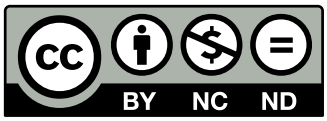
Regulación de blockchain e identidad digital en América Latina | El futuro de la identidad digital

BID | BID LAB | DIDI Identidad Digital para la Inclusión | AB ONG Bitcoin Argentina | LACCHAIN



Reconocimientos

Esta investigación fue llevada a cabo entre los años 2019 y 2020 por Andrés Chomczyk, con la edición a cargo de Javier Madariaga, líder del proyecto DIDI. El trabajo ha sido enriquecido con las sugerencias y la corrección lingüística y de estilo que llevó a cabo María Belén Félix. Por su parte, el diseño gráfico, la diagramación y el maquetado del documento es obra de Ezequiel Cafaro, quien trabajó bajo la coordinación de Lis Altamirano.

Un agradecimiento especial a Rodolfo Andragnes, Presidente de la A.C. DECODES por impulsar y apoyar esta investigación, a BID Lab, por facilitar los recursos para que la misma sea posible, a Erika Molina, Especialista BID Lab, y a Marcos Allende, líder de blockchain y SSI en el departamento de IT del BID, por acompañar el proceso. Por último, un agradecimiento a la Alianza Blockchain Iberoamérica y a IOV Labs por su apoyo en la difusión de este trabajo en toda la región.

Índice

Resumen ejecutivo1

A lo largo de los últimos años, motivado por el desarrollo de nuevas tecnologías, el debate en torno a la protección y utilización de los datos personales cobró fuerza, así como la problemática vinculada a las regulaciones de carácter legal sobre los mismos. En este contexto se enmarca el proyecto "Inclusión cívica social y económica de habitantes de barrios vulnerables en Buenos Aires mediante modelos de Blockchain" (DIDI), llevado adelante de manera conjunta entre el laboratorio de innovación del Grupo Banco Interamericano de Desarrollo ("BID Lab") y la Asociación Civil para el Desarrollo de Ecosistemas Descentralizados, DECODES (la "ONG Bitcoin Argentina"). Su objetivo es desarrollar e implementar una solución de identidad digital basada en la noción de *self-sovereign identity* para personas en entornos de pobreza e informalidad. La consolidación de una identidad digital para los habitantes de barrios populares en Argentina busca reducir la penalidad de la pobreza que sufren estas personas, entendida como el mayor costo relativo que enfrentan para acceder a bienes y servicios de calidad debido a la existencia de asimetría informativa.

Los desafíos de su implementación, así como la posibilidad de expandir y trasladar proyectos de características similares hacia otros países de la región, motivó la realización del presente informe que tiene dos objetivos: primero, dar cuenta de los marcos regulatorios actuales aplicables a la identidad digital auto soberana, el sistema de tecnología *blockchain* y las criptomonedas; y segundo, presentar recomendaciones, acciones y sugerencias para el mejoramiento de las condiciones legales en la región a modo de incentivar la implementación de proyectos que tengan como eje el empoderamiento de los sujetos a través de la construcción y control de la identidad digital y los datos personales a ella vinculados.

El informe analiza la situación legal en Argentina, Bolivia, Brasil, Chile, Colombia, Costa Rica, Cuba, Ecuador, El Salvador, Guatemala, Haití, Honduras, México, Nicaragua, Panamá, Paraguay, Perú, República Dominicana, Uruguay y Venezuela. Además, se establecen definiciones, tanto normativas como doctrinarias, en torno a los distintos conceptos abarcados en el trabajo (identidad digital auto soberana, datos personales y derechos asociados, *blockchain*, criptomonedas y monedas *token*, entre otros) y se incluyen observaciones sobre otras jurisdicciones que en la actualidad también trabajan en la implementación de soluciones de identidad digital.

¿Cuál es el marco legal de América Latina para la realización de este tipo de proyectos? ¿En qué estado de situación regulatoria se

cutivo resume
umen ejecutiv

encuentra la región con respecto a la identidad digital auto soberana, el sistema *blockchain* y las criptomonedas? ¿Qué modificaciones deberían ser llevadas adelante para mejorar estos marcos regulatorios? ¿Qué estrategias se sugieren de cara al futuro en la región para la implementación de proyectos que contemplen estos distintos componentes?

El presente trabajo pretende responder estas preguntas y avanzar en un análisis detallado del estado de situación legal en cada uno de los países seleccionados de la región en torno a: identidad, posesión de datos, mecanismo de acreditación, validez legal de la documentación digital, redes *blockchain*, firmas digitales, contratos inteligentes y criptoactivos, entre otros. Estos ejes temáticos fueron seleccionados a modo de reconocer y abarcar los aspectos legales pertinentes a posibles programas a desarrollar en el futuro que involucren la identidad digital mediante *blockchain* y la incorporación de una billetera digital para la gestión de criptoactivos.

Como resultado, la investigación permite reconocer que, en líneas generales, no se encuentran actualmente en los países estudiados las condiciones normativas necesarias para llevar adelante proyectos que involucren algunos de los temas que guían la investigación. En este sentido, se propone una serie de estrategias y líneas de acción posibles considerando como punto de partida las normativas legales actuales a modo de impulsar, apoyar y consolidar el desarrollo de proyectos con las características anteriormente descritas. Por ejemplo, todas las regulaciones en América Latina consideran a la persona como el titular de los datos y como la única que está en condiciones de determinar cómo serán tratados. Esto se alinea con el espíritu de los proyectos de identidad digital auto soberana sobre *blockchain*, tal como se describió anteriormente.

Por último, la investigación presenta recomendaciones de áreas de acción normativa, redactadas en términos generales, plausibles de ser utilizadas para la adopción de un nuevo marco legal en los países en donde se considere conveniente hacerlo. Si bien esta propuesta regulatoria puede requerir ciertas modificaciones a partir del desarrollo de experiencias o nuevos alcances en materia tecnológica, se considera que la misma representa un aporte a ser tenido en cuenta para cualquier tipo de reflexión y debate que se genere e impulse en torno a la identidad digital auto soberana, el desarrollo del sistema *blockchain* y la gestión de criptoactivos.

Introducción 2 Introducción

El presente informe fue realizado en el marco del proyecto conjunto del Laboratorio de innovación del Grupo Banco Interamericano de Desarrollo ("BID Lab") y la Asociación Civil para el Desarrollo de Ecosistemas Descentralizados, DECODES (la "ONG Bitcoin Argentina"), "Inclusión cívica social y económica de habitantes de barrios vulnerables en Buenos Aires mediante modelos de *Blockchain*" (DIDI).

El proyecto tiene como objetivo desarrollar e implementar una solución de identidad digital para personas en entornos de pobreza e informalidad, basada en la noción de self-sovereign identity, conocida en español como identidad auto-soberana[1]. En última instancia, el proyecto empodera a los individuos mejorando el control que tienen sobre su información personal, permitiéndoles utilizarla como un instrumento para reducir su penalidad de pobreza[2], entendida como el mayor costo relativo que enfrentan las personas en situación de vulnerabilidad para acceder a bienes y servicios debido a la existencia de asimetría informativa. A

1 El concepto de *self-soverign identity* a considerarse será el propuesto por Christopher Allen en su artículo "The Path to Self-Sovereign Identity", disponible en http://www.lifewithalacrity.com/previous/2016/04/index.html (Fecha de consulta 31 de diciembre de 2019). A grandes rasgos, esta identidad se caracteriza por ser descentralizada, controlada por el individuo, privada, portable, interoperable, verificable, inmutable, segura e inclusiva.

2 El mercado, al no contar con información sobre su identidad o comportamiento, no las incluye, o lo hace a un costo mucho más alto.

Introducción I
cción Introduc

través de la consolidación de una identidad digital relevante, accesible y confiable, el proyecto aspira a que la penalización de la pobreza de los habitantes de los barrios vulnerables se vea reducida y puedan mejorar sus oportunidades de inserción socioeconómica en la cuarta revolución industrial.

El proyecto DIDI está totalmente alineado con el trabajo de la Alianza Global LACChain, un proyecto liderado por el BID Lab con el objetivo del desarrollo del ecosistema *blockchain* en América Latina y el Caribe[3]. Este programa ha desarrollado y mantiene una infraestructura *blockchain* público-permisionada a disposición gratuita de cualquier entidad de América Latina y el Caribe. Esta infraestructura consta de "capas red" *blockchain*, identidad digital auto-soberana y dinero tokenizado. La capa de identidad digital auto-soberana consiste en una serie de estándares, protocolos y herramientas desarrolladas sobre la base de estándares internacionales. La solución DIDI está desplegada sobre la red LACChain y trabaja muy de cerca con el equipo de identidad de LACChain.

Esta publicación es la segunda de la saga "The future of digital identity" respaldada y esponsorizada por LACChain Academy. La primera, cuya lectura recomendamos como un complemento introductorio a este documento, presenta con detalle los conceptos de identidad,

3 www.lacchain.net

identidad digital e identidad digital auto-soberana, analizando el camino para la adopción con sus ventajas y desafíos, el impacto en diferentes sectores como educación o sanidad, y las necesidades regulatorias, tecnológicas y de establecimiento de marcos de confianza adecuados[4]. El presente documento examina con un mayor nivel de detalle los aspectos regulatorios de la identidad digital auto-soberana en América Latina.

La solución tecnológica propuesta en DIDI se materializa en i) una aplicación móvil llamada ai·di (porta documentos digital) que certifica y valida datos sociales, cívicos y económicos, a través de credenciales verificables[5] emitidas por terceros, y ii) un portal web de emisión de credenciales, a través del cual las instituciones o individuos que así lo deseen pueden operar, gestionar, emitir, y revocar esas credenciales. Es así como DIDI permite a los individuos disponer de información fehaciente, privada y portable, validada por entidades privadas y públicas, sobre sus tenencias y sus logros académicos, laborales, económicos y financieros, tanto formales como informales. Con la construcción de este registro digital, se espera que sus usuarios alcancen mayores probabilidades de acceder a mejores bienes y servicios y que construyan nuevos vínculos de confianza. Junto con la creación de una solución de identidad digital, el proyecto también ha creado distintas aplicaciones que permiten certificar los sistemas de ahorro y crédito autogestivos propios de los barrios populares. En un futuro, la solución podría incorporar una billetera digital donde los usuarios del sistema puedan utilizar una *stablecoin*[6] respaldada por pesos argentinos y captar, dentro de su identidad digital, el historial transaccional realizado a través de la misma.

El proyecto DIDI está siendo desarrollado sobre redes *blockchain* públicas no permisionadas, como RSK, y públicas permisionadas como la Blockchain Federal Argentina y LAC-Chain, a efectos de evitar la creación de cualquier tipo de barrera de entrada existente en los protocolos de redes privadas y garantizar su sostenibilidad más allá de la de cada una de estas redes. La identidad de cada persona estará alojada en su dispositivo móvil y tendrá una copia de seguridad en un servicio de almacenamiento SaaS de terceros, bajo la forma de credenciales. Toda operación sobre la identidad puede ser realizada únicamente con las claves privadas asociadas a ella, que son generadas por el usuario al darse de alta en el sistema.

En atención a ello, se ha avanzado en la confección del presente informe con miras a analizar el marco legal aplicable a las soluciones de identidad auto soberana, el marco legal aplicable a la tecnología *blockchain* y el marco legal aplicable a las criptomonedas de cara a analizar la posibilidad de implementar proyectos de características similares en otros países de la región. A tal efecto, el análisis incluido en el presente documento fue realizado sobre varios países de América Latina: Argentina, Bolivia, Brasil, Chile, Colombia, Costa Rica, Cuba, Ecuador, El Salvador, Guatemala, Haití, Honduras, México, Nicaragua, Panamá, Paraguay, Perú, República Dominicana, Uruguay y Venezuela. Sin perjuicio de lo anterior, se incluyen algunas observaciones sobre otras jurisdicciones que también están trabajando sobre la implementación de soluciones de identidad digital.

Al cierre del informe se esbozan recomendaciones para mejorar los marcos normativos de manera general a modo de facilitar la implementación de proyectos que contribuyan a empoderar a los individuos a partir de la construcción y control de su identidad digital y datos personales en la región.

4 ALLENDE, M. (2020) "Self Sovereignty, Digital wallets, and Blockchain. The Future of Digital Identity." Banco Interamericano de desarrollo.

5 Las credenciales verificables son certificados digitales, que acreditan mediante firma digital que una persona es portadora de ciertos atributos que tienen que ver con su identidad.

6 También conocidas como criptomonedas estables, son criptoactivos que emplean diferentes estrategias para reducir la volatilidad, principalmente coletarizadas (respaldadas) a otro valor externo para otorgarles estabilidad.

