se usó el correo electrónico de la compañía, en donde se acreditaba que dicha compañía vio el contrato, lo firmó el contrato y vio la versión final. Sin embargo, Moonwalkers no disputó los registros presentados por la institución financiera, sino simplemente afirmó que el firmante no estaba autorizado para hacerlo. El tribunal de primera instancia y el tribunal de apelación estuvo de acuerdo que las pruebas confirmaron que Moonwalkers ratificó el contrato como lo señaló la institución financiera. Pero aún así, le

Adicionalmente, debemos destacar que en algunos estados como Arizona[225] y Tenesse[226], se ha emitido legislación sobre el reconocimiento de *blockchain* como una firma electrónica, en donde se otorga valor probatorio a los documentos firmados a través de una cadena de bloques además de la firma electrónica simple.

3.5.9 Uruguay

Uruguay cuenta con una cédula de identidad digital desde 2015, que es un híbrido entre física y digital. Además de la foto, la firma y la huella dactilar, la Cédula de Identidad Digital incorpora dos chips: uno visible (con contacto), que contiene la Firma Digital, verificación de la huella digital y validación de identidad; y uno no visible (sin contacto), que contiene la información para documentos de viaje[227].

Este documento permite a los uruguayos hacer transacciones en todos los sectores, desde trámites con el Estado, firmar documentos con la misma validez que la firma autógrafa, hasta realizar operaciones bancarias y controles migratorios de forma automática[228]. Por su forma híbrida, este documento requiere un lector de tarjetas inteligentes que puede servir para la confrontación biométrica de huellas dactilares, autenticación y firma digital avanzada. El documento de identidad puede

---

otorgó la razón a la compañía al señalar que, si bien los registros de DocuSign son evidencia crítica, estos no son en sí mismos dispositivos de la validez o naturaleza vinculante con contrato. Find Law, "No. COA17-703", Carolina del Norte, 2018, Disponible en: https://caselaw.findlaw.com/nc-court-of-appeals/1893052.html (Fecha de consulta: 11 de julio de 2020)

[225] Ley de Transacciones Electrónicas de Arizona (El 29 de marzo de 2017) fue enmendada para agregar específicamente que (i) una "firma asegurada a través de la tecnología blockchain" es una firma electrónica, (ii) un "registro o contrato asegurado a través de la tecnología blockchain" como una forma o registro electrónico, y (iii) un "contrato inteligente" es legalmente válido y exigible. Gobierno de Estados Unidos, "44-7061", Estados Unidos, Disponible en: https://www.azleg.gov/ars/44/07061.htm (Fecha de consulta: 12 de julio de 2020)

[226] Ley Uniforme de Transacciones Electrónicas de Tennessee (22 de marzo de 2018) se modificó para (i) definir "tecnología de libro mayor distribuido" y "contrato inteligente", (ii) considerar registros asegurados a través de tecnología de libro mayor distribuido como un registro electrónico y (iii) considerar una "firma criptográfica que se genera y almacena a través de la tecnología de contabilidad distribuida ... para estar en forma electrónica y para ser una firma electrónica", Dickerson, Briggs, Harris, Yarbro, " PUBLIC CHAPTER NO. 591", Tennese, 2018, Disponible en: https://blockchain-lawguide.com/resources/Tennesee---Blockchain-Law---2018-03-22.pdf (Fecha de consulta: 12 de julio de 2020)

[227] Presidencia de la República, "Qué es la Cédula de Identidad Digital", Uruguay, 2020, Disponible en: https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/firma-digital/es-cedula-identidad-digital (Fecha de consulta: 13 de julio de 2020).

[228] Ídem.

utilizarse para hacer trámites por internet; firmar documentos; comprar por internet; transacciones bancarias y control migratorio[229].

La firma electrónica se regula por la Ley Nº 18.600, la Firma Digital[230], es en donde se contempla la firma electrónica simple y cualificada[231]. No obstante, sólo se reconoce el valor legal a la firma electrónica avanzada (cualificada), la cual puede utilizarse tanto en el sector público como privado.

Para la creación de la firma electrónica avanzada (cualificada), Uruguay cuenta con prestadores de servicios de certificación acreditados ante su Unidad de Certificación Electrónica[232]. Igualmente, reconoce a prestadores de servicios de certificación no acreditados, los cuales considera como aquellas personas, públicas o privada, nacional o extranjera, que expide certificados electrónicos en relación con la firma electrónica. Este último aspecto es relevante para el uso de la firma simple y el reconocimiento transfronterizo de firmas electrónicas como el caso de la Unión Europea. Igualmente, en Uruguay sólo puede reconocerse un certificado digital emitido por un prestador de servicios de certificación nacional o extranjero.

El caso de Uruguay es interesante, ya que, recordemos, cuentan con una cédula de identidad tanto física como digital expedida por su Dirección Nacional de Identificación Civil. Esta autoridad se encarga de gestionar la identidad física y digital, mediante una tarjeta que contiene un chip electrónico. Este chip es el que sirve para habilitar la firma electrónica que es expedida por un prestador de servicios de certificación acreditado, quien expide al ciudadano un certificado digital y un dispositivo físico de lectura del chip para la creación de su firma electrónica

---

[229] Idem.

[230] IMPO, Centro de Información Oficial, “Ley No. 18600”, Uruguay, 2009, Disponible en: https://www.impo.com.uy/bases/leyes/18600-2009 (Fecha de consulta: 13 de julio de 2020).

[231] La primera la define como los datos en forma electrónica anexos a un documento electrónico o asociados de manera lógica con el mismo, utilizados por el firmante como medio de identificación. La segunda, si bien la llama avanzada, lo cierto es que por sus características se trata de una firma electrónica cualificada, ya que, para su creación, además de contar con un certificado digital, requiere ser de un dispositivo cualificado para su creación; ambos proporcionados por un prestador de servicios de certificación. IMPO, Centro de Información Oficial, “Ley No. 18600”, Uruguay, 2009, Disponible en: https://www.impo.com.uy/bases/leyes/18600-2009 (Fecha de consulta: 13 de julio de 2020).

[232] Los prestadores de servicios de certificación acreditados en Uruguay son: Administración Nacional de Correos; Abitab S.A.; Ministerio del Interior; Administración Nacional de Telecomunicaciones; AGESIC, “Prestadores Acreditados”, Uruguay, 2020, Disponible en: https://www.gub.uy/unidad-certificacion-electronica/politicas-y-gestion/prestadores-acreditados, (Fecha de consulta: 14 de julio de 2020).

cualificada. Además, es importante señalar que, para la generación y validación de documentos electrónicos basados en firma electrónica cualificada, el gobierno de Uruguay, a través de su Agencia de Gobierno Electrónico y Sociedad de la Información (AGESIC), administra la "Plataforma de firma digital"[233] mediante la que cualquier persona puede suscribir y validar un documento electrónico con su firma electrónica.

3.5.10 Canadá

Para la gestión de su identidad digital, Canadá cuenta con el sistema *GBKey*[234] administrado por el gobierno, el cual es una credencial electrónica única (nombre de usuario y contraseña) que permite al usuario comunicarse de forma segura con los servicios gubernamentales en línea. Este servicio se otorga a aquellas personas que no tienen un socio bancario o prefieren no usar sus socios bancarios. Además, Canadá colabora con la empresa *SecureKey* como proveedor de identidad que permite a las personas autenticarse con sus credenciales bancarias[235]. La identidad digital en Canadá busca mejorar los servicios gubernamentales en línea.

Por otra parte, en Canadá se regula la firma electrónica simple a nivel federal por la Ley de Protección de Información Personal y Documentos Electrónicos[236], en donde se reconoce que una firma electrónica tiene validez jurídica en cualquier ámbito incluyendo el judicial. No obstante, por su conformación política en Quebec, cada provincia en Canadá ha adoptado la Ley Uniforme de Comercio Electrónico de 1999[237], en donde se define a la firma electrónica únicamente como información en

[233] AGESIC, "Firma digital", Uruguay, 2020, Disponible en: https://firma.agesic.gub.uy/, (Fecha de consulta: 14 de julio de 2020)
[234] Gobierno de Canadá, "What is GCKey?", Canadá, 2020, Disponible en: https://www.cic.gc.ca/english/helpcentre/answer.asp?qnum=794&top=23 (Fecha de consulta: 14 de julio de 2020).
[235] Gobierno de Canadá, "Using a Sign-in Partner", Canadá, Disponible en: https://www.canada.ca/en/revenue-agency/services/e-services/cra-login-services/sign-partners-help-faqs/using-a-sign-partner.html (Fecha de consulta: 14 de julio de 2020).
[236] Office of the Privacy commissioner of Canda, "The Personal Information Protection and Electronic Documents Act (PIPEDA)", Canadá, 2020, Disponible en: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/ (Fecha de consulta: 14 de julio de 2020).
[237] ULCC, CHLC, "Uniform Electronic Commerce Act Annotated 1999", Canadá, 1999, Disponible en: https://www.ulcc.ca/en/annual-meetings/359-1999-winnipeg-mb/civil-section-documents/1138-1999-

forma electrónica que una persona ha creado o adoptado para firmar un documento y que está adjunta o asociada con el documento.

Así, en Canadá podemos observar que se regula la firma electrónica simple en donde se establecen excepciones de uno en materias relacionadas con testamentos, fideicomisos o poderes notariales. Para validar una firma electrónica se requiere comprobar que (i) ha sido creada bajo el control total del firmante; (ii) es capaz de confirmar la identidad del firmante; (iii) es cien por ciento única y distintivo de la persona; (iii) se puede detectar cualquier cambio. Así, al igual que Estados Unidos, en Canadá se adopta un modelo legal abierto con la firma electrónica simple la cual es legalmente admisible a menos que se demuestre lo contrario. En estos países normalmente se cuente con empresas que ofrecen servicios de firma electrónica como *DocuSign*[238].

3.5.11 Argentina

En Argentina la identidad digital se gestiona a través de una plataforma desarrollada por el Estado "SID Sistema de Identidad Digital", que permite validar la identidad a distancia y en tiempo real con factores de autenticación biométrica. La plataforma está a cargo del Ministerio del Interior y la Secretaría de Innovación Pública. Para usar este servicio no es necesario acudir físicamente para la emisión de certificados digitales.

La plataforma interopera con prestadores de certificación y el Registro Nacional de Personas de Argentina. El usuario toma imágenes de frente y anverso de su cédula de identidad y una foto de su rostro, los cuales son enviados y validados con la base de datos del Registro Nacional de Personas y el sistema le devuelve la identificación al prestador de servicios de certificación y se le da acceso al ciudadano. Como elementos de seguridad, los datos biométricos nunca salen del Registro Nacional de Personas ni son almacenados en el dispositivo, y la

electronic-commerce-act-annotated#:~:text=The%20Uniform%20Electronic%20Commerce%20Act,relationship%20that%20may%20require%20documentation (Fecha de consulta: 14 de julio de 2020).

[238] Docusign, "Sitio web de la solución", Estados Unidos, 2020, Disponible en: https://www.docusign.com/ (Fecha de consulta: 14 de julio de 2020).

información se encuentra cifrada con algoritmos[239]. El SID en Argentina se puede utilizar para el sector financiero para fomentar la inclusión financiera.

La firma electrónica en Argentina se regula en la Ley 25.506 sobre Firma Digital[240], en donde se reconoce el uso de la firma electrónica simple y avanzada (denominada en su legislación como digital). La primera se define solamente como un conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación[241]. En cambio, la digital requiere de un certificado digital emitido por un "certificador licenciado" -prestador de servicios de certificación- que vincule los datos de la firma electrónica con su titular. El prestador de servicios de certificación puede ser una institución pública o privada acreditada por debidamente acreditada por su Jefatura de Gabinete de Ministros.

La firma electrónica puede ser utilizada tanto en el sector público como en el público. En Argentina, a diferencia de los países que hasta ahora hemos estudiado, separa la identidad digital de la firma digital. En Argentina, al igual que Uruguay, cuenta con una plataforma de creación y validación de documentos electrónicos suscritos con firma electrónica avanzada, denominada Plataforma de firma digital remota PFDR[242]. A través de esta plataforma se pueden crear certificados digitales en la nube dirigido para personas físicas. Este servicio está conectado con la plataforma de trámites públicos, en donde los ciudadanos pueden firmar y subir un documento PDF y firmarlo. Además, al igual que Uruguay y Chile, se reconoce en su legislación el reconocimiento de certificados digitales extranjeros, siempre y cuando (i) se cuente con un acuerdo de reciprocidad firmado por Argentina y el país

239 Gobierno de Argentina, "SID - Sistema de Identidad Digital", Argentina, 2020, Disponible en: https://www.argentina.gob.ar/interior/renaper/sid-sistema-de-identidad-digital, (Fecha de consulta: 15 de julio 2020).
240 InfoLEG, "Ley 25.506 de Firma Digital", Argentina, 2001, Disponible en: http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70749/texact.htm (Fecha de consulta: 15 de julio 2020).
241 Ídem.
242 Gobierno de Argentina, "Plataforma de Firma Digital Remota PFDR", Argentina, 2020, Disponible en: https://www.argentina.gob.ar/jefatura/innovacion-publica/administrativa/firmadigital/firmadigitalremota, (Fecha de consulta: 15 de julio de 2020).

de origen, o (ii) el certificado extranjero sea reconocido por un prestados de servicios de certificación acreditado en Argentina[243].

Otro aspecto para destacar es el uso de firma electrónica es en el Poder Judicial. Al igual que Uruguay, en Argentina, la Corte Suprema de Justicia de la Nación[244] aprobó el uso de la firma electrónico en procesos judiciales con base en la misma en la misma Ley 25.506 sobre Firma Digital. No obstante, se requiere utilizar el certificado digital emitido por el Poder Judicial de la Nación, y los documentos electrónicos judiciales son almacenados por la Dirección de Sistemas del Tribunal a través de su propia plataforma digital.

3.5.12 Chile

En Chile la identidad se regula a través del Registro Único Nacional administrado por con base en la Política de Identidad Digital Única (ClaveÚnica)[245], la cual constituye un servicio centralizado de autenticación para que las instituciones del Estado pongan sus trámites y beneficios a disposición de la población mediante sus plataformas digitales.

La identidad digital en Chile[246] (i) está basada en estándares abiertos *OpenId Connect* y *Oauth* 2.0, que permiten a las instituciones delegar el proceso de autenticación y autorización para que sus usuarios puedan ingresar a sus aplicativos y acceder a recursos protegidos de manera segura; (ii) es considerada uno de los pilares de sus Estrategia de Transformación Digital; (iii) permite firmar documentos electrónicos; (iv) permite ver el registro de acceso a la ClaveUnica del ciudadano; (v) interopera con las bases de datos del Servicio Nacional de Registro Civil e Identificación; (vi) está disponible en la nube, y (vii) el ciudadano genera una

[243] Prestadores de servicios de certificación en Argentina BOX CUSTODIA DE ARCHIVOS S.A.; DIGILOGIX S.A.; ENCODE S.A.; LAKAUT S.A.; OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN (ONTI); TECNOLOGÍA DE VALORES S.A.; MINISTERIO DE MODERNIZACIÓN. Gobierno de Argentina, "Autoridad Certificante Raíz de la República Argentina (ACRAIZ)", Argentina, 2020, Disponible en: https://www.argentina.gob.ar/jefatura/innovacion-publica/administrativa/firmadigital/acraiz, (Fecha de consulta: 15 de julio de 2020).
[244] Info Leg, CORTE SUPREMA DE JUSTICIA DE LA NACIÓN, "Acordada 11/2020", Ciudad de Buenos Aires, 2020, Disponible en: http://servicios.infoleg.gob.ar/infolegInternet/anexos/335000-339999/336345/norma.htm (Fecha de consulta: 15 de julio de 2020).
[245] Sitio de gobierno digital, "ClaveÚnica", Chile, 2020, Disponible en: https://digital.gob.cl/servicios/plataformas-compartidas/clave-unica, (Fecha de consulta: 15 de julio de 2020).
[246] Ídem.

contraseña única que funge como su identidad digital ante los trámites del sector público.

Por su parte, la firma electrónica se regula en la Ley 19799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma, que contempla la firma electrónica simple y avanzada[247]. Sólo existe una ley de firma electrónica avanzada que resulta aplicable a cualquier ámbito sea público, privado o judicial. Además, destaca que en Chile se establece la obligación de utilizar la firma electrónica avanzada en actuaciones de la administración pública. Para el sector público, la autoridad certificadora es la División de Gobierno Digital[248], adscrita al Ministerio Secretaría General de la Presidencia, quien expide los certificados digitales a las instituciones públicas, y creó la funcionalidad FirmaGob, la cual está dirigida para servidores públicos para la firma de documentos oficiales.

Al igual que la ClaveÚnica, la funcionalidad FirmaGob es considerada uno de los pilares de la Estrategia de Transformación Digital. En este sector, para la emisión y revisión de documentos electrónicos cuenta con la plataforma DocDigital[249].

En el sector privado, el Ministerio de Economía, Fomento y Turismo es la autoridad facultada para regular a los prestadores de servicios de certificación, quienes pueden proporcionar una firma electrónica simple o avanzada a los particulares. Para suscribir un documento digital, la firma electrónica se plasma en un PDF en donde su destinatario puede validar la firma electrónica emitida por un prestador de servicios de certificación autorizado[250].

---

[247] La primera se define como cualquier sonido, símbolo o proceso electrónico que permite al receptor de un documento electrónico identificar al menos formalmente a su autor. La segunda como aquella certificada por un prestador acreditado, que ha sido creada usando medios que el titular mantiene bajo su exclusivo control, de manera que se vincule únicamente al mismo y a los datos a los que se refiere, permitiendo la detección posterior de cualquier modificación, verificando la identidad del titular e impidiendo que desconozca la integridad del documento y su autoría. Biblioteca del Congreso Nacional de Chile, "Ley 19799, sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma", Chile, 2014, Disponible en: https://www.leychile.cl/Navegar?idNorma=196640 (Fecha de consulta: 15 de julio 2020).

[248] Sitio de gobierno Digital, "Firma Gob", Chile, 2020, Disponible en: https://digital.gob.cl/servicios/plataformas-compartidas/firma-gob (Fecha de consulta: 15 de julio 2020).

[249] Sitio de Gobierno Chile, "La nueva plataforma de Comunicaciones oficiales del Estado", Chile, 2020, Disponible en: https://doc.digital.gob.cl/ (Fecha de consulta: 15 de julio 2020).

[250] Los prestadores de servicios de certificación en Chile son E-CERT CHILE, ACEPTA.COM, E-SIGN S.A., CERTINET S.A., E-PARTNERS (Paperless), TOC, BPO-Advisors (IDok), Thomas Signe, Ministerio de Economía, Fomento y Turismo, "Entidades", Chile, 2020, Disponible en: https://www.entidadacreditadora.gob.cl/entidades/ . (Fecha de consulta: 15 de julio 2020).

En Chile también se regula el reconocimiento de certificados digitales extranjeros, siempre y cuando (i) cumpla con la legislación local, o (ii) se cuente con un convenio internacional ratificado y vigente por Chile. Hoy en día, Chile y Argentina cuentan con un acuerdo de reconocimiento de firmas electrónicas.

Para procesos judiciales, en Chile puede utilizarse una firma electrónica simple, la cual se conforma por un registro único nacional expedido por el registro civil, y la identidad digital proporcionada por la División de Gobierno Digital a través de ClaveUnica. Con estos elementos, a través de la Plataforma de la Oficina Judicial Virtual del Poder Judicial, se puede tramitar un juicio completamente en línea. A diferencia de Uruguay y Argentina, el Poder Judicial chileno admite la firma electrónica avanzada expedida por los prestados de servicios de certificación acreditados ante el Ministerio de Economía, Fomento y Turismo, para otorgar mayor seguridad a las transacciones judiciales electrónicas.

3.5.13 Brasil

Brasil se encuentra desarrollando una estrategia de identidad digital que tiene por objeto integrar las diversas credenciales de identidad (electoral, pasaporte y licencia de conducir) a través de su documento de identificación nacional DNI a cargo del Ministerio de Planificación, Desarrollo y Gestión, con el objeto de integrar diversos servicios y facilitar la vida cotidiana del ciudadano; integrar la bases de datos federales y eliminar viajes innecesarios; ahorrar tiempos de espera en fila; así como para la impresión de certificados y autenticación de documentos.[251]

El documento busca reunir los diferentes registros civiles en un solo documento a través de sistemas de interoperabilidad entre las bases de datos del gobierno federal, el poder judicial y el uso de datos biométricos del poder electoral[252].

[251] Agencia Brasil, “brasileños tendrán documento digital unificado de identificación”, Brasil, 2019, Disponible en: https://agenciabrasil.ebc.com.br/es/geral/noticia/2019-07/brasilenos-tendran-documento-digital-unificado-de-identificacion, (Fecha de consulta: el 20 de julio de 2020).

[252] Gobierno Federal, “Governo lança Documento Nacional de Identificação que dispensa apresentação de CPF e Título de Eleitor”, Brasil, 2018, Disponible en: https://www.gov.br/economia/pt-br/assuntos/noticias/planejamento/governo-lanca-documento-nacional-de-identificacao-que-dispensa-apresentacao-de-cpf-e-titulo-de-eleitor (Fecha de consulta: el 20 de julio de 2020).

Para garantizar la seguridad del documento de identidad se contempla lo siguiente: (i) la autenticación de los ciudadanos se realiza mediante un proceso de comprobación de claves de seguridad en un servidor protegido y con un chip integrado al documento de identidad; (ii) los datos que aparecerán en los dispositivos móviles de los ciudadanos serán encriptados, lo que también aumenta el resguardo de la información; (iii) estos datos en "códigos" sólo pueden ser correctamente leídos por quien posee una especie de "clave" secreta; (iv) la aplicación presentará un código QR que se creará de forma dinámica a cada nuevo acceso, manteniendo los datos de validación vinculados a la fecha ya la hora de su generación; (v) el documento de identidad mostrará en la esquina superior derecha, como marca de agua, un código de verificación que contiene 20 caracteres, precedido de la fecha y la hora en que se generó[253].

Brasil regula una firma electrónica avanzada a través del Decreto Número 3587[254], mediante el cual se encomendó al Ejecutivo Federal crear la infraestructura de claves públicas, aplicable a ciudadanos, gobierno, empresas y jueces[255], el cual está a cargo de SERPRO una empresa líder en el mercado de TI en el sector público[256].

3.5.14 Comparativo de sistemas de identidad y firma electrónica

Como observamos, los objetivos de contar con una identidad digital en los países son diversos pero todo ellos coinciden en tres aspectos: (i) proporcionar mejores servicios digitales a los ciudadanos; (ii) facilitar al ciudadano la gestión de su identidad a través de la integración en un sólo documento de las diversas

[253] Noticias electorales, "(Brasil) Identidad Digital Podrá Ser Emitida Para Todos Los Ciudadanos Registrados En El Programa Identidad Civil Nacional (Icn)", Brasil, 2019, Disponible en: https://www.noticiaselectorales.com/brasil-identidad-digital-podra-ser-emitida-para-todos-los-ciudadanos-registrados-en-el-programa-identidad-civil-nacional-icn/, (Fecha de consulta: el 20 de julio de 2020).
[254] Presidencia de la República, "Decreto número 3.587", Brasil, del 05 de septiembre de 2000, Disponible en: http://www.planalto.gov.br/ccivil_03/decreto/D3587.htm (Fecha de consulta: 20 de julio de 2020).
[255] SERPRO, "Certificación digital", Brasil, 2020, Disponible en: https://www.serpro.gov.br/clientes/certificacao_digital, (Fecha de consulta: 20 de julio de 2020).
[256] SERPRO, "El Serpro", Brasil, 2020, Disponible en: https://www.serpro.gov.br/menu/institucional/quem-somos, (Fecha de consulta: 20 de julio de 2020).

identidades como pasaporte, licencia de conducir, o credencial para votar, entre otras; y (iii) fomentar la economía digital.

También observamos que existen diferentes tipos de autoridades que intervienen en la gestión de la identidad, tales como las áreas de tecnología, los ministerios de seguridad, o los ministerios de gobierno; no obstante, observamos que en todos ellos existe interoperabilidad con los registros civiles nacionales, y en algunos otros es la autoridad responsable del registro civil la misma que provee el servicio de identidad digital.

Igualmente, nos percatamos que un tema importante en el diseño de la identidad digital se centra en dos aspectos, los tipos de datos utilizados y la seguridad de estos. En algunos casos como Estados Unidos, Nueva Zelanda y Chile se gestionan la identidad digital a través de un usuario y contraseña o clave única previa validación de identidad del usuario. En otros casos, se utilizan datos biométricos como reconocimiento facial o huellas dactilares que son protegidos mediante lectores integrados a una tarjeta física con chip y una clave como los casos de Uruguay, Estonia o Sudáfrica. Y otro grupo son aquellos que utilizan certificados digitales para acreditar la identidad en plataformas de internet y también en móviles.

Para facilitar más a detalle sobre los mecanismos de identidad, los invitamos a conocer el **ANEXO I,** sobre "*Mecanismos de identidad en el contexto internacional"* que resumen por país el nombre asignado a su mecanismo de identidad; institución responsable; mecanismo para acreditar la identidad, mecanismo de seguridad y sus principales objetivos.

Por otro lado, en cuanto a la firma electrónica observamos que países que ocupan los primeros lugares a nivel mundial en el EDGI como Estonia, Dinamarca, Singapur o Uruguay en América Latina, vinculan la identidad digital con la firma electrónica avanzada o cualificada. Es importante recordar que la firma electrónica nace del derecho mercantil internacional mediante el cual los países adoptaron su legislación nacional a la ley modelo de la CNUDMI. Por ello, es de distinguir que en el campo de la firma electrónica se deja principalmente su generación a través de medios electrónicos mediante los cuales las partes expresan su voluntad de

consentir un acto jurídico. Así, de la legislación analizada podemos observar lo siguiente:

- Todos los países cuentan sólo con una ley que regula el uso de la firma electrónica para cualquier sector, sea público, comercial, bancario o judicial; Países con un sistema jurídico anglosajón como Estados Unidos, Canadá, Nueva Zelanda o Australia regulan sólo el uso de la firma electrónica simple la cual es aplicable en cualquier acto jurídico ya sea público, comercial y judicial, la cual contempla excepciones de uso como el derecho de familia, testamentos o actos ante notarios.
- En otros países como Chile, Argentina, Uruguay, Corea del Sur o Singapur, regulan la figura del prestador de servicios de certificación, una persona jurídica que debe ser autorizada por una institución para prestar servicio asociados a la firma electrónica avanzada o cualificada en casos como Uruguay o Estonia.
- En América Latina podemos destacar el caso de Argentina, quien cuenta con una plataforma digital que permite a sus ciudadanos generar certificados en la nube los cuales pueden ser utilizados en trámites con entidades públicas y privadas, tales como relaciones impositivas, notificaciones judiciales, operaciones bancarias, contratos a distancia y documentos de comercio exterior[257].
- Países como Dinamarca, Estonia y Uruguay están dando un nuevo giro a la regulación de la identidad digital y firma electrónica. Desde el diseño de la identidad digital contemplan la integración de la firma electrónica que puede ser leída a través de dispositivos y/o sistemas a cargo de los prestadores de servicios de certificación, mediante la lectura de un chip digital contenido en la cédula única de identidad. Para facilitar la lectura de lo antes expuesto lo invitamos a consultar el **ANEXO II** del presente documento sobre "*Sistemas internacionales de firma electrónica"*, en donde se identifica por cada país analizado el tipo de fuma que, utilizada, el proveedor del servicio, los usos de la firma en dicho país y si se encuentra vinculada a su sistema de identidad digital.

[257] Jefatura de Gabinete de Ministros, "Plataforma de firma digital remota PFDR", disponible en https://www.argentina.gob.ar/jefatura/innovacion-publica/administrativa/firmadigital/firmadigitalremota, (Fecha de consulta: 20 de julio de 2020).

Como hemos analizado, debido a la cuarta revolución industrial, en donde los servicios digitales son cada vez más comunes entre los ciudadanos, ha llevado a que los Estados garanticen el derecho a la identidad de manera digital a través de diversos mecanismos. Ya sea a través de los registros civiles, o las unidades de gobierno digital, la interoperabilidad con las credenciales nacionales es un factor indispensable junto con los mecanismos de seguridad que se implementen para salvaguardar el derecho a la privacidad.

El número de transacciones electrónicas -gubernamentales, financieras, comerciales o judiciales- crece cada vez más acompañado de una sociedad más digital ante la necesidad global del distanciamiento social causado por COVID-19. La tecnología y los medios electrónicos nos han mostrado que no sólo nos ayudan a reducir costos y tiempos, sino también a ser una medida para combatir una emergencia sanitaria. No obstante, garantizar la confianza, la identidad y la seguridad jurídica de las transacciones electrónicas será un punto clave que los gobiernos deberán atender para prevenir posibles afectaciones a otros derechos o delitos cibernéticos como el fraude, el robo de identidad o de protección de datos personales.

Al respecto consideramos que contar con medidas de identidad digital sencillos, asequibles, seguros, e interoperables será un tema que debemos trabajar atendiendo las características de los registros de identidad en cada país, así como cuestiones técnicas, sociales, culturales, de infraestructura o de habilidades de la población para generar una identidad digital viable en el contexto nacional de cada Estado. Este elemento, junto con la firma electrónica que hace las veces de expresión de voluntad como lo hace una firma manuscrita-, serán aspectos que nos permitirán prevenir vulneraciones a los derechos humanos y a garantizar la seguridad jurídica de los derechos y obligaciones que se realizan mediante transacciones electrónicas.

Además de ello, y debido a que Internet no reconoce fronteras, consideramos que, si bien los modelos de identidad y firma deben atender el contexto nacional, también lo es que debe existir una base técnica y regulatoria definida a través de

modelos de cooperación internacional y regional para la validez y reconocimiento transfronterizo de identidades digitales y documentos firmados electrónicamente. Algunos aspectos relacionados con estos aspectos los podemos observar en los ejemplos de Chile, Argentina, el MERCOSUR, la ALADI, o la Unión Europea, que describiremos en el siguiente apartado.

3.6 Reconocimiento transfronterizo de identidad digital y firma electrónica

Algunos países como Chile, Uruguay o Argentina reconocer los certificados digitales emitidos en el extranjero conforme a su legislación de firma electrónica. Así, por ejemplo, Chile y Argentina cuentan con un acuerdo de reconocimiento muto de firmas digitales[258], a las cuales se les reconoce validez siempre que hayan sido emitidas por un prestador de servicios certificación que cumpla con: (i) estándares internacionales; (ii) que permita identificar al titular del certificado y al prestador de servicios de certificación; (iii) ser susceptible de verificación y que los datos permitan su identificación única; y (iv) tener la política de certificación bajo la cual fue emitido el certificado[259].

Además, se contempla que para el reconocimiento transfronterizo, Chile y Argentina deben armonizar aspectos operativos como control de acceso a servicios y perfiles, mecanismos de seguridad aplicados a datos personales, seguridad física, garantizar la continuidad del sistema, asegurar un sistema de acreditación y control de prestadores de servicios de certificación, contenido de los certificados, requisitos para los prestadores de servicios de certificación y procesos de validación entre otros aspectos críticos para la interoperabilidad de los sistemas en todas sus dimensiones. Las partes deben publicar en su sitio web las cadenas de confianza de los certificados digitales.

---

[258] Diario Oficial de la República de Chile, “Acuerdo de reconocimiento mutuo de certificados de firma digital con la República de Argentina”, Chile, 2019, Disponible en: https://documentos.camaraaduanera.cl/circ/2019/R212-19_DEC.%20N%C2%BA%20261,%20MIN.%20RR.%20EE.%20-%20Promulga%20Acuerdo%20Reconocimiento%20Mutuo%20de%20Certificados%20de%20Firma%20Digital%20con%20Argentina.%20ACE%20N%C2%B0%2016%20(D.O.).pdf (Fecha de consulta: 21 de julio de 2020).

[259] Ídem.

Por su parte, en el marco del acuerdo comercial del MERCOSUR, se contempla el Acuerdo de reconocimiento mutuo de firmas electrónicas[260], que tiene por objeto la digitalización de la economía, el intercambio de documentos fiscales y aduaneros, la firma de contratos entre empresas; trazabilidad de productos; reconocimiento automático de documentos electrónicos producidos a partir de certificados digitales. Con base en el citado acuerdo se establece que los Estados parte reconocerán los efectos jurídicos de la firma electrónica siempre y cuando hayan sido emitidos por un prestador de servicios de certificación bajo el sistema nacional de acreditación y control de cada país; responda a estándares reconocidos internacionalmente; contengan como mínimo la identificación del titular y el prestador de servicios de certificación, periodo de vigencia; ser susceptible de verificación; contemplar información necesaria para la verificación de la firma; e identificar la política de certificación bajo la cual fue emitido[261].

En el marco de la ALADI se reconoce la digitalización de certificados de origen a través del sistema digital de emisión de certificados de origen, basado en la constitución de una "Comunidad de Confianza" que garantice la autenticidad, la confiabilidad, la integridad y la aceptabilidad a través de la firma electrónica[262].

Adicionalmente, en América Latina, a través de la REDGEALC se cuenta con una línea de trabajo sobre firma digital y servicios transfronterizos que cuenta con tres ejes: firma digital transfronteriza, interoperabilidad transfronteriza y tecnologías emergentes[263]. A través de la iniciativa de "Bienes Públicos Regionales del BID" se aprobó el Programa para el fortalecimiento de las transacciones electrónicas transfronterizas en América Latina y el Caribe, con el que se busca generar capacidades y apoyar la instrumentación de la firma electrónica transfronteriza y los servicios digitales transfronterizos para acelerar su adopción en el entorno regional,

[260] Mercosur, "Reconocimiento de la eficacia jurídica del documento electrónico, la firma electrónica y la firma electrónica avanzada en el ámbito del MERCOSUR, MERCOSUR/gmc EXT./RES. Nº 37/06, 2006, Disponible em: http://www.sice.oas.org/trade/mrcsrs/resolutions/Res3706.pdf (Fecha de consulta 20 de julio de 2020).
[261] Ídem.
[262] ALADI, "Propuesta para la digitalización de certificados de origen en el ámbito de la ALADI, ALADI/SEC/dt 459/Rev.", 2004, Disponible en: http://www2.aladi.org/nsfweb/Documentos/459Rev2.pdf (Fecha de consulta 20 de julio de 2020).
[263] REDGEALC, "Firma digital y servicios transfronterizos", 2020, Disponible en: https://www.redgealc.org/lineas-de-trabajo/servicios-transfronterizos/, (Fecha de consulta 20 de julio de 2020).

fortaleciendo las transacciones electrónicas confiables y seguras como impulso a la economía digital y el gobierno digital en un marco de integración.

Por su parte, en la Unión Europea se contempla una regulación específica para la interoperabilidad de servicios de identidad y reconocimiento transfronterizo de firma electrónica. A través del Reglamento No. 910/2014, del Parlamento Europeo y del Consejo del 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[264], se reconoce la importancia del reconocimiento muto de la identificación electrónica, documento digital y firma electrónica con la finalidad de contribuir al mercado único digital de la Unión Europea. En términos del citado reglamento se establecen tres ejes para el reconocimiento transfronterizo de identidades y firmas electrónicas: interoperabilidad, seguridad y notificación de servicios de confianza de los gobiernos. Para ello, se estable que los Estado parte de la Unión Europea deben observar lo siguiente:

- La certificación de seguridad TI basada en normas internacionales (como ISO 15408 y métodos relacionados de evaluación y acuerdos de reconocimiento mutuo) es un importante instrumento para verificar la seguridad de dispositivos cualificados de creación de firmas electrónicas y debe fomentarse[265].
- Se reconocerá una identificación electrónica siempre que a) se encuentre en la lista publicada por la Comisión Europea, y b) cuente con un nivel de seguridad sustancial o alto, los cuales serán clasificados como sistemas de seguridad bajo, medio o alto[266].
- La notificación de los sistemas de identificación por parte de los Estados a la Comisión Europea deben contener lo siguiente: a) una descripción del sistema de identificación electrónica que incluya sus niveles de seguridad y el

[264] Reglamento No. 910/2014, del Parlamento Europeo y del Consejo del 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, Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32014R0910&from=PT, (Fecha de consulta 20 de julio de 2020).
[265] Ibídem, párrafo 55.
[266] Ibídem, artículo 6.

emisor o emisores de los medios de identificación electrónica en virtud de este sistema; b) el régimen de supervisión aplicable y la información sobre el régimen de responsabilidades respecto de la parte que expida los medios de identificación electrónica, y la parte que utilice el procedimiento de autenticación; c) la autoridad o autoridades responsables del sistema de identificación electrónica; d) información sobre la o las entidades que gestionan el registro de los datos únicos de identificación de la persona. La autenticación transfronteriza deberá ser gratuita cuando se realice en relación con un servicio en línea prestado por un organismo del sector público[267].

- La Comisión publicará en el Diario Oficial de la Unión Europea la lista de los sistemas de identificación electrónica notificados[268].
- Los sistemas nacionales de identificación electrónica deberán ser interoperables para lo cual se deberá establecer un marco de interoperabilidad que contemple principio de privacidad por diseño; normas técnicas internacionales; garantizar los datos personales; requisitos mínimos sobre niveles de seguridad; correlación entre los niveles de seguridad y los sistemas de identificación electrónica; requisitos mínimos técnicos de interoperabilidad; reglas de procedimiento y cooperación entre los Estado en el intercambio de información[269].
- Los servicios de confianza prestados por los prestadores de servicios de certificación serán reconocidos en un tercer país reconocidos legalmente[270].

El reconocimiento muto de identidad y firma electrónicas en la Unión Europea buscan fortalecer la economía digital, los servicios públicos y la asistencia sanitaria

[267] Ibídem, artículo 7.
[268] Actualmente, los países que han notificado a la Comisión Europea servicios de identificación electrónica son los siguientes: Alemanda, Italia, Croacia, Estonia, España, Lexemburgo, Bélgica, Portugal, Reino Unido, Chequia, Países Bajos, Eslovaquia, Letonia. Oficina de publicaciones de la unión Europea, "Sistemas de identificación electrónica notificados con arreglo al artículo 9, apartado 1, del Reglamento (UE) n.o 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior", Unión Europera, 2014, Disponible en: https://op.europa.eu/es/publication-detail/-/publication/9b18311a-2177-11ea-95ab-01aa75ed71a1 (Fecha de consulta: 19 de julio de 2020).
[269] Ibídem, artículo 12.
[270] Ibídem, artículo 14.

transfronteriza[271]. El reconocimiento transfronterizo se basa principalmente en los sistemas de identidad electrónicos a cargo de los países, quienes deben notificarlos a la Comisión Europea y cumplir con estándares de interoperabilidad y seguridad. Además, también se reconocen los certificados digitales emitidos por los prestadores de servicios de certificación siempre y cuando hayan sido notificados por cada Estado conforme a su legislación de la materia.

De esta forma, observamos que la identidad digital y la firma electrónica se encuentran vinculadas como elementos transformadores de servicios digitales y seguridad en las transacciones electrónicas. Si bien el desarrollo de la identidad digital depende del contexto nacional en cada país, a nivel internacional existe una armonización legal sobre la firma electrónica a través de la Ley Modelo de la CNUDMI sobre firma electrónica.

La identidad y firma digitales son elementos regulatorios y técnicos que contribuyen a la ejecución de medidas para salvaguardar los derechos humanos en medios electrónicos como el de protección de datos personales. Aunado a ello, elementos que permiten fomentar un entorno seguro en servicio digitales, transacciones comerciales y judiciales.

Por lo que consideramos que los gobiernos deben fortalecer no sólo el despliegue de infraestructura y de habilidades digitales como pilares centrales de la transformación digital, sino también deben fortalecer el diseño de normas que otorgue certeza jurídica en el derecho a la identidad a través de medios digitales y la regulación jurídica de transacciones electrónicas con base en la firma electrónica.

[271] Ibídem, párrafo 4.

Capítulo 4
Transformación Digital en México

Capítulo 4. Transformación Digital en México

Para efectos del presente trabajo analizaremos los apartados de identidad digital y firma electrónica en México. Lo anterior, con la finalidad de conocer su estado actual y poder proponer algunas acciones que consideramos podrían fortalecer su regulación jurídica actual en beneficio de la transformación digital en México. Nos parece importante analizar este tema con la finalidad de advertir la diversidad de identidades y firmas electrónicas que actualmente existen.

Además, identificaremos los principales programas y planes que actualmente México está implementando para afrontar los desafíos de la cuarta revolución industrial en temas vinculados con la infraestructura, habilidades y servicios digitales. Para ello, será importante destacar las funciones a cargo de las instituciones públicas competentes en materia de economía digital, servicios digitales, identidad, expediente electrónico, infraestructura, a partir del reconocimiento del derecho de acceso a las TIC e Internet en la CPEUM. Este nos permitirá identificar los puntos de conexión y coordinación que serán necesarios atender para implementar una estrategia de transformación digital que atienda las necesidades de brecha y desarrollo digital.

4.1. Regulación de acceso a las TIC e Internet

En México, en el artículo 6, inciso B, fracción I de la CPEUM se reconoce el derecho de acceso a las TIC, así como a los servicios de radiodifusión y telecomunicaciones, incluido el de banda ancha e internet[272]. A través del artículo 73, fracción XVII de la CPEUM se establece que el Congreso de la Unión está facultado para legislar en materia de vías generales de comunicación, TIC, radiodifusión, telecomunicaciones, incluida la banda ancha e Internet.

Así, en términos del artículo 3, fracción XXXII de la LFTR se define a internet como el "*conjunto descentralizado de redes de telecomunicaciones en todo el*

[272] Cámara de diputados del Gobierno, reforma publicada en el DOF, Art. 6 párrafo tercero de la CPEUM, México, 11 de junio de 2013, Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/1_080520.pdf (Fecha de consulta: 01 de febrero de 2020)

mundo, interconectadas entre sí, que proporciona diversos servicios de comunicación y que utiliza protocolos y direccionamiento coordinados internacionalmente para el enrutamiento y procesamiento de los paquetes de datos de cada uno de los servicios. Estos protocolos y direccionamiento garantizan que las redes físicas que en conjunto componen Internet funcionen como una red lógica única". Aunado a lo anterior, se define a Internet como una "*red global de redes que conecta a millones de usuarios en todo el mundo a través de muchas redes informáticas utilizando un sistema de direccionamiento común estándar simple y un protocolo de comunicaciones básico llamado TCP/IP (Protocolo de control de transmisión / Protocolo de Internet)*[273]*.*A través del citado protocolo, se emiten mensajes divididos en pedazos llamados paquetes que viajan a través de diversas rutas entre una computadora de origen y otra de destino[274].

Para garantizar el derecho de acceso a las TIC e internet se establece que el Ejecutivo Federal estará a cargo de la PIDU que consiste en un conjunto de planes y programas relacionados con infraestructura, accesibilidad y conectividad, TIC y habilidades digitales, así como los programas de gobierno digital, gobierno y datos abiertos, fomento a la inversión pública y privada en aplicaciones de telesalud, telemedicina y Expediente Clínico Electrónico y desarrollo de aplicaciones, sistemas y contenidos digitales[275].

Además, con el mismo objetivo de garantizar el derecho de acceso a las TIC e internet a toda la población, en los artículos 3, fracción XLIII, 9, fracciones III, V, VI, 15, fracción XXXI, 138, fracción VIII, 145, 146, 191, fracción VI, 202, 211, y 298, apartado B, fracción I de la LFTR, se regulan acciones de coordinación en materia de cobertura universal, cobertura social y acceso a las TIC e internet de banda ancha, entre las que podemos destacar las siguientes:

---

[273] MIT, Basic Internet Concepts, Disponible en: http://staff.um.edu.mt/mros1/wwww/basic_web_concepts.html, (Fecha de consulta: 02 de febrero de 2020).

[274] Protocolo de control de transmición TCP/IP, Disponible en: https://www.ibm.com/support/knowledgecenter/es/ssw_aix_72/network/tcpip_terms.html, (Fecha de consulta: 02 de Febrero de 2020).

[275] Artículo décimo cuarto transitorio de la CPEUM publicado en el DOF el 11 de junio de 2013. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/1_080520.pdf, (Fecha de consulta: 02 de febrero de 2020).

- La PIDU es un conjunto de programas y estrategias emitidos por el Ejecutivo Federal orientadas a brindar acceso a las TIC e Internet con especial atención a los grupos vulnerables, con el propósito de reducir la brecha digital.
- La SCT debe: a) coordinarse con el IFT para promover el acceso a las TIC, las telecomunicaciones, radiodifusión e Internet de banda ancha; b) planear, fijar e instrumentar programas de cobertura universal[276] y cobertura social; c) establecer programas anuales de banda ancha en sitios públicos hasta alcanzar la cobertura universal; c) definir los servicios de telecomunicaciones y radiodifusión que se incluirán en el programa de cobertura social, promoviendo los incentivos para la participación de los concesionarios; d) junto con el INEGI, definir y publicar los indicadores para medir la evolución de los servicios de telecomunicaciones en el territorio nacional; e) junto con el CONACYT, establecer mecanismos administrativos y técnicos para apoyar financiera y técnicamente a las instituciones públicas de educación superior y de investigación para la interconexión entre sus redes, formando una red nacional de educación e investigación.
- El IFT debe: a) realizar las acciones necesarias para contribuir al logro de los objetivos de la PIDU y de cobertura universal establecida por el Ejecutivo Federal; b) establecer a los concesionarios las obligaciones de cobertura geográfica, poblacional o social, de conectividad en sitios públicos y de conformidad con la cobertura universal en los términos de la LFTR.
- El título de concesión única debe contener como mínimo -entre otros aspectos-, los programas y compromisos de cobertura geográfica, poblacional o social, y de conectividad en sitios público a la cobertura universal que, en su caso, determine el IFT, para lo cual considerará anualmente las propuestas de la SCT conforme a los planes y programas respectivos[277].

[276] Acceso de la población en general a los servicios de telecomunicaciones determinados por la SCT bajo condiciones de disponibilidad, asequibilidad y accesibilidad. El objetivo de la cobertura universal es incrementar la cobertura de las redes y la penetración de los servicios de telecomunicaciones en zonas de atención prioritaria definidas por la SCT. “Espectro Radioeléctrico, Disponible en: http://www.ift.org.mx/sites/default/files/industria/espectroradioelectrico/radiodifusion/2016/6/apendiceda.pdf. (Fecha de consulta: 03 de febrero de 2020).

[277] Esta facultad del IFT que se plasma en los títulos de concesión única es sumamente relevante para colaborar con la cobertura universal en términos de los programas y planes que defina el IFT.

- El agende económico preponderante[278] está obligado a contar con presencia en los puntos de intercambio de tráfico de Internet en el territorio nacional, así como celebrar convenios que permitan a los proveedores de servicios de Internet el intercambio de tráfico de manera más eficiente y menos costosa en los términos que disponga el IFT.
- El Ejecutivo Federal, de conformidad con la EDN y el IFT debe promover el acceso de las personas con discapacidad a los nuevos sistemas y TIC, incluido el internet.

Derivado de lo anterior, es que actualmente se debate sobre si el internet debe ser un servicio público[279] -como el agua o la electricidad- a través del cual se garantice el interés general o colectivo. Por ejemplo, en algunos países como Chile y Colombia discute trabajan en sus legislaturas nacionales proyectos de reforma constitucional y legal para considerar a Internet como un servicio público; cuestión que cobró mayor relevancia con la pandemia por COVID-19[280].

En México podemos observar que, si bien no se reconoce internet como un

---

En dichos títulos se establece que "7.4. Con la finalidad de salvaguardar el acceso universal a los servicios de telecomunicaciones, el IFT podrá concertar la ejecución de programas de cobertura social, poblacional y conectividad en sitios públicos que serán obligatorios para el concesionario, atendiendo a la demanda de los servicios públicos que preste y considerando las propuestas que formule anualmente la SCT. *Cfr*. IFT, "Espectro Radioeléctrico, Disponible en: http://www.ift.org.mx/sites/default/files/industria/espectro-radioelectrico/radiodifusion/2016/6/apendiceda.pdf. (Fecha de consulta: 04 de febrero de 2020).

[278] Cualquiera que cuente con una participación nacional mayor al cincuenta por ciento, medido este porcentaje ya sea por el número de usuarios, suscriptores, audiencia, por el tráfico en sus redes o por la capacidad utilizada de las mismas. Artículo 262 de la LFTR. Los agentes económicos preponderante en México son Telmex, Telnor, Telcel, América Móvil, Grupo Carso y Grupo Inbursa, Cfr, "Pleno del IFT, 06 de marzo de 2014. IFT, Agentes económicos preponderantes, Disponible en: http://www.ift.org.mx/conocenos/acerca-del-instituto/historia/determina-ift-los-agentes-economicos-preponderantes. (Fecha de consulta: 04 de febrero de 2020).

[279] Como servicio público se entiende "en un sentido amplio como una actividad derivada de la función administrativa cuyos realizadores se apoyan en la obra pública existente, en su ampliación o en construcciones nuevas, para la continua, eficaz y regular satisfacción de un interés general o colectivo. Mientas que desde una óptica restringida… es una actividad derivada de la función administrativa cuyos realizadores poder ser entes públicos o privados, pero regulador los últimos por los primero, a fin de garantizar la debida satisfacción del interés general o colectivo, bajo los principios de continuidad. Mutabilidad e igualdad de los usuarios. Cfr. Yanome Yesaki, Mauricio, "El concepto de servicio público y su régimen jurídico en México", IIJ-UNAM, p. 698, Disponible en: https://archivos.juridicas.unam.mx/www/bjv/libros/6/2544/31.pdf, (Fecha de consulta: 04 de febrero de 2020).

[280] Senado Chile, Disponible en: https://www.senado.cl/internet-como-servicio-publico-comision-de-transportes-se-abocara-a/senado/2020-04-07/163923.html, (Fecha de consulta: 04 de febrero de 2020).

servicio público, sí se contempla que el Estado debe garantizar este servicio a toda la población. Es a través de la regulación de la concesión única que se contemplan obligaciones de cobertura universal a cargo de los concesionarios de telecomunicaciones con base en los lineamientos del IFT y el programa anual de cobertura universal de la SCT. Adicionalmente, como veremos más adelante, recientemente se creó en la *CFE Telecomunicaciones e Internet para Todos* que también busca proporcionar este servicio a los grupos más vulnerables. Igualmente, el derecho de acceso a las TIC se contempla en diversos programas y planes de gobierno con base en la PIDU que analizaremos en seguida.

4.1.1 Política de Inclusión Digital Universal

A nivel constitucional se establece que el Estado garantizará a la población su integración a la sociedad de la información y el conocimiento mediante una Política de Inclusión Digital Universal (PIDU) con metas anuales y sexenales, la cual está a cargo del Ejecutivo Federal e incluirán objetivos y metas vinculados con: 1) infraestructura; 2) accesibilidad y conectividad; 3) TIC y habilidades digitales; 4) gobierno digital; 5) gobierno abierto; 6) datos abiertos; 7) fomento a la inversión pública y privada en aplicaciones de telesalud, telemedicina; 8) expediente clínico electrónico, y 9) desarrollo de aplicaciones, sistemas y contenidos digitales, entre otros aspectos[281].

Igualmente, en el artículo 3, fracción XLIII de la LFTyR se establece que la PIDU "*es un conjunto de programas y estrategias emitidos por el Ejecutivo Federal orientadas a brindar acceso a las TIC, incluyendo el Internet de banda ancha para toda la población, haciendo especial énfasis en sus sectores más vulnerables, con el propósito de cerrar la brecha digital existente entre individuos, hogares, empresas y áreas geográficas de distinto nivel socioeconómico, respecto a sus oportunidades de acceso a las tecnologías referidas y el uso que hacen de éstas*[282]", en donde se

[281] Artículo décimo cuarto transitorio de la reforma constitucional de la CPEUM publicado en el DOF el 11 de julio de 2013, Disponible en: https://www.dof.gob.mx/nota_detalle.php?codigo=5301941&fecha=11/06/2013 (Fecha de consulta 05 de febrero de 2020).

[282] Ley Federal de Telecomunicaciones y Radiodifusión, Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFTR_240120.pdf. (Fecha de consulta 05 de febrero de 2020).

faculta al IFT para que realice las acciones necesarias para contribuir, en el ámbito de su competencia, al logro de los objetivos de la PIDU y cobertura universal establecidas por el Ejecutivo Federal; así como a los objetivos y metas fijados en el PND y los demás instrumentos programáticos relacionados con los sectores de radiodifusión y telecomunicaciones[283].

Es decir, en México, a nivel constitucional, se garantiza el derecho de acceso a las TIC y al Internet con base en la PIDU a cargo del Ejecutivo Federal, en donde el IFT está facultado para colaborar al logro de sus objetivos y metas. Actualmente, a través del PND 2018-2024[284] se establece como una de las principales metas en México proporcionar cobertura de Internet para todo el país. En el citado Plan se prevé que, con la instalación de Internet inalámbrico, se ofrecerá a toda la población conexión en carreteras, plazas públicas, centros de salud, hospitales, escuelas y espacios comunitarios. Además, se reconoce que el acceso a Internet será fundamental para combatir la marginación y la pobreza, así como para la integración de las zonas vulnerables a las actividades productivas.

Aunado a lo anterior, debemos destacar que en México existen diversas instituciones que cuentan con atribuciones sectorizadas y vinculadas con los objetivos constitucionales de la PIDU. Si bien aún no se cuenta con una agenda digital para el nuevo periodo presidencial, es de señalarse que los elementos que comprende una agenda digital como lo analizamos en el contexto internacional, en México existen principalmente once instituciones encargadas de liderar la transformación digital: CEDN; SFP; SCT; SEP; STPS; SSA; SE; SAT; SEGOB; CONAMER, y el IFT.

Para facilitar la identificación de cada una de las acciones a cargo de las autoridades mencionadas, en el **ANEXO III.** *Atribuciones institucionales sobre la transformación digital en México*, podemos identificar, en relación con temas vinculados con la transformación digital en México la (i) institución; (ii) atribución legal;

[283] Ibídem, artículo 3, fracción XXXI.
[284] Plan Nacional de Desarrollo 2018-2024, DOF 12 de julio de 2019, Disponible en: https://www.dof.gob.mx/nota_detalle.php?codigo=5565599&fecha=12/07/2019, (Fecha de consulta: 05 de febrero de 2020).

(iii) acciones planeadas o ejecutadas, y (iv) temas relacionados con la transformación digital y la PIDU[285].

Los elementos que regula cada una las instituciones descritas en el ANEXO III, reflejan los elementos para la transformación digital en México conforme al contexto internacional contemplado por la ONU y la UIT[286]. Estos elementos son evaluados a través del EDGI, en sus tres subíndices de: (i) infraestructura; (ii) competencias, y (iii) servicios digitales, mismos que son contemplados a través de la PIDU y en los diferentes planes y programas a cargo del Ejecutivo Federal. En los siguientes apartadas, conforme a los tres elementos del EDGI destacaremos las principales acciones de México.

4.1.2 Infraestructura

Proporcionar infraestructura de telecomunicaciones y acceso a internet a grupos sociales vulnerables es una prioridad para el gobierno mexicano que se reconocer como un derecho en términos del artículo 6 de la CPEUM. Observamos que son cuatro las instituciones encargadas para garantizar este derecho constitucional: la CEDN, la SCT, el IFT y la CFE Telecomunicaciones e Internet para todos.

La coordinación de sus funciones será clave para facilitar este derecho a grupos vulnerables y atender la brecha digital en México. Con base en el EDGI, México cuenta con un índice de infraestructura de telecomunicaciones del 0.5910; siendo la puntuación más alta del 1.000[287]. Además, con base en la *Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares*

[285] Véase: Anexo III. Atribuciones institucionales sobe la transformación digital en México.
[286] Visión, liderazgo, mentalidad; Marco institucional y regulatorio; Configuración y cultura organizacional; Pensamiento e integración de sistemas para la formulación de políticas y prestación de servicios; Garantizar la gestión estratégica y profesional de los datos para permitir la formulación de políticas basadas en datos, y acceso a información a través de datos abiertos; Infraestructura de TIC, asequibilidad y accesibilidad a la tecnología; Movilizar recursos y alinear prioridades, planes y presupuestos, incluso a través de asociaciones público-privado; Crear capacidad en el personal de la administración pública; Desarrollar capacidades sociales de inclusión digital y reducir la brecha digital, *Cfr*. ONU, Department of Economic and Social Affairs, "E-Government Survey 2020, Digital Government, op. cit., p. 18. Disponible en: https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2020-Survey/2020%20UN%20E-Government%20Survey%20(Full%20Report).pdf, (Fecha de consulta: 09 de febrero de 2020).
[287] Ibídem, p. 46.

2019[288], en México hay 80.6 millones de usuarios de Internet, que representan el 70.1% de la población de seis años o más, siendo que, del total de personas conectadas a internet, el 76.6% está concentrada en zonas urbanas y el 47.7% en zonas rurales. Por lo que para atender la brecha digital del 30% de la población que no cuenta con internet la función de las cuatro instituciones mencionadas será relevante.

Por ejemplo, la coordinación del *Programa de Cobertura Social de la SCT* y el proyecto de internet para todas a cargo de la CFE Telecomunicaciones Internet para todos, serán una acción clave para identificar y atender las brechas digitales de conectividad por grupo social vulnerable que permita, en colaboración con el IFT, la SCT, la CEDN y la CFE, diseñar políticas de conectividad inclusivas, equitativa y eficientes con los datos que se generen del referido programa, el cual contempla la identificación de grupos vulnerables sin internet y la georreferenciación de falta de infraestructura. Estos elementos sin duda apoyarán a la CFE Telecomunicaciones e Internet para Todos con la finalidad de llevar a cabo un despliegue eficiente de fibra óptica que facilite Internet en zonas y grupos poblacionales vulnerables.

Garantizar el derecho de acceso a internet es un mecanismo para garantizar otros derechos a través del uso de las TIC, en donde además consideramos importante contemplar las acciones a cargo de la Secretaría del Bienestar quien, con base en el artículo 32, fracción I de la LOAPF está facultada para:

> *"(…) fortalecer el bienestar, el desarrollo, la inclusión y la cohesión social en el país mediante la instrumentación, coordinación, supervisión y seguimiento de las políticas de: a) combate efectivo a la pobreza; b) atención específica a las necesidades de los sectores sociales más desprotegidos, en especial de los pobladores de las zonas áridas de las áreas rurales, así como de los colonos y marginados de las áreas urbanas; y c) atención preponderante a los derechos de la niñez, de la juven-*

[288] INEGI, Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares 2019, Disponible en: https://www.inegi.org.mx/programas/dutih/2019/, (Fecha de consulta: 09 de febrero de 2020).

tud, de los adultos mayores, de los pueblos indígenas y de las personas con discapacidad (…)[289].

4.1.3 Capital Humano

En cuanto al apartado de capital humano, podemos observar que el gobierno mexicano también cuenta con estrategias para el desarrollo de habilidades digitales, tanto en el sector educativo como laboral. No obstante, existen diferentes programas e iniciativas sectorizadas sobre habilidades digitales lideradas por la SEP, la STPS, la SE y la SCT.

Destaca el caso de la SEP quien, por mandato legal[290], está facultada para elaborar la Agenda Digital Educativa que comprende acciones para (i) capacitar a los docentes y estudiantes para desarrollar habilidades digitales; y (ii) fortalecer la educación a distancia a través de plataformas digitales y televisión educativa; esta última acción se fortaleció con el *Programa de capacitación en competencias digitales para docentes del Sistema Educativo Nacional,* con motivo de la pandemia por COVID-19.

Por su parte, la STPS cuenta a su cargo con el *Programa Jóvenes Construyendo el Futuro*[291], mediante el cual firmó un convenio de colaboración con Microsoft, el Instituto Mexicano de la Juventud y el Organismo Internacional de Juventud para Iberoamérica, con la finalidad de brindar capacitación en habilidades tecnológicas y competencias digitales a 40 mil jóvenes. También cuenta con el *Programa de Capacitación a Distancia para Trabajadores PROCADIST*, el cual constituye una "*plataforma educativa a distancia para trabajadores que ofrece el servicio de capacitación virtual gratuita, con el fin de contribuir al perfeccionamiento o desarrollo de competencias, capacidades y habilidades laborales"*[292].

---

[289] Artículo 32 LOAPF, Disponible en http://www.diputados.gob.mx/LeyesBiblio/pdf/153_110121.pdf, (Fecha de consulta 10 de febrero de 2020).
[290] Artículos 84 y 85 de la LGE, Disponible en: https://mexico.justia.com/federales/leyes/ley-general-de-educacion/capitulo-viii/seccion-2-del-recurso-administrativo/ (Fecha de consulta 10 de febrero de 2020).
[291] SCT, "Programa Jóvenes Construyendo el Futuro", Disponible en: https://jovenesconstruyendoelfuturo.stps.gob.mx/, (Fecha de consulta 10 de febrero de 2020).
[292] Gobierno de México, Trabajo, PROCADIST, Programa de Capacitación a Distancia para Trabajadores, Disponible en: https://www.procadist.gob.mx/portal/, (Fecha de consulta 10 de febrero de 2020).

La SE también contempla acciones para fortalecer las capacidades digitales en el sector empresarial a través de dos medias: (i) certificaciones con estándares internacionales, y (ii) mecanismos de vinculación entre instituciones académicas y la industria a fin de revisar los planes de estudio frente a las necesidades de los sectores productivos y la alta tecnología[293].

Además, la SCT tiene como una de sus estrategias sectoriales desarrollar habilidades y modelos para contribuir a la transformación digital de los individuos y las instituciones en México. Por ello, generó un proyecto sobre modelo de habilidades digitales las cuales clasifica en: (i) *básicas* -usar dispositivos, crear cuentas y perfiles, navegar en internet, localizar información, entre otras; (ii) *intermedias* -creación de contenidos, pensamiento computacional, creación de sistemas, programación de código, entre otras- y (iii) *avanzadas* - IA, emprendimiento digital, entre otras-.

Como observamos, la coordinación institucional entre estas cuatro entidades públicas (SEP, SE, STPS, SCT y CEDN), en materia de capital humano también será un tema relevante en México para armonizar y crear sinergias para el desarrollo de habilidades digitales en toda la población mexicana; con especial atención en grupos vulnerables. Por ejemplo, la SE, además de colaborar con las universidades y la industria, podría coadyuvar con la SEP para identificar y actualizar los programas de educación básica, media y superior con el objeto de mejorar el diseño de los planes de estudio basados en la oferta y demanda de profesiones del sector económico e industrial. Igualmente, puede generar sinergias con la STPS y la SCT para fortalecer un modelo de habilidades digitales que busque la certificación de profesionistas que demanda el sector industrial de nuestro país ante los desafíos de la era digital.

Las habilidades digitales sin duda será un sector estratégico en la búsqueda de la igualdad y equidad social. Al respecto, la OIT señala que el futuro del trabajo se caracterizará por una desigualdad creciente dentro de los países, por lo que sugiere a los encargados de formular políticas atender los desafíos que afrontan los

[293] SE, “Programa Sectorial 2020-2024, publicado en el DOF el 24 de junio de 2020, Disponible en: http://www.dof.gob.mx/nota_detalle.php?codigo=5595481&fecha=24/06/2020, (Fecha de consulta 20 de julio de 2020).

jóvenes ante la economía digital, la innovación, la IA, o la robotización, en donde la productividad y competitividad depende de la disponibilidad de elevadas competencias en ciencia, tecnología, ingeniería y matemáticas[294]

4.1.4 Servicios digitales

Proporcionar servicios digitales implica una diversidad de materias a analizar de manera integral. Además de la infraestructura de telecomunicaciones y el desarrollo de habilidades digitales, es importante contar con un marco regulatorio que otorgue seguridad jurídica, seguridad digital y confianza en los usuarios de las TIC. Es importantes la regulación y desarrollo de plataformas y estándares en temas como: identidad digital; firma electrónica; interoperabilidad; seguridad de la información; expediente electrónico (trámites y servicios, empresarial o médico); datos abiertos; gobierno abierto; innovación y tecnologías emergentes.

Estos elementos requieren tanto de su regulación jurídica como del uso de estándares comunes que faciliten el uso de medios digitales entre los ciudadanos y las instituciones públicas. Sin embargo, la sobre regulación y la falta de coordinación en estos rubros también puede traer consigo la duplicidad de funciones, incertidumbre jurídica y vulneración de los derechos humanos como la protección de datos personales o el derecho a la identidad.

Si bien México cuenta con acciones sobre estos rubros consideramos que es necesario fortalecer la armonización e integración de las atribuciones y disposiciones que emita: (i) la CEDN en materia de gobierno digital; (ii) la CONAMER en materia de expediente electrónico de trámites y servicios, interoperabilidad, seguridad de la información, digitalización, documento electrónico y firma electrónica en dicho expediente[295]; (iii) el SAT en materia de firma electrónica avanzada; (iv) la SE en materia de conservación de mensajes de texto y digitalización de documentos, así como la regulación de prestadores de servicios de certificación y firma electrónica avanzada; (v) la SEGOB en materia de identidad digital; (vi) la SFP en materia de

[294] Organización Internacional de Trabajo, “El futuro del Trabajo que queremos: un diálogo global”, p. 11, Disponible en: https://www.ilo.org/wcmsp5/groups/public/---dgreports/---cabinet/documents/publication/wcms_570288.pdf, (Fecha de consulta 10 de febrero de 2020).
[295] Lo anterior, de conformidad con el artículo 50 de la LGMR, Disponible en: http://www.diputados.gob.mx/LeyesBiblio/ref/lgmr.htm (Fecha de consulta: 12 de febrero de 2020).

datos abiertos y gobierno abierto; y (viii) la SSA en materia de expediente médico electrónico.

Como observamos en las estrategias digitales de los países que lideran el índice de servicios digitales en los cinco continentes, tales como Sudáfrica, Australia, Nueva Zelanda, Estonia, Dinamarca, Corea del Sur, Singapur, Estados Unidos, Canadá, Uruguay, Chile, Brasil y Argentina, consideran los elementos identidad digital, firma electrónica, interoperabilidad, seguridad, datos y servicios centrados en los ciudadanos como pilares de su transformación digital. Su regulación normativa y el uso de estándares técnicos, les ha permitido otorgar a sus ciudadanos seguridad y confianza en el uso de las TIC y servicios digitales.

4.1.5 Coordinación institucional para la transformación digital.

La transformación digital implica ejecutar una serie de acciones relacionados con temas como infraestructura digital; habilidades digitales; servicios digitales; interoperabilidad; seguridad; innovación; economía digital; datos personales y privacidad; marco normativo y diseño de estándares técnicos; identidad digital y firma electrónica; o tecnologías emergentes; brecha digital; transacciones electrónicas; o cooperación regional a través de tratados internacional como el T-MEC o el MERCUSOR que contemplan la regulación de dichos temas.

La gobernanza y armonización de dichos apartados resulta importante para evitar la duplicidad y orientar el desarrollo tecnología de manera inclusiva y equitativa que: (i) reduzca la brecha digital y se coordinen los esfuerzos en atender a los grupos vulnerables; (ii) garantizar un entorno seguro en el uso de las TIC ya sea en servicios públicos, transacciones comerciales, o procesos judiciales, y (iii) cooperación regional que favorezca los beneficios previstos en los tratados internacionales para toda la población con ayuda de la tecnología y programas de comercio exterior.

Es por ello por lo que el principio relativo a la *"función de los gobiernos y de todas las partes interesadas en la promoción de las TIC para el desarrollo"* previsto en el marco de la CMSI a través de la UIT y la ONU, resulta trascendental. En los países que analizamos, observamos que la política pública para la transformación digital está liderada por una autoridad que coordina el esfuerzo institucional y coordinación incluso con sectores privado, académico e internacional.