Conceptos básicos3Conceptos básicos

3 Conceptos básicos

Dada la amplitud y la especificidad de los temas que presenta este informe, es necesario presentar algunas definiciones que serán utilizadas a lo largo del documento para facilitar el desarrollo del análisis, la realización de reflexiones y la confección de las conclusiones. En esta sección se recopilan definiciones básicas de origen normativo o, en caso de que estas no existan, definiciones doctrinarias que se emplearán cuando se utilice el concepto en el presente informe.

a Identidad

Los instrumentos internacionales de derechos humanos suelen incluir la noción de identidad en términos del nombre, nacionalidad o reputación de una persona, particularmente en el caso de menores. Este es el caso en los artículos 12 y 15 de la Declaración Universal de Derechos Humanos de Naciones Unidas (la "DUDH"), los artículos 7 y 8 de la Convención sobre los Derechos de los Niños (la "CDN"), los artículos 17 y 24 del Pacto Internacional de Derechos Civiles y Políticos (el "PIDCP") y los artículos 11, 18 y 20 de la Convención Americana Sobre Derechos Humanos (el "Pacto de San José de Costa Rica"). Sin embargo, todos estos instrumentos abordan ciertos elementos de la identidad de las personas –que en efecto son fundamentales- pero no la abarcan de forma integral.

En consecuencia, a los efectos de definir qué se entenderá aquí y en el proyecto DIDI por identidad, usaremos la acepción proporcionada por el World Economic Forum en su informe de 2016 titulado "*A Blueprint for Digital Identity*"[7]. Siguiendo esta definición, la identidad no es un concepto integrado por un único elemento – como el nombre o la nacionalidad- sino que es el producto de la consolidación de diferentes aristas objetivas y subjetivas que permiten individualizar a un referente biológico como sujeto en la sociedad. Así, la identidad estaría dada por tres tipos de atributos de la personalidad: (i) aquellos que le son inherentes; (ii) aquellos que le son acumulados; y (iii) aquellos que le son asignados. Los primeros son los que forman parte esencial de

7 Cfr. WORLD ECONOMIC FORUM, "A Blueprint for Digital Identity – The Role of Financial Institutions in Building Digital Identity", agosto de 2016, http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf, pág. 41. (Fecha de consulta 31 de diciembre de 2019). La traducción es propia.

ásicos Concep
ceptos básico

la persona y responden principalmente a sus características biológicas inalterables. Los segundos son las características que se van obteniendo o desarrollando a lo largo de la vida, como el comportamiento, la autopercepción y autodefinición, el conocimiento, entre otros. Por último, los atributos asignados son aquellos que la persona adquiere a partir de sus relaciones con otras entidades, como por ejemplo un número de identificación estatal, un título obtenido de una institución educativa, o un número de teléfono. Buena parte de los elementos mencionados por los tratados de derechos humanos están incluidos dentro de esta noción de identidad que es mucho más amplia y abarcativa.

Un aspecto que resulta común a los elementos que forman parte de la identidad de las personas es que pueden ser clasificados como datos personales. Esto no es una cuestión menor porque implica que toda la problemática de la identidad digital debe ser abordada desde el régimen legal de la protección de los datos personales aplicable en cada jurisdicción.

La identidad no es algo que se presente de forma aislada, sino que se inserta en un sistema. Todo sistema de identidad, en mayor o menos medida, funciona con terceros de confianza que validan ciertos atributos que componen la identidad de las personas. Así, cuando estas quieren demostrar su identidad, recurren a esos terceros de confianza para solicitarles que validen la información presentada o para que confirmen la información ya validada. En líneas generales, los sistemas de identificación funcionan con cuatro roles: usuarios, proveedores de identidad, receptores de información y entidades de control. Todos contribuyen a que las entidades que necesitan acreditar su identidad puedan hacerlo gracias a las validaciones de los proveedores de identidad, bajo el control de una entidad que fija las reglas de procedimiento y los estándares a seguir[8].

Según el World Economic Forum, en la actualidad se pueden distinguir cinco tipos de sistemas de identidad: (i) sistemas de gestión de identidad internos; (ii) sistema de autenticación externa; (iii) sistemas centralizados de identidad; (iv) sistemas de autenticación federados; y (v) sistemas distribuidos de identidad. Estos últimos son los que más se acercan a los sistemas de identidad digital auto soberana.

b. Identidad auto soberana

Así como no hay una definición legal completa de identidad, tampoco hay una definición normativa sobre la noción de identidad auto soberana, con lo cual es necesario vol-

8 Cfr. WORLD ECONOMIC FORUM, pág. 47.

ver a establecer una definición a efectos de esta investigación. Este concepto fue sistematizado por Christopher Allen[9] al referirse a la historia de los sistemas de identidad inherentes al mundo digital creado por Internet. Allen distingue que se han atravesado, hasta el momento, tres etapas en materia de sistemas de identificación en Internet y se está comenzando a ingresar en la cuarta. Estos sistemas son los siguientes: (i) sistemas centralizados, como ICANN para la asignación de nombres de dominio; (ii) sistemas federados, como Passport de Microsoft; (iii) sistemas centrados en el usuario, como las soluciones basadas en OAuth; y (iv) sistemas de identidad auto soberana. A la fecha no hay ninguna implementación concreta de este último tipo de sistema.

Todos los sistemas de identificación desplegados hasta el momento presentan, en mayor o menor medida, el problema de depender de una entidad centralizada y, en consecuencia, quitar el foco del usuario. En otras palabras, todos estos sistemas siguen un esquema donde una entidad decide sobre los datos personales, con algunas intervenciones menores del usuario que generan una falsa sensación de control sobre los datos integrantes de la identidad. Allen sostiene que la única forma de generar una identidad que ponga el foco en el usuario y no en las entidades que validan la información es darle autonomía al usuario y hacerlo soberano de sus datos. Como se verá más adelante, el principal problema que presentan los sistemas de identidad auto soberanos es que todas las normativas analizadas sobre protección de datos personales y sistemas de identificación están basadas en relaciones de usuario-proveedor de servicios. Esta relación cambia en los sistemas auto soberanos y, en consecuencia, nos llevan a pensar cómo se debería interpretar la norma para acomodar estos sistemas.

c. Datos personales

Los elementos de la identidad son atributos de una persona que pueden ser clasificados como datos personales. Por lo tanto, resulta relevante reseñar definiciones existentes sobre este concepto en cada país que ha sido definido como ámbito de esta investigación. A continuación, se detallarán las definiciones que se han podido recoger:

Argentina Conforme la legislación argentina en materia de protección de datos personales, la Ley Nº 25.326 (la "Ley Argentina de Protección de Datos Personales")[10], por dato personal debemos entender "información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables".

La Ley Argentina de Protección de Datos Personales también proporciona una definición sobre el concepto de dato sensible y señala que se trata de "datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual". Dentro de este concepto puede incluirse la noción de dato biométrico, conforme la Resolución 4/2019 de la Agencia de Acceso a la Información Pública (la "AAIP"), que se define como "aquellos datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona humana, que permitan o confirmen su identificación única".

9 Cfr. ALLEN, Christopher, "The Path to Self-Sovereign Identity", *Life With Alacrity*, 25 de abril de 2016, http://www.lifewithalacrity.com/previous/2016/04/index.html (Fecha de consulta 31 de diciembre de 2019).

10 Para garantizar la coherencia y claridad del texto, a lo largo del informe se adaptará la denominación de las leyes de los distintos países analizados incluyendo en su nombre el ámbito de aplicación de manera de poder diferenciarlas entre sí. El documento cuenta con un glosario en el que se detallada a qué ley corresponde cada una.

Bolivia En Bolivia, no existe una normativa general aplicable a toda actividad de tratamiento de datos personales. La Constitución Política del Estado plurinacional de Bolivia prescribe que los bolivianos tienen derecho a la privacidad, conforme el artículo 21.2, y a plantear recursos de *habeas data*, en atención al artículo 130.
Sí existen definiciones sectoriales, como es el caso de la Ley Nº 164, de 8 del agosto de 2011, General de Telecomunicaciones, Tecnologías de la Información y Comunicación (la "Ley Boliviana de TIC"). Dicha norma, en su artículo 3.IV.a), define al dato personal como "toda información concerniente a una persona natural o jurídica quela identifica o la hace identificable".

Brasil La norma general sobre protección de datos personales en Brasil, la Ley Nº 13.709 del 14 agosto de 2018 (la "Ley Brasilera de Protección de Datos Personales") define al dato personal como "*informação relacionada a pessoa natural identificada ou identificável" y al dato sensible como "dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural*", conforme lo prescripto por esa norma en su artículo 5.

Chile Chile cuenta con una norma general sobre protección de datos personales: la Ley Nº 19.628 (la "Ley Chilena de Protección de Datos Personales"). Esta norma define, en su artículo 2, al dato personal como "cualquier información concerniente a personas naturales, identificadas o identificables" y a los datos sensibles como "aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual".

Colombia La Ley Nº 1581 de 17 del octubre de 2012 (la "Ley Colombiana de Protección de Datos Personales") define, en su artículo 3, a los datos personales como "cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables".
Por su parte, el Decreto Nº 1377/2013 incluye la definición de dato sensible, conforme el artículo 3, el cual debe entenderse como "aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos".

Costa Rica Según la Ley Nº 8.968 (la "Ley Costarricense de Protección de Datos Personales"), dato personal es "cualquier dato relativo a una persona física identificada o identificable".
Por su parte, dato sensible debe ser entendido como "información relativa al fuero íntimo de la persona, como por ejemplo los que revelen origen racial, opiniones políticas, convicciones religiosas o espirituales, condición socioeconómica, información biomédica o genética, vida y orientación sexual, entre otros".

Cuba En Cuba no existe un régimen general sobre la protección de datos ni previsiones al respecto de carácter constitucional. Por lo tanto, no es posible dar una definición legal del concepto de dato personal por esta jurisdicción.

Ecuador No existe una norma general que regule la protección de los datos personales en Ecuador. La única definición que existe sobre el concepto de dato personal es dada por la Ley Nº 67, del 17 de Abril del 2002, de Comercio Electrónico, Fir-

mas y Mensajes de Datos (la "Ley Ecuatoriana de E-Commerce"), la cual define a los datos personales como "aquellos datos o información de carácter personal o íntimo, que son materia de protección en virtud de esta Ley".

El Salvador No existe una definición general del concepto de dato personal en la normativa salvadoreña. Sin perjuicio de ello, el Decreto Nº 133 del 1 de octubre de 2015 (la "Ley Salvadoreña de Firma Electrónica") introduce el concepto de dato personal a los efectos de las actividades de tratamiento realizadas por los prestadores de servicios de certificación y los prestadores de servicios de almacenamiento de documentos electrónicos en los siguientes términos: "cualquier información numérica, alfabética, gráfica o fotográfica o de cualquier otro tipo, concerniente a personas naturales identificadas o identificables".

Guatemala No existe una definición general del concepto de dato personal en la normativa guatemalteca.

Haití No existe una definición general del concepto de dato personal en la normativa haitiana.

Honduras La Constitución de Honduras reconoce en su Capítulo I, Título IV el derecho al *habeas data*. Sin perjuicio de ello, no existe una definición general del concepto de dato personal en la normativa hondureña.
En la actualidad, existe un proyecto de ley que tiene por finalidad regular la materia y dar una definición de dato personal [11].

México El concepto de dato personal está definido en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares en su artículo 3.V. como "cualquier información concerniente a una persona física identificada o identificable".
En el apartado VI del mismo artículo, se define a los datos sensibles como "aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. En particular, se consideran sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual".

Nicaragua En Nicaragua, el concepto de dato personal está definido por la Ley Nº 787 (la "Ley Nicaragüense de Protección de Datos") en su artículo 3.e) como "toda la información sobre una persona natural o jurídica que la identifica o la hace identificable".
La norma también presenta definiciones para los conceptos de dato personal informático (apartado f), y para dato personal sensible (apartado g), los cuales son definidos como "datos personales tratados a través de medios electrónicos o automatizados" y "toda información que revele el origen racial, étnico, filiación política, credo religioso, filosófico o moral, sindical, relativo a su salud o vida sexual, antecedentes penales o faltas administrativas, económicos financieros; así como información crediticia y financiera y cualquier otra información que pueda ser motivo de discriminación", respectivamente.

Panamá La Ley Nº 81 del 26 de marzo de 2019 (la "Ley Panameña de Protección de Datos") define en su artículo 4.9 al dato personal como "cualquier información concerniente a personas naturales, que las identifica o las hace identificables".
En el mismo artículo 4 se define también al dato

11 Cfr. ARROYO, Verónica – SIERRA CASTRO, Hedme, "*Honduras necesita un debate urgente sobre datos personales y libertad de expresión*", *Access Now*, 20 de marzo de 2019, disponible en https://www.accessnow.org/honduras-igf/ (Fecha de consulta: 31 de diciembre de 2019).

sensible (apartado 11) como "aquel que se refiera a la esfera íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para este".
La norma prevé también otras definiciones derivadas de estos conceptos como la de dato confidencial, dato anónimo, dato caduco y dato disociado.

Paraguay Paraguay tiene una norma de protección de datos personales, la Ley Nº 1.682 con su modificación por la Ley Nº 1969 (la "Ley Paraguaya de Protección de Datos"), pero carece de un concepto definido de dato personal. Sin perjuicio de ello, cuenta con una definición de dato sensible en su artículo 4 caracterizándolos como "los referentes a pertenencias raciales o étnicas, preferencias políticas, estado individual de salud, convicciones religiosas, filosóficas o morales; intimidad sexual y, en general, los que fomenten prejuicios y discriminaciones, o afecten la dignidad, la privacidad, la intimidad doméstica y la imagen privada de personas o familias".

Perú El concepto de dato personal es definido por la Ley Nº 29.733 (la "Ley Peruana de Protección de Datos") como "toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados" en el artículo 2.4. Asimismo, el apartado 5 de dicho artículo proporciona una definición de dato sensible en los siguientes términos: "datos personales constituidos por los datos biométricos que por sí mismos pueden identificar al titular; datos referidos al origen racial y étnico; ingresos económicos, opiniones o convicciones políticas, religiosas, filosóficas o morales; afiliación sindical; e información relacionada a la salud o a la vida sexual".

República Dominicana La Ley Nº 172-13 (la "Ley Dominicana de Protección de Datos") en su artículo 6.9 define al dato personal como "cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables". En el mismo artículo apartado 8, se define al dato especialmente protegido como aquellos que "revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual".

Uruguay La Ley Nº 18.331 (la "Ley Uruguaya de Protección de Datos") en su artículo 4.d define al dato personal como "información de cualquier tipo referida a personas físicas o jurídicas determinadas o determinables". En el apartado e de dicho artículo tenemos la definición dato sensible, la cual es "datos personales que revelen origen racial y étnico, preferencias políticas, convicciones religiosas o morales, afiliación sindical e informaciones referentes a la salud o a la vida sexual".

Venezuela No existe una definición general del concepto de dato personal en la normativa venezolana.

Más allá de los matices, las definiciones sobre el concepto de dato personal en los países de América Latina suelen ser bastante similares. A efectos de esta investigación se entenderá por dato personal a toda información que permite identificar o hace identificable a una persona humana.

d. Derechos de los titulares de los datos

Ser titular de datos personales da lugar a derechos sobre ellos, y los derechos reconocidos en los marcos normativos de los países de América Latina son similares. Antes de analizar los derechos que cada ordenamiento jurídico latinoamericano reconoce a los titulares de los datos, corresponde hacer unas breves aclaraciones sobre lo que implica cada derecho en líneas generales. Esto no implica que su sentido sea el mismo en todas las jurisdicciones y se harán aclaraciones en cada caso en el que algún ordenamiento extienda o restrinja de cualquier manera el campo de ejercicio y alcance del derecho.

En este sentido, podemos reconocer los siguientes derechos sobre los datos personales:

- *Habeas data*: este derecho suele ser contemplado en los textos constitucionales y habilita a todo habitante de un determinado país a plantear una acción judicial de resolución expedita cuando exista alguna afectación sobre sus datos personales.
- Derecho de acceso: mediante este derecho el titular de los datos puede exigir que se le informen o muestren, según el caso y las circunstancias, los datos personales que la entidad requerida tiene bajo su control.
- Derecho de rectificación: este derecho le permite al titular de los datos solicitar que aquellos datos erróneos en poder de una entidad sean corregidos para mostrar los datos correctos, o bien proporcionar aquellos datos que hagan falta para que la información que tiene la entidad refleje la realidad. Es normal que este derecho sea ejercido en forma conjunta o posterior al derecho de acceso.
- Derecho de cancelación: este derecho le permite al titular de los datos solicitar que ciertos datos sean eliminados por diversos motivos, como podría ser que los mismos ya hayan cumplido la finalidad para la cual fueron recolectados o bien los mismos sean excesivos para la supuesta finalidad que motivó su recolección.
- Derecho de oposición: este derecho le concede la facultad al titular de los datos de solicitar que sus datos no sean tratados de cierta manera o se detenga una actividad de tratamiento de datos[12].
- Derecho al olvido: este derecho le concede al titular de los datos la posibilidad de solicitar a un intermediario de Internet o motores de búsqueda la eliminación de las referencias a cierta información por diversos motivos, generalmente la inexistencia de una finalidad que motive su difusión.
- Derecho a la portabilidad: este derecho le permite al titular de los datos solicitar una copia de todos los datos que tiene una entidad para que dejen de ser tratados por ella y comiencen a ser tratados con finalidades similares por otra entidad.
- Derecho de bloqueo: es una facultad que los ordenamientos jurídicos le dan al titular de los datos para que este pueda instruir al responsable del tratamiento a que deje de tratar los datos pero no disponga su eliminación puesto que pueden ser de utilidad para el titular de los datos.
- Derecho contra decisiones automatizadas: se trata del derecho que tiene el titular de los datos para evitar que este sufra las consecuencias jurídicas de una decisión tomada por una entidad que no sea un ser humano.

---

12 **Se refiere a cualquier operación o conjunto de operaciones efectuadas sobre datos personales mediante procedimientos manuales o automatizados relacionados con la obtención, uso, organización, conservación, utilización, comunicación, difusión, almacenamiento o cualquier forma de habilitación de acceso, cotejo, interconexión o transferencia.**

Tabla 1

Derechos sobre los datos personales reconocidos en los países de América Latina

	Habeas Data	Acceso	Rectificación	Cancelación	Oposición	Olvido	Portabilidad	Bloqueo	Automatizadas
Argentina	×	×	×	×	×				
Bolivia	×	×*	×*	×*	×*	×*			
Brasil	×	×	×	×	×		×		
Chile	×	×	×	×	×			×	
Colombia	×	×	×	×	×				
Costa Rica	×	×	×	×	×				
Cuba		×**	×**	×**	×**				
Ecuador	×								
El Salvador	×***	×*´	×*´	×*´	×*´				
Guatemala	×								
Haití									
Honduras	×								
Mé×ico	×	×	×	×	×				
Panamá	×	×	×	×	×		×		×
Paraguay	×	×							
Perú	×	×	×	×	×				×
República Dominicana	×	×	×	×	×			×	
Uruguay	×	×	×	×	×				×
Venezuela	×								

Referencias

* Significa que el derecho en cuestión presenta alguna particularidad en la jurisdicción que debe ser consultada en la Tabla 1.
* E×clusivamente dentro del campo de la Ley Boliviana de TICs
** Si bien la Constitución Nacional reconoce ciertos derechos, los mismos no son de aplicación directa y están supeditados al dictado de una ley formal.
*** Reconocido jurisprudencialmente
*´ Solo en el ámbito de la Ley Salvadoreña de Firma Electrónica

En la Tabla 1 se detallan los derechos que cada jurisdicción reconoce a los titulares de los datos.

e. Sujetos involucrados en el tratamiento de datos personales

Las normativas latinoamericanas siguen la estructura de las normas europeas de protección de datos personales, y presentan definiciones muy similares de las entidades que están involucradas en el tratamiento de datos personales. En los países de América Latina donde existen normas de protección de datos personales, estas reconocen la existencia de los siguientes sujetos: (i) el titular de los datos; (ii) el responsable del tratamiento; y (iii) el encargado del tratamiento. A estos sujetos se sumarán aquí los conceptos de importador y exportador de datos, dado que podría ocurrir que exista un flujo transfronterizo de datos personales y haya que atender a estos roles.

A fin de proporcionar una definición para cada uno de estos sujetos, y considerando la similitud entre las definiciones que las normas de protección de datos presentan entre sí, se emplearán los conceptos propuestos por el Observatorio Iberoamericano de Protección de Datos[13]. En ese sentido, y a efectos de esta investigación, se entenderá por:

- Titular de datos personales: "persona física o jurídica cuyos datos personales son objeto de tratamiento o procesamiento".
- Responsable del tratamiento: "persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento". Algunas jurisdicciones reconocen además la existencia del llamado "corresponsable" cuando existen dos o más responsables de un mismo tratamiento de datos, que definen de forma conjunta sus características.
- Encargado del tratamiento: "persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio".
- Exportador de datos personales: "persona física o jurídica, pública o privada, u órgano administrativo que realice una transferencia de datos de carácter personal a un país tercero".
- Importador de datos personales: "persona física o jurídica, pública o privada, u órgano administrativo receptor de los datos en caso de transferencia internacional de los mismos a un tercer país, ya sea responsable del tratamiento, encargada del tratamiento o tercero".

f. Relaciones entre los sujetos involucrados en el tratamiento de datos personales

Habiendo definido y determinado las posibles entidades que pueden formar parte de un tratamiento de datos, es necesario delimitar las relaciones que pueden establecerse desde una perspectiva jurídica entre los datos personales y las actividades de tratamiento. En este sentido, podemos identificar dos tipos de relaciones: (i) las que se configuran en atención a las acciones que pueden hacerse sobre los datos; y (ii) las que se configuran en atención al lugar donde se realizan las actividades de tra-

13 Cfr. OBSERVATORIO IBEROAMERICANO DE PROTECCIÓN DE DATOS, "Terminología jurídica", http://oiprodat.com/biblioteca/terminologia-juridica/ (Fecha de consulta 31 de diciembre de 2019)

tamiento. Es menester señalar que estas consideraciones se realizan sobre el proceso de creación de la identidad.

En cuanto a las relaciones que se configuran en atención a las acciones que pueden hacerse sobre los datos, podemos distinguir, en primer lugar, la relación primaria entre el titular de los datos personales y el responsable de su tratamiento. El responsable únicamente puede realizar aquellas actividades de tratamiento de datos personales para las cuales cuente con una base legal y haya cumplido con el deber de información, sin perjuicio del cumplimiento con el resto de las obligaciones que puedan existir, como ser la adopción de medidas de seguridad o mantener la confidencialidad de la información. Esta lógica está presente en todas las normas latinoamericanas de protección de datos y constituye el elemento fundamental para habilitar una actividad de tratamiento. La generalidad de los casos parte del supuesto de que el titular de los datos no es el responsable del tratamiento. Así, como sostiene Allen, el usuario no es el dueño de los datos en la práctica porque todos sus derechos reconocidos jurídicamente están condicionados a las acciones, voluntarias u obligados por un mandato legal o judicial, del responsable del tratamiento.

Las soluciones de identidad digital auto soberana tienen el potencial de girar esta premisa. En un esquema de estas características, el titular de los datos tiene la facultad de determinar cómo usar sus propios datos y qué medios serán empleados para la conformación de su identidad. Por lo tanto, el titular actúa también como responsable del tratamiento. Cabe preguntarse si corresponde trasladar a la persona la carga de cumplir con los deberes como responsable y, en particular, si queremos que el individuo sea considerado responsable frente a otros responsables y se relacione con estos en igualdad de condiciones. Las normativas de protección de datos personales pretenden proteger a la parte débil, el titular, frente a las acciones de una contraparte fuerte, el responsable. Al mezclarse en la misma entidad la figura del titular con la del responsable, no hay una entidad que deba responder ante el ejercicio de los derechos del titular de los datos. Este tipo de soluciones aún sigue en estudio a nivel internacional, particularmente en Europa, y hay muchas preguntas sin responder, entre ellas la pregunta por el rol que tiene la entidad que crea el software para su funcionamiento. Esta entidad sería la que fija cómo funciona el sistema, determina qué software (medios) pueden usarse, y qué puede hacerse con la identidad creada en el sistema (fines). Por lo tanto, parecería que también es un responsable del tratamiento.

Una segunda relación que existe en este sentido es aquella entre el responsable y el encargado del tratamiento, donde el encargado es una entidad que realiza una actividad de tratamiento de datos por cuenta y orden del responsable del tratamiento. Es decir, el encargado solo puede hacer con los datos lo que el responsable lo autorice. Cualquier tratamiento, por mínimo que sea, fuera de las instrucciones del responsable debe ser considerado como una infracción a los deberes asumidos por este. Habitualmente en los sistemas de identidad digitales tradicionales, el responsable del tratamiento le encomienda cierta tarea –por ejemplo, el almacenamiento de datos o su validación contra una base de datos independiente- a un encargado. Al considerar un sistema de identidad auto soberano, esta relación se podría transformar en tanto el titular de los datos es el responsable del tratamiento y por ende tendrá una relación directa con los encargados del tratamiento, si prospera el argumento de considerar al individuo como responsable. De lo contrario, el responsable deberá asegurarse que el titular de los datos esté debidamente informado sobre los posibles encargos de tratamiento de datos que se hagan en su interés.