En México estas medidas están a cargo del Ejecutivo Federal y actualmente, como podrá consultarse en el **ANEXO III.** *Atribuciones institucionales en México sobre Transformación Digital*, a la fecha se cuenta con diversas acciones que permiten atender las brechas de infraestructura digital y de habilidades digitales para la población. Igualmente, para el desarrollo de servicios digitales e impulsar la economía digital, México cuenta con diversas acciones en materia de gobierno digital, mejora regulatoria, identidad digital, innovación, expediente y firma electrónicos los cuales están a cargo de diversas instituciones con atribuciones legales y líneas programáticas específicas.

No obstante, la coordinación, seguimiento y evaluación de los resultados de estas acciones será un reto institucional en donde el rol de la CEDN del Ejecutivo Federal será indispensable para visualizar y dar a conocer todos los resultados que se obtengan de la transformación digital en México. En este aspecto, las atribuciones de la Secretaría del Bienestar también deberán ser consideradas en materia de brecha e inclusión digital.

En este contexto, con la finalidad de identificar las acciones en materia transformación digital en México, y con el objeto de fomentar su coordinación, en el siguiente cuadro proponemos una agrupación de pilares, objetivos, acciones y autoridades que actualmente lideras la transformación digital en México con la finalidad de evitar duplicidad de funciones y otras que nos permitirán avanzar más firme y rápido ante los retos de cuarta revolución industrial[296]:

PILAR	OBJETIVO	ACCIONES	AUTORIDADES
INFRAESTRUCTURA DIGITAL	Atender la brecha digital y proporcionar infraestructura de telecomunicaciones en zonas rurales.	• Detectar las brechas de conectividad a través del Programa de Cobertura Universas y Social. • Generar datos sobre las brechas sociales y de desigualdad en México. • Vincular los datos del programa de Cobertura Universal y universal, con el apartado de cobertura social previsto en los títulos de concesión ubica. • Desplegar infraestructura de telecomunicaciones en comunidades rurales. • Generar programas de inclusión digital en colaboración con la SB en especial.	SCT IFT INEGI CEDN SB SFP CFE Telecomunicaciones Internet e Internet para Todos.

[296] Algunas de estas acciones ya se contemplan en normas constitucionales, legales, planes y programas de política pública que identificamos en el **ANEXO III.**

		• Generar una política de datos abiertos y participación ciudadano en la detección y diseño del despliegue de infraestructura digital.	
HABILIDADES DIGITALES	Proporcionar capacitación a la población en general, estudiantes, docentes, grupos vulnerables y pymes	• Generar programas de inclusión digital en colaboración con la SB en especial atención a pueblos originarios, comunidades rurales, adultos mayores, jóvenes, mujeres y niñas. • Impulsar la Agenda Educativa Digital a nivel nacional y en colaboración con las Universidades, industria y educación básica, media y superior. • Fortalecer las plataformas de enseñanza tanto en el ámbito educativo como laboral (PROCADIST). • Generar acciones de capacitación educativa y certificación profesional a distancia junto con universidades nacionales.	SEP SE CEDN STPS SB
SERVICIOS DIGITALES	Proporcionar servicio público seguros, interoperables y centrados en las personas.	• Impulsar el proyecto de identidad digital a cargo de la SEGOB • Contar con una política de interoperabilidad y seguridad • Colaborar con la CONAMER en el registro nacional de trámites y servicios. • Proporcionar servicios digitales que atiendan la necesidad de las personas y contemplen la experiencia usuaria. • Mantener el canal de atención físico de trámites gubernamentales. • Incorporar la firma electrónica del SAT en los servicios públicos que requieran formalidades especiales en el ámbito del derecho administrativo. • Contemplar el uso de la firma electrónica en el expediente electrónica de trámites y servicios y en el expediente médico electrónico. • Generar servicios digitales con base en estándares de accesibilidad web para personas con discapacidad visual. • Generar datos abierto y fortalecer mecanismos de participación ciudadana en colaboración con todas las instituciones del sector público. • Generar una política de datos abiertos que fomente la innovación y mejora constante del sector público. • Generar una plataforma nacional de interoperabilidad en el marco de la LGMR	CEDN CONAME INAI SAT SEGOB RENAPO SSA INE SFP IFT SEDENA SEMAR CERT
ECONOMÍA DIGITAL	Impulsar la economía digital, la innovación y los tratados comerciales internacional, con base en los apartados de economía digital en beneficio de la economía nacional.	-Fomentar la economía digital, el desarrollo productivo mediante el desarrollo de habilidades y la adopción de tecnologías emergentes en colaboración con las pymes. -Promover el uso de la infraestructura tecnológica del sector público (laboratorios de universidades y centros de investigación) para que los sectores productivos desarrollen propuestas de innovación y alta tecnología. -Fortalecer la oferta de capital humano especializado en manufactura de alta tecnología mediante la promoción de programas de certificación con estándares internacionales.	CEDN SE SEP STPS SER SAT CONACYT

		-Fortalecer las competencias y especialización del capital humano en los sectores productivos para mejorar la competitividad de la economía. -Generar vínculos comerciales en materia de economía digital con base en el TMEC, MERCOSUR y ALADI.	
MARCO NORMATIVO	Desarrollar un marco jurídico que proporcione confianza en el uso de las TIC	• Modificar la LGP para regular la identidad digital en México. • Reformar la CPEUM para establecer facultades exclusivas al Congreso de la Unión en Materia de firma electrónica avanzada. • Impulsar una iniciativa de Ley General de Firma Electrónica Avanzada • Elaborar un estándar nacional de interoperabilidad • Elaborar un estándar nacional de seguridad de la información. • Generar una guía para el diseño de servicios digitales con base en el principio de privacidad por diseño. • Generar un registro nacional de prestadores de servicios de certificación y de identidad nacional con la finalidad de fortalecer el reconocimiento transfronterizo de firmas digitales.	CEDN CONAMER INAI SEGOB SAT SRE INE SEDENA SEMAR CERT SE
COOPERACIÓN REGIONAL	Impulsar la economía digital con base en la cooperación regional y reconocimiento transfronterizo de formas electrónicas en el marco de los tratados de libre comercio suscritos por México.	• Colaborar con los grupos técnicos de trabajo en la negociación de tratados internacionales, para analizar y proponer la armonización de los tratados internacionales con base en el apartado de economía digital, TMEC, MERCOSUR, ALADI; entre otros.	CEDN SE SRE IFT SEGOB SAT CONAMER

Cuadro 4. *Coordinación institucional para la transformación digital de México*
Fuente: Elaboración propia.

La agrupación de las actividades que describimos puede favorecer a encausar las actividades de coordinación a cargo del Ejecutivo Federal a través de la CEDN. Consideramos que deben contemplarse de forma armonizada las atribuciones y funciones previstas actualmente en el marco constitucional y legal que mencionamos en el capítulo 4, así como en el PND 2018-2024 y en los programas sectoriales de las distintas secretarias de estado.

Sin embargo, en cuanto al marco jurídico consideramos necesario atender principalmente normas sobre identidad digital, firma electrónica, interoperabilidad, seguridad de la información y procedimiento administrativo que permitan otorgar certeza jurídica y técnica sobre el uso de las TIC. Así, consideramos que la coordinación y regulación sobre estos aspectos, junto con los proyectos de infraestructura

y habilidades digitales que ya se cuenta, nos permitirán avanzar hacia una transformación digital inclusiva, equitativa, segura y dinámica en beneficio del desarrollo social de nuestro país.

4.2 El derecho a la identidad en México

En México, al igual que el resto del mundo, este derecho se consagra en las leyes de población y de registro civil. En el párrafo octavo del artículo 4 de la CPEUM se establece que toda persona tiene derecho a la identidad y a ser registrado de manera inmediata a su nacimiento.

Para garantizar el derecho a la identidad existen los registros civiles en los cuales se registran hechos y actos jurídicos de las personas como el nacimiento, el matrimonio o la muerte. En nuestro país esta tarea se encomienda a la SEGOB a través del RENAPO, en colaboración con los registros civiles de los Estados. En términos del artículo 93 de la LGP, las autoridades locales deben integrarse al RENAPO mediante convenios de colaboración con la finalidad de recibir información relativa a los nacimientos, discapacidad y defunciones de personas.

Igualmente, las autoridades judiciales de los tres órdenes de gobierno y la SRE deben informar al RENAPO sobre las resoluciones judiciales que impliquen modificar los datos de registro de una persona, y sobre la expedición de documentos por autoridades consulares. Es decir, en términos de la LGP, las entidades federativas, el poder judicial de los tres órdenes de gobierno y el consulado mexicano, son auxiliares de la SEGOB en materia del RENAPO para garantizar el derecho a la identidad.

No obstante, si bien el derecho a la identidad se regula principalmente a través de la LGP mediante el RENAPO, México cuenta con diversas autoridades que expiden documentos de identidad tales como:

- El SAT a través de la firma electrónica avanzada;
- El INE con la credencial para votar;
- La SRE con el pasaporte;
- La SEDENA con la cartilla militar;
- La SEP con la cédula profesional;

4.2.1 Identidad RENAPO

El RENAPO se integra por tres bases de datos: (i) registro nacional de ciudadanos, (ii) el registro de menores de edad, y el (iii) catálogo de los extranjeros residentes en la República Mexicana[297]. En estas bases de datos se concentra prácticamente toda la información de personas físicas -mexicanos y extranjeros residentes-. Al incorporar a una persona en el RENAPO se le expide una clave denominada CURP el cual sirve para identificar individualmente a una persona[298], la cual se integra por 18 dígitos que contienen la primera constante y vocal del primer; la primera letra del segundo apellido y del nombre, fecha de nacimiento; sexo; lugar de nacimiento; y el carácter asignado por el RENAPO, quien cuenta con registro histórico y vigente de más de 190 millones[299].

Con la reforma del 22 de julio de 1992 a la LGP, se contempló la expedición de la Cédula de Identidad Ciudadana. En términos de los artículos 97 y 107 de la ley en comento, mediante este documento las personas pueden ejercer su derecho a la identidad. No obstante, a la fecha, en México no se expide la cédula de identidad ciudadana y únicamente se mantiene el CURP como clave de identidad a través del RENAPO. No obstante, cabe resaltar que en términos de la LGP se establece que los datos que debe contener dicha cédula de identidad son: nombre y apellido; CURP; fotografía; lugar y fecha de nacimiento; firma y huella dactilar; biométricos.

Por otro lado, actualmente a través del PND 2018-2024 se establece como una medida para la articulación de la seguridad nacional, la seguridad pública y la paz, construir las bases para la creación de un documento único de identificación nacional biometrizado. Así, conforme a las acciones previstas en el *Programa Sectorial de la SEGOB*[300], se encuentran (i) garantizar a todas las personas el derecho fundamental y primigenio a la identidad para que ejerzan sus demás derechos en

---

[297] Artículo 88 de la LGP, Disponible en: https://mexico.justia.com/federales/leyes/ley-general-de-poblacion/, (Fecha de consulta 13 de febrero de 2020).
[298] Ídem.
[299] SEGOB, CURP, Disponible en: https://www.gob.mx/segob/renapo/es/articulos/sabes-como-se-conforma-tu-curp?idiom=es (Fecha de consulta el 13 de febrero de 2020).
[300] Programa Sectorial de Gobernación 2020-2024, Disponible en: https://www.gob.mx/cms/uploads/attachment/file/563303/PSG_2020_-_2024.pdf (Fecha de consulta 13 de febrero de 2020).

condiciones de certeza y seguridad, a través del registro universal y oportuno de la población y por medio de un servicio nacional de identidad e identificación, y (ii) establecer normas, métodos y procedimientos encaminados a la expedición del documento único digital de identificación nacional biometrizado.

Esto resulta trascedente ya que, para el acceso a servicio digitales de forma segura, se requiere una gestión sólida de la identidad digital con mecanismo de seguridad y protección de datos personales. Por ello, es de destacarse que la estrategia de contar con un *documento único digital de identificación nacional biometrizado* se contemple dentro de las acciones de seguridad pública del PND 2018-2024[301] y en el Programa Sectorial de SEGOB para ofrecer una identidad digital en México.

Ahora bien, para poder realizar un modelo de gobernanza de la identidad digital en el marco de las atribuciones de la SEGOB a través del RENAPO, consideramos importante que se tenga en cuenta los antecedentes sobre identidad en México, los cuales describimos en seguida.

4.2.2 Identidad fiscal

Con base en el artículo 17-D del CFF se establece que cuando las obligaciones fiscales obliguen a presentar documentos éstos deberán ser digitales y contener una firma electrónica avanzada. Dicha firma es expedida por el SAT y los contribuyentes deberán acudir personalmente ante sus oficinas para obtenerla y acreditar su identidad. En términos del párrafo nueve del artículo 17-D del CFF, los datos de identidad que recabe el SAT formarán parte del sistema integrado de registro de población. Así, ante la autoridad fiscal, los contribuyentes acreditan su identidad digital mediante la firma electrónica avanzada.

La firma electrónica tiene una vigencia de cuatro años. El SAT recaba datos biométricos como huellas dactilares y fotografía de frente para expedir un certificado digital[302]. Dicho certificado cuenta con una llave pública y otra privada basadas en el uso de criptografía. En el caso de personas morales se vincula el nombre del

[302] Disponible en: https://www.sat.gob.mx/tramites/17074/obten-el-certificado-de-e.firma-para-tu-empresa-(antes-firma-electronica), (Fecha de consulta 13 de febrero de 2020).

representante legal. A mayo de 2020, el padrón fiscal cuenta con un total de 78,595,530 de contribuyentes de los cuales: 29,948,893 son personas físicas; 40,495 personas físicas-grandes contribuyentes; 46,439,874 asalariados; 2,157,440 personas morales, y 8,828 personas morales-grandes contribuyentes[303]. Es decir, en México 76,429,262 personas físicas cuentan con una identidad digital a través de la firma electrónica del SAT.

4.2.3 Identidad electoral

En materia electoral, el INE emite la credencial para votar en México a las personas físicas mayores de 18 años que les permite acreditar su identidad en los comicios y ejercer su derecho al voto. Para obtenerla, en términos de los artículos 136 de la LGIPE los ciudadanos tienen la obligación de acudir a las oficinas o módulos que determine el INE.

Conforme al artículo 159 de la LGIPE, la credencial de elector es una credencial física que contiene, entre otros datos, una clave de elector expedida por el INE, firma y huellas dactilares del ciudadano. Para 2020, el registro en el padrón electoral asciende a 90,036,367 ciudadanos[304]. Recientemente, el INE ofrece el trámite de la *Constancia Digital de la Credencial para Votar* que se ofrece a la ciudadanía ante el cierre de Módulos de Atención Ciudadana, con motivo de las medidas sanitarias tomadas ante la pandemia por COVID-19.

4.2.4 Identidad pasaporte

Con base en el *Reglamento de pasaportes y del documento de identidad y viaje*[305], las SRE está facultada para emitir el pasaporte el cual es un documento de viaje que se expide a los mexicanos para acreditar su nacionalidad e identidad, y solicitar

---

[303] Disponible en: http://omawww.sat.gob.mx/cifras_sat/Paginas/datos/vinculo.html?page=giipTipCon.html, (Fecha de consulta 14 de febrero de 2020).
[304] Disponible en: https://www.ine.mx/credencial/estadisticas-lista-nominal-padron-electoral/, (Fecha de consulta 14 de febrero de 2020).
[305] Publicado en el DOF el 05 de agosto de 2011, y su última reforma el 17 de agosto de 2016, Disponible en: https://sre.gob.mx/component/phocadownload/category/2marconormativo?download=205:repasdoc2540815 (Fecha de consulta 14 de febrero de 2020).

a las autoridades extranjeras permitan el libre paso, proporcionen ayuda y protección, el cual constituye un documento físico con un número de registro otorgada por la SRE. Durante el 2019 se expidieron 3,178,816[306].

4.2.5 Identidad militar

En términos del artículo 49 de la Ley del Servicio Militar, se establece que todos los mexicanos de edad miliar recibirán una tarjeta de identificación expedida por la SÉDENA en la que consten sus generales, huellas dactilares, clase a que pertenecen y si ha cumplido con el servicio de las armas o si está excluidos o aplazados. La SEDENA únicamente proporciona un documento físico con un numero de cartilla militar expedido sólo a hombres[307].

4.2.6 Identidad cédula profesional

Con base en el artículo 32 del Reglamento de la Ley *Reglamentaria del artículo 5º constitucional, relativo al ejercicio de las profesionales en la Ciudad de México*[308], se establece que una vez realizada la inscripción de un título profesional o grado académico se entregará, por medios electrónicos, la cédula profesional electrónica que contiene, entre otros datos, el CURP, datos del registro profesional, número de cédula, nombre del profesionista; nombre y clave de carrera; institución educativa; código QR de verificación; código de barras de verificación; cadena digital de cédula electrónica[309]. La emisión de la cédula profesional electrónica está a cargo de la SEP quien administra el Registro Nacional de Profesionistas[310].

---

306 Disponible en: https://datos.gob.mx/busca/dataset/produccion-mensual-de-pasaportes/resource/81d26c47-670d-4591-b0d6-2ab68e80eb85, (Fecha de consulta 14 de febrero de 2020).
307 Disponible en: https://www.gob.mx/sedena/acciones-y-programas/servicio-militar-nacional (Fecha de consulta 14 de febrero de 2020).
308 Publicado en el DOF el 05 de abril de 2018, Disponible en: http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LRArt5C_050418.pdf (Fecha de consulta 14 de febrero de 2020)
309 Disponible en: https://www.gob.mx/cedulaprofesional (Fecha de consulta 14 de febrero de 2020).
310 Disponible en: https://www.cedulaprofesional.sep.gob.mx/cedula/presidencia/indexAvanzada.action (Fecha de consulta 14 de febrero de 2020).

4.2.7 Licencia de conducir

En México, las licencias de conducir se otorgan por distintas autoridades. Existen las licencias de conducir a cargo de cada una de las 32 entidades federativas, y las de carácter federal a cargo de la SCT. A nivel federal se regulan de conformidad con el *Acuerdo por el que se establecen las categorías de la licencia federal de conductor, atendiendo al tipo de transporte y clase de servicio que se presta*[311], la expedición de las licencias tipo A[312], B[313], C[314], D[315], E[316] y F, en donde se solicita a los conductores requisitos como acta de nacimiento o identificación oficial expedida por el INE, Pasaporte, Cartilla Militar o Cédula Profesional que acredite tener ser mayor de edad, comprobantes de domicilio, y firma electrónica avanzada, entre otros[317].

Las licencias para conducir un vehículo particular se expiden por cada Entidad Federativa en donde, por ejemplo, en la Ciudad de México, a través de su Secretaría de Movilidad, se solicitan a los ciudadanos requisitos como identificación

[311] Acuerdo por el que se establecen las categorías de la licencia federal de conductor, atendiendo al tipo de transporte y clase de servicio que se presta Publicado en el DOF el 25 de febrero de 2016, Disponible en: https://www.dof.gob.mx/nota_detalle.php?codigo=5427046&fecha=25/02/2016, (Fecha de consulta 14 de febrero de 2020).

[312] Categoría “A”, Autoriza a conducir vehículos destinados para la prestación del servicio de autotransporte federal de pasajeros (excepto en la modalidad de transporte de o hacia puertos marítimos y aeropuertos federales) y de turismo (excepto en la modalidad de chofer-guía), y para el transporte privado de personas. Ibídem, artículo primero.

[313] Categoría “B”, Autoriza a conducir vehículos destinados para la prestación del servicio de autotransporte federal de carga, y para el transporte privado de carga, en sus diferentes modalidades, excepto los doblemente articulados, así como los que transportan materiales, residuos, remanentes y desechos peligrosos. Ídem.

[314] Categoría "C". Autoriza a conducir vehículos de dos o tres ejes (rabón o torton) destinados para la prestación del servicio de autotransporte federal de carga en sus diferentes modalidades, y para el transporte privado de carga en sus diferentes modalidades, excepto los que transportan materiales, residuos, remanentes y desechos peligrosos. Ídem.

[315] Categoría "D”. Autoriza a conducir vehículos destinados para la prestación del servicio de autotransporte federal de turismo en su modalidad de chofer-guía., Ídem.

[316] Categoría "E". Autoriza a conducir: a) Tractocamiones doblemente articulados (TSR y TSS) en todas sus variantes, destinados para la prestación del servicio de autotransporte federal de carga general, y para el transporte privado de carga general; y/o, b) Vehículos destinados para la prestación del servicio de carga especializada que transporta materiales, residuos, remanentes y desechos peligrosos, y para el transporte privado de los mismos.

[317] Ibídem, artículos segundo y quinto.

con fotografía (credencial para votar, cartilla militar, pasaporte, cédula profesional); comprobante de domicilio, y pago de derechos[318].

4.2.8 Identidad digital financiera

En el artículo 51 Bis 6 de la *Resolución que modifica las disposiciones de carácter generar aplicables a las instituciones de crédito*[319], se establece el procedimiento que deberán seguir las instituciones de crédito para validar la identidad de los usuarios de servicios bancarios de forma "no presencial", en donde destaca que: (i) deberán validar la existencia del CURP con el RENAPO; (ii) comprobar las fotografías de la credencial para votar el y rostro a fin de hacer reconocimiento facial entre estas; (iii) verificar la coincidencia de los datos de la credencial para votar en colaboración con el INE, con base en los datos relacionados con el código identificador de la credencia, nombre, año de registro, clave de elector, así como número y año de emisión; (iv) uso de datos biométricos para la autenticación de los usuarios de la banca.

Como observamos, en México un ciudadano puede acreditar su identidad a través de diversos documentos a cargo de distintas autoridades del orden tanto federal como local. Esto genera duplicidad de esfuerzos administrativos y de recursos económicos, así como que una persona deba cargar consigo diversas tarjetas físicas para acreditar su identidad; tales como la credencia para votar, la licencia para conducir, el pasaporte, o la cartilla militar. En este contexto, advertimos los siguientes aspectos sobre la identidad en México:

- Distintas autoridades solicitan a una misma persona los mismos datos personales como su nombre, domicilio, edad, sexo, fotografía y, en algunos casos, datos biométricos a través de las huellas dactilares. Es decir, los datos personales de una persona obras en distintas bases de datos gestionados por el

[318] Gobierno de la Ciudad de México, Secretaría de Movilidad, Trámites y Servicios, Licencias, Disponible en https://www.semovi.cdmx.gob.mx/tramites-y-servicios/vehiculos-particulares/automovil/licencias, (Fecha de consulta 14 de febrero de 2020).
[319] Resolución que modifica las disposiciones de carácter generar aplicables a las instituciones de crédito, publicada en el DOF el 29 de agosto de 2017, Disponible en: https://www.dof.gob.mx/nota_detalle.php?codigo=5495299&fecha=29/08/2017 (Fecha de consulta 15 de febrero de 2020).

mismo gobierno y, en otros casos, por las autoridades locales y el INE como órgano constitucional autónomo en materia electoral, tal como se observa en el siguiente cuadro:

Documento de identidad	Datos que contiene	Imagen
CURP[320]	• Nombre completo. • Fecha de nacimiento • Lugar de nacimiento • Sexo • Entidad federativa de nacimiento • Clave.	
Cédula de identidad ciudadana[321]	• Apellido paterno, apellido materno y nombre (s); • CURP; • Fotografía del titular; • Lugar de nacimiento; • Fecha de nacimiento; y • Firma y huella dactilar.	
Credencial para votar[322]	• Nombre completo • Fotografía • Domicilio • CURP • Clave de elector • Fecha de nacimiento • Sexo • Sección (Estado, municipio y localidad).	
Cédula de identificación fiscal[323] **del RFC.**	• Nombre completo • RFC (se conforma con base en el CURP para personas físicas) • Fecha de inicio de operaciones • Estatus en el padrón • Fecha de cambio de último estado • Domicilio fiscal • Actividad económica • Fecha de inicio • Régimen fiscal • Obligaciones	

320 CURP, gob.mx, Disponible en https://consultas.curp.gob.mx/CurpSP/html/informacione-curpPS.html, (Fecha de consulta 15 de febrero de 2020).
321 Artículo 107 de la LGP. A la fecha del presente trabajo aún no opera la cédula de identidad nacional en México.
322 INE, "Conoce tu credencial pada votar", Disponible en: https://www.ine.mx/conoce-tu-credencial-para-votar/, (Fecha de consulta 15 de febrero de 2020).
323 SAT, "Instructivo para la emisión de la cédula de identificación fiscal del RFC", M Disponible en: https://www.gob.mx/cms/uploads/attachment/file/29194/instructivo-para-la-emision-del-rfc.pdf, (Fecha de consulta 15 de febrero de 2020).

Cartilla militar[324]	• Nombre completo • Fotografía • CURP • Año y lugar de nacimiento • Nombre y apellidos de los padres • Estado civil • Ocupación • Grado máximo de estudios	
Cédula profesional	• Nombre completo • CURP • Número de cédula • Datos del registro profesional • Nombre y clave de la carrera • Nombre y clave de la institución educativa • Fecha de expedición	
Pasaporte[325]	• Nombre completo • Nacionalidad • Fotografía • Fecha de nacimiento • Lugar de nacimiento • CURP • Clave de país • Número de pasaporte	
Licencia de conducir federal[326]	• Nombre completo • CURP • Fotografía • Tipo de licencia • Vigencia • Número de licencia	
Licencia de conducir local	• Nombre completo • CURP • Fotografía • Tipo de licencia • Vigencia • Número de licencia • RFC • Tipo sanguíneo	

Cuadro 5. *Documentos de identidad en México*
Fuente: Elaboración propia.

- Es importante recordar que, desde el ámbito internacional, el derecho a la identidad se garantiza a través de los registros civiles, siendo que en México está a cargo de la SEGOB a través del RENAPO en coordinación con las 32 entidades federativas. El derecho a la identidad se vincula con otros derechos como a la

[324] SEDENA, "Corrección de los datos base de la cartilla de identidad del Servicio Militar Nacional", Disponible en https://www.gob.mx/sedena/documentos/corrige-los-datos-erroneos-de-tu-cartilla; (Fecha de consulta 15 de febrero de 2020).
[325] SRE, "Pasaporte mexicano", Disponible en: https://www.gob.mx/sre/acciones-y-programas/pasaporte-mexicano, (Fecha de consulta 15 de febrero de 2020).
[326] SCT, "Expedición de licencia federal de conductor modalidad nacional", Disponible en: https://www.gob.mx/tramites/ficha/expedicion-de-licencia-federal-de-conductor-modalidad-nacional/SCT1100, (Fecha de consulta 15 de febrero de 2020).

nacionalidad, la personalidad jurídica o el ejercicio del derecho al voto, a la salud o a la educación. Igualmente, una deficiente gestión del derecho a la identidad puede vulnerar otros derechos como el de protección de datos personales o el acceso servicios públicos.

- Contar con un marco sólido en materia de identidad no sólo permitirá garantizar otros derechos humanos sino también podrá facilitar al Estado diseñar mejores políticas públicas. Pensemos, por ejemplo, en la gestión de programas sociales en donde los apoyos proporcionados pueden duplicarse o proporcionarse debido a la diversidad de credenciales de identidad y bases de datos, lo cual va en contra de los principios de la gestión pública tales como economía, eficiencia y eficacia.
- Por otro lado, los servicios digitales demandan una gestión de identidad digital que sea sencilla, segura y asequible a toda la población, así como que cumpla con principios de seguridad, interoperabilidad y protección de datos personales.
- Ante la crisis sanitaria los servicios digitales tienen mayor demanda por los ciudadanos y aquellos trámites y servicios que, si bien pueden estar totalmente digitalizados para contribuir al distanciamiento social, si un ciudadano no puede acreditar su identidad en medios electrónicos le será complicado acceder al servicio en aquellos trámites que no se encuentren en línea e interoperables con la autoridad proveedora de la identidad digital.
- Es por ello por lo que destacamos las presente acciones en el Plan Sectorial de la SEGOB con la finalidad de trabajar un documento único de identidad digital. No obstante, debido al contexto histórico y nacional sobre la diversidad de credenciales de identidad, consideramos que dicha acción requerirá de una mayor certeza jurídica a través de la regulación de la identidad digital en la LGP. Así, aunque actualmente se contempla en la citada ley que la cédula nacional de identidad puede contener datos biométricos se advierte que coexistirán el resto de las identidades y prevalecerá la duplicidad de funciones y esfuerzos hasta en tanto no se logre un consenso nacional en la materia a través de la ley general de la materia.

- Por lo que hace a los datos biométricos, consideramos que su recolección deberá considerar los principios proporcionalidad, finalidad y privacidad por diseño. Además, se requerirá contar con mecanismos de infraestructura y seguridad de la información que permitan salvaguardar los derechos de identidad y de protección de datos personales. Consideramos que la plataforma digital que administre la identidad digital en México debe ser considerada una infraestructura crítica, ya que su vulneración afectaría la prestación de un servicio público y también la vulneración de otros derechos.

4.2.8 Hacia un modelo de identidad digital en México

México cuenta con diversos documentos de identidad. En el proceso de transformación digital, diversos países del mundo han buscado estrategias para garantizar el derecho a la identidad del entorno físico y digital. Este proceso ha implicado la adecuación y coordinación institucional en estrategias para garantizar la identidad digital de las personas en medios electrónicos.

Durante este proceso es importante considerar el contexto nacional en cuanto a las autoridades encargadas de gestionar la identidad, las bases de datos existentes y la forma en que una persona puede acreditar su identidad en medios digitales. En México, observamos que una persona puede acreditar su identidad a través de diferentes documentos tales como la credencial para votar, cartilla militar, cédula profesional o pasaporte. Contar con esa información en formato digital representa un reto en la transformación digital.

A nivel internacional existen diferentes modelos de identidad digital en donde resaltan aquellos que son gestionados por las autoridades del registro civil interoperables con instituciones del sector público y privado, y que integran una identidad física y digital en un solo documento. Tales son los casos de Estonia, Uruguay o Sudáfrica. Algunos otros gestionan su identidad con mecanismos propios de plataformas digitales a través de un usuario y contraseña como los casos de Dinamarca, Singapur o Chile; no obstante, son interoperables con el registro civil para autenticar la identidad de las personas. Otros, optan por la emisión de certificados digitales

para garantizar la identidad digital a través de la criptografía, como Dinamarca, Estonia o Corea del Sur.

En México se regula la cédula de identidad nacional en la LGP que contempla, entre otros aspectos, el uso de datos biométricos. Por ello, es de destacarse que recientemente, a través del PND 2018-2024 y el Programa Sectorial de Gobernación 2018-2024, se contempla llevar a cabo el *documento único de identificación nacional biometrizado*. Sin embargo, consideramos que el reto de su implementación dependerá de diseñar dicho documento considerado el contexto nacional sobre la identidad que actualmente de regula a través de diferentes documentos y normas. Se debe contemplan una estrategia nacional para la identidad digital en su conjunto con especial protección de los datos personales.

Para llevar a cabo el diseño del documento de identidad digital en México, vemos importante atender los principios de la UIT y el Banco Mundial para la creación del modelo nacional de identidad digital.

El pasado 03 de diciembre de 2020, se publicó en la Gaceta Parlamentaria de la Cámara de Diputados, el *Dictamen de la nueva Ley General de Población*[327]*,* sobre la que podemos destacar los siguientes puntos:

- Tiene por objeto establecer las bases de coordinación interinstitucional en materia de población y garantizar el derecho a la identidad.
- Señala que la SEGOB es la autoridad competente para emitir la Cédula Única de Identidad Digital y presidir el Sistema Nacional de Identidad Digital.
- Establece atribuciones a la SEGOB en los tres niveles de gobierno, tales como presta servicios de gestión de identidad; recaba información sobre la identidad de las personas; determinar métodos de identificación y procedimientos de registro de personas en la administración pública federal de los tres niveles de gobierno, y establecer las características de los documentos oficiales de identificación de los tres órdenes de gobierno.

[327] Cámara de Diputados, Gaceta Parlamentaria, Dictamen de la nueva Ley General de Población, 03 de diciembre de 2020, Congreso de la Unión, México, disponible para su consulta en: http://gaceta.diputados.gob.mx/PDF/64/2020/dic/20201203-V.pdf (Fecha de consulta 15 de diciembre de 2020).

- Para la implementación de la ley, las entidades federativas deben contribuir al Registro Nacional de Población y las legislaturas locales destinar recursos.
- La iniciativa de ley contempla cuatro figuras relevantes: a) El Registro Nacional de Población administrado por la SEGOB e integrado con los datos de los registros civiles, de la Secretaría de Relaciones Exteriores, el Instituto Nacional de Migración, y la Comisión Mexicana de Ayuda a Refugiados; a través de dicho registro la SEGOB establecerá los mecanismos de actualización, seguridad y uso de datos biométricos; b) la Cédula Única de Identidad Digital, el cual constituye el documento fundacional de carácter nacional que incluye datos biométrico; c) Documentos oficiales de identificación nacional, los cuales son expedidos por diversas autoridades en los tres órdenes de gobierno y se contempla su vinculación con la firma electrónica avanzada; d) Sistema Nacional de Identificación Nacional, es un servicio de interés público del Estado mediante el cual se puede validar, consultar, verificar y acreditar la identidad de una persona a través de medios digitales; las personas privadas pueden usar este servicio mediante el pago de derechos.
- Como comentarios a la iniciativa de la ley, consideramos relevante contemplar las facultades del Congreso de la Unión para legislar en esta materia conforme al artículo 73 de la Carta Magna, toda vez que establece atribuciones de coordinación en los tres niveles de gobierno, siendo que actualmente esa colaboración se realiza entre la SEGOB y los registros civiles mediante convenios. No obstante, en la iniciativa de ley se prevé interacciones con cualquier autoridad en los tres niveles de gobierno e, incluso, sobre el tema de recursos a través de las legislaturas locales.
- La recolección de los datos biométricos debe considerarse los principios de proporcionalidad y finalidad, en el entendido que dichos datos son considerados como sensibles y, por ende, su recolección debe ajustarse a ciertas pautas. Un ejemplo sobre regulación en este punto es el artículo 9 del RGPD, y 7, 22, 75 y 75 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; en donde se considera la prohibición de

recolectar datos biométricos salvo excepciones particulares en el caso europeo y en la mexicana realizar una evaluación de impacto del tratamiento de dichos datos personales.