Otro aspecto de las relaciones entre los sujetos involucrados en el tratamiento de datos personales tiene que ver con el lugar en donde estas se desarrollan. En particular, una transferencia internacional de datos, ya sea de un responsable a otro responsable o de un responsable a un encargado del tratamiento, tiene características y relaciones propias. Aquí las figuras que pasan a cobrar relevancia son las de exportador e importador de datos, cuyos roles son la emisión y recepción, respectivamente, de datos personales involucrados en una comunicación entre diferentes jurisdicciones. El criterio general sobre este punto es que no se permiten las transferencias de datos a jurisdicciones que no proporcionen un nivel adecuado de protección de datos, el cual suele ser, como mínimo, el mismo que la jurisdicción de origen de los datos. La cuestión tiene impacto y se relaciona con el punto anterior ya que, si el titular del dato es el responsable del tratamiento, puede decidir libremente a donde van a ir sus datos; ahora bien, si el responsable del tratamiento es quien pone a disposición esa plataforma o solución de identidad digital auto soberana, será necesario contar, al menos, con el consentimiento del titular de los datos para comunicar los datos a terceros.

g. *Blockchain*, criptomonedas y *tokens*

Aún no existe una norma jurídica que defina el concepto de *blockchain* debido a lo novedoso de esta tecnología. Por lo tanto, y como se ha realizado con otros conceptos, recurriremos a la doctrina para su definición. Siguiendo a Andreas Antonopoulos[14], *blockchain* es una forma de estructurar una base de datos mediante un listado de bloques que contienen información almacenada y están unidos de forma consecutiva. Cada bloque nuevo del listado está unido al anterior al contener, de forma simplificada mediante un hash[15], toda la información del bloque precedente. La tecnología encuentra su origen en el protocolo Bitcoin, propuesto[16] e implementado[17] originalmente por Satoshi Nakamoto, aunque hoy en día es la base tecnológica de muchos otros protocolos, como puede ser Ethereum.

La particularidad que tiene la tecnología es que, a diferencia de otras formas de estructurar bases de datos, puede ser implementada de forma distribuida, sin la necesidad de contar con una entidad o un conjunto de entidades que actúen como reguladoras o controladoras de esa red para evaluar la validez de la información. En ese sentido, mientras la operación que se pretenda asentar en la *blockchain* cumpla con los requisitos fijados en el código informático, no será rechazada por la red. Gracias a esta lógica, es posible llevar un registro preciso de información sin tener que contar con una entidad que la centralice. De allí que esta tecnología haya podido resolver el problema del doble gasto de recursos digitales sin necesidad de contar con una entidad coordinadora. Las entidades que hacen este trabajo de procesamiento de información reciben como recompensa una unidad asociada al protocolo; a modo de ejemplo, las unidades en la *blockchain* de Bitcoin son bitcoins, en la *blockchain* de Ethereum son ethers, etc.

Existen varias formas de clasificar una *blockchain*: *blockchains* públicas y privadas, las permisionadas y no-permisionadas, y las

14 Cfr. ANTONOPOULOS, Andreas M., "Mastering Bitcoin: Programming the Open Blockchain", Edit. O'Reilly Media, 2da edición, versión para Kindle, capítulo 10.

15 La función criptográfica hash, conocida también como función de resumen, es un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija, con el objetivo de asegurar que no se ha modificado un archivo, hacer ilegible una contraseña, o firmar digitalmente un documento, entre otras.

16 Cfr. NAKAMOTO, Satoshi, "Bitcoin: Un Sistema de Efectivo Electrónico Usuario-a-Usuario", traducción de Angel Leon, https://bitcoin.org/files/bitcoin-paper/bitcoin_es_latam.pdf (Fecha de consulta 31 de diciembre de 2019).

17 El Nakamoto Institute mantiene copias del código original desarrollado por Nakamoto entre 2008 y 2009. Se puede acceder a esas copias por medio del siguiente enlace https://satoshi.nakamotoinstitute.org/code/ (Fecha de consulta 31 de diciembrede 2019).

híbridas. Los nombres de estas variantes reflejan su estructuración, así como sus ventajas e inconvenientes. Sin entrar en detalles que excederían al marco de esta investigación, mientras más pública sea una *blockchain*, más complejo será su funcionamiento y gobernanza y viceversa. Ello se debe a que las *blockchains* públicas parten del supuesto de que ninguno de sus miembros guarda confianza con los otros, con lo cual es necesario implementar mecanismos técnicos para garantizarla.

En cuanto a las aplicaciones que puede tener esta tecnología, su campo es amplio dado su funcionamiento intrínseco. Básicamente toda base de datos sobre la cual resulte conveniente mantener un registro distribuido, con independencia del grado de publicidad y apertura que tenga, es susceptible de utilizar tecnología *blockchain* de forma eficiente. En el caso que motiva la producción de este informe, contar con un fichero donde se consigne datos sobre la identidad de una persona de forma transparente, al mismo tiempo que se resguarda la privacidad de la información, podría ser beneficioso para todos los actos de la vida civil y comercial de las personas. Acreditar identidad de forma certera e indubitable resulta esencial para demostrar quién es la persona que se está presentando. Asimismo, permitir a la persona elegir que atributos quiere mostrar contribuye a no revelar datos personales de forma innecesaria. Por ejemplo, la *app* de DIDI genera un código de identificación en la *blockchain* que se conoce como DID (identificador descentralizado), el cual utiliza un protocolo de desafío/respuesta para probar la propiedad y permitir el uso de una identidad en particular a partir de la validación de datos biométricos con el Registro Nacional de las Personas (RENAPER), y sobre la cual se asocian las credenciales verificables [18].

En última instancia, esta tecnología de contabilidad distribuida (*distributed ledger technology –DLT*) propia de *blockchain*, permite llevar una anotación de actos y hechos con relevancia jurídica a nivel internacional de forma distribuida cuya existencia es independiente de cualquier organización individual, y, por lo tanto, resistente a la manipulación y censura, siempre y cuando se cumplan con los requisitos informáticos del protocolo mediante el uso de las unidades asociadas a cada *blockchain*.

El comportamiento de estas unidades define su naturaleza jurídica. A efectos de este informe y siguiendo las clasificaciones propuestas por diferentes reguladores internacionales[19], las unidades asociadas a un *blockchain* pueden ser clasificados en tres grandes categorías: (i) *tokens* de pago; (ii) *tokens* de utilidad; y (iii) *tokens* de activos. El primero de estos *tokens* corresponde a las llamadas criptomonedas y su propósito principal, el cual configura su valor, es actuar como un medio de pago. Por otro lado, los *tokens* de utilidad son aquellos cuyo uso da lugar al ejercicio de un derecho determinado y que es reconocido por la red donde es aceptado ese *token*. Finalmente, los *tokens* de activos son aquellos que actúan como una representación de un activo subyacente; estos generalmente son empleados para la representación de valores negociables, pero se está comenzando a explorar otros potenciales usos.

Sin perjuicio de esta clasificación, pocas jurisdicciones han reconocido el uso de las criptomonedas como dinero o moneda a nivel internacional. El uso de las criptomonedas de forma especulativa ha opacado el potencial que estas tienen para la realización de pagos de forma más ágil, horizontal e internacional.

---

18 **Las credenciales verificables son medios por el cual podemos probar hechos sobre el propietario de un DID, acreditando de manera digital y segura que una persona es portadora de ciertos atributos que tienen que ver con su identidad. Las credenciales, además de contener información sobre el titular, contiene el DID del emisor, que es el equivalente a la firma de la entidad emisora.**

19 **CASEY, Michael J., "Regulators Are Slowly Starting to Get It: Utility Tokens Are Real", *CoinDesk*, 11 de julio de 2018, disponible en https://www.coindesk.com/regulators-are-slowly-starting-to-get-it-utility-tokens-are-real (Fecha de consulta 31 de diciembre de 2019).**

En atención a ello, es oportuno preguntarse, i) si estas pueden ser consideradas como dinero, y ii) si tienen curso legal, es decir si pueden ser usadas como medio de pago con poder cancelatorio de obligaciones. Ambas cuestiones tienen consecuencias prácticas de importante relevancia.

En cuanto a la primera, su respuesta condiciona el tratamiento jurídico que tendrán las obligaciones de dar cantidades de criptomonedas. Por ejemplo, si la entrega de criptomonedas se considera como la entrega de una cosa, se debe entregar la cosa en cuestión y, únicamente de forma excepcional, podrá indemnizarse a la otra parte; en cambio, si se considera que son monedas o dinero y su entrega se ve imposibilitada, podría ser posible la entrega del equivalente en moneda fiduciaria local. Respecto de la segunda pregunta, la misma tiene implicancias sobre el uso de las criptomonedas como medio de pago ya que si carecen de poder cancelatorio -curso legal- la aceptación de estas para cumplir con una obligación queda a exclusiva voluntad de la persona que las reciba, a diferencia de lo que ocurre con el dinero fiduciario cuya aceptación no puede ser rechazada.

Un punto intermedio, y aún sin una respuesta clara en la legislación y la doctrina, es el caso de los *tokens* de pago respaldados en moneda fiduciaria. Tradicionalmente, la representación digital de monedas fiduciarias se ha instrumentado mediante los sistemas de dinero electrónico. Ahora bien, el soporte de estas representaciones no ha usado tecnologías de registro distribuido. Con lo cual, la pregunta gira en torno a la categoría jurídica que revisten estos *tokens* de pago con un respaldo en moneda fiduciaria local. Ello es de fundamental importancia porque el emisor de estos *tokens* tiene ciertas obligaciones frente a los tenedores de estos instrumentos, así como también el uso de los *tokens* estaría condicionado al análisis efectuado en el párrafo anterior.

Situación jurídica en América Latina en materia de identidad digital autosoberana

4

La situación normativa en la cual se podría implementar un sistema privado digital de identidad auto soberano es diferente para cada país. Para facilitar la consulta de esta información, la Tabla 2 resume brevemente las principales características del marco normativo de cada país que serán descritos en detalle en este apartado.

dica en Améri
ria de identida
berana Situaci

Tabla 2

Marco normativo para la implementación de un sistema privado de identidad digital auto soberano

País	¿Hay un concepto legal de identidad?	¿Quién es el dueño** de los datos personales?	¿Hay una forma única para acreditar la identidad?	¿Los datos personales pueden ser transferidos al exterior?	¿Tiene validez un documento digital?
Argentina	No	El individuo	No*	No*	Sí
Bolivia	No	El individuo	No	Sí	Sí
Brasil	No	El individuo	No*	No*	Sí
Chile	No	El individuo	No*	No*	Sí
Colombia	No	El individuo	Sí*	No*	Sí
Costa Rica	No	El individuo	Sí*	Sí*	Sí
Cuba	No	El individuo	Sí	Sí*	Sí*
Ecuador	Sí	El individuo	Sí*	No*	Sí
El Salvador	No	El individuo	Sí*	Sí	Sí
Guatemala	No	El individuo	Sí	Sí	Sí
Haití	No	El individuo	No	Sí	Sí
Honduras	No	El individuo	Sí*	No	Sí
México	No	El individuo	No	No*	Sí
Nicaragua	No	El individuo	Sí*	No*	Sí
Panamá	No	El individuo	Sí	No*	Sí
Paraguay	No	El individuo	No	Sí	Sí
Perú	Sí	El individuo	Sí*	No*	Sí
República Dominicana	No	El individuo	No	No*	Sí
Uruguay	No	El individuo	No*	No*	Sí
Venezuela	No	El individuo	No*	Sí	Sí

* La respuesta proporcionada en este punto no es absoluta y es necesario revisar el análisis realizado del punto para tener un conocimiento pleno de la situación.
** Se utilizará el término "dueño" para facilitar la lectura aunque se deja en claro que, dado la concurrencia de derecho humanos en el concepto de identidad, no existe una relación de dominio sobre los datos en los términos de la legislación civil y comercial de cada jurisdicción

a. Argentina

i. ¿Hay una definición legal de identidad?

En la República Argentina no existe un concepto de identidad, ya sea física o digital, de origen legal. Las normas que sí existen en Argentina en materia de identidad están íntimamente relacionadas con las consecuencias del gobierno de facto del periodo 1976-1983 sobre la identidad de los menores de edad. Durante ese período, cientos de menores fueron separados de sus padres por la fuerza, por lo tanto, las normas existentes tienden a instrumentar mecanismos para permitir su reidentificación y la conexión con sus familias originales. A modo de ejemplo, podemos mencionar la Ley Nº 23.511, la Ley Nº 25.457 o la Ley Nº 26.001. Asimismo, existen otras normas que tratan sobre aspectos delimitados de la identidad de las personas, como la Ley Nº 17.671 que versa sobre el documento nacional de identidad o la Ley Nº 26.743 que define y reconoce el derecho a la identidad de género. Finalmente, la Disposición Nº E-9/2016 que crea el llamado "Perfil del Ciudadano Digital: Mi Argentina", que puede ser considerada una identidad digital de los ciudadanos argentinos de uso voluntario a efectos gubernamentales.

En atención a ello, y aplicando el principio protectorio en materia de datos personales, hay que concluir que en Argentina todos los datos personales de una persona forman parte de su identidad. Con lo cual, todo atributo de la personalidad debe ser considerado como dato personal y protegido de conformidad con las prescripciones de la Ley Argentina de Protección de Datos Personales.

ii. ¿Quién es el dueño de los datos según la normativa?

Si bien la Ley Argentina de Protección de Datos Personales no lo menciona expresamente, la norma nos lleva a concluir que, dadas las facultades que reconoce al titular de los datos, la persona física es la dueña de los mismos. Las entidades que los gestionan únicamente pueden hacerlo en respeto de esas facultades.

iii. ¿Qué mecanismos son válidos para acreditar la identidad de una persona?

Sobre esta cuestión, atento a la falta de una regulación especial, es necesario hacer un análisis acto por acto de la vida jurídica de la persona para determinar cómo tiene que acreditar su identidad en cada caso. Dada la existencia de un documento nacional de identidad otorgado por el Estado, ciertos actos realizados con entidades reguladas, como podría ser una entidad financiera o un sujeto obligado a cumplir con normas de prevención de lavado de activos, es necesario presentar este documento para acreditar la identidad.

iv. ¿Existen entidades reguladas para brindar servicios de identificación de personas?

Sí. El Decreto 182/2019 establece que los prestadores de servicios de confianza[20] pueden brindar servicios de identificación, aunque a la fecha de este informe están pendientes los detalles de tal regulación.

v. ¿Qué validez tienen los documentos digitales o electrónicos?

Dado que los proyectos de identidad auto soberana implican la creación de un sistema informático, es necesario considerar si un documento generado por medios electrónicos tiene validez legal o no en la Argentina.

Conforme el Código Civil y Comercial de la Nación de la República Argentina (el "CCyCN"), los actos jurídicos pueden expresarse por medios escritos, ya sean físicos o digitales. El artículo 286 indica que:

20 De acuerdo al decreto 182/2019, podrán brindar servicios de confianza las personas humanas, jurídicas, consorcios, entes públicos, entes públicos no estatales, de acuerdo a los procedimientos, estándares y condiciones que determine la Secretaría de Modernización Administrativa de la Jefatura de Gabinete de Ministros.

> La expresión escrita puede tener lugar por instrumentos públicos, o por instrumentos particulares firmados o no firmados, excepto en los casos en que determinada instrumentación sea impuesta. Puede hacerse constar en cualquier soporte, siempre que su contenido sea representado con texto inteligible, aunque su lectura exija medios técnicos.

Si el acto está documentado en un instrumento público, el mismo hace plena fe de los hechos de relevancia jurídica, sin importar su soporte; en todo caso, la admisibilidad de los soportes electrónicos para tal acto deberá analizarse para cada acto en cuestión y ver si la normativa que regula ese instrumento permite que sea realizado por medios electrónicos. Teniendo en cuenta el proceso de digitalización del Estado argentino[21], es de esperar que los documentos públicos digitales sean equivalentes a sus contrapartes físicas, o directamente pasen a reemplazarlos.

Por otro lado, si el acto está documentado en un instrumento privado, su validez dependerá si está firmado digital o electrónicamente, en consonancia con las prescripciones de la Ley Argentina de Firma Digital. Dado que en Argentina la gran mayoría de los documentos creados por medios informáticos están firmados electrónicamente, los consideramos como instrumentos particulares y, por lo tanto, su validez se aprecia en función del artículo 319 del CCyCN, que señala lo siguiente:

> El valor probatorio de los instrumentos particulares debe ser apreciado por el juez ponderando, entre otras pautas, la congruencia entre lo sucedido y narrado, la precisión y claridad técnica del texto, los usos y prácticas del tráfico, las relaciones precedentes y la confiabilidad de los soportes utilizados y de los procedimientos técnicos que se apliquen.

Considerando lo que plantea el CCyCN y la Ley Argentina de Firma Digital, no hay inconvenientes en el uso de documentos electrónicos para la preservación de atributos de la identidad de cada usuario.

vi. ¿Los datos relativos a la identidad deben almacenarse en el país o pueden ser transferidos al exterior?

No existe una prohibición para que los datos de una persona sean transferidos al exterior; es decir, y a menos que se dicte una norma especial al respecto, no hay obligación de mantener los datos en el país. Ahora bien, conforme el artículo 12 de la Ley Argentina de Protección de Datos Personales, los datos personales de una persona no pueden ser transferidos a una jurisdicción que no presente un nivel adecuado de protección de datos personales. Conforme la Disposición Nº 60/2016 de la Dirección Nacional de Protección de Datos Personales y la Resolución Nº 34/2019 de la AAIP, las siguientes jurisdicciones son adecuadas: Estados miembros de la Unión Europea y miembros del Espacio Económico Europeo (EEE), Reino Unido de Gran Bretaña e Irlanda del Norte, Confederación Suiza, Guernsey, Jersey, Isla de Man, Islas Feroe, Canadá (aplica solo su a sector privado), Principado de Andorra, Nueva Zelanda, República Oriental del Uruguay y Estado de Israel (aplica solo a los datos que reciban un tratamiento automatizado). Fuera de estos países, es necesario adoptar un mecanismo suplementario, como puede ser un acuerdo de transferencia internacional de datos.

21 Desde el 2016 se incrementaron las políticas de modernización del Estado con el fin de transformar las burocracias basadas en papel, en burocracias digitales más agiles. A su vez, se dieron los primeros pasos en el uso de herramientas de gobierno inteligente como *blockchain*, *big data*, e inteligencia artificial (IA).

b. Bolivia

i. ¿Hay una definición legal de identidad?

Al igual que sucede con muchas otras jurisdicciones que son objeto de este estudio, Bolivia carece de una definición legal de identidad. Sin perjuicio de esto, Bolivia suscribe a varios de los tratados internacionales de derechos humanos reseñados en la introducción de esta investigación, con lo cual a partir de ellos es posible dar protección a ciertos aspectos del derecho a la identidad. Asimismo, Bolivia cuenta con algunas normas, como la Ley Nº 807 del 21 de mayo de 2016, que protegen especialmente ciertos aspectos de la identidad en materia de género. Fuera de ello, la identidad también estaría cubierta por el artículo 21.2 de la Constitución boliviana que cubre a la identidad de igual manera que los instrumentos internacionales de derechos humanos.

Al igual que ocurre en otros países, existe un sistema nacional de identidad creado por la Ley del Servicio General de Identificación Personal y del Servicio General de Licencias Para Conducir el 27 de junio de 2011 (la "Ley Boliviana del SEGIP"), la cual crea el Servicio General de Identificación Personal (el "SEGIP"). El SEGIP tiene a su cargo la expedición de las cédulas de identidad así como también la custodia del Registro Único de Identificación.

ii. ¿Quién es el dueño de los datos según la normativa?

Si bien no existe una previsión expresa sobre la titularidad de los datos personales, es posible considerar que la persona física es la titular de los mismos ya que el ordenamiento jurídico boliviano, extremo confirmado por el Tribunal Constitucional en su sentencia 0965/2004-R, le reconoce el derecho al titular de los datos de reclamar su protección vía el *habeas data*.

iii. ¿Qué mecanismos son válidos para acreditar la identidad de una persona?

Conforme la Ley Boliviana del SEGIP, las personas físicas pueden recurrir a los servicios del SEGIP para validar su identidad frente a terceros.

Por otro lado, el uso de la cédula de identidad es suficiente para acreditar la identidad de la persona, ya sea nacional o extranjero, en el territorio de Bolivia, así como en otros países los cuales tengan un acuerdo internacional de reconocimiento recíproco de documentos de identificación estatal.

iv. ¿Existen entidades reguladas para brindar servicios de identificación de personas?

Al respecto de ello, no existen normas especiales, más allá de la aplicación analógica y en lo que resulte pertinente de la Ley Boliviana de TIC, sobre la posibilidad que privados brinden servicios de identificación de personas, menos aún sobre su validez.

Sobre esta cuestión, recordamos que el SEGIP tiene facultades para brindar este servicio tanto a requerimiento de la persona como de terceros que quieran validar su identidad.

v. ¿Qué validez tienen los documentos digitales o electrónicos?

La Ley Boliviana de TIC establece que los documentos digitales tienen plena validez jurídica, conforme su artículo 78, salvo que se trate de uno de los supuestos prohibidos por el artículo 79, a saber:

> Se exceptúan los siguientes actos y hechos jurídicos de su celebración por medios electrónicos:
> 1. Los actos propios del derecho de familia.
> 2. Los actos en que la Ley requiera la concurrencia personal física de alguna de las partes.
> 3. Los actos o negocios jurídicos señalados en la Ley que, para su validez o producción de determinados efectos, requieran de documento físico o por acuerdo expreso de partes.

La norma reglamentaria de la Ley Boliviana de TIC amplia esto y señala, en su artículo 34.I, que:

> Cuando una Firma Digital ha sido inscrita en un documento digital o mensaje de datos, se presume la voluntad del titular de la firma digital para acreditar ese documento digital o mensaje electrónico de datos, y se adscribe y vincula con el contenido de la información de los mismos.

A ello es necesario sumar los siguientes requisitos fijados por el artículo 34.II:

> Los mensajes electrónicos de datos o documentos digitales ambos con firma digital adquieren plena validez jurídica probatoria bajo las siguientes condiciones:
> a) Ser individual y estar vinculada exclusivamente a su titular;
> b) Que permita verificar inequívocamente la autoría e identidad del signatario, mediante procedimientos de autenticación y de seguridad y esté conforme a la normativa vigente;
> c) Que su método de creación y verificación sea confiable, seguro e inalterable para el propósito para el cual el mensaje fue generado o comunicado;
> d) Que al momento de creación de la firma digital, los datos con los que se creare se hallen bajo control exclusivo del signatario;
> e) Que la firma sea controlada por la persona a quien pertenece.

vi. ¿Los datos relativos a la identidad deben almacenarse en el país o pueden ser transferidos al exterior?

No hay norma que limite o indique requisitos para la transferencia internacional de datos.

c. Brasil

i. ¿Hay una definición legal de identidad?

El punto de partida para nuestro análisis del concepto legal de identidad en el marco normativo brasileño es la Constitución de la República. Si bien no existe una protección directa y especifica del derecho a la identidad, hay varios artículos que protegen aristas de este derecho, como lo son los artículos 5 incisos VI, IX, X, XVI, XVII, entre otros. Asimismo, es necesario tener en cuenta que la República de Brasil forma parte de los instrumentos internacionales de derechos humanos reseñados al comienzo de este informe, quedando el derecho a la identidad también protegido por esas normas jurídicas.

Fuera de la protección constitucional y de rango internacional, la Ley Nº 6.015 del 31 de septiembre de 1973 (la "Ley Brasileña del Registro Civil") crea todos los registros públicos operativos en Brasil. En particular, conforme el artículo 29 de la citada norma, en el registro civil de las personas naturales se inscriben todos los actos civiles de relevancia para la vida de las personas. La información de las delegaciones de los registros civiles está centralizada en el Sistema Nacional de Información del Registro Civil, conforme el Decreto Nº 8270/2014.

A ello debemos agregar la Ley Nº 13.444 del 11 de mayo de 2017 (la "Ley Brasileña sobre Identifiaciòn Civil Nacional"), la cual regula el documento de identificación civil nacional que permite la identificación del brasileño en sus relaciones sociales con el Estado y los privados. Entre sus fuentes para expedir el documento se usan: la base de datos biométricos de la Justicia Electoral, la base de datos del Sistema Nacional de Información del Registro Civil así como la Central Nacional de Información del Registro Civil, y otras bases de datos públicas del Estado. El artículo 8 prescribe que: "*É criado o Documento Nacional de Identidade (DNI), com fé pública e validade em todo o território nacional.*"

En este sentido, el mismo artículo 8 señala que el DNI es un instrumento superador de los documentos usados para crearlo. Es decir, basta la presentación del DNI para acreditar la edad, siendo innecesario presentar una partida de nacimiento. Asimismo, se pretende que el DNI sea superador también de la anterior cedula de identidad, el documento que era usado por defecto por los brasileños para acreditar su identidad; si bien las cédulas de identidad siguen estando vigentes, la intención del gobierno brasileño es su paulatino reemplazo.

ii. ¿Quién es el dueño de los datos según la normativa?

Si bien la Ley Brasileña de Protección de Datos Personales no lo menciona expresamente, una lectura sistemática de la norma nos lleva a concluir que, dada las facultades reconocidas al titular de los datos, la persona física es la dueña de los mismos. Las entidades que los gestionan únicamente pueden hacerlo en respeto de esas facultades.

iii. ¿Qué mecanismos son válidos para acreditar la identidad de una persona?

El DNI es el instrumento principal para acreditar la identidad, conforme lo rese-

ñado en el punto i. En ese sentido, todo acto que requiera de él por obligación legal solo podrá cumplirse con los requisitos de identificación presentándolo. Para los casos donde no es necesario la presentación del DNI, quedará a criterio de las partes que mecanismos serán considerados como válidos para acreditar la identidad.

iv. ¿Existen entidades reguladas para brindar servicios de identificación de personas?