Así, en el siguiente cuadro enlistamos el principio, su descripción y aportamos algunas consideraciones para México para el diseño del documento de identidad digital se requiere considerar los siguientes aspectos conforme a los principios de un MNID propuestos por la UIT:

En el contexto de la transformación digital, un modelo de identidad digital en México debe prestar especial atención a aspectos como la privacidad por diseño, la protección de datos personales, la interoperabilidad, la seguridad de la información, y el contar con una plataforma y sistemas robustos para garantizar la gestión de la identidad digital. De esta forma, consideramos los siguientes ejes pueden ayudar a la SEGOB a diseñar un documento de identidad digital en México que atienda los desafíos de la cuarta revolución industrial:

- Privacidad por diseño para salvaguardar el derecho a la protección de datos personales, en donde consideramos será importante trabajar juntamente con el INAI en este aspecto, en donde se debe contemplar los principios de proporcionalidad y finalidad, así como la experiencia de la Unión Europea en cuanto a datos biométricos de conformidad con el artículo 9 del RGPD, y 22, 75 y 75 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- Identificar e integrar las identidades existentes en todo el país a cargo del INE, la SRE, el SAT, la SEP, SEDENA, y las entidades federativas a través de las licencias de conducir, para lo cual será importante modificar la LGP que considere un modelo nacional de identidad nacional con base en el principio de legalidad.
- Estándares de interoperabilidad y seguridad de la información que otorgue confianza y seguridad tanto a las instituciones que pueden compartir bases de datos como para los usuarios en el cuidado de sus datos personales, considerando además el uso de datos biométricos. Se debe considerar a la plataforma nacional de identidad digital como infraestructura criticas toda vez

que su vulneración afectaría los servicios públicos basados en identidad digital y la afectación de derechos humanos en caso de un ciberataque o fuga de información.

- Considerar la interoperabilidad con la firma electrónica, en donde se opte por una identidad digital a través de certificados digitales como pasa con los países que ocupan los primeros lugares del mundo en desarrollo digital como Estonia, Dinamarca o Corea del Sur.
- Contar con un plan de inversión para el soporte y seguridad de la infraestructura de la plataforma que administrará la información de la cédula de identidad en un modelo de escala.
- Colaborar con la CONAMER en el diseño de una norma nacional de interoperabilidad, y con las áreas de seguridad nacional y seguridad públicas en un estándar nacional se de seguridad. Para ello, será necesario una reforma ya sea a la LGP o la LGMR conforme al principio de legalidad.
- Considerar los principios del modelo de identidad nacional de la UIT y el Banco Mundial.
- Analizar el contexto nacional con la finalidad de evitar la duplicidad de funciones, ahorrar costos de operación, contar con calidad de los datos registrados y, sobre todo, contar un marco jurídico sobre este aspecto tan importante que impacta no sólo en el derecho a la identidad sino también a otros derechos humanos.
- Algunos modelos de identidad digital que consideramos pueden aportar algunas ideas al modelo mexicano son los casos de Argentina, Uruguay, Singapur, Estonia, Dinamarca, Corea del Sur y Chile.

4.3 La firma electrónica en México

En México, la firma electrónica se regula por diversas normas jurídicas. Primero, se reguló a través del CCOM en el año 2003, con la finalidad de armonizar los actos de comercio electrónico y el uso de la firma electrónica en el derecho mercantil internacional con base en la Ley Modelo de la CNUDMI. Posteriormente, se reguló para la APF desde el 2012 con la LFFEA, y para cada una de las 32 entidades

federativas desde el año 2006 encontramos regulación, y en el ámbito fiscal a través del CFF desde el año 2004.

Con la pandemia por COVID-19, el uso de la firma electrónica cobreó relevancia en el proceso judicial. Si bien el PJF ya contaba con regulación desde el 2013, recientemente los poderes judiciales del ámbito local han comenzado a emitir su propia normatividad o políticas para el uso de firma electrónica. La normatividad sobre firma electrónica avanzada en México es muy amplia en comparación con otros países que sólo cuentan con una sola ley aplicable para cualquier sector (privado, público o judicial), basada en la Ley Modelo de la CNUDMI sobre firma electrónica.

México, en cambio, actualmente cuenta con más de 36 leyes sobre firma electrónica avanzada, tales como: (i) la LFFA, (ii) 23 leyes locales de firma electrónica[328]; (iii) la del PJF; (iv) la del CFF; (v) la del CCOM[329], y recientemente (vi) la diversa legislación y políticas de firma electrónica emitidas por los poderes judiciales de los estados.

4.3.1 Comercio electrónico

La firma electrónica en México se reguló por primera vez en el CCOM [330]; lo anterior, atendiendo a un proceso de armonización sobre comercio y firma electrónicos con base en las leyes modelo de la CNUDMI que revisamos anteriormente. En el ámbito del CCOM se regula tanto la firma electrónica simple como la firma electrónica avanzada.

La firma electrónica simple se define como *los datos en 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*

[328] Véase **ANEXO VI**. Legislación de firma electrónica en México.
[329] Anexo Único sobre legislación en materia de firma electrónica avanzada en México. Disponible en: https://www.dof.gob.mx/nota_detalle.php?codigo=5522027&fecha=09/05/2018 (Fecha de consulta 19 de febrero de 2020).
[330] Código de Comercio, y su reforma publicada en el DOF el 29 de agosto de 2003, DECRETO por el que se reforman y adicionan diversas disposiciones del Código de Comercio en Materia de Firma Electrónica, Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/3_301219.pdf (Fecha de consulta 19 de febrero de 2020).

en el Mensaje de Datos, y que produce los mismos efectos jurídicos que la firma autógrafa, siendo admisible como prueba en juicio[331]. Mientras tanto, para la firma electrónica avanzada, en términos del artículo 97 del CCOM, se establece que debe contener como requisito que: (i) los datos de creación de la firma corresponden exclusivamente al firmante; (ii) los datos de creación de la firma estaban bajo el control exclusivo del firmante, y (iii) es posible detectar cualquier alteración posterior de la firma y del mensaje de datos.

Con la reforma al CCOM del 07 de abril de 2016, se introdujo que la figura de prestador de servicios de certificación[332] la desempeñan los notarios o corredores públicos; las personas morales de carácter privado, y las instituciones públicas conforme a las leyes aplicables. En términos del artículo 101 del CCOM, los prestadores de servicios de certificación están autorizados para verificar la identidad de los usuarios y vincularlos con los medios de identificación electrónica; comprobar la integridad y suficiencia del mensaje de datos y verificar la firma electrónica de quien firma; llevar un registro de los elementos de identificación del firmante; expedir sellos digitales de tiempo; constancias de conservación de mensajes de datos; y digitalización de documentos.

En el marco del CCOM, además de la firma electrónica avanzada se regulan las características que deben cumplir la conservación de mensajes de datos[333] y la digitalización de documentos físicos[334]. Estos conceptos se regulan por la norma ofi-

---

[331] Artículo 89 Código de Comercio, Disponible en: https://mexico.justia.com/federales/codigos/codigo-de-comercio/libro-segundo/titulo-segundo/capitulo-i/ (Fecha de consulta 19 de febrero de 2020)

[332] Los prestadores de servicios de certificación se reglamentan en términos del Reglamento del Código de Comercio en materia de prestadores de servicios de certificación, publicado en el DOF el 19 de julio de 2004 (sin reformas), Disponible en: http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_CComer_MPSC.pdf. Actualmente, los prestadores de servicios de certificación son ADVANTAGE SECURITY, S. DE R.L. DE C.V. ; PSC WORLD, S.A. DE C.V.; CECOBAN, S.A. DE C.V.; EDICOMUNICACIONES MÉXICO, S.A. DE C.V.; SEGURIDATA PRIVADA, S.A. DE C.V.; LEGALEX GS, S.A. DE C.V., Disponible en: http://www.firmadigital.gob.mx/directorio.html (Fecha de consulta 19 de febrero de 2020).

[333] Un mensaje de datos es la información generada, enviada, recibida o archivada por medios electrónicos, ópticos o cualquier otra tecnología, artículo 89 del Código de Comercio. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf_mov/Codigo_de_Comercio.pdf (Fecha de consulta 20 de febrero de 2020).

[334] Por digitalización a la migración de documentos impresos a mensajes de datos, artículo 89 del Código de Comercio, Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf_mov/Codigo_de_Comercio.pdf (Fecha de consulta 20 de febrero de 2020).

cial mexicana *NOM-151-SCFI-2016 Requisitos que deben observarse para la conservación de mensajes de datos y digitalización de documentos*[335], en la que se establecen, principalmente, requisitos técnicos para (i) plasmar en el mensaje de datos un sello de tiempo, y (ii) la migración y digitalización de documentos en soporte físico a digital.

4.3.2 Administración Pública Federal

La LFFEA[336] regula su uso en el ámbito de la APF en donde se entiende por firma electrónica avanzada "*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"*[337]. Igualmente, en el artículo 8 de la citada ley, se establece que la firma electrónica avanzada debe cumplir con seis principios, a saber: equivalencia funcional[338]; autenticidad[339]; integridad[340]; neutralidad tecnológica[341]; no repudio, y confidencialidad.

---

[335] NOM-151-SCFI-2016 Requisitos que deben observarse para la conservación de mensajes de datos y digitalización de documentos, publicada en el DOF el 30 de marzo de 2017, Disponible en: https://dof.gob.mx/nota_detalle.php?codigo=5478024&fecha=30/03/2017 (Fecha de consulta: 20 de febrero de 2020).

[336] Ley Federal de Firma Electrónica Avanzada, publicada en el DOF el 11 de enero de 2012, (sin reformas) Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFEA.pdf, (Fecha de consulta: 20 de febrero de 2020).

[337] Artículo 2, fracción XIII de la Ley Federal de Firma Electrónica Avanzada, Disponible en: http://www.diputados.gob.mx/LeyesBiblio/ref/lfea.htm (Fecha de consulta 20 de febrero de 2020)

[338] Consiste en que la firma electrónica avanzada en un documento electrónico o en su caso, en un mensaje de datos, satisface el requisito de firma del mismo modo que la firma autógrafa en los documentos impresos, Disponible en: http://www.diputados.gob.mx/LeyesBiblio/ref/lfea.htm (Fecha de consulta 21 de febrero de 2020).

[339] Consiste en que la firma electrónica avanzada en un documento electrónico o, en su caso, en un mensaje de datos, permite dar certeza de que el mismo ha sido emitido por el firmante de manera tal que su contenido le es atribuible al igual que las consecuencias jurídicas que de él deriven, Disponible en: http://www.diputados.gob.mx/LeyesBiblio/ref/lfea.htm (Fecha de consulta 21 de febrero de 2020).

[340] Consiste en que la firma electrónica avanzada en un documento electrónico o, en su caso, en un mensaje de datos, permite dar certeza de que éste ha permanecido completo e inalterado desde su firma, con independencia de los cambios que hubiere podido sufrir el medio que lo contiene como resultado del proceso de comunicación, archivo o presentación. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/ref/lfea.htm (Fecha de consulta 21 de febrero de 2020).

[341] Consiste en que la tecnología utilizada para la emisión de certificados digitales y para la prestación de los servicios relacionados con la firma electrónica avanzada será aplicada de modo tal que no

En el artículo 23 de la LFFEA se establece que la SFP[342], la SE y el SAT son autoridades certificadoras, es decir, están facultadas para emitir proporcionar firmas electrónicas y servicios asociadas a la misma, tales como firmado de documentos, verificación de vigencia de certificados digitales, verificación y validación de la clave pública, consulta de certificados revocados, entre otros.

En esta LFFEA se contempla el reconocimiento de certificados digitales a través de convenios de colaboración con los poderes legislativo y judicial, federales; los órganos constitucionales autónomos, y los gobiernos de las entidades federativas y municipios. Además de la ley, debemos atender lo dispuesto en el *Reglamento de la Firma Electrónica Avanzada*[343], y las *Disposiciones Generales de la Ley de Firma Electrónica Avanzada*[344] emitidas de forma conjunta entre la SFP, la SE y el SAT en donde se establecen las características, estándares y mecanismos tecnológicos que deberán cumplir las instituciones de la APF y los prestadores de servicios de certificación que adquieran la calidad de autoridad certificadora en términos de la ley.

Con base en la LFFEA se establece que pueden adquirir la calidad de autoridad certificadora los prestadores de servicios de certificación establecidos conforme al CCOM, tales como notarios y corredores públicos, así como las personas morales de carácter privado. Igualmente, para la emisión de mensajes de datos y digitalización de documentos, establece que será aplicable la norma oficial mexicana que emita la SE, es decir, la NOM-151.

---

excluya, restrinja o favorezca alguna tecnología en particular, Disponible en: http://www.diputados.gob.mx/LeyesBiblio/ref/lfea.htm (Fecha de consulta 21 de febrero de 2020).

[342] Con la reforma del 30 de noviembre de 2018 a la LOAPF, se estableció las funciones en materia de gobierno digital a cargo de la SFP pasaron a formar parte de la CEDN. No obstante, en la LFFEA no se estableció expresamente la modificación en materia de firma electrónica avanzada, Disponible en: http://www.diputados.gob.mx/LeyesBiblio/ref/lfea.htm (Fecha de consulta 21 de febrero de 2020)

[343] Reglamento de la Ley Federal de Firma Electrónica Avanzada, publicado en el DOF el 21 de marzo de 2014 (sin reformas) Disponible en: http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFEA.pdf, (Fecha de consulta: 21 de febrero de 2020).

[344] Disposiciones Generales de la Ley de Firma Electrónica Avanzada, publicadas en el DOF el 21 de octubre de 2016, Disponible en: https://www.dof.gob.mx/nota_detalle.php?codigo=5457756&fecha=21/10/2016 (Fecha de consulta 21 de febrero de 2020).

Por otro lado, con la reforma constitucional del 05 de febrero de 2017[345], se derogó el apartado de mejora regulatoria previsto en la LFPA para establecer como facultad exclusiva del Congreso de la Unión legislar en materia de mejora regulatoria, con lo cual el 18 de febrero de 2018 se publicó en el DOF la LGMR que regula, entre otros aspectos, el expediente electrónico de trámites y servicios. En términos del artículo 53, fracción IV de la cita ley se establece que los sujetos obligados integrarán al Expediente para Trámites y Servicios los documentos firmados autógrafamente cuando se encuentre en su poder el documento original y cuente con la Firma Electrónica Avanzada del servidor público.

Igualmente, en términos del artículo 50 de la LGMR se establece que el Expediente para Trámites y Servicios operará conforme a los lineamientos que apruebe el Consejo Nacional de Mejora Regulatoria que deberán considerar mecanismos de seguridad, disponibilidad, integridad, autenticidad, confidencialidad y custodia. Es en el artículo tercero transitorio de los *Lineamientos Generales para la operación del Expediente para Trámites y Servicios*[346], que se establece que las bases, mecanismo y lineamientos para la operación del expediente deberá contar, entre otros aspectos, con la política de firma electrónica de los sujetos obligados. Es decir, ante la diversidad de leyes en materia de firma, y la LGMR, al aplicar a nivel nacional, debe contemplar de manera abierta la aplicación de la normatividad vigentes o las políticas de firma que cada institución cuente.

Esto implicará que en la práctica la CONAMER deba desarrollar una plataforma capaz de interoperar con todos los sistemas públicos en materia de certificados digitales para el reconocimiento de las diversas firmas electrónicas con que una persona puede contar en todas las entidades federativas. Además, se genera la dudas sobre cual firma debe utilizar un ciudadano en aquellos casos que el servicio estatal sea interoperable con el federal tal como se establece en la LGMR. Sin duda

[345] CPEUM, reforma publicada en el DOF el 05 de febrero de 2017, Disponible en http://www.diputados.gob.mx/LeyesBiblio/ref/dof/CPEUM_ref_230_05feb17.pdf (Fecha de consulta 21 de febrero de 2020).
[346] Lineamientos Generales para la operación del Expediente para Trámites y Servicios publicados en el DOF el 13 de julio de 2020, Disponible en http://dof.gob.mx/nota_detalle.php?codigo=5596610&fecha=13/07/2020 (Fecha de consulta 21 de febrero de 2020).

serán temas que tienen que discutirse con la finalidad de diseñar un marco normativo sencillo y que otorgue certeza jurídica en el desarrollo digital del país.

4.3.3 Firma electrónica en materia fiscal

En materia fiscal, la firma electrónica avanzada se regula desde el 2004 en el CFF[347]. Desde entonces, en el segundo párrafo del artículo 17-D del citado Código, se establece como regla general que los documentos en materia fiscal deben presentarse en formatos digitales y contener una firma electrónica avanzada. Si bien no se establece un concepto de firma electrónica sí se contempla que esta deberá contar con un certificado que permita confirmar el vínculo entre un firmante y los datos de creación de la firma electrónica avanzada, el cual deberá ser expedido por el SAT cuando se trate de personas morales y por un prestador de servicios de certificación autorizado por el Banco de México cuando se trate de personas físicas[348]. No obstante, en la práctica, tanto los certificados para personas físicas como morales se expiden por el SAT y los prestadores de servicios de certificación que menciona el CFF son a los autorizados por la SE y no por el Banco de México.

Ahora bien, en términos del CFF se establece que las personas deben comparecer ante del SAT para obtener su firma electrónica. Aquí hay un aspecto a destacar. A diferencia del CCOM y de la LFFEA, en el párrafo noveno del artículo 17-D del CFF, se vincula de forma expresa a la firma electrónica con la identidad para personas físicas regulada conforme al REANPO en términos de la LGP al señalar que "*los datos de identidad que el Servicio de Administración Tributaria obtenga con motivo de la comparecencia, formarán parte del sistema integrado de registro de población, de conformidad con lo previsto en la Ley General de Población y su Reglamento, por lo tanto dichos datos no quedarán comprendidos dentro de lo dispuesto por los artículos 69* -secreto fiscal- *de este Código y 18 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental* [349]".

---

[347] Código Fiscal de la Federación, reforma publicada en el DOF el 05 de enero de 2004, Disponible en: http://www.diputados.gob.mx/LeyesBiblio/ref/cff/CFF_ref31_05ene04.pdf (Fecha de consulta: 22 de febrero de 2020).

[348] Ídem.

[349] La ley vigentes es la Ley Federal de Transparencia y Acceso a la Información Pública, publicada en el DOF el 09 de mayo de 2016, y reformada el 27 de enero de 2017, Esta ley fue abrogada en la

Por otra parte, de conformidad con las reglas 2.2.1., 2.2.2., de la *Resolución Miscelánea Fiscal*[350] se establece que la contraseña otorgada por el SAT se considera una firma electrónica que funciona como mecanismos de acceso a los servicios electrónicos del SAT. Igualmente, en las reglas 2.4.1., 2.4.4., 2.4.5., 2.4.12., se establece que las personas físicas podrán inscribirse al RFC con su CURP y contar con una cédula de identidad fiscal. Es decir, en México, una persona puede tener dos identidades, la identidad a través del CURP y la del RFC. Ahora bien, en relación con el RFC, para el año 2020, de los 120 millones de mexicanos 76 millones de personas físicas cuentan con un RFC y un CURP.[351]. En este sentido, será relevante que tanto el RENAPO como el SAT coordinen sus atribuciones en materia de identidad y firma electrónica con la finalidad de evitar la duplicidad de funciones.

Por último, debemos destacar que es la firma electrónica expedida por el SAT la que en la práctica es utilizada incluso por otras instituciones y organismos públicos. Por ejemplo, a través de convenios de colaboración, el SAT provee el componente de firma electrónica avanzada a las treinta y dos entidades federativas, y a catorce municipios[352]. Incluso, ha suscrito convenios de colaboración con la ASF[353] y el TFJA.

4.3.4 Firma electrónica en la administración local

De conformidad con el artículo 73 de la CPEUM, la firma electrónica avanzada no constituye una facultad exclusiva del Congreso de la Unión[354]; lo que implica que es materia de las entidades federativas al no operar el principio de reserva de ley. Así,

---

que se contemplaban los supuestos de información confidencial, Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFTAIP_270117.pdf. (Fecha de consulta 22 de febrero de 2020).

[350] Resolución Miscelánea Fiscal, Publicada en el DOF el 28 de diciembre de 2019, Disponible en https://dof.gob.mx/20191228-2.pdf (Fecha de consulta 22 de febrero de 2020).

[351] SAT, Padrón RFC, Disponible en: http://omawww.sat.gob.mx/cifras_sat/Paginas/datos/vinculo.html?page=giipTipCon.html, (Fecha de consulta 22 de febrero de 2020).

[352] Convenios de firma electrónica avanzada, actualizado al 13 de febrero de 2019, Disponible en: https://www.gob.mx/sfp/documentos/convenios-de-firma-electronica-avanzada, (Fecha de consulta 24 de febrero de 2020).

[353] SAT y ASF suscriben convenio para el uso de la e.firma, 18 de junio de 2019, Disponible en: https://www.gob.mx/sat/prensa/sat-y-asf-suscriben-convenio-para-el-uso-de-la-e-firma-032-2019?idiom=es, (Fecha de consulta 24 de febrero de 2020).

[354] Artículo 73 de la CPEUM, Disponible en: http://www.diputados.gob.mx/LeyesBiblio/ref/cpeum.htm (Fecha de consulta 24 de febrero de 2020).

actualmente 23 entidades federativas[355] cuentan con su propia legislación de firma electrónica[356], aunque en la práctica cuenten con convenios de colaboración con el SAT. Destacan los casos de Sonora, Guerrero y Colima quienes contaban con ley de firma electrónica avanzada desde el 2006, 2008 y 2009, respectivamente, es decir, antes de la ley federal y poco después del CFF.

4.3.5 Firma electrónica en el Poder Judicial Federal y Local

El PJF también cuenta con su propia regulación de firma electrónica avanzada desde el año 2013, de conformidad con el *Acuerdo general conjunto número 1/2013, de la suprema corte de justicia de la nación, del tribunal electoral del poder judicial de la federación y del consejo de la judicatura federal, relativo a la firma electrónica certificada del poder judicial de la federación (FIREL) y al expediente electrónico*[357], y las *Políticas para la obtención y uso de la firma electrónica certificada el Poder Judicial de la Federación, así como para la operación de su infraestructura tecnológica*[358].

La tecnología ha permeado también al poder judicial en México, en donde podemos destacar *Líneas Generales de Trabajo 2019-2022*[359], de la SCJN y el CJF, a cargo del Ministro Arturo Zaldívar, en donde se establece como estrategias en el Poder Judicial las siguientes: (i) Fortalecer y modernizar las estrategias de comunicación digital; (ii) profundizar el uso del expediente digital; (iii) buscar mecanismos para compartir datos e información, así como interactuar en materia jurisdiccional a

---

[355] Anexo Único. Sobre legislación nacional sobre firma electrónica avanzada. Disponible en: https://www.gob.mx/sfp/documentos/firma-electronica-avanzada-fiel (Fecha de consulta 24 de febrero de 2020).

[356] Ídem.

[357] Acuerdo general conjunto número 1/2013, de la suprema corte de justicia de la nación, del tribunal electoral del poder judicial de la federación y del consejo de la judicatura federal, relativo a la firma electrónica certificada del poder judicial de la federación (FIREL) y al expediente electrónico, Disponible en: https://www.pjf.gob.mx/Docs/Acuerdo%20General%20Conjunto1-2013%20(FIREL)%20Version%20Aprobada.pdf (Fecha de consulta 21 de febrero de 2020).

[358] Políticas para la obtención y uso de la firma electrónica certificada el Poder Judicial de la Federación, así como para la operación de su infraestructura tecnológica Aprobado el 10 de junio de 2004, Disponible en: https://www.pjf.gob.mx/Docs/Politicas%20Firel%20con%20rubricas%20y%20firmas.pdf, (Fecha de consulta 25 de febrero de 2020).

[359] Zaldívar Lelo de Larrea, Arturo, "Líneas Generales de Trabajo 2019-2022, SCJN-CJF, 2018, Disponible en: https://www.scjn.gob.mx/sites/default/files/carrusel_usos_multiples/documento/2019-01/lineas-grales-trabajo-mp-arturo_zaldivar_lelo_de_larrea.pdf, (Fecha de consulta 25 de febrero de 2020).

través de plataformas digitales. Sin embargo, un reto para los abogados postulantes será la gestión de diversas firmas electrónicas ante el poder judicial local y federal, ya que, al no existir una ley con estas características, debe seguir aplicándose las leyes de firma electrónica que cada autoridad emita.

El uso de la firma electrónica en el proceso judicial ha cobrado especial importancia hoy en día debido al uso masivo de medios digitales motivado por la pandemia por COVID-19. No obstante, a nivel de la justicia local también comienzan a emitirse disposiciones que regulan el uso de la firma electrónica en proceso judiciales[360]. Esto puede crear incertidumbre jurídica al contar con diversa legislación que regula la firma electrónica para cada autoridad local tanto en el ámbito del poder ejecutivo como en el judicial.

4.3.6 Hacia una ley general de firma electrónica avanzada en México

México, a diferencia de otros países, cuenta con una amplia legislación en materia de firma electrónica. Lo anterior consideramos puede generar incertidumbre jurídica ante la aplicación de diversas leyes en la materia. Además, implica para el sector público la duplicidad de esfuerzo y recursos en la emisión y gestión de firma electrónicas. Pensemos, por ejemplo, en el SAT, quien debido a su infraestructura de firma electrónica se ha convertido en el principal proveedor de este componente para el sector público incluyendo a las entidades federativas, lo que le implica gestionar convenios de colaboración institucional para su uso en otras instituciones.

Además, debemos destacar la importancia del expediente de trámites y servicios a cargo de la CONAMER, en donde se contempla que los documentos que obren en dicho expediente deben contener la firma electrónica del servidor público. Ante la diversidad de firmas electrónicas consideramos que esto incluso puede ocasionar complejidad para la operación del expediente de trámites y servicios que se regula a nivel nacional, así como la duplicidad de recursos públicos en los diferentes

[360] Poder Judicial del Estado de México, "Términos y Condiciones de Uso de los Certificados Digitales de la FEJEM", Disponible en http://fejem.pjedomex.gob.mx/fejem/Politic.htm, (Fecha de consulta: 25 de febrero de 2020).

poderes y niveles de gobierno para la gestión de firmas electrónicas en contravención de los principios de economía, eficiencia y eficacia de la gestión pública plasmado en el artículo 134 de la CPEUM.

Por otro lado, la firma electrónica es considerada en los tratados de libre comercio como un componente para habilitar la economía digital y su reconocimiento transfronterizo es una pieza clave para su operación. Para ello es importante que los países identifiquen a los prestadores de servicios de certificación con base en la legislación nacional, siendo que en México existe una variedad de normas en la materia que podría dificultar el reconocimiento transfronterizo de la firma electrónico en perjuicio de la economía digital.

En este contexto, consideramos que la regulación de la firma electrónica debe ser una facultad exclusiva del Congreso de la Unión en términos del artículo 73 de la CPEUM, con la finalidad que emita, al igual en que la LGMR o la LGP, una ley general en materia de firma electrónica en el entendido que estos tres rubros (mejora regulatoria, identidad digital y firma electrónica) son pieza clave para la implementación de transformación digital del país y deben abordarse de manera articulada.

Como observamos a lo largo del presente documento, las revoluciones industriales presentan desafío de diversa índole incluyendo aspectos normativos. En la cuarta revolución industrial la infraestructura y habilidades digitales son habilitadores para reducir brechas digitales con el objeto de que mayor parte de la población de vea beneficiada de las TIC. Pero, por otro lado, contamos con elementos operacionales de la transformación digital en donde el derecho juega un rol trascendental para proporcionar un entorno seguro en el uso de la tecnología. Por lo que aspecto como la identidad digital y la firma electrónica son componentes que impactan en los derechos humanos y en la expresión de la voluntad a través de medios digitales.

Conclusiones

Conclusiones

A lo largo de cuatro capítulos advertimos el impacto de las revoluciones industriales en el desarrollo económico y social de los países. Observamos que si bien el desarrollo tecnológico presenta beneficios de diversa índole también implican riesgos y vulneraciones a los derechos humanos.

Procurar un desarrollo sostenible requiere de la colaboración de todos los sectores de la sociedad y del diseño de normas jurídicas y políticas públicas que establezcan las bases y principios para afrontar los desafíos del uso y aprovechamiento de las TIC. Es importante atender la brecha digital y contar con servicios digitales inclusivo; la pandemia por COVID-19 nos mostró que la falta de conectividad incrementa las brechas sociales.

Por otro lado, observamos que la innovación y los nuevos modelos de desarrollo tecnológico impactan en la forma en que interactuamos y también en nuevos procesos y derechos humanos. Así, las revoluciones industriales representan *hitos* históricos en el desarrollo económico y social a nivel mundial pero también para la evolución y protección de los derechos humanos. Por ejemplo, el uso de máquinas industriales y de procesos de producción en serie representaron retos en los derechos laborales. O la apertura comercial y la globalización dieron paso a los derechos económicos, sociales y culturales.

En la cuarta revolución industrial tecnologías como IA, *blockchain*, *big data*, conducción autónoma, cómputo en la nube, Internet de las Cosas, así como el intercambio masivo de información y la crisis sanitaria a causa de COVID-19, han replanteado la forma en que se garantizan los derechos a través de medios digitales. Han surgido conceptos como teletrabajo, telesalud, educación a distancia o economía digital. Incluso los TLC ya no solo incorporan aspectos sobre el libre tránsito de personas y mercancías, sino también aspectos relacionados con las telecomunicaciones, la interoperabilidad, el reconocimiento de firmas electrónica o la ciberseguridad.

Es aquí en donde el derecho juega un rol relevante ya que, como señala Hans Kelsen, "*el derecho no es una categoría eterna y absoluta, sino que su*

contenido cambia con la historia[361]" y podemos agregar con también lo hace junto con desarrollo tecnológico. Un ejemplo de lo anterior es la consulta pública sobre la Carta de Derechos Digitales que lanzó el Ministerio de Asuntos Económicos y Transformación Digital del Gobierno de España, en donde contempla nuevos derechos humanos tales como: derecho a la protección de datos; derecho a la identidad en el entorno digital; derecho al pseudonimato; derecho a no ser localizado y perfilado; derecho a la seguridad digital; derecho a la herencia digital; derecho a la neutralidad de Internet; derecho a la educación digital; derecho a la desconexión digital en el ámbito laboral; derechos ante la Inteligencia artificial, entre otros[362].

En cada una de las revoluciones industriales el derecho ha proporcionado un conjunto de normas jurídicas que buscan salvaguardar los derechos humanos y propiciar un orden social. Pensemos, por ejemplo, en el auge del derecho laboral ante la producción en serie, o en el derecho ambiental ante la sobreexplotación de los recursos naturales.

Ahora, con la IA se enfatiza el uso ético de los datos. Aunque la ética los derechos humanos han estado presentes en las etapas industriales con el objeto de orientar el desarrollo social y económico con respeto a la dignidad humano. Quizá algunos derechos humanos han tenido mayor presencia en cierta época que otros. Como los derechos civiles y políticos en la primera revolución industrial. Los derechos sociales y laborales en la segunda. Los derechos económicos, sociales y culturales en la tercera. Y por último los derechos digitales como la protección de datos personales en la cuarta revolución industrial.

Para afrontar los retos de la tecnología se requiere no sólo atender aspectos técnicos sino también se requiere de un cambio global en las instituciones y las personas para conocer los beneficios y los riesgos en el uso y aprovechamiento de las TIC. Este cambio requiere de un proceso continuo y alineado con los derechos humanos, los ODS de la ONU y los principios de la CMSI. Para ello, los países han

---

[361] Kelsen, Hans, "La teoría pura del derecho", Buenos Aires, Editorial Losada, S.A, s.a. p. 45.

[362] Cfr. Gobierno de España, Ministerio de Asuntos Económicos y Transformación Digital, DOCUMENTO PARA CONSULTA PÚBLICA Carta de Derechos Digitales, 19 de noviembre de 2020, Disponible en: https://portal.mineco.gob.es/RecursosArticulo/mineco/ministerio/participacion_publica/audiencia/ficheros/SEDIACartaDerechosDigitales.pdf, (Fecha de consulta 20 de diciembre de 2020).

adoptado agendas digitales que les permiten guiar el rumbo la transformación digital con base en su contexto nacional.

No obstante, existen elementos comunes en todas ellas en aspectos como infraestructura; habilidades digitales; marco jurídico y política públicas; cambio organización y de procesos; servicios digitales; liderazgo y coordinación institucional. Cada uno de estos rubros atienden al contexto nacional de los gobiernos a través de sus agendas digitales, en donde advertimos como temas centrales los siguientes: (i) seguridad de la información; (ii) infraestructura digital; (iii) habilidades digitales; (iv) gestión de datos; (v) servicios digitales centrados en las personas; (vi) interoperabilidad; (vii) identidad digital, y (viii) firma electrónica.

En las agendas digitales que analizamos de los países que cuentan con un mayor índice de desarrollo digital en cada uno de los cinco continentes[363], observamos que cuentan con líneas de acción relacionadas con dichos temas, y una regulación clara sobre identidad digital y firma electrónica; los cuales son considerados clave para la transformación digital. Por lo que consideramos relevante advertir las principales conclusiones en estos dos rubros, incluyendo el caso de México.

Identidad digital

La identidad es un derecho humano que está vinculado a otros derechos como el de nacionalidad y es la llave para el ejercicio de otros como la salud, la educación o el trabajo. Este derecho se reconoce a nivel internacional y se garantiza a través de los registros civiles. Sin embargo, con el uso exponencial de las TIC la identidad a mutuado de los registros civiles a los registros digitales y ahora cualquier dato

[363] Estos países son: Sudáfrica, Isla de Mauricio, República de Corea, Singapur, Estonia, Dinamarca, Australia, Nueva Zelanda, Estados Unidos, Uruguay, Canadá, Argentina, Chile, Brasil, y México. ONU, Department of Economic and Social Affairs, "E-Government Survey 2020, Digital Government in the Decade of Action for Sustainable Development", Nueva York, 2020, pp 37-62. Disponible en: https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2020-Survey/2020%20UN%20E-Government%20Survey%20(Full%20Report).pdf (Fecha de consulta: 21 de julio de 2020).

personal que permita identificar a una persona está vinculado con la identidad digital de las personas.

Inclusive, una persona puede ser identificada con base en su huella digital y patrones de consumo en medios electrónicos. Es aquí en donde el vínculo entre el derecho a la identidad y el de protección de datos personales debe analizarse en su conjunto en su formato digital.

Ahora bien, los gobiernos han evolucionado el concepto tradicional de identidad legal considerando el uso de las TIC y han adoptado un rol activo para garantizar este derecho a sus ciudadanos en el entorno digital. Los motivos para ello, son diversos en cada país entre los que podemos destacar los siguientes: asegurar servicios gubernamentales; reducir el fraude y el robo de identidad; proporciona una identificación digital única a nivel nacional; elimina la necesidad de llevar múltiples documentos de identificación; mejora la confianza en las credenciales de identidad oficiales; acelera los controles de identidad en el cruce de fronteras; llevar a cabo la votación electrónica; realizar transacciones comerciales y bancarias; proporcionar recetas médicas y residencia digital.

Son diversos los modelos de identidad digital que los países han adoptado, los cuales podemos agrupar en cuatro tipos: (i) tarjeta física con chip; (ii) clave y usuario; (iii) certificados digitales, y (iv) sistemas de validación de identidad a través de plataformas digitales mediante el uso de datos biométricos.

La tarjeta física con chip combina la identidad física con la digital, en donde se utilizan elementos criptográficos y/ datos biométricos para acreditar la identidad digital de una persona. Son los casos de Uruguay, Estonia o Sudáfrica. Las tarjetas coindicen y contar con un chip de seguridad, un código QR, un código de barras; códigos de validación y contraseñas gestionadas por el propio usuario. Este modelo se combina en algunos casos como el de Estonia con la identidad digital a través del móvil o plataformas digitales. Además, en ambos figura el registro civil como la autoridad a cargo de la identidad digital que es aplicable y reconocida en cualquier, ya sea para trámites, transacciones comerciales, bancarias o procesos judiciales. En este tipo de identidad también coincide en contar con datos biométricos como la huella dactilar o reconocimiento fácil para acreditar la identidad de los usuarios.

La identidad mediante clave y contraseña busca fomentar el gobierno digital en donde, previa acreditación de la identidad por el registro civil, se les otorga una identidad digital a las personas mediante clave y usuarios únicos para acceder a los servicios públicos. Son casos como Canadá, Argentina, Chile, Dinamarca, Singapur y Estados Unidos. La gestión de este tipo de identidades está a cargo principalmente de las unidades de gobierno digital, pero interoperan con el registro civil. En algunos casos, para la gestión de la identidad, se colabora con el sector privado previamente autorizados por el gobierno; similar a lo que sucede con los prestadores de servicios de certificación en la firma electrónica. En estos casos, se solicita principalmente la validación de identidad a través de datos biométricos o la interoperabilidad con el registro civil como el caso chileno. En otros casos como Argentina, la empresa autorizada recaba una fotografía del usuario y la coteja con la base de datos del registro civil para acreditar la identidad, la cual, además, se lleva a cabo en la nube. Los países que utilizan software para la gestión de su identidad como Dinamarca o Estonia cuentan la firma electrónica basada en criptografía para el firmado de documentos electrónicos.

Países como Dinamarca, Corea del Sur y Estonia prefieren utilizar certificados digitales para acreditar la identidad digital de las personas. Eso les ha permitido mantener la seguridad de la información y de los datos personales a través de certificados digitales que los usuarios pueden utilizar en sus teléfonos y/o plataformas electrónicas. Incluso, este tipo de identidad digital, como en el caso de Corea del Sur está evolucionando a una identidad descentralizada con el uso de *blockchain* en donde la persona tiene control de sus datos. El cuarto grupo utiliza plataformas de validación de identidad digital con el uso de datos biométricos como los casos de Singapur, Argentina y el Reino Unido.

En el caso de México observamos que aún no existe una regulación y hoja de ruta clara sobre la adopción de un modelo de identidad digital. Existen diversos documentos con los que una persona puede acreditar su identidad -credencial para votar, CURP, pasaporte, o cédula profesional-. Si bien en la LGP se contempla la cédula nacional de identidad, lo cierto es en la práctica los mexicanos no contamos con un documento único de identidad.

No obstante, debemos destacar dos temas recientes. El primero, el que se contempla en el PND 2018-2024 que cuenta con una línea de acción para que la SEGOB, a través del RENAPO, desarrolle el "documento único digital de identificación nacional biometrizado". El segundo, la iniciativa de la nueva LGP que contempla una Sistema Nacional de Identificación Digital a través de la RENAPO y la emisión de una Cédula Única de Identidad Digital. Con los elementos que analizamos, podemos concluir que en México la tendencia en materia de identidad digital es contar con un sistema de validación de identidad a través de plataformas digitales mediante el uso de datos biométricos, como los casos de Singapur o Reino Unido.

Sin embargo, consideramos que, en el deseño de este documento, es importante que la SEGOB observar los principios del MNID propuestos por la UIT y el Banco Mundial en materia de identidad digital, y en donde proponemos algunas acciones que se podemos resumir en los siguientes puntos:

- Privacidad por diseño para salvaguardar el derecho a la protección de datos personales, en donde es importante trabajar juntamente con el INAI en este aspecto. Además, será necesario contar con una manifestación de impacto que analice los riesgos de tratamientos de datos biométricos; así como considerar el artículo 9 del RGPD, y 7, 22, 75 y 75 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; en donde se considera la prohibición de recolectar datos biométricos salvo excepciones particulares en el caso europeo y en la mexicana realizar una evaluación de impacto del tratamiento de dichos datos personales.
- Observar los estándares de identificación electrónica previstos en el *Reglamento Europeo relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior*[364], así como en el *Proyecto de disposiciones sobre la utilización y el reconocimiento*

[364] Diario Oficial de la 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 la que se deroga la Directiva 1999/93/CE, Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32014R0910&from=ES, (Fecha de consulta: 04 de mayo de 2021).

transfronterizo de sistemas de gestión de la identidad y servicios de confianza de la CNUDMI[365], en donde se contemplan, entre otros aspectos, mecanismos de identificación electrónica, seguridad, interoperabilidad y servicios de confianza en materia de identidad digital.

- Identificar e integrar las identidades existentes en todo el país a cargo del INE, la SRE, el SAT, la SEP, SEDENA, y las entidades federativas a través de las licencias de conducir, para lo cual será importante modificar la LGP o crear una nueva como la que se dictaminó el 03 de diciembre de 2020 en la Cámara de Diputados.
- Generar estándares de interoperabilidad y seguridad de la información para otorgar confianza y seguridad jurídica a las personas e instituciones. Diseñar el modelo de identidad digital en colaboración con instituciones como la CONAMER, el SAT, la SEP, la SRE, la SEDENA, el INE, la SE, con el objeto de incluir no sólo la recolección de datos sobre identidad sino también su uso nacional e internacional en beneficio de la economía digital y desarrollo social del país. En materia de seguridad, se deberá analizar a la infraestructura y bases de datos de identidad digital como infraestructura critica para fortalecer las medidas de seguridad ante ciberataques.
- Considerar la interoperabilidad con la firma electrónica y contar con un plan de inversión para el soporte y seguridad de la infraestructura de la plataforma que administrará la información de la cédula de identidad en un modelo de escala. En la iniciativa de la nueva LGP se contempla en el artículo 8 transitorio del dictamen.
- Analizar el contexto nacional con la finalidad de evitar la duplicidad de funciones, ahorrar costos de operación, contar con calidad de los datos registrados y, sobre todo, contar un marco jurídico sobre este aspecto tan importante que impacta no sólo en el derecho a la identidad sino también a otros derechos humanos. Se debe diseñar el modelo de identidad digital a nivel nacional con base en los

[365] CNUDMI, Proyecto de disposiciones sobre la utilización y el reconocimiento transfronterizo de sistemas de gestión de la identidad y servicios de confianza, 5 a 9 de abril de 2021, Disponible en: https://undocs.org/es/A/CN.9/WG.IV/WP.167, (Fecha de consulta: 04 de mayo de 2021).

principios de eficiencia, eficacia, economía, transparencia y rendición de cuentas previsto en el artículo 134 de la CPEUM.

- Algunos modelos de identidad digital que consideramos pueden aportar algunas ideas al modelo mexicano son los casos de Corea del Sur, Dinamarca, Uruguay, Singapur, Estonia y Chile.
- Por último, consideramos que si bien se prevé desarrollar un *"Documento único digital de identificación nacional biometrizado"* a cargo de RENAPO, consideramos que la discusión sobre identidad digital en México no debe centrarse únicamente en concentrar o interoperar con las diferentes bases de datos de las autoridades que generar algún tipo de identidad -fiscal, ciudadana, electoral, militar o profesional-, sino debe ampliarse a la forma en que los ciudadanos interactúan en entornos gubernamental, comerciales, financieros y judiciales, con la finalidad de proporcionar una identidad digital única en entornos seguro y confiables en el uso de las TIC, por lo que la coordinación de las autoridades competentes en dichos rubros, también será un factor para fortalecer la gestión de la identidad digital nacional.

Firma electrónica avanzada

La firma electrónica tiene su antecedente en el derecho mercantil internacional a través de la Ley Modelo de la CNUDMI sobre firma electrónica. Con el flujo de información a través del correo electrónico y los mensajes de datos, la compraventa internacional tuvo un gran auge. Sin embargo, ante los derechos y obligaciones que se adquieren en un acto comercial era necesario poder identificar a las partes en el comercio electrónico y validar la expresión de su voluntad para realiza un acto jurídico.

Así, la firma electrónica surge como un mecanismo de confianza en el derecho mercantil internacional a través de técnicas de autenticación los cuales deben permitir acreditar tres elementos: (i) identificar a una persona; (ii) dar certeza de la participación en el acto de firmar, y (iii) asociar a esa persona con el contenido del documento.

Al igual que en el mundo físico, en el ámbito del comercio electrónico se contemplaba ya desde entonces la necesidad de identificar al firmante y asociar su expresión de voluntad al texto del documento suscrito. Lo anterior, con la finalidad de otorgar mayor certeza jurídica a las partes signantes.

Igualmente, debemos destacar que el concepto tradicional de firma cambió en su forma, pero no en su fondo. Vemos que la firma escrita tiene como característica un gráfico; mientras que la electrónica la de ser cualquier dato que identifique a la persona. Pero ambas constituyen la expresión de la voluntad de una persona para obligarse al contenido de un documento por lo que esta debe estar libre de vicios en la conformación del consentimiento.

Posteriormente, el uso de la firma electrónica se extendió a otros usos como el gubernamental, el bancario y judicial. El uso de la firma electrónica ha sido un pilar para la transformación digital. En los países que analizamos observamos que, si bien la regulación de la firma electrónica tiene su base en la Ley Modelo de la CNUDMI sobre firma electrónica, lo cierto es que en sus estrategias digitales los países la consideran como elemento transversal independientemente del sector en que se utilice. En este contexto, en cuanto a la firma electrónica en el contexto internacional y nacional, podemos destacar lo siguiente:

- La firma electrónica presenta tres modalidades: simple, avanzada y cualificada. La simple requiere únicamente acreditar tres elementos identificar a la persona, acreditar su participación en el acto de firmar y asociar a la persona con el contenido del documento. La segunda, se basa en criptografía y además de los elementos anteriores, necesita de una infraestructura de clave pública; ser creada bajo control exclusivo del firmante; y de un certificado digital expedido por un prestador de servicios de certificación autorizado. Por último, la cualificada, además de los elementos de la simple y la avanzada, requiere de un dispositivo cualificado para su creación.
- La firma electrónica avanzada es utilizada por la mayoría de los países con la finalidad de otorgar mayor seguridad en las transacciones digitales. Algunos otros países, de tradición anglosajona como Estados Unidos o Nueva Zelanda, prefieren usar la firma electrónica simple bajo el principio de libertad contractual.

- Los países que cuentan con un mayor índice de desarrollo digital cuentan con la firma electrónica cualificada; tal es el caso de Estonia en Europa o Uruguay en América Latina. Además, en estos países, al igual que Dinamarca, Singapur y Argentina, existe una tendencia en vincular la firma electrónica con la identidad digital desde su diseño. Es decir, con estos modelos de firma electrónica una persona puede suscribir un documento utilizando su documento de identidad digital.
- Todos los países cuentan con una sola legislación de firma electrónica, la cual se reconoce su uso para servicios públicos, transacciones comerciales y/o procesos judiciales.
- Actualmente, y siendo que el origen de la firma electrónica se encuentra en el derecho mercantil internacional, como revisamos en el capítulo 1, los TLC regulan aspectos como firma electrónica transfronteriza, interoperabilidad, seguridad y economía digital, entre otros. Lo anterior, con el objeto de fomentar la economía regional y en donde el reconocimiento transfronterizo de la firma electrónica e identidad digital guardan un rol importante para el deseño de marco normativos nacionales e infraestructura digital.
- En México la firma electrónica se regula por diversas leyes: CFF, LFFEA, CCOM, así como la legislación de las 23 entidades federativa, la emitida por el PJF y los poderes judiciales locales. En el sector público, el SAT ofrece el servicio de la firma electrónica a través de convenios de colaboración, lo que le implica una carga administrativa en la gestión de dichos convenios los cuales han cobrado mayor auge debido a la contingencia sanitaria por COVID-19. México es el único país en el mundo que cuenta con más de 32 leyes de firma electrónica.
- Al respecto, consideramos que la sobrerregulación en materia de firma electrónica en México, además de duplicar esfuerzos regulatorios y costos administrativos de implementación en el sector público, ocasiona confusión e inseguridad jurídica en su uso por parte de las personas ya sea en el ámbito comercial, gubernamental, financiero o judicial. Consideramos que la armonización de la legislación nacional permitirá acelerar la transformación

digital en el ámbito nacional y fortalecer su armonización con la legislación internacional a efecto de potenciar la economía digital a través de los TLC como el T-MEC, la Alianza del Pacífico, la Unión Europea o los países del MERCOSUR.

- Por otro lado, debemos destacar la reforma constitucional en materia de mejora regulatoria que regula el expediente de trámites y servicios, en el cual se contempla el uso de la firma electrónica avanzada como uno de sus requisitos. Al respecto, consideramos que, ante la sobrerregulación de leyes en materia de firma electrónica su uso en el expediente de trámites y servicios a cargo de la CONAMER representará un reto para su reconocimiento y validez dentro de dicho expediente en los tres niveles de gobierno.
- Será necesario contar con una sola ley de firma electrónica que otorgue certeza jurídica y fomente su uso en las transacciones electrónicas, ya sea en el sector gubernamental, comercial, judicial o internacional. Para ello, vemos necesario una reforma constitucional en materia de firma electrónica para otorgar facultades exclusivas al Congreso de la Unión para legislar en esta materia, al igual que en el rubro de identidad digital.
- Además, consideramos que la legislación secundaria que derive de la reforma constitucional en materia de firma electrónica debe estar vinculada a tres grandes temas: (i) identidad digital; (ii) reconocimiento transfronterizo, e (iii) interoperabilidad y seguridad de la información. Igualmente, nos parece importante que una ley general sobre firma electrónica en México debe contempla la regulación de los siguientes elementos: firma electrónica cualificada; prestadores de servicios de certificación con base en el principio de neutralidad tecnológica, incluyendo notarios y corredores públicos; considerar al SAT como el proveedor de servicios de certificación para el sector público con la finalidad de evitar la duplicidad de esfuerzo y recursos económicos; establecer procedimientos para notificar internacionalmente las listas de confianza de los prestadores de servicio de certificación autorizados conforme a la legislación nacional; definir la plataforma digital para la validación de documentos electrónicos, en donde consideramos importante generar sinergias

con la CONAMER en materia de expediente de trámites y servicios y la SSA con el diseño del expediente médico electrónico; reconocer su uso en cualquier ámbito, ya sea gubernamental, comercial, judicial o financiero, por lo que se deberá de considerar el impacto en las disposiciones jurídicas del Código de Comercio, la Ley Federal de Firma Electrónica Avanzada, el Código Fiscal de la Federación, las legislaciones locales, y las disposiciones judiciales en materia de firma electrónica avanzada.

- Para el caso de la firma electrónica transfronteriza, será importante que México se sume a los esfuerzos de la RedGealc en el marco de la *Iniciativa de Bienes Públicos Regionales* del Banco Interamericano de Desarrollo que cuenta con tres ejes: firma digital transfronteriza, interoperabilidad transfronteriza y tecnologías emergentes[366]. En noviembre de 2020 se realizó una prueba técnica entre Brasil, Chile, Colombia y Uruguay quienes validaron mutuamente sus certificados digitales[367]. La RedGealc cuenta con el *Documento de Promoción de la Firma Digital Transfronteriza* en el que se destaca, entre otros aspectos:

  > *"1.- Expresar su voluntad de avanzar en los aspectos de gobierno digital que sirvan como base para un futuro reconocimiento mutuo de firma digital entre los países que así lo resuelvan mediante los mecanismos que sus propias legislaciones indiquen.*
  >
  > *2.-Destacar los consensos no vinculantes alcanzados por el grupo de trabajo de Red GEALC en asuntos técnicos de firma digital transfronteriza, y recogidos en un documento de síntesis elaborado con el apoyo de la Iniciativa de Bienes Públicos Regionales del BID.*
  >
  > *3.- Impulsar desde Red GEALC la instalación en los países que así lo decidan de los software públicos necesarios para el reconocimiento mutuo de firma digital, tales como @firma y Tlmanager (donados a la región por el Gobierno de España), o el validador internacional ofrecido por Brasil, o similar software que los países decidan implementar.*
  >
  > *4.- Recomendar que los planes de trabajo de Red GEALC tomen en cuenta, cada año, las acciones necesarias para ayudar a superar las asimetrías técnicas y legales*

[366] Red de gobierno electrónico de América Latina y el Caribe, *Firma Digital Transfronteriza, Disponible* en: https://www.redgealc.org/lineas-de-trabajo/servicios-transfronterizos/ (Fecha de consulta: 21 de diciembre de 2020).
[367] Red de gobierno electrónico de América Latina y el Caribe, *Validación certificados digitales 4 países*, en: https://www.redgealc.org/contenido-general/noticias/validacion-certificados-digitales-entre-4-paises/ (Fecha de consulta: 21 de diciembre de 2020).

existentes entre los países, a efectos de que la mayor cantidad de los mismos se puedan beneficiar de la firma digital transfronteriza."[368]

- México, Chile, Colombia y Perú, en el marco de la Alianza del Pacífico, acordaron el reconocimiento de certificados de firma electrónica avanzada[369]. Lo que ahora se necesita es una reforma en materia de firma electrónica a nivel nacional que regule el uso de firma electrónica transfronteriza acorde a los requerimientos técnicos que se revisen en el grupo de la Alianza del Pacífico. Esto podría favorecer la reactivación económica entre los cuatro países en cuestión de forma segura e interoperable.

Algunas propuestas para México en materia de identidad digital y firma electrónica

Para facilitar el desarrollo digital en México, consideramos importante contar con un proyecto a nivel nacional sobre identidad digital y firma electrónica. Como *primera recomendación*, se sugiere dotar de atribuciones constitucionales al Congreso de la Unión en el artículo 73 de la CPEUM para establecer la coordinación de atribuciones en los tres órdenes de gobierno sobre estos dos temas. De lo contrario se corre el riesgo de contar con una sobrerregulación en materia de identidad digital y firma electrónica.

Recordemos que, como derivó del estudio comparado, México es el único país a nivel internacional que cuenta con más de 32 leyes en materia de firma electrónica. Aspecto similar está sucediendo en materia de identidad digital como es el caso de la *Ley de Ciudadanía Digital de la Ciudad de México*[370]*.* De la lectura

[368] Red de Gobierno Electrónico de América Latina y el Caribe, VI Reunión Ministerial y XIV Asamblea anual, 18-20 de noviembre de 2020, Documento de Promoción de la Firma Digital Transfronteriza, Disponible en: https://www.redgealc.org/site/assets/files/12445/final_documento_de_promocion_de_la_firma_digital_transfronteriza.pdf, (Fecha de consulta: 20 de diciembre de 2020).

[369] Cfr. Artículo 13.10 del *Primer Protocolo Modificatorios del Protocolo Adicional al Acuerdo Marco de la Alianza del Pacífico*, del 10 de febrero de 2014, Disponible en: https://alianzapacifico.net/descarga-documentos-protocolos-modificatorios-del-protocolo-adicional-al-acuerdo-marco-de-la-alianza-del-pacifico/

[370] Gaceta Oficial de la Ciudad de México, Vigésima Primera Época, 09 de enero de 2020, Disponible en https://data.consejeria.cdmx.gob.mx/portal_old/uploads/gacetas/52bc93885f065b575b8bd18f7f10bbd3.pdf, (Fecha de consulta: 21 de julio de 2020).

a los artículos 36, 39, 48, fracción I y 52 de la citada Ley se observa que en la Ciudad de México la identidad de una persona para acceder a servicios públicos se realiza a través de los certificados digitales que se emiten a través de la firma electrónica avanzada local. Así, para que las personas puedan acreditar su identidad y acceder a los servicios digitales de la Ciudad de México, el Gobierno Local desarrolló el "*Sistema Llave*"[371]. Del aviso de privacidad del sistema se observa que la recolección de datos personales tiene como finalidad "*generar una Cuenta Llave CDMX para autenticar su identidad ante los canales digitales de la Administración Pública y las Alcaldías de la Ciudad de México, para gestionar digitalmente trámites o servicios"*[372]*.*

Consideramos que el modelo de la Ciudad de México debe considerarse en el diseño y desarrollo del modelo nacional que se pretende regular en el marco de la LGP a cargo de RENAPO. Del estudio comparado que realizamos en materia de identidad digital, observamos que los países que lideran los primeros lugares de desarrollo digital, tales como Dinamarca, Corea del Sur y Estonia, utilizan este tipo de modelo de identidad digital a través de certificados digitales vinculados a la firma electrónica del ciudadano. Por lo que este modelo otorga mayor seguridad técnica y jurídica a las personas en el tratamiento de sus datos personales a través del uso de la criptografía, en donde si bien, para su otorgamiento se recaban datos biométricos, lo cierto es que una vez que se emite el certificado digital dichos datos biométricos no son utilizados constantemente para que el ciudadano valide su identidad cada vez que así lo requiera para acceder a servicios digitales.

Así, una *segunda recomendación* en el diseño de un modelo de identidad digital en México es compartir experiencias con la Ciudad de México en materia de certificados digitales. Este modelo, incluso, la plataforma LLAVE CDMX puede ser reutilizada por la CONAMER para el desarrollo del expediente único electrónico.

---

[371] Gobierno de la Ciudad de México, LLAVE CDMX, Disponible en https://llave.cdmx.gob.mx/oauth.xhtml?client_id=20191017135030123 4&redirect_url=https%3A%2F%2Fllave.cdmx.gob.mx%2Findex.xhtml&state=-VbxMMqNs8qBhnSO_yfq21gloRrFK1X3IyI3223JNj8gPM-PNdOecFLF9eNwzVW-, (Fecha de consulta 12 de septiembre de 2020).

[372] Gobierno de la Ciudad de México, Aviso de Privacidad LLAVE CDMX, Disponible en: https://llave.cdmx.gob.mx/resources/docs/aviso.pdf, Fecha de consulta 12 de septiembre de 2020).

Pero, para ello, la colaboración entre el SAT, la SE y la SFP será relevante ya que, de conformidad con la LFFEA, tienen el carácter de autoridades certificadoras. Vemos viable una mesa de trabajo entre RENAPO, CONAMER, SAT, SE, SFP, SRE, INAI y PJF para diseñar un modelo integral de identidad digital única y firma electrónica que favorezca el desarrollo digital de México con base en principios de interoperabilidad y seguridad en un contexto digital nacional e internacional.

La *tercera recomendación* es aprovechar la infraestructura de clave pública que México ha desarrollado desde el año 2004 a través de la firma electrónica avanzada a cargo del SAT, en observancia de los principios de eficiencia, eficacia y economía de los recursos públicos previstos en el artículo 134 de la CPEUM.

Actualmente, de los casi **120 millones de mexicanos**, a mayo de 2020, en el padrón fiscal se cuenta con un total de **78.5 millones** de contribuyentes, de los cuales **76.3 millones son personas físicas** y **2.1 millones son personas morales.** Según cifras el INEGI al 2018, del total de la población en México, **38.3 millones son niñas, niños y adolescentes de 0 a 17 años**. Es decir, sólo aproximadamente 3.2 millones de las personas físicas adultas en México[373] no cuentan con una firma electrónica y, por ende, con una identidad digital.

Esto resulta relevante porque en México -a diferencia de otros países- cuenta con la gran ventaja de, prácticamente, **el 80% de la población adulta, cuenta con una identidad digital y firma electrónica a nivel nacional**. Esta gran ventaja debe contemplarse en el diseño de la cédula de identidad nacional, máxime que, como analizamos, instituciones de los tres órdenes de gobierno, así como otros poderes públicos, han suscrito convenios con el SAT para reutilizar el componente de la firma electrónica en sus procedimientos locales.

Si bien, dicha firma se regula en el CFF y, por ende, puede ser discriminatorio en materia de identidad digital para aquellas personas que no cuenten con un RFC o sean menores de edad, no debemos perder de vista la importancia del artículo 17-D del CFF en materia de identidad y firma electrónica. Consideramos que la

[373] INEGI, Encuesta Nacional de Ocupación y Empleo, abril de 2019, Disponible en: https://www.inegi.org.mx/contenidos/saladeprensa/aproposito/2019/nino2019_Nal.pdf, (Fecha de consulta 12 de septiembre de 2020).

aplicación de este artículo destrabaría la regulación y tecnicismos de la identidad digital en México. No obstante, nos da la impresión de que la interpretación de este artículo en relación con el RENAPO se ha dejado a un lado.

En términos del citado artículo se establece que los datos de identidad que recabe el SAT formarán parte del sistema integrado de registro de población a cargo de RENAPO. Es decir, se requiere de la interoperabilidad entre RENAPO y SAT para garantizar a la población una identidad digital a través de certificados digitales como lo realizan los países más avanzados en desarrollo digital. Algunas propuestas para fortalecer la interoperabilidad entre estas dos instituciones son:

(i) Analizar la viabilidad de vincular a los menores de edad con los certificados digitales de los tutores o quienes tengan la patria potestad;
(ii) Identificar a los 3.2 millones de personas físicas que no cuenten con un certificado digital, para que, RENAPO, en colaboración con la Secretaría del Bienestar, el SAT y los registros civiles locales, puedan emitir certificados digitales asociados a su CURP;
(iii) Los menores de edad deben ser representados por su tutor(a) para realizar actos jurídicos o acceder a ciertos servicios públicos, por lo que en el diseño de servicios digitales consideramos importante asociar el CURP del menor con el certificado digital del tutor(a);
(iv) La homologación de identidad digital y firma electrónica entre personas físicas y jurídicas facilitará su reconocimiento transfronterizo y, por ende, la economía digital a través de los TLC suscritos por México.

Contar con sistema de identidad nacional sencillo, interoperable, armonizado, escalables, sostenible y seguro puede mejorar la eficiencia y eficacia en la gestión de programas sociales para la población, fomentar la economía digital y evitar la duplicidad de esfuerzos. No obstante, para ello es necesario articular una reforma legal en materia de identidad y firma electrónica con impacto nacional, considerando las disposiciones previstas en el CFF, la LGP, el CCOM, la LFFEA, la legislación local y las disposiciones judiciales en la materia. Además, consideramos

que lo anterior permitirá evitar la duplicidad de esfuerzos y recursos en el diseño e implementación de la cédula de identidad digital con biométricos que contempla la SEGOB en su programa 2018-2024 o en la iniciativa de la nueva LGP.

La *cuarta recomendación* es contar con una tarjeta de identidad física y digital como ocurre en Estonia, Uruguay o Sudáfrica. Esto, atendiendo las brechas digitales que en México pueden limitar a una persona acceder a servicios públicos por carecer de conectividad o bien, opte por un canal presencial ante la falta de habilidades digitales. En los países mencionados, se incorporar elementos digitales a la tarjeta física de identidad. Tanto en Estonia como Uruguay garantizan este modelo a través de su autoridad de registro civil quien interoperar con el resto de las entidades públicas.

En Estonia, por ejemplo, la autoridad del registro civil es el proveedor de la identidad digital que es a su vez interopera con instituciones públicas y privadas a través de la plataforma X-ROAD. A través de este mecanismo garantiza la seguridad de los sistemas del registro civil y la protección de los datos personales. Para hacer posible este tipo de identidad digital, tanto Estonia como Uruguay contemplan cuatro elementos en las tarjetas físicas de identificación, los cuales pueden ser considerados por México:

(i) **Chip sin contacto.** Constituye un mecanismo de seguridad que contiene toda la información personal y gráfica que está a la vista de forma electrónica. La información del documento y el tipo de chip[374]. La tecnología sin contacto se ha utilizado, además de las credenciales de identidad, en las tarjetas bancarias con la finalidad de otorgar mayor seguridad a la identidad y las transacciones de las personas. Incorpora la tecnología *Near Field Communication* (NFC) la cual es una tecnología de conectividad inalámbrica de corto alcance basada en estándares facilita el intercambio de contenido digital y la conexión entre dispositivos electrónicos de forma segura[375].

(ii) **Chip con contacto.** Dispositivo de seguridad que contiene un *software* configurado con: cuatro huellas principales del usuario; los certificados de la

[374] Ibidem, p. 14.
[375] NCF, Forum, "¿Qué es NFC?", Disponible para su consulta en https://nfc-forum.org/what-is-nfc/. (Fecha de consulta 12 de septiembre de 2020).

firma electrónica avanzada, y el *Match on Card* configurado con dichos elementos[376]. Estos son los datos que contiene el chip con contacto en Uruguay. Estos chips siguen el estándar EMV sobre medios de pago definido por los sistemas internacionales de VISA y MasterCard. Es un estándar de interoperabilidad de tarjetas con Chip para la autenticación de pagos mediante tarjetas de crédito y débito[377].

(iii) **Firma electrónica.** Es importante incorporar en la cédula de identidad, los componentes de la firma electrónica avanzada. En el caso de México, y para evitar la duplicidad de funciones, consideramos necesario incorporar la firma electrónica emitida por el SAT a la cédula de identidad[378], siendo que actualmente más del 80% adulta cuenta con una firma electrónica.

(iv) **Código MRZ**. Este código constituye se contiene en los documentos oficiales de viaje o de identidad de muchos países. Contienen una zona legible por máquina (MRZ, por sus siglas en inglés) con información codificada de datos personales. Contiene 2 o 3 líneas con el texto de fuente *OCR-B escrito de acuerdo con el Documento 9303 de la OACI*[379]. Estos datos normalmente son: lugar de emisión, material utilizado; fecha de nacimiento, fecha de emisión del documento; nacionalidad; fecha de vencimiento del documento; nombre y apellidos. En este punto será relevante la interoperabilidad con la SRE para para la expedición del pasaporte mexicano.

---

[376] Ministerio del Interior de Uruguay, Dirección Nacional de Identificación Civil, “Manuela de Documento (…) p. 14. (Fecha de consulta 12 de septiembre de 2020).

[377] Galeano, Jonnhy. “Seguridad en transacciones con tarjetas EMV”, Universidad Piloto de Colombia, p. 3, Disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2925/00001203.pdf?sequence=1. (Fecha de consulta 12 de septiembre de 2020).

[378] En el caso de Uruguay, la firma electrónica se emite por la Unidad de Certificación Electrónica, un órgano desconcentrado de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento dotada de la más amplia autonomía técnica. Véase, artículo 12 de la Ley Nº 18.600. documento y firma electrónicos, Disponible en: https://legislativo.parlamento.gub.uy/temporales/leytemp8209035.htm (Fecha de consulta 12 de septiembre de 2020).

[379] Disponible en: https://www.refworld.org/cgi-bin/texis/vtx/rwmain/opendocpdf.pdf?reldoc=y&docid=5319964d4. (Fecha de consulta 12 de septiembre de 2020).

A través de mecanismos criptográficos, una adecuada gestión tanto de usuarios y claves entre la SEGOB, la CONAMER y el SAT, el modelo de identidad digital en México puede cobrar forma y cumplir con los estándares internacionales sobre identidad digital, interoperabilidad y seguridad[380]. La información ya existe, los mecanismos también, sólo falta fortalecer el marco normativo en las citadas leyes y propiciar mecanismos de cooperación que faciliten un modelo único y seguro de identidad digital en México.

Por último, la *quinta recomendación* es la integración de la firma electrónica avanzada de SAT al Sistema Nacional de Mejora Regulatoria. En términos del artículo 9 de la LGMR, esta Ley tiene por objeto coordinar a las autoridades de todos los tres órdenes de gobierno en materia de mejora regulatoria. Dicha coordinación cobra relevancia ya que en términos del artículo 50 de la LGMR se establece la creación del expediente de trámites y servicios el cual operará conforma a los lineamientos que apruebe el Consejo Nacional de Mejora Regulatoria. Entre los elementos que debe contemplar los lineamientos están los temas de: seguridad, disponibilidad, integridad, autenticidad, confidencialidad y custodia. Para ello, la identidad digital y firma electrónica resultan clave.