Fuera de los servicios proporcionados por el Estado (mencionados en el punto i), no hay regulación para la provisión de servicios de identificación de personas en ambientes digitales.

v. ¿Qué validez tienen los documentos digitales o electrónicos?

Respecto a la validez de documentos digitales o electrónicos, la Medida Provisional Nº 2.200-2 de 24 de agosto de 2001 (el "Marco Normativo Brasileño de Firma Digital") establece en su artículo 10 lo siguiente:

> Consideram-se documentos públicos ou particulares, para todos os fins legais, os documentos eletrônicos de que trata esta Medida Provisória.
> § 1o As declarações constantes dos documentos em forma eletrônica produzidos com a utilização de processo de certificação disponibilizado pela ICP-Brasil presumem-se verdadeiros em relação aos signatários, na forma do art. 131 da Lei no 3.071, de 1o de janeiro de 1916 - Código Civil.
> § 2o O disposto nesta Medida Provisória não obsta a utilização de outro meio de comprovação da autoria e integridade de documentos em forma eletrônica, inclusive os que utilizem certificados não emitidos pela ICP-Brasil, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento.

Es decir, los documentos electrónicos, con independencia del tipo de firma que usen, son equivalentes a sus contrapartes físicas. A ello se suma el artículo 441 del Código Civil que toma como válidos aquellos documentos generados por medios electrónicos con consonancia con la normativa especial, es decir el Marco Normativo Brasileño de Firma Digital.

vi. ¿Los datos relativos a la identidad deben almacenarse en el país o pueden ser transferidos al exterior?

Conforme la Ley Brasileña de Protección de Datos Personales, los datos personales de una persona no pueden ser transferidos a una jurisdicción que no presente un nivel adecuado de protección de datos personales, salvo que se cumpla con alguna de las autorizaciones previstas en la norma para poder realizar la transferencia a pesar de ello.

d. Chile

i. ¿Hay una definición legal de identidad?

Si bien en Chile no existe una definición legal del concepto de identidad, la identidad está protegida por la adhesión de Chile a los instrumentos internacionales de derechos humanos antes reseñados, ya que los mismos obligan al Estado chileno a velar por su protección. Esto lo confirma además la Sentencia Nº 1340-09 del 29 de septiembre de 2009 del Tribunal Constitucional. Al margen de ello, al igual que ocurre en otros países de la región, ciertas expresiones en particular de la identidad comienzan a estar protegidas especialmente mediante el dictado de leyes concretas como es el caso de la Ley Nº 21.120 sobre identidad de género.

Al margen de ello, existe en Chile el concepto de identidad nacional proporcionada por el Estado bajo las funciones del Servicio de Registro Civil e Identificación, el cual opera bajo la Ley Nº 19.477 (la "Ley Chilena del Registro Civil"). En esta línea, una de las funciones principales del Servicio de Registro Civil e Identificación, conforme el artículo 4.4., es "establecer y registrar la identidad civil de las personas y otorgar los documentos oficiales que acreditan la identidad".

En lo que hace a la temática de identidad digital, el gobierno chileno ha impulsado un sistema llamado "ClaveÚnica", que tiene por finalidad transformar esa identidad del mundo físico que el Servicio de Registro Civil e Identificación tiene a su cargo en una identidad digital que los ciudadanos y extranjeros debidamente registrados en Chile puedan interactuar con el Estado chileno por medios informáticos.

ii. ¿Qué es el dueño de los datos según la normativa?

Si bien la Ley Chilena de Protección de Datos Personales no lo menciona expresamente, una lectura sistemática de la norma nos lleva a concluir que, dada las facultades reconocidas al titular de los datos, es la persona física la dueña de los mismos. Las entidades que gestionan estos únicamente pueden hacerlo en respeto de esas facultades.

iii. ¿Qué mecanismos son válidos para acreditar la identidad de una persona?

Conforme el artículo 4.4 de la Ley Chilena del Registro Civil, los documentos que el Servicio de Registro Civil e Identificación otorguen

son los que sirven para acreditar de forma plena la identidad de una persona; ello sin perjuicio que las partes de un determinado acto jurídico, en la medida que sea aplicable la autonomía de la voluntad, puedan acordar y admitir otras medidas para acreditar una identidad. En el caso de los documentos oficiales, el principal documento a tales efectos es la cédula de identidad.

iv. ¿Existen entidades reguladas para brindar servicios de identificación de personas?

En Chile no existe normativa que regule a las entidades encargadas de brindar servicios de identificación de forma privada. En la faz pública, como bien señalamos antes, el Servicio de Registro Civil e Identificación es la entidad que tiene la potestad exclusiva y la obligación de brindar el servicio de identificación de las personas que habiten en territorio chileno o sean nacionales de tal país.

v. ¿Qué validez tienen los documentos digitales o electrónicos?

La Ley Nº 19.799 (la "Ley Chilena de Firma Digital") reconoce las firmas electrónicas simples y las avanzadas; la diferencia entre ambas es que las segundas hacen uso de un certificado digital otorgado por un certificador licenciado pro el Estado chileno que cumpla con las prescripciones de la Ley Chilena de Firma Digital y sus reglamentaciones.

Al respecto de ello, el artículo 3 de la Ley Chilena de Firma Digital establece la equivalencia funcional entre los documentos firmados en papel y los documentos firmados electrónicamente haciendo uso de firma electrónica. Sin perjuicio de ello, el mismo artículo señala que la firma electrónica no es válida para aquellos actos que: (i) sean incompatibles con la firma electrónica; (ii) los que requieran la presencia física de las partes; y (iii) los actos jurídicos del derecho de familia.

En lo que hace a los documentos que tienen que hacerse por instrumento público, únicamente pueden celebrarse haciendo uso de firmas electrónicas avanzadas. Al respecto del uso de la firma electrónica avanzada, si un documento privado es firmado de esta forma adquiere categoría de documento público, salvo en lo que hace a su fecha.

e. Colombia

i. ¿Hay una definición legal de identidad?

El artículo 266 de la Constitución Política de Colombia, el cual prescribe lo siguiente:

"El Registrador Nacional del Estado Civil (...) ejercerá las funciones que establezca la ley, incluida la dirección y organización de las elecciones, el registro civil y la identificación de las personas, así como la de celebrar contratos en nombre de la Nación, en los casos que aquella disponga."

A pesar de este mandato, no existe una definición legal del concepto de identidad. La obligación mencionada en la Constitución se efectiviza mediante el Decreto Nº 1260 de 1970 (el "Decreto Colombiano del Estatuto del Registro del Estado Civil de las Personas"). Esta norma pone el foco sobre el estado civil de las personas como elemento central de su identidad, con énfasis en el nombre y las relaciones de familia, así como también el registro de los hechos que impactan sobre la identidad. Como consecuencia de este registro, el Estado colombiano dispone la emisión de documentos de identidad bajo el nombre de cédula de ciudadanía, las cuales están regladas por la Ley Nº 39 de 1961 (la "Ley Colombia del Documento Nacional").

ii. ¿Quién es el dueño de los datos según la normativa?

Si bien la Ley Colombiana de Protección de Datos Personales no lo menciona expresamente, una lectura sistemática de la norma nos lleva a concluir que, dada las facultades reconocidas al titular de los datos, la persona física es la dueña de los mismos. Las entidades que los gestionan únicamente pueden hacerlo en respeto de esas facultades.

iii. ¿Qué mecanismos son válidos para acreditar la identidad de una persona?

Conforme el artículo 1 de la Ley Colombia del Documento Nacional, el único documento válido para identificarse en todos los actos civiles, políticos, administrativos y judiciales es la cédula de identidad. Fuera de ello, no hay normativa que indique cómo debe ser la identificación para los actos de la vida comercial en general.

iv. ¿Existen entidades reguladas para brindar servicios de identificación de personas?

No hay regulación sobre las entidades privadas que brindan servicios de identificación. Sin perjuicio de ello, puede considerarse que las entidades de certificación, según la Ley Colombiana de Firma Digital, realizan actividades de identificación en lo que hace a la expedición de certificados de firma digital y otras actividades relacionadas con los mensajes de datos. Si la actividad de identificación de personas puede ser subsumida en alguno de estos servicios, debería darse cumplimiento a tal normativa.

v. ¿Qué validez tienen los documentos digitales o electrónicos?

La Ley Nº 527 de 1999 (la "Ley Colombiana de Firma Digital") establece la categoría de mensajes de datos y su equivalencia funcional a la forma escrita conforme el artículo 6 de dicha norma. Con lo cual, cuando una formalidad tenga que hacerse por escrito, alcanza con usar medios electrónicos para ello en la medida que se reúnan los requisitos fijados por la Ley Colombiana de Firma Digital para los mensajes de datos.

vi. ¿Los datos relativos a la identidad deben almacenarse en el país o pueden ser transferidos al exterior?

Conforme la Ley Colombiana de Protección de Datos Personales, en principio están prohibidas las transferencias de datos personales a una jurisdicción que no sea considerada como adecuada. Si bien existen varios supuestos en el artículo 26 de dicha norma que actúan como excepciones, en el caso que no se caiga en ninguna de ellas, es posible requerir una autorización especial, conocida con el nombre de declaración de conformidad, a la Superintendencia de Industria y Comercio para que se permita la transferencia internacional de datos.

f. Costa Rica

i. ¿Hay una definición legal de identidad?

Al igual que sucede con otros países de la región, Costa Rica carece de un concepto normativo de identidad. Sin perjuicio de ello, la identidad goza de protección legal por la adhesión de Costa Rica a los instrumentos internacionales de derechos humanos mencionados en la sección introductoria de este informe. Sin embargo, en la Constitución de Costa Rica se menciona que es deber del Estado proporcionar a los ciudadanos documentos de identidad para ejercer sus derechos políticos.

En línea con esta obligación, la Ley Nº 3.504 del 10 de mayo de 1965 (la "Ley Costarricense del Registro Civil") encomienda al Tribunal Supremo de Elecciones el mantenimiento y operación del Registro Civil, el cual lleva el registro de todos los actos de relevancia de la vida civil de las personas. En función de la información allí consignada, se procede a la expedición de las cédulas de identidad, la cual contiene una serie de datos sobre la persona conforme el artículo 90 de la Ley Costarricense del Registro Civil.

ii. ¿Quién es el dueño de los datos según la normativa?

Si bien la Ley Costarricense de Protección de Datos Personales no lo menciona expresamente, una lectura sistemática de la norma nos lleva a concluir que, dada las facultades reconocidas al titular de los datos, la persona física es la dueña de los mismos. Las entidades que los gestionan únicamente pueden hacerlo en respeto de esas facultades.

iii. ¿Qué mecanismos son válidos para acreditar la identidad de una persona?

Conforme el artículo 95 de la Ley Costarricense del Registro Civil, la cédula de identidad es el único documento válido para los siguientes actos:

a) Emitir el voto;
b) Todo acto o contrato notarial;
c) Iniciar gestiones o acciones administrativas o judiciales;
d) Firmar las actas matrimoniales, ya sean civiles o católicas;
e) Ser nombrado funcionario o empleado del Estado, sus instituciones y Municipalidades;
f) Formalizar contratos de trabajo;
g) Firmar obligaciones a favor de instituciones autónomas, semiautónomas o de las Juntas Rurales de Crédito y Oficinas de Ayuda al Agricultor;
h) Obtener pasaporte;
i) Formalizar el Seguro Social, sin que esta

disposición pueda amparar al patrono de las consecuencias que la ley y Reglamento de la Caja Costarricense de Seguro Social le imponen;
j) Recibir giros del Estado, Municipalidades e Instituciones Autónomas o Semiautónomas;
k) Matricular los padres o encargados a sus hijos o pupilos en escuelas y colegios, públicos o privados;
l) Obtener o renovar la licencia de conductor de vehículos; y
m) Cualquier otra diligencia u operación en que sea del caso justificar la identidad personal.

El mismo artículo señala que en otros casos, a saber, "en las escrituras públicas, en los contratos privados, en los expedientes administrativos y judiciales, pagarés y certificados de prenda (...)", es necesario consignar el número de la cédula sin ser necesaria su exhibición, con lo cual las personas tienen mayor margen para acreditar su identidad, aunque siempre deberían indicar este dato.

iv. ¿Existen entidades reguladas para brindar servicios de identificación de personas?

No existen normas que regulen los servicios de identificación en Costa Rica. En todo caso, deberá repararse en el apartado final del artículo 95 de la Ley Costarricense del Registro Civil y el servicio a ser brindado deberá contemplar, al menos, que las entidades verifiquen este número de cédula.

v. ¿Qué validez tienen los documentos digitales o electrónicos?

La Ley Nº 8.454 (la "Ley Costarricense de Firma Digital") establece en sus artículos 3, 4 y 5 que los documentos electrónicos tienen equivalencia con sus contrapartes físicas y deben reconocerse los mismos efectos que a los documentos físicos. La normativa reglamentaria de la Ley Costarricense de Firma Digital hace la distinción entre los documentos digitales y los documentos electrónicos en función del tipo de firma digital empleada.

vi. ¿Los datos relativos a la identidad deben almacenarse en el país o pueden ser transferidos al exterior?

Conforme la Ley Costarricense de Protección de Datos Personales, los datos pueden transferirse a otros países solo con el consentimiento del titular de los mismos, salvo que exista una disposición legal que indique lo contrario.

g. Cuba

i. ¿Hay una definición legal de identidad?

En la actualidad no existe un concepto de identidad digital en Cuba. La situación de Cuba en esta materia se ve dificultada aún más por la inexistencia de una normativa sobre protección de datos personales. A pesar de ello, Cuba es parte de algunos de los instrumentos de derechos humanos mencionados anteriormente, con lo cual es posible sostener que la identidad de las personas está conformada por los atributos que la identifican. Asimismo, la Constitución de la República de Cuba, en su artículo 48, establece que las personas tienen derecho a su identidad, sin entrar en detalles sobre cómo se encuentra conformada, más allá de algunas menciones en el mismo artículo sobre su imagen y su voz. Por otro lado, en Cuba existe un documento de identidad otorgado por el Estado: el carné de identidad. Conforme el Decreto-Ley 248 (la "Ley Cubana del Sistema de Identificación"), este documento se nutre a partir de información en los registros públicos cubanos.

ii. ¿Quién es el dueño de los datos según la normativa?

Cuba carece de una norma sobre protección de datos que determine quién es el efectivo titular de los mismos, pero por aplicación del artículo 48 y del artículo 97 es posible considerar que la persona humana es el titular de los datos.

iii. ¿Qué mecanismos son válidos para acreditar la identidad de una persona?

Según la Ley Cubana del Sistema de Identificación, se establece, en el artículo 2, que los documentos válidos para acreditar la identidad en suelo cubano son: (i) carné de identidad; (ii) tarjeta de menor; (iii) documento de identidad provisional; (iv) pasaporte de la República de Cuba para los que viajen o residan en el exterior; y (v) carné de las Fuerzas Armadas Revolucionarias, para los militares de esa Institución en servicio activo. En el caso de los extranjeros en territorio cubano, conforme el artículo 4, la identidad se acredita mediante: (i) carné de identidad del extranjero; (ii) tarjeta del menor de 16 años extranjero; y/o (iii) pasaporte o documento de viaje vigente.

iv. ¿Existen entidades reguladas para brindar servicios de identificación de personas?

Siguiendo con el esquema de la Ley Cubana del Sistema de Identificación, solo el Registro del Estado Civil es apto para proveer datos identificatorios de los ciudadanos cubanos.

v. ¿Qué validez tienen los documentos digitales o electrónicos?

Si bien existe regulación sobre los sistemas de firma digital en Cuba, principalmente la Resolución Nº 2/2016 del Ministerio del Interior cubano (el "Reglamento Cubano sobre el funcionamiento de la Infraestructura de Llave Pública"), esta norma señala expresamente, en su artículo 4, que:

> El Reglamento, no establece equivalencia jurídica entre la firma digital de documentos electrónicos realizada con los métodos criptográficos asociados a los certificados digitales de llave pública, y la firma manuscrita tradicional.

Si bien la norma no prohíbe estos documentos, tampoco da ningún tipo de equivalencia con sus contrapartes en papel.

vi. ¿Los datos relativos a la identidad deben almacenarse en el país o pueden ser transferidos al exterior?

No existe regulación que indique que los datos deben almacenarse exclusivamente en el país.

h. Ecuador

i. ¿Hay una definición legal de identidad?

El punto de partida para el análisis de este punto es la Constitución ecuatoriana de 2008. Esta norma prescribe en su artículo 66 inciso 28 lo siguiente:

> Se reconoce y garantizará a las personas (...) El derecho a la identidad personal y colectiva, que incluye tener nombre y apellido, debidamente registrados, y libremente escogidos; y conservar, desarrollar y fortalecer las características materiales e inmateriales de la identidad, tales como la nacionalidad, la procedencia familiar, las manifestaciones espirituales, culturales, religiosas, lingüísticas, políticas y sociales.

A esta definición de la identidad tenemos que agregar las prescripciones de la Ley Orgánica de Gestión de la Identidad y Datos Civiles publicada en el Segundo Suplemento al Registro Oficial Nº 684 del 4 de febrero de 2016 (la "Ley Ecuatoriana de Identidad"), que regula expresamente el derecho a la identidad. Esta norma dispone todos los derechos y obligaciones que existen en torno a la identidad de cada una de las personas que habita en el territorio ecuatoriano, así como también dispone la inscripción en el Registro Civil de todos los actos que afecten de alguna manera a la identidad de la persona.

ii. ¿Quién es el dueño de los datos según la normativa?

Si bien la Ley Ecuatoriana de E-Commerce no lo menciona expresamente, una lectura sistemática de la norma nos lleva a concluir que, dada las facultades reconocidas al titular de los datos, la persona física es la dueña de los mismos. Las entidades que gestionan estos únicamente pueden hacerlo en respeto de esas facultades.

iii. ¿Qué mecanismos son válidos para acreditar la identidad de una persona?

Conforme al artículo 97 de la Ley Ecuatoriana de Identidad, la cédula de identidad es el mecanismo óptimo para acreditar la identidad de una persona. En ese sentido, el artículo prescribe lo siguiente:

> La identificación de una persona se acreditará en sus actos públicos y/o privados con la presentación de la cédula de identidad.

La redacción de la norma no habla de obligatoriedad ni exclusividad con lo cual es posible acreditar la identidad por otros medios que las partes acuerden de forma voluntaria y de común acuerdo.

iv. ¿Existen entidades reguladas para brindar servicios de identificación de personas?

No existe regulación alguna en Ecuador que determine cómo debe ser brindado este servicio ni quiénes pueden o no dar este servicio. Por lo tanto, se aplican las consideraciones generales sobre cualquier otro negocio digital, en particular la Ley Ecuatoriana de E-Commerce.

v. ¿Qué validez tienen los documentos digitales o electrónicos?

El artículo 2 de la Ley Ecuatoriana de E-Commerce prescribe la equivalencia entre los documentos electrónicos y los documentos físicos. En tal sentido, esta norma menciona lo siguiente:

> Los mensajes de datos tendrán igual valor jurídico que los documentos escritos. Su eficacia, valoración y efectos se someterá al cumplimiento de lo establecido en esta ley y su reglamento.

El artículo 3 de la citada norma agrega la validez de los documentos electrónicos adjuntados en forma de enlace o anexo a un documento electrónico, en la medida que las partes declaren de forma expresa conocer y aceptar el contenido de los documentos incorporados por remisión.

En línea con el artículo 2, el artículo 6 agrega que el documento electrónico será suficiente para tener por satisfecho el requisito de la forma escrita si puede ser consultado de forma posterior. Por otro lado, el artículo 7 indica el documento electrónico original será aquel que pueda demostrar su integridad.

Conforme el artículo 52 de la misma ley, la valoración de un documento electrónico será realizada a la luz de las reglas fijadas por el Código de Procedimiento Civil

vi. ¿Los datos relativos a la identidad deben almacenarse en el país o pueden ser transferidos al exterior?

La normativa reseñada en el caso de Ecuador es poco clara en relación a la transferencia internacional de datos. El único punto sobre el cual podríamos establecer una conclusión es que cuando se trate de datos sometidos a los alcances de la Ley Ecuatoriana de E-Commerce, las transferencias al exterior no serían posibles sin el consentimiento expreso del titular de los datos o cuando se esté tratando datos usando como base legal una de las excepciones previstas en la norma.

i. El Salvador

i. ¿Hay una definición legal de identidad?

El Salvador carece de un concepto jurídico que permita definir de forma comprensiva la noción de identidad de las personas. Sin perjuicio de ello, es posible construir un concepto de identidad a partir de ciertos artículos de la Constitución salvadoreña, en particular los artículos 2, 34 y 36, así como ciertos instrumentos de derechos fundamentales de los que El Salvador es parte, como la CDN, la DUDH, el Pacto de San José de Costa Rica o el PIDCP. En ese sentido, también son aplicables algunas disposiciones como el Decreto Nº 677 del 11 de octubre de 1993 (el "Código Salvadoreño de Familia") sobre la identidad de los menores, y la Ley Nº 552 del 21 de diciembre de 1995 (la "Ley Salvadoreña del Registro Nacional de las Personas Naturales").

ii. ¿Quién es el dueño de los datos según la normativa?

En atención a las prescripciones que se reseñaron en el punto anterior y los derechos reconocidos por la Ley Salvadoreña de Firma Electrónica, es posible concluir que el dueño de los datos es su titular.

iii. ¿Qué mecanismos son válidos para acreditar la identidad de una persona?

La Ley Nº 581 del 18 de octubre de 2001 (la "Ley Salvadoreña Reguladora de la Emisión del Documento Único de Identidad") regula el llamado documento único de identidad. Este documento estatal, según el artículo 3 de la Ley Salvadoreña Reguladora de la Emisión del Documento Único de Identidad, "es el documento oficial, suficiente y necesario para identificar fehacientemente a toda persona natural, salvadoreña, en todo acto público o privado, tanto dentro del país, como en el extranjero, cuando dichos actos surtan efectos en El Salvador". El rol de este instrumento no es menor porque según el Decreto Nº 34 del 23 de mayo de 2000 (el "Decreto Salvadoreño Reglamentario de la Ley Salvadoreña del Registro Nacional de las Personas Naturales") en su artículo 6 "el DUI será el único documento que identificará fehacientemente a las personas naturales en todo acto público o privado, tanto dentro del país, como en el extranjero cuando dichos actos surtan efectos en El Salvador". Lo interesante es el uso del término 'fehaciente', el cual lo único que imprime la norma sobre el documento estatal salvadoreño es una presunción sobre la identidad cuando se exhibe este, no prohibiendo el uso de medios alternativos para acreditar la identidad. Asimismo, también debe repararse en el hecho que el documento que tiene esos efectos legales el documento físico entregado por el Estado.

iv. ¿Existen entidades reguladas para brindar servicios de identificación de personas?

El único tipo de regulación que es posible encontrar en el marco jurídico salvadoreño referido a los servicios de identificación de personas está contenido en la Ley Salvadoreña de Firma Electrónica. Allí se establece que los proveedores de servicios de certificación tienen la obligación de solicitar identificación a sus usuarios para la entrega de los certificados digitales con los cuales pueden firmar. Al respecto, ello no obsta a la existencia de prestadores no licenciados que dan certificados digitales no oficiales, los cuales no tienen los beneficios legales de los certificados homologados por el régimen de la Ley Salvadoreña de Firma Electrónica, así como tampoco otras entidades que ofrecen servicios de identificación, los cuales tienen validez conforme su marco normativo.

v. ¿Qué validez tienen los documentos digitales o electrónicos?

Según el artículo 8, los documentos generados con medios electrónicos tienen validez legal en El Salvador en los siguientes términos: "Los documentos en soporte electrónico utilizando firma electrónica, tendrán el mismo valor que los consignados de manera tradicional. Quedan excluidas aquellas actuaciones que para su perfeccionamiento requieren formalidades y solemnidades especiales". A ello, hay que sumar el artículo 10 que prescribe que "cuando el documento privado fuera generado con firma electrónica certificada y se refiera a actos jurídicos que no se encuentren excluidos por la presente Ley, el valor será el mismo que el reconocido en manera tradicional".

vi. ¿Los datos relativos a la identidad deben almacenarse en el país o pueden ser transferidos al exterior?

Dado que no existen prescripciones al respecto, no hay limitaciones en cuanto al lugar donde los datos deben ser almacenados.

j. Guatemala

i. ¿Hay una definición legal de identidad?

No existe una definición legal sobre el concepto de identidad, ya sea digital o no. A ello debemos sumar la inexistencia de normativa sobre protección de datos personales. Sin perjuicio de ello, dado que Guatemala es parte de algunos de los instrumentos de derechos humanos mencionados anteriormente, es posible sostener que la identidad de las personas está conformada por los atributos que la identifican.

El único aspecto de la identidad de las personas que se encuentra regulado en la normativa guatemalteca es aquel vinculado a la relación Estado-ciudadano, instrumentada en el documento personal de identificación previsto por el Decreto 90/2005 (el "Ley Guatemalteca del Registro Nacional de las Personas").

ii. ¿Quién es el dueño de los datos según la normativa?

Siguiendo con la falta de normativa en Guatemala, tampoco es posible concluir de forma certera quién es el verdadero dueño de los datos. Sin perjuicio de ello, dado que Guatemala es parte de ciertos instrumentos de derechos humanos, la persona humana debería ser dueña de su identidad.

iii. ¿Qué mecanismos son válidos para acreditar la identidad de una persona?