Actualmente, los "*Lineamientos Generales para la operación del Expediente para Trámites y Servicios*", establecen que el expediente de trámites y servicios deberá contener un sistema de gestión de procesos común a nivel nacional, el cual, a su vez, podrá obtener los documentos electrónicos contenidos en el expediente[381] y poner a disposición de los sujetos obligados un catálogo de estandarización para la digitalización de trámites y servicios digitales[382]. Entre los requisitos del sistema

---

[380] Así, podría solucionarse el eterno desacuerdo entre la SEGOB y el INE para compartir datos biométricos del padrón electoral. Antonio Baranda, "Mantienen SEGOB e INE desacuerdo por cédula", Reforma, 22 enero 2020, Ciudad de México, https://www.reforma.com/aplicacioneslibre/preacceso/articulo/default.aspx?__rval=1&urlredirect=https://www.reforma.com/mantienen-segob-e-ine-desacuerdo-por-cedula/ar1858568?referer=--7d616165662f3a3a6262623b727a7a7279703b767a783a--. Sin duda, un órgano constitucional autónomo como el INE tiene la obligación legal de cuidar los datos personales del padrón electoral y utilizarlos para los fines con los que fueron recabados.

[381] Artículo vigésimo séptimo de los Lineamientos, *Lineamientos Generales para la operación del Expediente para Trámites y Servicios,* publicado en el DOF el 13 de julio de 2020, Disponible en: https://dof.gob.mx/nota_detalle.php?codigo=5596610&fecha=13/07/2020

[382] Ídem, artículo vigésimo octavo de los Lineamientos.

de gestión se establece el uso de la firma electrónica[383] de los sujetos obligados, los cual consideramos que también debe incluir la firma electrónica de los ciudadanos en aquellos casos en que sea necesario, con la finalidad de otorgar certeza jurídica de las transacciones desde su origen. Este este modelo, la experiencia de la Ciudad de México será relevante para evitar duplicidad de esfuerzos y recursos, y garantizar a las personas el derecho a la identidad digital de forma única, segura e interoperable a nivel nacional.

[383] Ídem, artículo vigésimo octavo, fracción X, y tercero transitorio, fracción V de los Lineamientos.

Bibliografía

- Acuerdo por el que se crea la CFE Telecomunicaciones para todos, publicado en el DOF el 02 de agosto de 2019, Disponible en: http://www.dof.gob.mx/nota_detalle.php?codigo=5567088&fecha=02/08/2019
- ACUERDO por el que se modifican las políticas y disposiciones para la Estrategia Digital Nacional, en materia de Tecnologías de la Información y Comunicaciones, y en la de Seguridad de la Información, así como el Manual Administrativo de Aplicación General en dichas materias, publicado en el DOF el 08 de mayo de 2014 Última reforma publicada DOF 23-07-2018, Disponible en: https://www.gob.mx/cms/uploads/attachment/file/380408/MAAGTICSI_compilado__20182208.pdf, http://www.diputados.gob.mx/LeyesBiblio/pdf/140_120718.pdf;
- Adobe, “Electronic Signature Laws & Regulations - South Korea”, 2020, Disponible en: https://helpx.adobe.com/sign/using/legality-south-korea.html
- Agencia Brasil, “Brasileños tendrán documento digital unificado de identificación”, Brasil, 2019, Disponible en: https://agenciabrasil.ebc.com.br/es/geral/noticia/2019-07/brasilenos-tendran-documento-digital-unificado-de-identificacion.
- Agencia del Gobierno de Singapur, “Conceptos clave”, Singapur, 2020, Disponible en: https://www.imda.gov.sg/regulations-and-licensing-listing/electronic-transactions-act-and-regulations/controller-of-certification-authorities/key-concepts,
- Agency for Digitisation, Ministry of Finance, “National identity and signing”, Dinamarca, 2020, Disponible en: https://en.digst.dk/digitisation/eid/
- Agenda Digital APEC, Disponible en: https://www.apec.org/-/media/APEC/Publications/2019/11/APEC-Framework-for-Securing-the-Digital-Economy/219_TEL_APEC-Framework-for-Securing-the-Digital-Economy.pdf
- Agenda Digital CEPAL, Disponible en: https://www.cepal.org/es/elac2020/agenda-digital-2020,

- Agenda Digital del Mercosur, Disponible en: http://www.sice.oas.org/Trade/MRCSRS/Decisions/DEC_027_2017_s.pdf.
- AGESIC, “Agenda Digital del Uruguay, Uruguay, 2019, Disponible en: https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/politicas-y-gestion/programas/agenda-digital-del-uruguay, https://www.gub.uy/agencia-(Fecha de consulta: 25 de junio de 2020). gobierno-electronico-sociedad-informacion-conocimiento/sites/agencia-gobierno-electronico-sociedad-informacion-conocimiento/files/2019-08/Descargar%20Agenda%20Digital%202020%20%28Mayo%202019%29%20%28.pdf%20318%20KB%29.pdf
- AGESIC, “Firma digital”, Uruguay, 2020, Disponible en: https://firma.agesic.gub.uy/
- AGESIC, “Prestadores Acreditados”, Uruguay, 2020, Disponible en: https://www.gub.uy/unidad-certificacion-electronica/politicas-y-gestion/prestadores-acreditados.
- ALADI, “Propuesta para la digitalización de certificados de origen en el ámbito de la ALADI, ALADI/SEC/dt 459/Rev.”, 2004, Disponible en: http://www2.aladi.org/nsfweb/Documentos/459Rev2.pdf
- Alianza del Pacífico, Subgrupo de Agenda Digital, Disponible en: https://alianzapacifico.net/wp-content/uploads/Hoja-de-Ruta-SGAD2016-2017.pdf
- Allende López, Marcos, “Blockchain Cómo desarrollar confianza en entornos complejos para generar valor de impacto social, Banco Interamericano de Desarrollo”, Washington, 2018, p. 27, Disponible en: http://governance40.com/wp-content/uploads/2018/11/Blockchain-Como-desarrollar-confianza-en-entornos-complejos-para-generar-valor-de-impacto-social-1.pdf
- Álvarez, Rosa María, “Derecho a la identidad”, IIJ-UNAM, México, 2002, p. 118, Disponible en: https://archivos.juridicas.unam.mx/www/bjv/libros/9/4242/8.pdf
- Amenta, Valentina, Lazzaroni, Adriana y ABBA Laura, “Internet identity and the right to be forgotten: International Trends and regulatory perspectives”, IGI

Global - International Publisher of Progressive Academic Research, USA, 2015, Disponible en: https://www.iit.cnr.it/sites/default/files/Internet-Identity-and-the-Right-to-be-Forgotten--International-Trends-and-Regulatory-Perspectives.pdf

- ANGWIN, Julia, LARSON, Jeff, MATTU, Surya, and KIRCHNER, Lauren, “Machine Bias, Tehe´s software used across de country to predict future criminals. And it´s biased against blacks”, Pro Publica, mayo 23, 2016, https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing
- Asamblea General de la ONU, Resolución A/RES/55/2, “Declaración del Milenio”, Disponible en: https://www.un.org/spanish/milenio/ares552.pdf
- Asamblea General de la ONU, Resolución A/RES/70/1, Transformar nuestro mundo: la Agenda 2030 para el Desarrollo Sostenible, 21 de octubre de 2015, Disponible en: https://www.un.org/ga/search/view_doc.asp?symbol=A/RES/70/1&Lang=S.
- Baltierra Guerrero, Alfredo, La firma autógrafa en el derecho bancario, UNAM-IIJ, México, Disponible en: https://revistas-colaboracion.juridicas.unam.mx/index.php/rev-facultad-derecho-mx/article/view/30813/27804.
- Barreto Zuñiga, Lizbeth Angélica, “Evolución de la firma autógrafa a la firma electrónica avanzada”, Revista Digital Universitaria, 1 de marzo 2011 • Volumen 12 Número 3, p. 5, Disponible en: http://www.revista.unam.mx/vol.12/num3/art34/art34.pdf.
- Biblioteca de la Universidad de Alicante, “La huella digital”, Universidad de Alicante, España, p. 2-3, Disponible en: https://rua.ua.es/dspace/bitstream/10045/79601/1/CI2_intermedio_2017-18_Huella-digital.pdf
- Biblioteca del Congreso Nacional de Chile, “Ley 19799, sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma”, Chile, 2014, Disponible en: https://www.leychile.cl/Navegar?idNorma=196640

- Biblioteca del Congreso Nacional de Chile, “Ley de Transformación Digital del Estado”, Chile, 11 de noviembre de 2019, Disponible en: https://www.leychile.cl/Navegar?idNorma=1138479
- Biblioteca del Congreso Nacional de Chile, “Ley sobre documentos electrónicos, firma electrónica y servicios de certificación”, Chile, 2002, Disponible en: https://www.leychile.cl/Navegar?idNorma=196640
- Bill Of Rights, “Ley que Declara los Derechos y Libertades de los Ingleses y Establece el Orden de Sucesión de la Corona”, Inglaterra, 1689, Disponible en https://www.dipublico.org/3664/bill-of-rights-ley-que-declara-los-derechos-y-libertades-de-los-ingleses-y-establece-el-orden-de-sucesion-de-la-corona-inglaterra-1689/.
- Chavero González, Adrián, “La tercera revolución industrial en México: diagnóstico e implicaciones”, IIJ-UNAM, México, 1992, pp. 166, 261 y 263, Disponible en http://ru.iiec.unam.mx/1223/1/LaTerceraRevolucion.pdf
- Chávez Palacios, Julián, Desarrollo tecnológico en la primera revolución industrial, Universidad de Extremadura, Norba, Revista de Historia, Vol. 17, 2004, p. 93-109, Disponible en: https://dialnet.unirioja.es/descarga/articulo/1158936.pdf.
- CMSI-ODS Matriz, “Vinculación de las líneas de acción de la CMSI con los Objetivos de Desarrollo Sostenible”, Disponible en: https://www.itu.int/net4/wsis/sdg/Content/Documents/wsis-sdg_matrix_document.pdf
- CNUDMI, “Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónicas”, ONU, Viene, 2009, p. 3, Disponible en: https://www.uncitral.org/pdf/spanish/texts/electcom/08-55701_Ebook.pdf
- CNUDMI, “Panorama general de la gestión de la identidad digital”, A/CN.9/WG.IV/WP.120, 27 de julio de 2012, p. 5, Disponible en: https://www.uncitral.org/pdf/spanish/workinggroups/wg_iv/46th_WG_IV/wp_120_s.pdf .

- Código de Comercio, Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf_mov/Codigo_de_Comercio.pdf;
- Código de Comercio, y su reforma publicada en el DOF el 29 de agosto de 2003, DECRETO por el que se reforman y adicionan diversas disposiciones del Código de Comercio en Materia de Firma Electrónica, Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/3_301219.pdf
- Código Fiscal de la Federación, reforma publicada en el DOF el 05 de enero de 2004, Disponible en: http://www.diputados.gob.mx/LeyesBiblio/ref/cff/CFF_ref31_05ene04.pdf.
- Comisión Europea, Despliegue seguro de la 5G en la EU, Bruselas, Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020DC0050&from=FR,
- Comisión Europea, Estrategia Europea de Datos, Bruselas, Disponible en: https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf,
- Comisión Europea, Una Agenda Digital para Europa, Bruselas, 19.5.2010 COM(2010)245 final, Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52010DC0245&from=es
- Comisión Europea, Una Estrategia para el Mercado Único Digital de Europa, Bruselas, 6.5.2015, COM(2015) 192 final, Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:52015DC0192
- Congreso de Estados Unidos, “21st Century Integrated Digital Experience Act, 05 de octubre de 2018”, Estados Unidos, Disponible en: https://www.congress.gov/bill/115th-congress/house-bill/5759/text
- Convenios de firma electrónica avanzada, actualizado al 13 de febrero de 2019, Disponible en: https://www.gob.mx/sfp/documentos/convenios-de-firma-electronica-avanzada.

- Corte de los Estados Unidos, “Case 16-22134”, Estados Unidos, 2016, Disponible en: https://www.govinfo.gov/content/pkg/USCOURTS-caeb-2_16-bk-22134/pdf/USCOURTS-caeb-2_16-bk-22134-0.pdf
- Corte Interamericana de Derechos Humanos, “Caso de las Hermanas Serrano Cruz Vs. El Salvador”, 2005, p. 71, Disponible en: https://www.corteidh.or.cr/docs/casos/articulos/seriec_120_esp.pdf
- CPEUM, reforma publicada en el DOF el 05 de febrero de 2017, Disponible en http://www.diputados.gob.mx/LeyesBiblio/ref/dof/CPEUM_ref_230_05feb17.pdf.
- Crosby Michael, Nachiappan, Pradhan Pattanayak, Sanjeev Verma Y Kalyanaraman, Vignesh, “Blockchain Technology”, Uc Berkeley, San Francisco, California, Octubre, 2015, p. 30, Disponible en: https://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf
- Declaración de los Derechos del Hombre y del Ciudadano de 1789, Disponible en: https://www.conseilconstitutionnel.fr/sites/default/files/as/root/bank_mm/espagnol/es_ddhc.pdf
- Declaración Universal de Derechos Humanos, Disponible en: https://www.un.org/es/documents/udhr/UDHR_booklet_SP_web.pdf
- Department of telecomunications and postal services, “National e-Government Strategy and Roadmap, República de Sudáfrica, 2017, Disponible en: https://www.dtps.gov.za/images/phocagallery/Popular_Topic_Pictures/national_e-Gov_Strategy.pdf
- Department telecomunication and postal services, Republic of South Africa, “National Integrated ICT Policy White Paper”, 2016, Disponible en: https://www.dtps.gov.za/images/phocagallery/Popular_Topic_Pictures/National_Integrated_ICT_Policy_White.pdf
- Diario Oficial de la República de Chile, “Acuerdo de reconocimiento mutuo de certificados de firma digital con la República de Argentina”, Chile, 2019, Disponible en: https://documentos.camaraaduanera.cl/circ/2019/R212-

19_DEC.%20N%C2%BA%20261,%20MIN.%20RR.%20EE.%20-%20Promulga%20Acuerdo%20Reconocimiento%20Mutuo%20de%20Certificados%20de%20Firma%20Digital%20con%20Argentina.%20ACE%20N%C2%B0%2016%20(D.O.).pdf

- Diario Oficial de la 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 la que se deroga la Directiva 1999/93/CE”, Europa, 2014, Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32014R0910&from=IT
- Disposiciones Generales de la Ley de Firma Electrónica Avanzada, publicadas en el DOF el 21 de octubre de 2016, Disponible en: https://www.dof.gob.mx/nota_detalle.php?codigo=5457756&fecha=21/10/2016.
- Docusign, “Sitio web de la solución”, Estados Unidos, 2020, Disponible en: https://www.docusign.com/
- Durán Villán, Carlos, “Historia y descripción general de los derechos económicos, sociales y culturales, en González Monguí, Pablo Elías (coord), Derechos económicos, sociales y culturales, Universidad Libre de Colombia, Colombia, 2009, p.10, Disponible en: http://www.corteidh.or.cr/tablas/26759.pdf
- e-estonia, “e-Identity”, Estonia, 2020, Disponible en: https://e-estonia.com/solutions/e-identity/
- e-estonia, “How Estonia became a global heavyweight in cyber security”, Estonia, 2020, Disponible en: https://e-estonia.com/how-estonia-became-a-global-heavyweight-in-cyber-security/
- e-estonia, “Interoperability servicies e-Estonia”, Estonia, 2020, Disponible en: https://e-estonia.com/solutions/interoperability-services/x-road/
- e-estonia, “we have built a digital society and we can show you how”, Estonia, 2020, Disponible en: https://e-estonia.com/,

- Estrada Corona, Adrián, “Protocolos TCP/IP de Internet”, Revista Digital Universitaria, UNAM, Volumen 5, Número 8, México 2004, p. 2, Disponible en: http://www.revista.unam.mx/vol.5/num8/art51/sep_art51.pdf.
- Fernández Lara, Rosa María, “La revolución francesa: bases sociales, ideológicas y proceso de institucionalización”, Proyecto CLIO, número 36, s.a., Disponible en: http://clio.rediris.e
- Fernández Ruíz, Jorge, “El Registro del Estado Civil de las Personas”, UNAM-IIJ, México, p. 11, Disponible en: https://archivos.juridicas.unam.mx/www/bjv/libros/7/3100/5.pdf,
- FJELD, Jessica, ACHTEN, Nele, HILLIGOSS, Hannah, CHRISTOPHER, Adam, MADHULIKA SRIKUMAR, Nagy, “Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-based Approaches to Principles for AI”, Harvard, Berkman Klein Center, Research Publication No. 2020-1 January 15, Boston, Estados Unidos, 2020, https://cyber.harvard.edu/publication/2020/principled-ai.
- Gaceta Gubernamental, “Electronic communicatios and transactions Acta 2002”, Sudáfrica, 2002, Disponible en: https://www.gov.za/sites/default/files/gcis_document/201409/a25-02.pdf
- Gobierno de Argentina, “Agenda Digital”, Argentina, 2018, Disponible en: http://servicios.infoleg.gob.ar/infolegInternet/anexos/315000-319999/318677/res138.pdf
- Gobierno de Argentina, “Autoridad Certificante Raíz de la República Argentina (ACRAIZ)”, Argentina, 2020, Disponible en: https://www.argentina.gob.ar/jefatura/innovacion-publica/administrativa/firmadigital/acraiz.
- Gobierno de Argentina, “Plataforma de Firma Digital Remota PFDR”, Argentina, 2020, Disponible en: https://www.argentina.gob.ar/jefatura/innovacion-publica/administrativa/firmadigital/firmadigitalremota.
- Gobierno de Argentina, “SID - Sistema de Identidad Digital”, Argentina, 2020, Disponible en: https://www.argentina.gob.ar/interior/renaper/sid-sistema-de-identidad-digital

- Gobierno de Australia, “An easy and secure way to prove who you are online”, Australia, 2020, Disponible en: https://www.mygovid.gov.au/,
- Gobierno de Australia, “Digital Transformation Strategy”, Australia, 2018, Disponible en: https://dta-www-drupal-20180130215411153400000001.s3.ap-southeast-2.amazonaws.com/s3fs-public/files/digital-transformation-strategy/digital-transformation-strategy.pdf
- Gobierno de Australia, “Electronic Transactions Regulations”, Australia, 2000, Disponible en: https://www.legislation.gov.au/Details/F2019C00345,
- Gobierno de Australia, “How do I get set up?”, Australia, 2020, Disponible en: https://www.mygovid.gov.au/how-do-i-get-set-up,
- Gobierno de Australia, “myGovID Terms of use – User”, Australia, 2019, Disponible en: https://www.mygovid.gov.au/mygovid-terms-of-use-user.
- Gobierno de Brasil, “DECRETO Nº 10.332, DE 28 DE ABRIL DE 2020”, Brasil, 2020, Disponible en: https://www.redgealc.org/site/assets/files/10577/decreto_n_10_332-_de_28_de_abril_de_2020.pdf
- Gobierno de Canadá, “Plan Estratégico del Gobierno de Canadá para la Gestión de la Información y la Tecnología de la Información 2017 a 2021”, Canadá, 2016, Disponible en: https://www.canada.ca/en/treasury-board-secretariat/services/information-technology/strategic-plan-2017-2021.html
- Gobierno de Canadá, “Using a Sign-in Partner”, Canadá, Disponible en: https://www.canada.ca/en/revenue-agency/services/e-services/cra-login-services/sign-partners-help-faqs/using-a-sign-partner.html
- Gobierno de Canadá, “What is GCKey?”, Canadá, 2020, Disponible en: https://www.cic.gc.ca/english/helpcentre/answer.asp?qnum=794&top=23
- Gobierno de Chile, “Estrategia de Transformación Digital del Estado”, Chile, 2019, Disponible en: https://digital.gob.cl/doc/estrategia_de_transformacion_digital_2019_.pdf

- Gobierno de Corea del Sur, “Korea e-Government Master Plan 2020”, Korea, 2017, Disponible en: https://www.kdevelopedia.org/resource/view/04201706080147946.do#.Xws4mShKjIU
- Gobierno de Dinamarca, “Digital Strategy 2016-2020” Dinamarca, 2016, Disponible en: https://en.digst.dk/media/14144/ds_spread_uk_web.pdf
- Gobierno de Estados Unidos, “Digital Government Strategy”, Estados Unidos, 2012, Disponible en: https://www.state.gov/digital-government-strategy/#:~:text=A%20comprehensive%20Digital%20Government%20Strategy,launched%20on%20May%2023%2C%202012.&text=U.S.%20Government%20agencies%20are%20asked,services%20to%20the%20American%20people.%E2%80%9D
- Gobierno de Estados Unidos, “Open Government Initiative”, Estados Unidos, 2020, Disponible en: https://www.state.gov/open-government-initiative/
- Gobierno de Estados Unidos, “Open Source Software”, Estados Unidos, 2016, Disponible en: https://sourcecode.cio.gov/OSS/.
- Gobierno de Estados Unidos, “Project Open Data”, Estados Unidos, 2020, Disponible en: https://project-open-data.cio.gov/
- Gobierno de Estados Unidos, Public Law, “Electronic signatures in global and national commerce Act”, U.S, 2000, Disponible en: https://www.govinfo.gov/content/pkg/PLAW-106publ229/pdf/PLAW-106publ229.pdf
- Gobierno de Estonia, “Population Register”, Estonia, 2020, Disponible en: https://www.siseministeerium.ee/en/population-register
- Gobierno de Nueva Zelanda, “Strategy for a Digital Public Service”, Nueva Zelanda, 2020, Disponible en: https://www.digital.govt.nz/assets/Digital-government/Strategy/Strategy-for-a-Digital-Public-Service.pdf
- Gobierno de Singapur, “Marco de Acción para la Economía Digital en Singapur”Singapur, 2018, Disponible en: https://www.imda.gov.sg/-/media/Imda/Files/SG-Digital/SGD-Framework-For-Action.pdf

- Gobierno de Sudáfrica, “Conoce la nueva Tarjeta de Identificación Inteligente”, Sudáfrica, 2020, Disponible en: http://www.dha.gov.za/index.php/id-smart-card,
- Gobierno Federal, “Governo lança Documento Nacional de Identificação que dispensa apresentação de CPF e Título de Eleitor”, Brasil, 2018, Disponible en: https://www.gov.br/economia/pt-br/assuntos/noticias/planejamento/governo-lanca-documento-nacional-de-identificacao-que-dispensa-apresentacao-de-cpf-e-titulo-de-eleitor
- Harbitz, Mia, Tamargo, María del Carmen, “El significado de la identidad legal en situaciones de pobreza y exclusión social”, Banco Interamericano de Desarrollo, Washington DC, 2010, p. 2, https://publications.iadb.org/publications/spanish/document/El-significado-de-la-identidad-legal-en-situaciones-de-pobreza-y-exclusi%C3%B3n-social-El-subregistro-de-nacimientos-y-la-indocumentaci%C3%B3n-desde-la-perspectiva-de-g%C3%A9nero-y-etnia-en-Bolivia-Ecuador-y-Guatemala.pdf
- Husenovic, Kemal, “Sentando las bases para la 5G: Oportunidades y desafíos”, ITU, Ginebra, Suiza, 2018, p. 3, Disponible en: https://www.itu.int/dms_pub/itu-d/opb/pref/D-PREF-BB.5G_01-2018-PDF-S.pdf
- IFT, “Espectro Radioeléctrico, Disponible en: http://www.ift.org.mx/sites/default/files/industria/espectro-radioelectrico/radiodifusion/2016/6/apendiceda.pdf.
- IFT, Agentes económicos preponderantes, Disponible en: http://www.ift.org.mx/conocenos/acerca-del-instituto/historia/determina-ift-los-agentes-economicos-preponderantes.
- IMPO, Centro de Información Oficial, “Ley No. 18600”, Uruguay, 2009, Disponible en: https://www.impo.com.uy/bases/leyes/18600-2009
- INEGI, Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares 2019, Disponible en: https://www.inegi.org.mx/programas/dutih/2019/

- Info Leg, CORTE SUPREMA DE JUSTICIA DE LA NACIÓN, “Acordada 11/2020”, Ciudad de Buenos Aires, 2020, Disponible en: http://servicios.infoleg.gob.ar/infolegInternet/anexos/335000-339999/336345/norma.htm
- InfoLEG, “Ley 25.506 de Firma Digital”, Argentina, 2001, Disponible en: http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70749/texact.htm
- Instituto de Ingeniería del Conocimiento, “7 herramientas del big data para tu empresa”, octubre 13, 2016, Disponible en: https://www.iic.uam.es/innovacion/herramientas-big-data-para-empresa/
- Instituto Nacional de Ciberseguridad “Cloud computing”, guía de aproximación para el empresario, España, s.a., p. 5, Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia-cloud-computing_0.pdf
- ITU, “Connect 2030 Agenda, access a better world”, Goal 1 – Growth, Target 1.4: By 2023, all countries adopt a digital agenda/strategy”, Ginebra, 2020, Disponible en: https://itu.foleon.com/itu/connect-2030-agenda/growth/
- Jóvenes Construyendo el Futuro Recibirán Capacitación en Habilidades Tecnológicas, BOLETÍN DE PRENSA No. 26 / 2019, Disponible en: https://www.gob.mx/stps/prensa/jovenes-construyendo-el-futuro-recibiran-capacitacion-en-habilidades-tecnologicas?idiom=es
- KANE, Gerald C. “‘Digital Transformation” Is a Misnomer, It’s not about digital or transformation. It’s about adaptation”, MIT Sloan Management Review, Bostón, Estados Unidos, Agosto, 2017, Disponible en https://sloanreview.mit.edu/article/digital-transformation-is-a-misnomer/#:~:text=At%20its%20most%20fundamental%20level,wrought%20by%20evolving%20digital%20technologies.&text=Digitally%20mature%20organizations%20exhibit%20certain,nothing%20to%20do%20with%20technology
- Kaplan, Marcos, “Estado y globalización”, Instituto de Investigaciones Jurídicas, México, 2002, pp. 149-221, Disponible en: https://archivos.juridicas.unam.mx/www/bjv/libros/1/277/3.pdf

- Kelsen, Hans, “La teoría pura del derecho”, Buenos Aires, Editorial Losada, S.A, s.a. p. 45.
- Korea La, “Electronic Signature Act (ESA)”, Korea, 2017, Disponible en: https://elaw.klri.re.kr/eng_service/lawView.do?hseq=42625&lang=ENG
- Korea Law, “Digital Signature Act, Korea”, 2017, Disponible en: https://elaw.klri.re.kr/eng_service/lawView.do?hseq=42625&lang=ENG#:~:text=The%20purpose%20of%20this%20Act,and%20advancing%20social%20benefit%20and
- Landes, D.S. Progreso tecnológico y revolución industrial, Madrid, Tecnos, 1979, p. 15
- Lansiti, Marco , Karim R. Lakhani, “The Truth About Blockchain”, from the january–february 2017 issue, Harvard Business Publishing, Disponible en: https://hbr.org/2017/01/the-truth-about-blockchain
- Leinerp Barry M., kahn Robert E., “Brief History of the Internet 1997”, internetsociety.org, p, 9, Disponible en https://www.internetsociety.org/wp-content/uploads/2017/09/ISOC-History-of-the-Internet_1997.pdf
- Ley de Firma Electrónica Avanzada, publicada en el DOF el 11 de enero de 2012, Disponible en: http://www.diputados.gob.mx/LeyesBiblio/ref/lfea.htm
- Ley de Transacciones Electrónicas de Arizona, Gobierno de Estados Unidos, “44-7061”, Estados Unidos, Disponible en: https://www.azleg.gov/ars/44/07061.htm
- Ley Federal de Telecomunicaciones y Radiodifusión, publicada en el DOF el 11 de junio de 2013, Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFTR_240120.pdf.
- Ley General de Mejora Regulatoria, Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LGMR_180518.pdf

- Ley Korea, “Framework Act on electronic documents and transactions”, 2016, Disponible en: http://www.law.go.kr/lsInfoP.do?lsiSeq=179518&lsId=002000&chrClsCd=010202&urlMode=engLsInfoR&viewCls=engLsInfoR#0000
- Ley Uniforme de Transacciones Electrónicas de Tennessee (22 de marzo de 2018), PUBLIC CHAPTER NO. 591”, Tennese, 2018, Disponible en: https://blockchainlawguide.com/resources/Tennesee---Blockchain-Law---2018-03-22.pdf
- Lineamientos generales para la operación del expediente para trámites y servicios, publicados en el DOF el 13 de julio de 2020, Disponible en: http://dof.gob.mx/nota_detalle.php?codigo=5596610&fecha=13/07/2020
- Lyons, Tom, Courcelas, Ludovic, TIMSIT, Ken, “Blockchain and digital identity”, EU Blockchain Observatory & Forum, Mayo 2019, p. 12, Disponible en: https://www.eublockchainforum.eu/sites/default/files/report_identity_v0.9.4.pdf
- M. Turing, “Computing Machinery And Intelligence”, Mind 49: 433-460, Disponible en: https://www.csee.umbc.edu/courses/471/papers/turing.pdf
- MELL, Peter, GRANCE, Timothy, “The NIST Definition of Cloud Computing”, NIST, Computer Security Division Information Technology Laborator, September 2011, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf
- Mercosur, “Reconocimiento de la eficacia jurídica del documento electrónico, la firma electrónica y la firma electrónica avanzada en el ámbito del MERCOSUR, MERCOSUR/gmc EXT./RES. Nº 37/06, 2006, Disponible em: http://www.sice.oas.org/trade/mrcsrs/resolutions/Res3706.pdf
- MILogin, “Sitio web de la solución de identidad del estado de Michigan”, Michigan, 2020, Disponible en: https://milogin.michigan.gov/
- Ministerio de Tecnología, Comunicación e Innovación, “Digital Mauritius 2030”, República de Mauricio, 2018, Disponible en: http://mitci.govmu.org/English/Do-

cuments/2018/Launching%20Digital%20Transformation%20Strategy%20191218/DM%202030%2017%20December%202018%20at%2012.30hrs.pdf

- Ministry of Communications and Information, “Plan de planeación digital de Singapur”, Singapur, 2020, Disponible en: https://www.mci.gov.sg/en/portfolios/digital-readiness/digital-readiness-blueprint
- MIT, “What is Artificial Intelligence (AI)?”, 6.825 Techniques in Artificial Intelligence, Washington, s.a., pp. 3-7, Disponible en: https://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-825-techniques-in-artificial-intelligence-sma-5504-fall-2002/lecture-notes/Lecture1Final.pdf
- MIT, Basic Internet Concepts, Disponible en: http://staff.um.edu.mt/mros1/wwww/basic_web_concepts.html.
- Mustapich, J.M. Tratado de Derecho Notarial, T.1., p 260.
- Nelken-Terner, Antoinette, “Globalización o mundialización ¿Indiscutibles? ¿Incuestionables?”, Política y Cultura, número 10, Universidad Autónoma Metropolitana Unidad Xochimilco, Ciudad de México, 1998, p. 63, Disponible en: https://www.redalyc.org/pdf/267/26701005.pdf
- Nem ID, “NemID and Digital Denmark”, Dinamarca, 2020, Disponible en: https://studycph.dk/nemid-digital-denmark/
- Nem ID, “Sitio web de proveedor de servicios”, Dinamarca, 2020, Disponible en: https://www.medarbejdersignatur.dk/
- Nem ID, “Use the same NemID for all services”, Dinamarca, 2020, Disponible en: https://www.nemid.nu/dk-en/help_for_nemid/use_one_nemid/,
- Nemid, “NemID conditions for online banking and public digital signatures, v.7), 2020, Disponible en: https://www.nemid.nu/dk-en/about_nemid/nemid_conditions/NemID-rules-for-online-banking-and-public-digital-signature-version-7.pdf

- NOM-024-SSA3-2012, sobre sistemas de información de registro electrónico para la salud .Intercambio de información en salud, Disponible en: http://dof.gob.mx/nota_detalle.php?codigo=5280847&fecha=30/11/2012
- NOM151, publicada en el DOF el 30 de marzo de 2017, Disponible en: https://dof.gob.mx/nota_detalle.php?codigo=5478024&fecha=30/03/2017
- Noticias electorales, "(Brasil) Identidad Digital Podrá Ser Emitida Para Todos Los Ciudadanos Registrados En El Programa Identidad Civil Nacional (Icn)", Brasil, 2019, Disponible en: https://www.noticiaselectorales.com/brasil-identidad-digital-podra-ser-emitida-para-todos-los-ciudadanos-registrados-en-el-programa-identidad-civil-nacional-icn/.
- OEA, "Globalización y su impacto en el comercio mundial y regional", 1993 Disponible en: https://www.oas.org/dsd/publications/unit/oea33s/ch32.htm
- OEA, "Programa interamericano para el registro civil universal y "derecho a la identidad", AG/RES. 2362 (XXXVIII-O/08), 2008, Disponible en: http://www.oas.org/sap/docs/puica/RES_2362_ProgramaInteramericano_s.pdf
- Office of the Privacy commissioner of Canada, "The Personal Information Protection and Electronic Documents Act (PIPEDA)", Canadá, 2020, Disponible en: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/
- OH ID, "Portal de acceso a Ohio ID", Ohio, 2020, Disponible en: https://ohid.ohio.gov/wps/portal/ohid/business/login/!ut/p/z1/fY3BCoJAFEW_Zra-h46l7cYWRZAREenbhMo4iubIODW_n1CboLq7czmXCwQZ0FA8WlXYVg9FP3NOi6t_XIttssE0CuMlijQ4iyQ--ZxzuAAB_VEO_C3gjwiEHZDqdfm6E0MZRArIyFoaaby7mevG2nFaMWTonPOU1qqXXqVvDL9NGj1ZyD5NGLuu3tswfwIviP2a/dz/d5/L2dBISEvZ0FBIS9nQSEh/
- ONU e ITU, Declaración de Principios CONSTRUIR LA SOCIEDAD DE LA INFORMACIÓN: UN DESAFÍO GLOBAL PARA EL NUEVO MILENIO, Documento WSIS-03/GENEVA/4-S 12 de mayo de 2004, Disponible en:

https://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!PDF-S.pdf,

- ONU e ITU, Plan de Acción, Documento WSIS-03/GENEVA/5-S 12 de mayo de 2004, Disponible en: https://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0005!!PDF-S.pdf, , y Declaración de la CMSI+10 relativa a la aplicación de los resultados de la CMSI, Disponible en: http://www.itu.int/net/wsis/implementation/2014/forum/inc/doc/outcome/362828V2S.pdf
- ONU, “Ley Modelo de la CNUDMI sobre Comercio Electrónico”, 1996, Disponible en: https://www.uncitral.org/pdf/spanish/texts/electcom/05-89453_S_Ebook.pdf.
- ONU, “Ley Modelo de la CNUDMI sobre Firmas Electrónicas”, Nueva York, 2002, Disponible en: https://www.uncitral.org/pdf/spanish/texts/electcom/ml-elecsig-s.pdf
- ONU, Department of Economic and Social Affairs, “E-Government Survey 2020, Digital Government in the Decade of Action for Sustainable Development”, Nueva York, 2020, p. XXII, Disponible en: https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2020-Survey/2020%20UN%20E-Government%20Survey%20(Full%20Report).pdf
- ONU, Resolución aprobada por la Asamblea General, 56/183. Cumbre Mundial sobre la Sociedad de la Información, Disponible en: http://www.itu.int/net/wsis/docs/background/resolutions/56_183_unga_2002-es.pdf,
- Organización Internacional de Trabajo, “El futuro del Trabajo que queremos: un diálogo global”, p. 11, Disponible en: https://www.ilo.org/wcmsp5/groups/public/---dgreports/---cabinet/documents/publication/wcms_570288.pdf
- Pacto Internacional de Derechos Económicos, Sociales y Culturales, Disponible en: https://www.ohchr.org/SP/ProfessionalInterest/Pages/CESCR.aspx .
- Parlamento Europeo, Estrategia de Ciberseguridad de la Unión Europea, 2013, Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52013JC0001.

- Parlamento Mauricio, “The electronic transactions Act 2000”, República de Mauricio, 2000, Disponible en https://www.icta.mu/docs/laws/eta.pdf [1] Korea III, “Número de registro de residente”, 2020, Disponible en:
- Peemes, Jean-Philippe, “Revoluciones industriales, modernización y desarrollo”, Universidad Católica de Lovaina, Junio 1992, p. 4, Disponible en: https://www.researchgate.net/publication/26498690_Revoluciones_industriales_modernizacion_y_desarrollo
- Plan Nacional de Desarrollo 2018-2024, DOF 12 de julio de 2019, Disponible en: https://www.dof.gob.mx/nota_detalle.php?codigo=5565599&fecha=12/07/2019,
- Planiol y Ripet, Traité Practiqué de Droit Civiel Francais, VII, No. 1458.
- Poder Judicial del Estado de México, “Términos y Condiciones de Uso de los Certificados Digitales de la FEJEM”, Disponible en http://fejem.pjedomex.gob.mx/fejem/Politic.htm.
- Políticas para la obtención y uso de la firma electrónica certificada el Poder Judicial de la Federación, así como para la operación de su infraestructura tecnológica Aprobado el 10 de junio de 2004, Disponible en: https://www.pjf.gob.mx/Docs/Politicas%20Firel%20con%20rubricas%20y%20firmas.pdf.
- Portal de Gobierno de la República de Mauricio, “”Card layout and Design New ID Card”, República de Mauricio, 2020, Disponible en: http://mnis.govmu.org/English/ID%20Card/Pages/Card-Design.aspx
- Presidencia de la República, “Decreto número 3.587”, Brasil, del 05 de septiembre de 2000, Disponible en: http://www.planalto.gov.br/ccivil_03/decreto/D3587.htm
- Presidencia de la República, “Qué es la Cédula de Identidad Digital”, Uruguay, 2020, Disponible en: https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/firma-digital/es-cedula-identidad-digital

- Programa de capacitación en competencias digitales para docentes del Sistema Educativo Nacional, Disponible en: https://www.gob.mx/sep/es/articulos/boletin-no-82-lanza-sep-programa-de-capacitacion-en-competencias-digitales-para-docentes-del-sistema-educativo-nacional?idiom=es
- Programa de Cobertura Social, Disponible en: https://www.gob.mx/sct/acciones-y-programas/programa-de-cobertura-social;
- Programa sectorial de economía 2020-2024, Disponible en: https://www.dof.gob.mx/nota_detalle.php?codigo=5595481&fecha=24/06/2020;
- Programa Sectorial de Función Pública 2020-2024, publicado en el DOF el 26 de junio de 2020, https://www.dof.gob.mx/nota_detalle.php?codigo=5595678&fecha=26/06/2020
- Programa Sectorial de Gobernación 2020-2024, Disponible en: https://www.gob.mx/cms/uploads/attachment/file/563303/PSG_2020_-_2024.pdf
- Programa Sectorial de la SCT 2020-2024, Disponible en: http://dof.gob.mx/nota_detalle.php?codigo=5596042&fecha=02/07/2020; y https://www.gob.mx/cms/uploads/attachment/file/500252/2019-10-02_PCS_version_web_miercoles_9_octubre.pdf
- Programa Sectorial de la SEP, publicado en el DOF el 06 de julio de 2020 Disponible en: https://www.gob.mx/cms/uploads/attachment/file/562380/Programa_Sectorial_de_Educaci_n_2020-2024.pdf
- Propuesta para la digitalización de certificados de origen en el ámbito de la ALADI, Disponible en http://www2.aladi.org/nsfweb/Documentos/459Rev2.pdf,
- Protocolo de control de transmisión TCP/IP, Disponible en: https://www.ibm.com/support/knowledgecenter/es/ssw_aix_72/network/tcpip_terms.html.

- Proyecto de Modelo de Habilidades Digitales SCT, Disponible en: https://www.gob.mx/cms/uploads/attachment/file/444450/Marco_de_habilidades_digitales_vf.pdf
- Public Law, “Electronic Signatures In Global And National Commerce Act”, Estados Unidos, 2000, Disponible en: https://www.govinfo.gov/content/pkg/PLAW-106publ229/pdf/PLAW-106publ229.pdf
- REDGEALC, “Firma digital y servicios transfronterizos”, 2020, Disponible en: https://www.redgealc.org/lineas-de-trabajo/servicios-transfronterizos/.
- Redl, Christoph, Muente-Kunigami, Arturo, “Blockchain en la Administración Pública ¿Mucho ruido y pocos bloques?”, Banco Interamericano de Desarrollo, Washington, Estados Unidos, 2019, p. 84, Disponible en: https://publications.iadb.org/publications/spanish/document/Blockchain_en_la_administraci%C3%B3n_p%C3%BAblica_Mucho_ruido_y_pocos_bloques_es.pdf
- Reglamento de la Ley Federal de Firma Electrónica Avanzada, publicado en el DOF el 21 de marzo de 2014 (sin reformas) Disponible en: http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFEA.pdf.
- Reglamento Interior de la SCT, Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/153_220120.pdf
- Reglamento Interior de la SFP, publicado en el DOF el 16 de abril de 2020, Disponible en: http://www.dof.gob.mx/nota_detalle.php?codigo=5591703&fecha=16/04/2020; y el
- Republica de Estonia, “Become an e-resident), Estonia, 2020, Disponible en: https://e-resident.gov.ee/become-an-e-resident/
- Resolución Miscelánea Fiscal, Publicada en el DOF el 28 de diciembre de 2019, Disponible en https://dof.gob.mx/20191228-2.pdf.
- Resolución que modifica las disposiciones de carácter generar aplicables a las instituciones de crédito, publicada en el DOF el 29 de agosto de 2017, Disponible

en: https://www.dof.gob.mx/nota_detalle.php?codigo=5495299&fecha=29/08/2017

- Reuters, Thomson, “Electronic signature platforms key contractual issues”, PLC Magazine, Reino Unido, January/February 2017, Disponible en: https://ec.europa.eu/futurium/en/system/files/ged/plc_article_on_e-signature_platforms_final_feb_2017.pdf
- Rose, Karen, Scott, Lyman Chapin,“Internet de las cosas- una breve reseña, Internet Society, Octubre 2015, p. 5, Disponible en: https://www.internetsociety.org/wp-content/uploads/2017/09/report-InternetOfThings-20160817-es-1.pdf
- Sandra Segeran, y M. Li. “Identity Management” en ZHANG, Y., “Handbook of Research on Wireless Security”, Harvey PA: IGI-Global, p 15.
- SAT, firma electrónica, Disponible en: http://omawww.sat.gob.mx/ForoTributarioDeServiciosElectronicos2015/Paginas/Documentos/ConveniosColaboracion_FirmaElectronica.pdf
- SAT, Padrón RFC, Disponible en: http://omawww.sat.gob.mx/cifras_sat/Paginas/datos/vinculo.html?page=giipTipCon.html.
- SE, Prestadores de servicios de certificación, Disponible en: http://www.firmadigital.gob.mx/directorio.html
- SEGOB, CURP, Disponible en: https://www.gob.mx/segob/renapo/es/articulos/sabes-como-se-conforma-tu-curp?idiom=es
- SERPRO, “Certificación digital”, Brasil, 2020, Disponible en: https://www.serpro.gov.br/clientes/certificacao_digital.
- SERPRO, “El Serpro”, Brasil, 2020, Disponible en: https://www.serpro.gov.br/menu/institucional/quem-somos.

- Singapur Statutes Online, “Electronic Transactions (Certification Authority) Regulations 2010”, Singapur, 2010, Disponible en: https://www.imda.gov.sg/-/media/Imda/Files/Regulation-Licensing-and-Consultations/Acts-Regulations/Electronic-Transactions-Certification-Authority.pdf?la=en
- Sitio de Gobierno Chile, “La nueva plataforma de Comunicaciones oficiales del Estado”, Chile, 2020, Disponible en: https://doc.digital.gob.cl/
- Sitio de gobierno digital, “ClaveÚnica”, Chile, 2020, Disponible en: https://digital.gob.cl/servicios/plataformas-compartidas/clave-unica.
- Sitio de gobierno Digital, “Firma Gob”, Chile, 2020, Disponible en: https://digital.gob.cl/servicios/plataformas-compartidas/firma-gob
- Smart Nation Singapur, “Agenda Digital”, Singapur, 2020, Disponible en: https://www.smartnation.gov.sg/
- Smart Nation Singapur, “Estrategia de Ciberseguridad de Singapur”, Singapur, 2020, Disponible en: https://www.smartnation.gov.sg/why-Smart-Nation/secure-smart-nation
- Smart Nation Singapur, “National Digital Identity (NDI), Singapur, 2020, Disponible en: https://www.smartnation.gov.sg/what-is-smart-nation/initiatives/Strategic-National-Projects/national-digital-identity-ndi
- Tamargo, María del Carmen, “Identidad legal, ciudadanía y vulnerabilidad social. Notas para el estudio del subregistro de nacimientos y la indocumentación con perspectiva de género y etnicidad”, XXVII Congreso de la Asociación Latinoamericana de Sociología. VIII Jornadas de Sociología de la Universidad de Buenos Aires. Asociación Latinoamericana de Sociología, Buenos Aires, 2009, p. 3, Disponible en http://cdsa.aacademica.org/000-062/655.pdf
- Televisión Educativa, Disponible en: https://www.televisioneducativa.gob.mx/ingenioTV.html

- T-MEC, Capítulo 19 Comercio Digital, Disponible en: https://www.gob.mx/cms/uploads/attachment/file/465801/19ESPComercioDigital.pdf
- Trans-Lex, University of Colage, “Danish Contracts Act”, 2020, Disponible en: https://www.trans-lex.org/604900/_/danish-contracts-act/
- Tratado de Asunción para la Constitución de un Mercado Común, del 26 de marzo de 1991, Disponible en: https://www.mercosur.int/documento/tratado-asuncion-constitucion-mercado-comun/
- UIT, “Digital identity roadmap guide”, 2018, p. 4, Disponible en: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-DIGITAL.01-2018-PDF-E.pdf
- ULCC, CHLC, “Uniform Electronic Commerce Act Annotated 1999”, Canadá, 1999, Disponible en: https://www.ulcc.ca/en/annual-meetings/359-1999-winnipeg-mb/civil-section-documents/1138-1999-electronic-commerce-act-annotated#:~:text=The%20Uniform%20Electronic%20Commerce%20Act,relationship%20that%20may%20require%20documentation.
- UNICEF, “Convención sobre los Derechos del Niño”, 2006, p. 12, Disponible en: https://www.un.org/es/events/childrenday/pdf/derechos.pdf
- Viktor Mayer-Schönberger y Kenneth Cukier, Big Data, la revolución de los datos masivo, Disponible en: http://catedradatos.com.ar/media/3.-Big-data.-La-revolucion-de-los-datos-masivos-Noema-Spanish-
- Villena Román, Julio, Crespo García, Raquel M., García Rueda, José Jesús, “Historia de la Inteligencia Artificial”, Universidad Carlos III de Madrid, Madrid, España, s.a., p. 4, Disponible en: http://ocw.uc3m.es/ingenieria-telematica/inteligencia-en-redes-de-comunicaciones/material-de-clase-1/01-historia-de-la-inteligencia-artificial
- Visión regulatoria de las telecomunicaciones y la radiodifusión, 2019-2023, septiembre 2018, Disponible en: http://www.ift.org.mx/sites/default/files/contenido-general/transparencia/1vision19-23.pdf

- Windley, P. J., “Digital Identity: Unmasking Identity Management Architecture (IMA). O'Reilly Media inc., Estados Unidos de América, 2005, p. 9.
- Xiaomeng Su, “Introduction to Big Data”, Institutt for informatikk og e-læring ved NTNU, Suecia, s.a., p. 3, Disponible en: https://www.ntnu.no/iie/fag/big/lessons/lesson2.pdf
- Yanome Yesaki, Mauricio, “El concepto de servicio público y su régimen jurídico en México”, IIJ-UNAM, p. 698, Disponible en: https://archivos.juridicas.unam.mx/www/bjv/libros/6/2544/31.pdf.
- Zaldívar Lelo de Larrea, Arturo, “Líneas Generales de Trabajo 2019-2022, SCJN-CJF, 2018, Disponible en: https://www.scjn.gob.mx/sites/default/files/carrusel_usos_multiples/documento/2019-01/lineas-grales-trabajo-mp-arturo_zaldivar_lelo_de_larrea.pdf.

ANEXOS

ANEXO I. Mecanismos de identidad digital en el contexto internacional

Mecanismos de Identidad en el Contexto Internacional					
País	**Nombre asignado**	**Institución responsable (Pública-Privada)**	**Mecanismo para acreditar ña identidad digital**	**Mecanismo de seguridad**	**Objetivo**
Sudáfrica	**Tarjeta de identificación inteligente**	Departamento del Interior (Pública)	• Huella digital biométrica. • Verificación y un código pin conocido solo por el usuario. • Un software seguro integrado con su microprocesador contiene de manera segura detalles de identificación y garantiza que solo las autoridades autorizadas puedan leer y verificar los datos de la tarjeta utilizando escáneres legibles por máquina sin contacto.	• Características de seguridad física en el cuerpo de la tarjeta, como hologramas, grabado láser y detalles personales que proporcionan una verificación visual de la tarjeta e identifican fácilmente las tarjetas manipuladas. • Seguridad lógica que incluye datos biométricos de huellas dactilares y datos biográficos integrados en el chip de la tarjeta de 80 kilobytes. • Personalización con grabado láser de detalles demográficos y fotografías.	• Asegurar servicios gubernamentales. • Reducir el fraude y el robo de identidad. • Una identificación electrónica nacional única para todos los ciudadanos. • Plataforma futura para un conjunto de servicios de administración electrónica que incluye en línea autenticación y firmas digitales. • Beneficios para ciudadanos. • Elimina la necesidad de llevar múltiples documentos de identificación. • Mejora la confianza en las credenciales de identidad oficiales. • Acelera los controles de identidad en el cruce de fronteras. • Establece la ciudadanía en el Registro Nacional de Población para votar y otras interacciones cívicas
Isla Mauricio	**Tarjeta de Identidad Nacional de Mauricio**	Oficina del Primer Ministro (Pública)	• Número de ID • Tinta óptica variable • Patrón de debilitamiento • Impresión lenticular e impresión labrada.	• Los datos grabados en diferentes capas de la tarjeta se almacenan en el 'chip', lo que ayuda a evitar que otras personas alteren o usen tarjetas perdidas o robadas. Los datos de cada tarjeta de identificación inteligente se protegen electrónicamente y solo se pueden validar a través de la Autoridad de Certificación MNIS (MNIS CA) que garantiza la autenticidad de la identidad del individuo. • Incluye una serie de características de	• Conveniencia: ya no será necesario llevar varios documentos a varias organizaciones, como bancos y otras agencias gubernamentales, para probar la identidad y el comprobante de domicilio. • Servicio de calidad; la tarjeta de identificación inteligente ayudará en el avance de los futuros servicios del gobierno electrónico. Aplicación adicional: El logotipo 'SC' en la

				• seguridad visual que incluyen impresión de líneas entrecruzadas, microimpresión, impresión ultravioleta (UV), etc. y utiliza grabado láser para imprimir en diferentes capas de las tarjetas de identificación. • Todas y cada una de las tarjetas Smart ID tienen un Número de Control de Tarjeta (CCN) único. Estas características de seguridad proporcionan el mecanismo para detectar cualquier caso de falsificación.	tarjeta de identificación inteligente permite la tarifa gratuita de autobús para ciudadanos de 60 años o más.
Corea del Sur	**Sistema de tarjeta de identificación de residente**	Ministerio del Interior y Seguridad (Pública)	• Número de registro de residente de 13 dígitos que contiene nombre, número de registro, domicilio, huella digital y fotografía.	Un dígito de control, que se utiliza para verificar que el número ha sido transcrito correctamente. Se genera a partir del resto de los dígitos utilizando un algoritmo	• Servicios gubernamentales • Servicios financieros. • Autenticación en sitios web.
Singapur	**DNI**	Agencia Tecnológica del Gobierno (Pública)	• Huella digital biométrica, • Reconocimiento facial. • Plataforma y móvil	• Código de acceso de 6 dígitos. • Token físico para ciudadanos en el extranjero; • Criptografía;	• Trámites gubernamentales • Transacciones comerciales: Remesas móviles transfronterizas digitales. • Solicitudes de tarjeta de crédito. • Solicitudes en línea para cuentas corrientes y de ahorro, préstamos para automóviles y tarjetas de crédito en transacciones de propiedad con StreetSine; • Compra de seguro de vida.
Estonia	**e-identity; ID-Crad; Mobile-ID; e-Residency; Smart-ID**	Empresas autorizadas por el gobierno que interoperan con el registro de población (Público-Privada)	• Tarjeta física con chip • Teléfono Móvil • Dispositivo cualificado	• Chip cifrado con clave pública • Tarjeta SIM Móvil especial que se debe solicitar al operador móvil • Código PIN • Dispositivo cualificado	• Identificación legal • Seguro de salud • Cuentas bancarias • Firmas digitales Votación • Registros médicos • Recetas médicas • Residencia digital
Dinamarca	**NEMID NemID Code App NemID for all services Nets DanID A/S**	Agencia Danesa de Digitalización Nets DanID A / S (Público-Privada)	• Código para sesión en Internet • Nube • Móvil • Interopera con el Registro de Población	• Token de código • Software instalado en la computadora el usuario • Contraseña • PIN	• Servicios públicos • Servicios financieros • Interacción con empresas

Australia	**myGovID**	Oficina de Impuestos de Australia. Se basa en un modelo descentralizado, fue concebido como una 'federación de identidad' que consta de proveedores y servicios de identidad del sector público y privado	• Servicio de verificación facial. • Almacena el nombre de una persona, fecha de nacimiento, número de teléfono móvil, identificadores de documentos de identidad personal y dirección de correo electrónico	• Estándares de seguridad y los principios de privacidad, • seguridad e integridad del gobierno australiano como: datos personales, • Acreditación con documentos de identidad física, • Autoridad de Supervisión • Consentimiento	• Crear una identidad digital que luego se puede utilizar para iniciar sesión en los servicios • Gubernamentales en línea. • Evitar nuevos aumentos en el costo del delito de identidad
Nueva Zelanda	**RealMe**	Departamento de Asuntos Internos (Pública)	Nombre de usuario y contraseña únicos	• Evaluación de impacto de seguridad independiente cada vez que realizan un cambio significativo en RealMe o en el código que lo respalda. • Evaluación de impacto de privacidad cada vez que realizan un cambio importante en RealMe. • Programa continuo de pruebas de seguridad.	• Sitios y servicios gubernamentales de Nueva Zelanda. • Abrir una cuenta bancaria • Solicitar el primer pasaporte • Inscribirse para votar
Estados Unidos	**Cada Estado se encarga de gestionar la identidad digital en su ámbito local, algunos ejemplos son MILogin (Michigan) OHIID (Ohio)**	Departamento administrativo de gobierno locales (Pública)	Usuario y contraseña	Claves únicas, usuario y contraseña	Mejorar servicios públicos
Uruguay	**Cédula de Identidad Digital (tarjeta física con chip)**	Dirección Nacional de Identificación (Pública)	Tarjeta física con chip uno visible y otro sin contacto.	• Lectura de chip • Lectura de datos biométricos • Huella digital • PIN	• Servicios públicos • Transacciones comerciales • Transacciones bancarias • Control migratorio • Firma electrónica • Compras por internet
Canadá	**1) GBKey 2(SecureKey**	Gobierno Bancos (Público-Privado)	Software	Usuario y contraseña	• Servicios en línea • Servicios bancarios
Argentina	**SID Sistema de Identidad Digital**	Ministerio del Interior y la Secretaría de Innovación Pública	Software - plataforma, interoperable con el Registro Nacional de Personas en Argentina	• Certificados digitales • Autenticación biométrica • Prestador de servicios de certificación	• Servicios financieros
Chile	**Clave Única**	Registro Civil	Clave única a través de una página web o aplicación móvil	• Contraseña • Protocolo Openid Connect • Validación de identidad utilizando el Servicio del	• Servicios públicos

				Registro Civil e Identificación	
Brasil	**Documento de Identificación Nacional (DNI)**	Servicio interoperable entre las bases de datos del gobierno federal (Ministerio de Planificación, Desarrollo y Gestión) y el poder judicial y el uso de EET basado en biometría.	Tarjeta física con chip que integra datos biométricos.	• Chip • Claves de seguridad en un servidor protegido. • Criptografía • Código QR • Marca de agua • Código de verificación que contiene 20 caracteres, precedido de la fecha y la hora en que se generó.	• Integración de diversos servicios y facilitar la vida cotidiana del ciudadano. • Integración de bases de datos federales y eliminando viajes innecesarios, tiempos de espera en colas, impresión de certificados y autenticación de documentos.

Fuente: Elaboración propia.

Fuente: ONU. EDGI. 2020.

ANEXO II. Sistemas internacionales de firma electrónica

Sistemas de Firma Electrónica				
País	**Tipo (Simple, avanzada o cualificada)**	**Proveedor**	**Usos**	**Vinculada con su sistema de Identidad Digital**
Sudáfrica	• **Avanzada**	Proveedores de servicios de certificación	• Admisible por el Tribunal. Uso comercial general • Transacciones con organismos públicos y privados, instituciones y ciudadanos	No
Isla Mauricio	• **Simple** • **Avanzada**	Proveedores de servicios de certificación	• Comercio electrónico • Servicios de gobierno • Notarios • Tribunal de justicia	No
Corea del Sur	• **Simple** • **Avanzada**	Proveedores de servicios de certificación	• Firmar contratos comerciales generales • Contratos de trabajo • Contratos de arrendamiento • Tribunales y jueces • Actos de comercio • Servicios gubernamentales	No
Singapur	• **Simple** • **Avanzada**	• Gobierno Digital Government Blueprint • Proveedores de servicios de certificación	• Usos comerciales • Transacciones electrónicas • Transacciones con el gobierno	SI
Estonia	• **Avanzada** • **Cualificada**	Proveedores de certificación	• Identificación legal • Seguro de salud • Cuentas bancarias • Firmas digitales • Votación • Registros médicos • Recetas médicas • Residencia digital	Si
Dinamarca	• **Certificada**	• Prestadores de servicios de certificación • Instituciones financieras, a través de la interoperabilidad del Pasaporte o licencia de conducir	• Servicios públicos • Servicios financieros • Interacción con empresas	Si
Australia	• **Simple**	Sin proveedor	• Uso comercial • Tribunal • Transacciones con las empresas • Transacciones con el gobierno	No
Nueva Zelanda	• **Simple**	Sin proveedor	• Contratos • Venta de bienes • Transacciones electrónicas • Transporte de mercancías • Asuntos comerciales, incluidos agentes mercantiles y conocimientos de embarque.	No

Estados Unidos	• **Simple**	Sin proveedor	• Sector público, privado, con excepción de los actos jurídicos que requieren una formalidad, como el derecho de familia o sistema financiero	No
Uruguay	• **Simple** • **Avanzada** • **Cualificada**	Proveedores de servicios de certificación	• Sector público • Sector privado • Transacciones bancarias	SI
Canadá	• **Simple**	Sin proveedor	• Público • Comercial • Proceso judicial • Con excepción de testamentos, fideicomisos o poderes notariales	No
Argentina	• **Simple** • **Avanzada**	Proveedores de servicios de certificación	• Trámites con entidades públicas y privadas • Relaciones impositivas • Notificaciones judiciales • Operaciones bancarias • Contratos a distancia • Documentos de comercio exterior	No
Chile	• **Simple** • **Avanzada**	• Gobierno para el sector público firma digital • Prestadores de servicios de certificación sector privado	• Servicios púbicos • Privado • Proceso judicial	No
Brasil	• **Avanzada** • **Cualificada**	El Gobierno lleva la gestión de las políticas y cuenta con una cadena de autoridades de certificación.	• Usos comerciales • Tribunal	No

Fuente: Elaboración propia.

ANEXO III. Atribuciones institucionales sobre la transformación digital en México

Atribuciones institucionales en México sobre Transformación Digital			
Institución	**Atribución**	**Acciones planeadas o ejecutadas**	**Temas Transformación digital / pidu**
Presidencia de la República (CEDN)[384]	• Está facultada para definir las políticas del gobierno federal en los temas de informática, TIC y gobierno digital. • Define a la EDN el plan de acción del Ejecutivo Federal para aprovechar el potencial de las TIC, incluidos los servicios de banda ancha e Internet, como elemento catalizador del desarrollo del país, mediante su incorporación a la vida cotidiana de las personas, y a la APF el uso de la informática y el desarrollo del gobierno digital. Es la encargada de (i) elaborar, dar seguimiento y evaluar la EDN en la APF; (ii) definir y coordinar las políticas y programas de gobierno digital, promoviendo la innovación, apertura, transparencia, colaboración y participación ciudadana para mejorar la inclusión digital; (iii) establecer mecanismos de coordinación para el cumplimiento de políticas en materia de informática, gobierno digital y TIC.	Si bien a la fecha de elaboración del presente documento aún no se cuenta con la publicación de la EDN -lo anterior, considerando que recientemente se publicó el nuevo Reglamento de la Oficina de la Presidencia de la República, el pasado 09 de diciembre de 2019- consideramos relevante fortalecer los servicios de banda ancha e Internet y de gobierno digital, en colaboración con las autoridades competentes como la SCT y el IFT[385]. Lo anterior, toda vez que si bien en el 2020, México figura con un elevado índice de servicios digitales (0.8235) conforme al EDGI, lo cierto es que respecto al índice te infraestructura y cobertura es bajo (0.5910), así como el de capital humano con (0.6337). Por lo será relevante para México fortalecer acciones de infraestructura y capital humano. Además, consideramos importante que en la elaboración de la EDN se contemplen los elementos legales previstos en los artículos 201, 202, 2014, 2018 y 2019 de la LFTR, en donde se establece que: • El Ejecutivo Federal debe promover la implementación de los portales de la APF con funciones de accesibilidad en los sectores público y privado. • El Ejecutivo Federal, de conformidad con la EDN y el IFT, deberán promover el acceso de las personas con discapacidad a los nuevos sistemas y las TIC, incluido internet. • El IFT debe apoyar programas de cobertura social y de conectividad. • A la SEP le corresponde, en términos de la EDN, promover el uso de las TIC en el sector de la educación. • A la SSA le corresponde, en los términos que se establezca en el EDN, promover, en colaboración con la SCT, el uso de las TIC en el sector salud.	**1.** TIC; **2.** Gobierno digital; **3.** Servicios de banda ancha e Internet. **4.** Innovación **5.** Apertura u transparencia. **6.** Colaboración y participación ciudadana. **7.** Inclusión digital

[384] Artículo 8, de la LOAPF, LOAPF, publicada en el DOF el 30 de noviembre de 2018, Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/153_220120.pdf, y artículos 2 y 36 del Reglamento de la Oficina de la Presidencia de la República, publicado en el DOF el 09 de diciembre de 2019, Disponible en: https://dof.gob.mx/nota_detalle.php?codigo=5581283&fecha=09/12/2019 (Fecha de consulta 05 de febrero de 2020)

[385] No obstante, el antecedente inmediato en México es la EDN 2013-2018, se contemplaban cinco objetivos 1) transformación gubernamental; 2) economía digital; 3) educación de calidad; 4) salud universal y efectiva, y 5) seguridad ciudadana. Igualmente, contaba con cinco habilitadores: 1) conectividad; 2) inclusión y habilidades digitales; 3) interoperabilidad; 4) marco jurídico; y 5) datos abiertos. Disponible en: https://www.inr.gob.mx/Descargas/trc/EstrategiaDigital.pdf, (Fecha de consulta 05 de febrero 2020).

SFP[386]	• Vigilar la aplicación de las políticas de gobierno digital, y definir las de gobierno y datos abiertos de la Administración Pública Federal. • Establecer lineamientos y programas que coadyuven al cumplimiento y aplicación del combate a la corrupción, gobierno y datos abiertos en la APF.	Entre las acciones que contempla la SFP para cumplir con estas atribuciones, están las siguientes: • Implementar acciones para que la información pública se genere y difunda de conformidad con los principios de datos abiertos, y asegurar su calidad y utilidad pública mediante la mejora de los sistemas de información, los sitios web y los buscadores y repositorios de transparencia proactiva y de datos abiertos. • Fomentar la adopción de estándares internacionales de transparencia y publicación de datos abiertos en materias prioritarias para la prevención y combate a la corrupción. • Instrumentar acciones para impulsar la innovación en los procesos de diseño, implementación y evaluación de políticas públicas, en el marco de los principios de gobierno abierto. • Instrumentar una estrategia de involucramiento de la ciudadanía en la toma de decisiones públicas para garantizar que los proyectos, programas y políticas contribuyan en todo momento al interés público, así como generar sinergias en materia de combate a la corrupción.	**1.** Vigilar el cumplimiento de la política de gobierno digital; **2.** Gobierno abierto. **3.** Datos abiertos
SCT[387]	• Elaborar políticas de telecomunicaciones y radiodifusión del Gobierno Federal. • Planear y conducir las políticas y programas de cobertura universal y cobertura social. • Coordinarse con el IFT para promover, en el ámbito de sus respectivas atribuciones, el acceso a las TIC y a los servicios de radiodifusión y telecomunicaciones, incluido el de banda ancha e Internet, en condiciones de competencia efectiva. • Realizar las acciones tendientes a garantizar el acceso a Internet de banda ancha en edificios e instalaciones de la APF y coad-	Entre los objetivos principales de la SCT está el de promover la cobertura, el acceso y el uso de servicios postales, de telecomunicaciones y radiodifusión, en condiciones que resulten alcanzables para la población, con énfasis en grupos prioritarios y en situación de vulnerabilidad, para fortalecer la inclusión digital y el desarrollo tecnológico. Por ello, la SCT desarrollo el Programa de Cobertura Social388, mediante el cual se busca: (i) identifican las localidades sin servicios de telecomunicaciones, incluyendo banda ancha e Internet, para facilitar las acciones del gobierno, de los concesionarios y de la sociedad civil con el objetivo de llevar estos servicios a donde actualmente no existen; (ii) coadyuvar con la empresa CFE Telecomunicaciones e Internet para Todos a identificar las principales localidades sin servicio y pone especial énfasis en las zonas marginadas del país, a efecto de que todas las personas, en particular las que se encuentran en situación de vulnerabilidad, tengan acceso a las nuevas tecnologías, buscando cerrar la	**1.** Cobertura universal **2.** Cobertura social **3.** Acceso a las TIC y servicios de telecomunicaciones y radiodifusión **4.** Acceso a Internet en APF y en sitios públicos. **5.** Transformación digital

[386] Artículo 37 de la LOAPF; Reglamento Interior de la SFP, publicado en el DOF el 16 de abril de 2020, Disponible en: http://www.dof.gob.mx/nota_detalle.php?codigo=5591703&fecha=16/04/2020; y el Programa Sectorial de Función Pública 2020-2024, publicado en el DOF el 26 de junio de 2020, https://www.dof.gob.mx/nota_detalle.php?codigo=5595678&fecha=26/06/2020 (Fecha de consulta 05 de febrero de 2020).

[387] Artículo 36 de la LOAPF; artículo 9 de la LFTR; Reglamento Interior de la SCT, Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/153_220120.pdf (Fecha de consulta 06 de Febrero de 2020)

[388] Programa de Cobertura Social, Disponible en: https://www.gob.mx/sct/acciones-y-programas/programa-de-cobertura-social; Programa Sectorial de la SCT 2020-2024, Disponible en: http://dof.gob.mx/nota_detalle.php?codigo=5596042&fecha=02/07/2020; y https://www.gob.mx/cms/uploads/attachment/file/500252/2019-10-02_PCS_version_web_miercoles*_9_octubre.pdf (Fecha de consulta 06 de febrero de 2020)

	yuvar con Estados y Municipios para cumplir con este objetivo. • Establecer programas de acceso a banda ancha en sitios públicos que identifiquen el número de sitios a conectar cada año de manera progresiva, hasta alcanzar la cobertura universal. • Atender las disposiciones que en materia de EDN.	brecha digital para lograr altos niveles de desarrollo social sin discriminación; (iii) incorporar información sobre la geolocalización de diversos proyectos y programas prioritarios del Gobierno de México, que coordinan, con diversas instituciones del sector público, la integración de las zonas deprimidas a través de las telecomunicaciones y la radiodifusión, incluida la banda ancha e Internet, a las actividades de salud, educativas, de cultura y productivas, y (iv) generar sinergias con el IFT para establecer a los concesionarios las obligaciones de cobertura geográfica, poblacional o social y de conectividad en sitios públicos, en done se contempla que serán los concesionarios de telecomunicaciones y radiodifusión los responsables de ampliar el despliegue de las redes en condiciones de competencia, atendiendo además sus compromisos de cobertura y penetración. Como una de sus estrategias prioritarias en el programa sectorial de la SCT, está el de contribuir a la transformación digital de México, para lo cual contempla "desarrollar habilidades y modelos para la transformación digital de los individuos y las instituciones, incluyendo a los grupos en situación de vulnerabilidad". Así, la SCT generó un proyecto sobre "Modelo de habilidades digitales" en el que clasifica las habilidades digitales en: (i) básicas -usar dispositivos, crear cuentas y perfiles, navegar en internet, localizar información, entre otras; (ii) intermedias -creación de contenidos, pensamiento computacional, creación de sistemas, programación de código, entre otras- y (iii) avanzadas -inteligencia artificial, emprendimiento digital, entre otras-389. Para el desarrollo de habilidades digitales, la SCT considera importante la participación de gobierno, industria, academia y sociedad civil organizada.	
CFE TELECOM[390]	Prestar y proveer servicios de telecomunicaciones sin fines de lucro, para garantizar el derecho de acceso a las TIC, incluido el de banda ancha e internet. •	Para llevar a cabo su objeto principal, la CFE Telecomunicaciones e internet para todos, está facultada para llevar a cabo las siguientes acciones: • Conformar una red pública de telecomunicaciones sin fines de lucro. • Promover y facilitar el desarrollo social y económico de la población mediante la prestación de servicios de telecomunicaciones. • Maximizar en forma coordinada y centralizada la infraestructura aplicable a servicios de telecomunicaciones, haciendo uso de las capacidades de la Red Nacional de Fibra Óptica, la infraestructura pasiva y activa. • Celebrar con cualquier ente público y con personas físicas y morales toda clase de actos,	**1.** Internet **2.** Telecomunicaciones

[389] Proyecto de Modelo de Habilidades Digitales SCT, Disponible en: https://www.gob.mx/cms/uploads/attachment/file/444450/Marco_de_habilidades_digitales_vf.pdf (Fecha de consulta 06 de febrero de 2020)

[390] Acuerdo por el que se crea CFE Telecomunicaciones para todos, publicado en el DOF el 02 de agosto de 2019, Disponible en: http://www.dof.gob.mx/nota_detalle.php?codigo=5567088&fecha=02/08/2019 (Fecha de consulta 06 de febrero de 2020).

		convenios, contratos, suscribir títulos de crédito y otorgar todo tipo de garantías. • Celebrar contrato con particulares bajo esquemas que le generen un mayor valor social; • Crear empresas filiales y participar en asociaciones y alianzas nacionales y extranjeras para cumplir con su objeto.	
IFT[391]	• En su carácter de organismo constitucional autónomo en materia de telecomunicaciones y radiodifusión, está facultado para contribuir al logro de los objetivos de la PIDU establecida por el Ejecutivo Federal; así como a los objetivos y metas fijados en el PND y los demás instrumentos programáticos relacionados con los sectores de radiodifusión y telecomunicaciones.	Además de la regulación del espectro radioeléctrico, el IFT presentó su *Visión regulatoria de las telecomunicaciones y la radiodifusión, 2019-2023*[392], en el que contempla cinco objetivos para la transformación digital: **1.** Infraestructura e insumos esenciales: despliegue y compartición de infraestructura en telecomunicaciones y radiodifusión, e identificación de insumos esenciales e impulso a la competencia económica: **2.** Administración del espectro radioeléctrico: planeación, herramientas de gestión de espectro radio eléctrico; valuación y asignación de espectro, e ingeniería del espectro: **3.** Desarrollo de internet y regulación de telecomunicaciones en un ecosistema digital: gobernanza de internet; neutralidad de la red; IPV6; ciberseguridad; big data y explotación de datos; economía digital; servicios OTT; Internet de las Cosas; inteligencia artificial: **4.** Derechos de usuario y audiencias: contenidos audiovisuales en telecomunicaciones y radiodifusión; empoderamiento del usuario; **5.** Innovación institucional: cooperación intersectorial; comportamiento colaborativo, y regulación de vanguardia y moderna.	**1.** Telecomunicaciones y radiodifusión. **2.** Espectro radioeléctrico **3.** Derechos de las audiencias.
SEP[393]	• Organizar, vigilar y desarrollar en las escuelas oficiales, incorporadas o reconocidas: la enseñanza preescolar, primaria, secundaria y normal, urbana, semiurbana y rural; la enseñanza técnica, industrial, comercial y de artes y oficios, incluida la educación que se imparta a los adultos; la enseñanza	**6.** Por mandato legal, la Agenda Digital Educativa394 a cargo de la SEP, busca utilizar el avance de las TIC, y el conocimiento y aprendizaje digital, con la finalidad de fortalecer los modelos pedagógicos de enseñanza-aprendizaje, la innovación educativa, el desarrollo de habilidades y saberes digitales de los educandos, además de establecer programas de	**1.** Habilidades digitales **2.** Educación a distancia

[391] Artículo 15, fracción XXXI de la LFTR, Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFTR_240120.pdf (Fecha de consulta 06 de febrero de 2020)

[392] Visión regulatoria de las telecomunicaciones y la radiodifusión, 2019-2023, septiembre 2018, Disponible en: http://www.ift.org.mx/sites/default/files/contenidogeneral/transparencia/1vision19-23.pdf (Fecha de consulta 06 de febrero de 2020)

[393] Artículo 38 de la LOAPF; artículos 84 y 85 de la Ley General de Educación, publicada en el DOF el 30 de septiembre 2019; Reglamento Interior de la SEP, publicado en el DOF, Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LGE_300919.pdf; (Fecha de consulta 07 de febrero de 2020)

[394] Agenda Digital Educativa, Disponible en: https://infosen.senado.gob.mx/sgsp/gaceta/64/2/2020-02-05-1/assets/documentos/Agenda_Digital_Educacion.pdf; Programa Sectorial de la SEP, publicado en el DOF el 06 de julio de 2020 Disponible en: https://www.gob.mx/cms/uploads/attachment/file/562380/Programa_Sectorial_de_Educaci_n_2020-2024.pdf (Fecha de consulta 07 de febrero de 2020)

	agrícola, con la cooperación de la Secretaría de Agricultura, Ganadería, Desarrollo Rural, Pesca y Alimentación; la enseñanza superior y profesional; la enseñanza deportiva y militar, y la cultura física en general. • La SEP establecerá una Agenda Digital Educativa.	educación a distancia y semi presencial para cerrar la brecha digital y las desigualdades en la población, los cuales serán utilizadas como un complemento de los demás materiales educativos, incluidos los libros de texto gratuitos. **7.** **8.** Con la Agenda Digital Educativa se dirige, de manera progresiva, los modelos, planes, programas, iniciativas, acciones y proyectos pedagógicos y educativos, que permitan el aprovechamiento de las TIC, el conocimiento y el aprendizaje digital, la cual incluye, entre otros aspectos: • El aprendizaje y el conocimiento que impulsen las competencias formativas y habilidades digitales de los educandos y docentes; • El uso responsable, la promoción del acceso y la utilización de las TIC, conocimiento y aprendizaje digital en los procesos de la vida cotidiana; • La adaptación a los cambios tecnológicos; • El trabajo remoto y en entornos digitales; • Creatividad e innovación práctica para la resolución de problemas, • Diseño y creación de contenidos. • Igualmente, en términos del artículo 86 de la Ley General de Educación, se establece que las autoridades educativas de los tres órdenes de gobierno, en el ámbito de su competencia, (i) promoverán la formación y capacitación de maestras y maestros para desarrollar las habilidades necesarias en el uso de las TIC, conocimiento y aprendizaje digital para favorecer el proceso educativo; y (ii) fortalecerán los sistemas de educación a distancia, mediante el aprovechamiento de las multiplataformas digitales, la televisión educativa y las tecnologías antes referidas • Con motivo de la contingencia sanitaria por COVID-19, la SEP también lanzó el Programa de capacitación en competencias digitales para docentes del Sistema Educativo Nacional395, mediante el cual Maestras y maestros podrán acceder a partir del lunes 30 de marzo a diplomados, cursos masivos abiertos en línea y diversos servicios formativos a través de la página web de Televisión Educativa396. • Por otra parte, en su programa sectorial de trabajo, contempla como principales estrategias: (i) desarrollar servicios educativos que fortalezcan los aprendizajes regionales y comunitarios, mediante el uso social de las lenguas indígenas y de las tecnologías de la información, comunicación, conocimiento y aprendizaje digital; (ii) Revisar los planes curriculares de las escuelas normales, a fin de	

[395] Programa de capacitación en competencias digitales para docentes del Sistema Educativo Nacional, Disponible en: https://www.gob.mx/sep/es/articulos/boletin-no-82-lanza-sep-programa-de-capacitacion-en-competencias-digitales-para-docentes-del-sistema-educativo-nacional?idiom=es (Fecha de consulta 07 de febrero de 2020)

[396] Televisión Educativa, Disponible en: https://www.televisioneducativa.gob.mx/ingenioTV.html (Fecha de consulta 07 de febrero 2020)

		garantizar el desarrollo de capacidades cognitivas, pedagógicas, éticas, socioemocionales y digitales de los futuros docentes; (iii) Asegurar la disponibilidad de personal docente para impartir las clases relacionadas con arte, cultura, deporte, habilidades digitales e inglés.	
STPS[397]	**1.** Promover la inserción laboral y facilitar a través de mecanismos idóneos, la vinculación tanto de la población objetivo como de integrantes del sector público, privado y social con el Programa Jóvenes Construyendo el Futuro, para desarrollar y fortalecer hábitos de trabajo y habilidades técnicas que permitan mejorar su empleabilidad. **2.** **3.** En la elaboración de los planes y programas de capacitación, adiestramiento y productividad de las empresas y registrar las listas de las constancias de competencias o de habilidades laborales expedidas a los trabajadores, conforme a los lineamientos que para tal efecto emita la Dirección General de Concertación y Capacitación Laboral. **4.**	**5.** En el marco del Programa Jóvenes Construyendo el Futuro, STPS firmó un convenio de colaboración con la empresa Microsoft, el Instituto Mexicano de la Juventud y el Organismo Internacional de Juventud para Iberoamérica, con el objetivo de brindar capacitación en habilidades tecnológicas y competencias digitales a través del proyecto Laboratorio de habilidades en competencias digitales que en una primera etapa busca atender a 40 mil jóvenes398. **6.** **7.** También cuenta con el Programa de Capacitación a Distancia para Trabajadores PROCADIST399, la cual constituye una plataforma educativa a distancia para trabajadores que ofrece el servicio de capacitación virtual gratuita, con el fin de contribuir al perfeccionamiento o desarrollo de competencias, capacidades y habilidades laborales. **8.**	**9.** Competencias y habilidades digitales en al ámbito laboral. **10.** Capacitación virtual
SSA[400]	• Promover el desarrollo de los servicios de salud con base en la integración de las TIC para ampliar la cobertura y mejorar la calidad de atención a la salud. • Promover la incorporación, uso y aprovechamiento de las TIC en los servicios de salud.	Como una de sus estrategias en el Programa Sectorial se salud, en relación con las TIC, es Implementar progresivamente TIC tendientes a mejorar los sistemas de información, digitalización de expedientes e interoperabilidad entre los diferentes niveles de atención y entre los sectores público y privado del sector salud. En noviembre de 2019, entregó el certificado del expediente médico electrónico de la Secretaría de Marina, conforme a la NOM-024-SSA3-2012, sobre sistemas de información de registro electrónico para la salud. Intercambio	**1.** Servicios de salud a través de las TIC. **2.** Expediente médico electrónico

[397] Artículo 40 de la Ley Federal de Trabajo; Reglamento Interior de la STyPS, publicado en el DOF el 23 de agosto de 2019, Disponible en: https://dof.gob.mx/nota_detalle.php?codigo=5570275&fecha=23/08/2019 (Fecha de consulta 07 de febrero de 2020)

[398] Jóvenes Construyendo el Futuro Recibirán Capacitación en Habilidades Tecnológicas, **BOLETÍN DE PRENSA No. 26 / 2019, Disponible en:** https://www.gob.mx/stps/prensa/jovenes-construyendo-el-futuro-recibiran-capacitacion-en-habilidades-tecnologicas?idiom=es (Fecha de consulta 07 de febrero de 2020)

[399] PROCADIST, Disponible en: https://productividadlaboral.stps.gob.mx/index.php/130-temas/capacitacion-y-adiestramiento/292-programa-de-capacitacion-a-distancia (Fecha de consulta 08 de febrero de 2020)

[400] Artículo 6, fracción IX de la Ley General de Salud, Disponible en*: http://www.diputados.gob.mx/LeyesBiblio/pdf/142_240120.pdf;* Programa Sectorial de Salud 2018-2024, Disponible en: *https://amepresmexico.org.mx/wp-content/uploads/2019/11/191001-PROSESA-2019-2024.pdf* (Fecha de consulta 08 de febrero de 2020)

		de información en salud[401].	
SE[402]	• Organizar, unificar e implementar el sistema informático que establecerá expedientes electrónicos empresariales con la finalidad de simplificar los trámites que los interesados realizan ante la administración pública federal centralizada y paraestatal. • Con base en el Código de Comercio, la SE es la autoridad facultada para regular a los prestadores de servicios de certificación[403], y tiene a su cargo la NOM151 que contempla los requisitos que deben observarse para la conservación de mensajes de datos y digitalización de documentos[404]. • Por otra parte, en el sector público, junto con el SAT y la SFP -cuyas funciones pasaron a la CEDN en materia de gobierno digital-, es considerada una autoridad certificadora en términos de la Ley de Firma Electrónica Avanzada, por lo que, aunque actualmente no emite certificados digitales, si cuenta con dichas atribuciones.	**1.** Entre sus principales líneas de acción están: **2.** Fomentar el desarrollo de la economía digital; **3.** Fomentar la innovación y el desarrollo económico de los sectores productivos; **4.** Promover la adopción de nuevas tecnologías para transitar hacia la Industria 4.0.; **5.** Facilitar los procesos de adopción de tecnologías, así como el control y diseño de los procesos productivos.; **6.** Promover el uso de la infraestructura tecnológica del sector público (laboratorios de universidades y centros de investigación) para que los sectores productivos desarrollen propuestas de innovación y alta tecnología; **7.** Fortalecer la oferta de capital humano especializado en manufactura de alta tecnología mediante la promoción de programas de certificación con estándares internacionales. **8.** Fortalecer las competencias y especialización del capital humano en los sectores productivos para mejorar la competitividad de la economía. **9.** Generar mecanismos para la vinculación entre las instituciones académicas y la industria, a fin de revisar los planes de estudio frente a las necesidades de los sectores productivos y la alta tecnología.	**10.** Expediente electrónico empresarial **11.** Firma electrónica en el sector privado. **12.** Economía digital **13.** Innovación **14.** Conservación de mensajes de datos y digitalización de documentos. **15.** Capital humano especializado.
SAT [405]	• En términos del CFF está autorizado para emitir certificados digitales para efectos fiscales. Igualmente, junto con la SE y la SFP -cuyas funciones pasaron a la CEDN en materia de gobierno digital-, es considerada una autoridad certificadora en términos de la Ley	Actualmente es quien, en México, en la práctica, ofrece el servicio de firma electrónica avanzada en la APF, en las entidades federativas, y otros organismo y poderes autónomos, a través de convenios de colaboración[406]	**1.** Firma electrónica avanzada. **2.** Registro Federal de Contribuyentes.

[401] NOM-024-SSA3-2012, sobre sistemas de información de registro electrónico para la salud .Intercambio de información en salud, Disponible en: http://dof.gob.mx/nota_detalle.php?codigo=5280847&fecha=30/11/2012 (Fecha de consulta 08 de febrero de 2020)

[402] Artículo 34 de la LOAPF; Programa sectorial de economía 2020-2024, Disponible en: https://www.dof.gob.mx/nota_detalle.php?codigo=5595481&fecha=24/06/2020; Código de Comercio, Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf_mov/Codigo_de_Comercio.pdf; y Ley de Firma Electrónica Avanzada, publicada en el DOF el 11 de enero de 2012, Disponible en: http://www.diputados.gob.mx/LeyesBiblio/ref/lfea.htm (Fecha de consulta 08 de febrero de 2020) (Fecha de consulta 08 de febrero de 2020)

[403] SE, Prestadores de servicios de certificación, Disponible en: http://www.firmadigital.gob.mx/directorio.html (Fecha de consulta 08 de febrero de 2020)

[404] NOM151, publicada en el DOF el 30 de marzo de 2017, Disponible en: https://dof.gob.mx/nota_detalle.php?codigo=5478024&fecha=30/03/2017, (Fecha de consulta 08 de febrero de 2020)

[405] Artículo 17-D del Código Fiscal de la Federación, Ley de Firma Electrónica Avanzada. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/8_090120.pdf; (Fecha de consulta 08 de febrero de 2020)

[406] SAT, firma electrónica, Disponible en: http://omawww.sat.gob.mx/ForoTributarioDeServiciosElectronicos2015/Paginas/Documentos/ConveniosColaboracion_FirmaElectronica.pdf (Fecha de consulta 8 de febrero 2020)

	de Firma Electrónica Avanzada.		
SEGOB[407]	• Formular y conducir la política de población e interculturalidad y operar el servicio nacional de identificación personal, en términos de las leyes aplicables • Registro y acreditación de la identidad de todas las personas residentes en el país y de los nacionales que residan en el extranjero.	En el PND 2019-2024 se establece, como una medida para la articulación de la seguridad nacional, la seguridad pública y la paz, construir las bases para la creación de un documento único de identificación nacional biometrizado. Igualmente, entre las acciones previstas en el Programa Sectorial de la SEGOG, se encuentran las siguientes: • Garantizar a todas las personas el derecho fundamental y primigenio a la identidad para que ejerzan sus demás derechos en condiciones de certeza y seguridad, a través del registro universal y oportuno de la población y por medio de un servicio nacional de identidad e identificación. • Establecer normas, métodos y procedimientos encaminados a la expedición del documento único digital de identificación nacional biometrizado.	**1.** Registro Nacional de Población. **2.** Identidad digital **3.** Documento único digital de identificación nacional biometrizado
CONAMER[408]	• Está facultado para regular el Expediente para Trámites y Servicios el cual deberá considerar deberá considerar mecanismos confiables de seguridad, disponibilidad, integridad, autenticidad, confidencialidad y custodia, y en el cual se utilizará la firma electrónica avanzada el servidor público.	Emitió los *lineamientos generales para la operación del expediente para trámites y servicios*[409] aplicable a los tres órdenes de gobierno, en donde se regulan aspectos como (i) integración del expediente, a través de mecanismos de interoperabilidad y carga manual; (ii) transferencia de información, la cual se realizará ante una solicitud a la autoridad central a cargo del sistema del expediente electrónico (CONAMER); (iii) características del expediente; (iv) sistemas de gestión de procesos. Entre las disposiciones destaca el uso de la firma electrónica en el expediente, y se contempla una serie de instrumentos y lineamientos para el desarrollo y aplicación del expediente electrónico tales como: esquemas de interoperabilidad, estándares abiertos, digitalización, política de firma electrónica, intermediación, integración y reutilización de datos, modelos de datos, gestión de documentos electrónicos, conexión del expediente:	**1.** Expediente electrónico de trámites y servicios **2.** Interoperabilidad **3.** Seguridad **4.** Firma electrónica

Fuente: Elaboración propia con base en la legislación, planes y programas consultados.

[407] Artículo 27, fracción VI de la LOAPF, artículo 85 de la LGP, ACUERDO por el que se modifican las políticas y disposiciones para la Estrategia Digital Nacional, en materia de Tecnologías de la Información y Comunicaciones, y en la de Seguridad de la Información, así como el Manual Administrativo de Aplicación General en dichas materias, publicado en el DOF el 08 de mayo de 2014 Última reforma publicada DOF 23-07-2018, Disponible en: https://www.gob.mx/cms/uploads/attachment/file/380408/MAAGTICSI_compilado__20182208.pdf, http://www.diputados.gob.mx/LeyesBiblio/pdf/140_120718.pdf; Programa Sectorial de Gobernación 2020-2024,. https://www.gob.mx/cms/uploads/attachment/file/563303/PSG_2020_-_2024.pdf; (Fecha de consulta 08 de febrero de 2020)

[408] Artículo 24 de la Ley General de Mejora Regulatoria, Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LGMR_180518.pdf (Fecha de consulta 09 de febrero de 2020)

[409] Lineamientos generales para la operación del expediente para trámites y servicios, publicados en el DOF el 13 de julio de 2020, Disponible en: http://dof.gob.mx/nota_detalle.php?codigo=5596610&fecha=13/07/2020 (Fecha de consulta 09 de febrero de 2020)

ANEXO IV. Legislación en México sobre firma electrónica avanzada

Legislación en México sobre firma electrónica avanzada				
	Federación / Entidad / Institución	**Legislación**	**Fecha de publicación**	**Vínculo electrónico**
1	**Federación**	Ley de Firma Electrónica Avanzada	11.01.2012	http://legislacion.scjn.gob.mx/Buscador/Paginas/AbrirDocArticulo.aspx?q=tKw/oZYzmgAUbF8mLnfbgWPDo4K9TSo/KsEDYa7ma/fkXgn8JaQdFh+ztDMYsidhHxA9KXTaSXNMPQWoJadsqg==
2	**Chiapas**	Ley de Firma Electrónica Avanzada del Estado de Chiapas	28.11.2012	http://legislacion.scjn.gob.mx/Buscador/Paginas/AbrirDocArticulo.aspx?q=JiStXgpSjkMH98qQCT4M8qBd5PKToYfMjNDUYC5fabuxCXKrCdNyqTFLp5SHAm5WT8Nf1M06RyLuT++CnaFAYw==
3	**Oaxaca**	Ley de Firma Electrónica Avanzada del Estado de Oaxaca	15.10.2016	http://legislacion.scjn.gob.mx/Buscador/Paginas/AbrirDocArticulo.aspx?q=QxMukt/ZJuuBLDl52fEGK66XdmTeeORMKwUEfYxF0I0yV03EoEXBNS/XqqEytizwvOtlXuqYfTwRdIUp5biGHw==
4	**Durango**	Ley de Firma Electrónica para el Estado de Durango	19.07.2018	http://legislacion.scjn.gob.mx/Buscador/Paginas/AbrirDocArticulo.aspx?q=tIFEvy7+QsLyzc4S0sTNHsmu7jjDXT/rUyh0iIYxYsx4Dn6nKOI91bi/79Rb0kHsXM8c50Cl9Cnc1qK4+1CoEQ==
5	**Jalisco**	Ley de Firma Electrónica Avanzada para el Estado de Jalisco y sus Municipios	26.12.2013	http://legislacion.scjn.gob.mx/Buscador/Paginas/AbrirDocArticulo.aspx?q=aCmzwlfsYLlrJkjKpvELCwlOhVM7glWd5XkWZKqgHQoX3cGwFZNfAdhua7I9adsqx3kbcPKTGHH5oeDxKk3HOA==
6	**Tamaulipas**	Ley de Firma Electrónica Avanzada para el Estado de Tamaulipas	17.09.2013	http://legislacion.scjn.gob.mx/Buscador/Paginas/AbrirDocArticulo.aspx?q=9puCi4g9lyPemOd4Vgo7rYEaWcdQ951AKbUP5pMbN83EK8O9JCpQhsMHe2mZm8pl+UFg+6RGvJg0KGsacIuxuq==
7	**Tlaxcala**	Ley de Firma Electrónica Avanzada para el Estado de Tlaxcala	22.10.2015	http://legislacion.scjn.gob.mx/Buscador/Paginas/AbrirDocArticulo.aspx?q=QxMukt/ZJuuBLDl52fEGK9M1CgEvaALEhayDSQpw5x3P+jxijw96VzfPSh0oehHvNy5MNSL17I/bYo/DYiHcJw==
8	**Campeche**	Ley de Firma Electrónica	22.12.2016	http://legislacion.scjn.gob.mx/Buscador/Pa

		Avanzada y uso de medios electrónicos del Estado de Campeche		ginas/AbrirDocArticulo.aspx?q=u+uol4XmeVVQSBV20oBZUyYLWz2c+EMOAdPp2m2U4ANWqJJJiJPiJjVUi5Hk1HKSfEEsihpMHwVkyaJg6DnYWg==
9	Michoacán	Ley de Firma Electrónica Certificada del Estado de Michoacán de Ocampo	29.12.2016	http://legislacion.scjn.gob.mx/Buscador/Paginas/AbrirDocArticulo.aspx?q=QxMukt/ZJuuBLDl52fEGK3kZv/68crJ+xNHyC93OaP6goz97OKnlDwOepdN/y6dXsOVr9RSdwfuxAqTsfyMPIQ==
10	Ciudad de México	Ley de Firma Electrónica del Distrito Federal	08.10.2014	http://legislacion.scjn.gob.mx/Buscador/Paginas/AbrirDocArticulo.aspx?q=JiStXgpSjkMH98qQCT4M8tp24dehhiXNqT4vEw66CtXLAkKWN3g97kQDAE42+xVPdPabM5YLIHX7YLFIfwHb1A==
11	Zacatecas	Ley de Firma Electrónica del Estado de Zacatecas	15.01.2014	http://legislacion.scjn.gob.mx/Buscador/Paginas/AbrirDocArticulo.aspx?q=+7Tg6RyhcYwKtjU1u1zWDmi8XmANOAm32mr++iuzyVKkfWDTfLXS5zo6OGtZvKlbRXDRam+6BRjnEhQwLcR2IA==
12	Morelos	Ley de Firma Electrónica del Estado Libre y Soberano de Morelos	08.03.2017	http://legislacion.scjn.gob.mx/Buscador/Paginas/AbrirDocArticulo.aspx?q=TkggvIwUhRUETh+shGn+mEliSJxSwvdab9IbfyvnH2HLW1kCevE8Hff/mL0Ih5VoWXUYU3bQAfryz3EZ4epGaw==
13	Baja California	Ley de Firma Electrónica para el Estado de Baja California	15.02.2013	http://legislacion.scjn.gob.mx/Buscador/Paginas/AbrirDocArticulo.aspx?q=JiStXgpSjkMH98qQCT4M8g9vVLOEafhfJ/b6bR+916Dgv8f2MvAFf8lK6sbmeDKhvyVjnMQy65qxYVV3q9h7aw==
14	Tabasco	Ley de Gobierno Digital y Firma Electrónica para el Estado de Tabasco y sus Municipios	07.03.2018	http://legislacion.scjn.gob.mx/Buscador/Paginas/AbrirDocArticulo.aspx?q=Upmvcxia2ntX3YVztB0yTogsHjaL9jJMaiafVQ0zMk7DfISWHsSlX6berQvaa7LNfwPp7ejMHs7CLzUeT3Cefg==
15	Sonora	Ley Número 250 sobre el Uso de Firma Electrónica Avanzada para el Estado de Sonora	06.07.2006	http://legislacion.scjn.gob.mx/Buscador/Paginas/AbrirDocArticulo.aspx?q=D5XzDyLJANrluvfWVC602aXZPx4ZuNgfEu7UUVjtRpXRbcxPYc94+GUpLym+K98fgZaj6MypcRll9DrZOw2YfA==
16	Guerrero	Ley Número 874 que regula el uso de la Firma Electrónica Certificada del Estado de Guerrero	30.12.2008	http://legislacion.scjn.gob.mx/Buscador/Paginas/AbrirDocArticulo.aspx?q=KI4542Bt0wKPVXqqP3p1HOtcgkHlXMw/v1S91ZCR2QwqHBG4NyYkPepYlL4hkGX7t0Cvh8aVq5vsiwntAWtEMw==
17	San Luis Potosí	Ley para la Regulación de la Firma Electrónica Avanzada del Estado de San Luis Potosí	13.04.2017	http://legislacion.scjn.gob.mx/Buscador/Paginas/AbrirDocArticulo.aspx?q=YiqNwbqwp//Pdft7eX1UN/i1RRz20zhiJdoWkj4JsNCpFlAIPdM2lmkAuCb827LwDNfGEq+JVmXSzCVyUYNT1Q==
18	Hidalgo	Ley sobre el uso de medios y firma electrónicos avanzada para el Estado de Hidalgo	10.03.2008	http://legislacion.scjn.gob.mx/Buscador/Paginas/AbrirDocArticulo.aspx?q=zy4gXHqKh4KpyBLzCEYD2H9A7pQg0RA6dUuL8AiiRyCJcvd216f1EONbRo/jFCtSLyEOZXufg8mSYH9XaB6orQ==
19	Yucatán	Ley sobre el uso de medios y firma electrónicos del	28.12.2016	http://legislacion.scjn.gob.mx/Buscador/Paginas/AbrirDocArticulo.aspx?q=/TOSAel91

		Estado de Yucatán		TK6msi4ofAiLuiDcTNDkasae7YU7K9OcAy+wM+ZgsjdVvZarSR2vXAaSyY3vu1fzEdQht2Qr+l7GA==
20	**Colima**	Ley sobre el uso de medios electrónicos y firma electrónica para el Estado de Colima	30.05.2009	http://legislacion.scjn.gob.mx/Buscador/Paginas/AbrirDocArticulo.aspx?q=/TOSAel91TK6msi4ofAiLk4uAH/a5YAPmvZtAJzH8qbPKN8HgC+sf1nH/BdJ9q+AFDKtNq/NAVn8LRXrocM75g==
21	**Veracruz**	Ley Número 563 de firma electrónica avanzada para el Estado de Veracruz de Ignacio de la Llave	25.05.2015	http://legislacion.scjn.gob.mx/Buscador/Paginas/AbrirDocArticulo.aspx?q=u+uol4XmeVVQSBV20oBZUwdSzD9E5ouobAAOYawPcl1HZHGkypFMkEDMqzq2ZJ2doQcKyKCZb6oiR2KWF+jlYA==
22	**Guanajuato**	Ley sobre el uso de medios electrónicos y firma electrónica para el Estado de Guanajuato y sus municipios	07.06.2013	http://legislacion.scjn.gob.mx/Buscador/Paginas/AbrirDocArticulo.aspx?q=1vgDEVdMMZD6s8UENeVd/iiJXcLyi81vibvfx/qyY9MZuw//U4RmWq4+s2bTry3+1IeG2V2SuSB54eSMl9HhSw==
23	**Quintana Roo**	Ley sobre el uso de medios electrónicos, mensajes de datos y firma electrónica avanzada para el Estado de Quintana Roo	30.04.2013	http://legislacion.scjn.gob.mx/Buscador/Paginas/AbrirDocArticulo.aspx?q=tIFEvy7+QsLyzc4S0sTNHvyKKNple7aS8/6Uy/AtXlyZaErpsm++9F161iNSQCWEq4acSTfTKOCwwupddj1Lqw==
24	**Tribunal Electoral del Poder Judicial de la Federación**	Acuerdo General 1/2015 de la Sala Superior del tribunal Electoral del Poder Judicial de la Federación, por el que se establece el procedimiento para la obtención de la firma electrónica certificada del Poder Judicial de la Federación en el Tribunal Electoral	22.04.2015	http://legislacion.scjn.gob.mx/Buscador/Paginas/AbrirDocArticulo.aspx?q=u+uol4XmeVVQSBV20oBZU5mr4Z+oyFdrmVXoZeAPv9y45P81KTLW0rxMs/4Pr1ZlOIzFvpdI4mUz8101f5NaGg==
25	**Poder Judicial de la Federación**	Acuerdo General 01/2018 de la Junta Local de Conciliación y Arbitraje de la Ciudad de México, por el que se regula el uso de la firma electrónica, la interconexión en los sistemas electrónicos del Poder Judicial de la Federación, el expediente electrónico de amparo y el amparo en línea	17.09.2018	http://legislacion.scjn.gob.mx/Buscador/Paginas/AbrirDocReforma.aspx?q=Upmvcxia2ntX3YVztB0yTmJhiJKwwyIRR5vHHK/aD+/ba6ptbsuNkt5U2AZ4oPF0sedkzUD1KDVhX5CB9GI00Tr5sqUZTqBfVrt4EVVGh9d5FUqg+vA7YPz6I63Ed8y2
26	**SCJN, Tribunal Electoral del Poder Judicial de la Federación y el Consejo de la Judicatura Federal**	Acuerdo General conjunto número 1/2013 de la Suprema Corte de Justicia de la Nación, del Tribunal Electoral del Poder Judicial de la Federación y del Consejo de la Judicatura Federal (relativo a la firma electrónica del Poder Judicial de la Federación (FIREL) y al expediente electrónico	08.07.2013	http://legislacion.scjn.gob.mx/Buscador/Paginas/AbrirDocArticulo.aspx?q=9puCi4g9lyPemOd4Vgo7rQoZQYYjl9fg0rg9BGdSS1u+kZU7r90C/mYh+UcBJAW6Xsao0lCKItFq2jqVvLjXWw==
27	**SCJN, Poder Judicial**	Acuerdo General de	27.08.2014	http://legislacion.scjn.gob.mx/Buscador/Pa

	de la Federación	Administración II/2014 del Comité de Gobierno y Administración (por el que se regula el uso de la firma electrónica certificada del Poder Judicial de la Federación (FIREL), en la Suprema Corte de Justicia de la Nación)		ginas/AbrirDocArticulo.aspx?q=u+uol4XmeVVQSBV20oBZUzYwhYnLa5Lm4E5QAgVVyO3N0iHk8e+5pDQYXnWYLqejSA+HJm96wsSZggg7QLFxQQ==
28	**SAT**	Código Fiscal de la Federación	31.12.1981, última reforma 25.06.2018	http://www.diputados.gob.mx/LeyesBiblio/pdf/8_250618.pdf
29	**Comerciantes**	Código de Comercio	07.10 al 13.12 de 1888, y su última reforma el 23.03.2018	http://www.diputados.gob.mx/LeyesBiblio/pdf/3_280318.pdf

Fuente: Elaboración propia. Elaborado al 30 de enero de 2020.