Conforme el artículo 50 de la Ley Guatemalteca del Registro Nacional de las Personas, el documento personal de identificación es el único instrumento habilitado para acreditar la identidad, lo cual es prescripto de la siguiente manera:

> (…) Constituye el único Documento Personal de Identificación para todos los actos civiles, administrativos y legales, y en general para todos los casos en que por ley se requiera identificarse. Es también el documento que permite al ciudadano identificarse para ejercer el derecho de sufragio (…)

El artículo 52 de tal norma indica que su uso es obligatorio para todos los nacionales y extranjeros domiciliados en el país.

iv. ¿Existen entidades reguladas para brindar servicios de identificación de personas?

En virtud de la Ley Guatemalteca del Registro Nacional de las Personas, el Registro Nacional de las Personas es el único organismo habilitado para brindar estos servicios.

v. ¿Qué validez tienen los documentos digitales o electrónicos?

Conforme los artículos 7, 8, 9 y 33 del Decreto Nº 47/2008 (el "Decreto Guatemalteco de Firma Electrónica"), los documentos electrónicos tienen la misma validez que los documentos en soporte papel.

vi. ¿Los datos relativos a la identidad deben almacenarse en el país o pueden ser transferidos al exterior?

Al no existir una normativa que regule la materia, no hay limitación alguna sobre la ubicación de los datos.

k. Haití

i. ¿Hay una definición legal de identidad?

No existe una definición legal sobre el concepto de identidad. La situación de Haití en esta materia se ve dificultada aún más por la inexistencia de una normativa sobre protección de datos personales. A pesar de ello, Haití es parte de algunos de los instrumentos de derechos humanos mencionados anteriormente, con lo cual es posible sostener que la identidad de las personas está conformada por los atributos que la identifican.

ii. ¿Quién es el dueño de los datos según la normativa?

Siguiendo con la falta de normativa en Haití, tampoco es posible concluir de forma certera quién es el verdadero dueño de los datos. Sin perjuicio de ello, dado que Haití es parte de ciertos instrumentos de derechos humanos, la persona humana debería ser la dueña de su identidad.

iii. ¿Qué mecanismos son válidos para acreditar la identidad de una persona?

Sobre esta cuestión, atento a la falta de una regulación especial, es necesario hacer un análisis acto por acto de la vida jurídica de la persona para determinar cómo tiene que acreditar su identidad en cada caso.

iv. ¿Existen entidades reguladas para brindar servicios de identificación de personas?

No existen entidades reguladas, fuera del Estado, para brindar servicios de identificación de personas.

v. ¿Qué validez tienen los documentos digitales o electrónicos?

Conforme la ley sobre firmas electrónicas del 17 de marzo de 2017 (la "Ley Haitiana de Firma Electrónica"), las firmas electrónicas son equivalentes a las firmas manuscritas. En atención a ello, un documento firmado electrónicamente es equivalente a un documento en papel.

vi. ¿Los datos relativos a la identidad deben almacenarse en el país o pueden ser transferidos al exterior?

Al no existir una normativa que regule la materia, no hay limitación alguna sobre la ubicación de los datos.

1. Honduras

i. ¿Hay una definición legal de identidad?

No existe una definición legal de identidad en el marco normativo hondureño. Sin perjuicio de ello, es posible construir un concepto de identidad a partir de ciertos artículos de la Constitución Nacional de Honduras, así como ciertos instrumentos de derechos fundamentales de los que Honduras es parte, como la CDN, la DUDH, el Pacto de San José de Costa Rica o el PIDCP.

Por lo tanto, el punto de partida para el análisis de este concepto tiene que ser la Constitución de la República de Honduras. Al respecto de ello, el artículo 40 señala que es una obligación de todo ciudadano la obtención de una tarjeta de identidad para acreditar quién es; en el mismo texto legal, se establece que el Registro Nacional de las Personas es la entidad a cargo de colaborar con los ciudadanos para el cumplimiento de ese deber, según el artículo 55.

Las funciones del Registro Nacional de las Personas están regladas por el Decreto Nº 62/2004, junto con sus modificaciones del Decreto Nº 108/2007 y Nº 20/2009, (la "Ley Hondureña del Registro Nacional de las Personas"). Conforme esta ley, la identidad de las personas se integra por ciertos hechos de relevancia de la vida civil de las personas (nacimiento, matrimonio, elección del nombre, defunción, entre otros). Esa información queda plasmada en el llamado 'expediente de vida', según el artículo 43, que nutre de información a la Tarjeta de Identidad. Todas las personas tienen la obligación de gestionar esta tarjeta de forma directa o indirecta, según el caso, y las autoridades no pueden negar su entrega cuando corresponda según la norma citada.

ii. ¿Quién es el dueño de los datos según la normativa?

Si bien no existe una regulación especial en materia de protección de datos en Honduras, considerando la existencia del recurso de *habeas data* y las normas constitucionales e internacionales de derechos humanos vigentes en Honduras, es posible concluir que los datos le corresponden siempre a su titular.

iii. ¿Qué mecanismos son válidos para acreditar la identidad de una persona?

Conforme el artículo 88 de la Ley Hondureña del Registro Civil de las Personas, la tarjeta de identidad es el mecanismo por excelencia para acreditar quién es la persona; en concreto, el artículo 88 dice que es:

> (...) obligatorio para que el ciudadano pueda ejercitar todos los actos políticos, académicos, civiles, financieros, administrativos, judiciales, notariales, policiales y en general para todos aquellos casos en que por mandato legal deba ser presentada.

El giro final del artículo da pie a interpretar que, para los casos en los que la tarjeta de identidad no es obligatoria, la identidad puede ser acreditada por los medios que las partes de cierto acto jurídico dispongan de común acuerdo.

iv. ¿Existen entidades reguladas para brindar servicios de identificación de personas?

Al momento del presente informe no existen en Honduras entidades reguladas para brindar servicios de identificación de personas fuera del Registro Nacional de las Personas.

v. ¿Qué validez tienen los documentos digitales o electrónicos?

Conforme el artículo 6 del Decreto Nº 149-2013 (la "Ley Hondureña de Firma Electrónica"), los documentos electrónicos son equivalentes a los documentos físicos salvo en materia donde la ley exija expresamente la forma física o de familia.

vi. ¿Los datos relativos a la identidad deben almacenarse en el país o pueden ser transferidos al exterior?

Al no existir una normativa que regule la materia, no hay limitación alguna sobre la ubicación de los datos.

m. México

i. ¿Hay una definición legal de identidad?

El punto de partida para el análisis del concepto legal de identidad en el ordenamiento jurídico mexicano es su Constitución Política. En ese sentido, es posible traer a colación el artículo 4 párrafo 8 que dice lo siguiente:

> Toda persona tiene derecho a la identidad y a ser registrado de manera inmediata a su nacimiento. El Estado garantizará el cumplimiento de estos derechos. La autoridad competente expedirá gratuitamente la primera copia certificada del acta de registro de nacimiento.

Como normativa de segundo nivel, es posible mencionar la Ley publicada en el Diario Oficial de la Federación el 7 de enero de 1974 y su última reforma publicada en el Diario Oficial de la Federación el 12 de julio de 2018 (la "Ley Mexicana General de Población"). Esta norma le impone al Registro Nacional de Población, a cargo de la Secretaría de Gobernación, la tarea de registrar a todas las personas que forman parte de la población mexicana con datos que permitan certificar y acreditar la identidad de esta. En este sentido, el artículo 91 de la norma referenciada señala que:

> Al incorporar a una persona en el Registro Nacional de Población, se le asignará una clave que se denominará Clave Única de Registro de Población. Esta servirá para registrarla e identificarla en forma individual.

Junto con ello, el artículo 103 establece que las personas reciben una cédula de identidad al ser dados de alta en el Registro Nacional de Población, la cual contiene la siguiente información sobre la persona: apellido paterno, apellido materno, nombre, Clave Única de Registro de Población, fotografía, lugar de nacimiento, fecha de nacimiento, firma y huella dactilar. Sus implicancias legales serán analizadas más adelante.

ii. ¿Quién es el dueño de los datos según la normativa?

Si bien la Ley Mexicana de Protección de Datos Personales no lo menciona expresamente, una lectura sistemática de la norma nos lleva a concluir que, dadas las facultades reconocidas al titular de los datos, la persona física es la dueña de los mismos. Las entidades que los gestionan únicamente pueden hacerlo en respeto de esas facultades.

iii. ¿Qué mecanismos son válidos para acreditar la identidad de una persona?

Los artículos 104 y 105 de la Ley General de Población establecen lo siguiente:

> "La Cédula de Identidad Ciudadana es el documento oficial de identificación, que hace prueba plena sobre los datos de identidad que contiene en relación con su titular."

> "La Cédula de Identidad Ciudadana tendrá valor como medio de identificación personal ante todas las autoridades mexicanas ya sea en el país o en el extranjero, y las personas físicas y morales con domicilio en el país."

Atento a que los artículos mencionados no tienen una prohibición sobre el uso de otros instrumentos para acreditar la identidad, es posible que las partes elijan otros mecanismos para ello, siempre y cuando el acto jurídico en cuestión lo permita.

iv. ¿Existen entidades reguladas para brindar servicios de identificación de personas?

Al momento del presente informe no existen en México entidades reguladas para brindar servicios de identificación de personas fuera del Registro Nacional de Población.

v. ¿Qué validez tienen los documentos digitales o electrónicos?

La Ley publicada en el Diario Oficial de la Federación el 11 de enero de 2012 (la "Ley Mexicana de Firma Electrónica") debería ser la principal norma de referencia para analizar la validez de los documentos generados por medios informáticos. Sin embargo, no es posible encontrar un artículo donde se hable expresamente de la validez de estos documentos en forma general. Por lo tanto, es necesario recurrir a otras normas del sistema jurídico mexicano, a saber, el Código Federal de Procedimientos Civiles y el Código de Comercio.

En cuanto al Código Federal de Procedimientos Civiles, su artículo 210-A establece lo siguiente:

> (...) la información generada o comunicada que conste en medios electrónicos, ópticos o en cualquier otra tecnología.
>
> Para valorar la fuerza probatoria de la información a que se refiere este artículo, se estimará primordialmente la fiabilidad del método en que haya sido generada, comunicada, recibida o archivada y, en su caso, si es posible atribuir a las personas obligadas el contenido de la información relativa y ser accesible para su ulterior consulta.

Cuando la ley requiera que un documento sea conservado y presentado en su forma original, ese requisito quedará satisfecho si se acredita que la información generada, comunicada, recibida o archivada por medios electrónicos, ópticos o de cualquier otra tecnología, se ha mantenido íntegra e inalterada, a partir del momento en que se generó por primera vez en su forma definitiva y pueda ser accesible para su ulterior consulta.

Por su parte, el Código de Comercio fija en sus artículos 1205 y 1298-A la validez de los documentos electrónicos en estos términos:

> Son admisibles como medios de prueba todos aquellos elementos que puedan producir convicción en el ánimo del juzgador, acerca de los hechos controvertidos o dudosos y, en consecuencia, serán tomados como pruebas las declaraciones de las partes, terceros, peritos, documentos públicos o privados, inspección judicial, fotografías, facsímiles, cintas cinematográficas, de videos, de sonido, mensajes de datos, reconstrucciones de hechos y, en general, cualquier otra similar u objeto que sirva para averiguar la verdad.
>
> Se reconoce como prueba los mensajes de datos. Para valorar la fuerza probatoria de dichos mensajes, se estimará primordialmente la fiabilidad del método en que haya sido generada, archivada, comunicada o conservada.

vi. ¿Los datos relativos a la identidad deben almacenarse en el país o pueden ser transferidos al exterior?

Conforme la Ley Mexicana de Protección de Datos Personales, los datos pueden transferirse a otros países solo con el consentimiento del titular de los mismos, salvo disposición legal en contrario que autorice a hacerlo sin su consentimiento.

n. Nicaragua

i. ¿Hay una definición legal de identidad?

El punto de partida para el análisis legal del concepto de identidad en el marco normativo nicaragüense debe ser la Constitución Política de la República de Nicaragua. Si bien esta norma fundamental carece de una noción y protección general de la identidad, sí es posible construir ese concepto a partir de la protección de diferentes aspectos de la identidad, como puede ser la dignidad, la pertenencia a los pueblos originarios, entre otros. Además de ello, tenemos que tomar en cuenta los instrumentos internacionales de los cuales Nicaragua es parte y que contribuyen a enriquecer la noción de identidad que se encuentra legalmente protegida.

Al margen de las prescripciones constitucionales generales que rigen en Nicaragua, la Ley Nº 152 (la "Ley Nicaragüense de Identidad") regula la cédula de identidad ciudadana. Se trata del documento público que identifica a los ciudadanos de ese país y contiene, en su artículo 17, toda la información que el Estado registra para la expedición de ese documento. En base a esto, podemos concluir que el listado de información recabada por el Estado para el otorgamiento del documento prescribe todos los elementos que forman parte de la identidad de una persona. El Estado tiene la obligación de proporcionar este documento y no puede denegarlos.

ii. ¿Quién es el dueño de los datos según la normativa?

Si bien la Ley Nicaragüense de Protección de Datos Personales no lo menciona expresamente, una lectura sistemática de la norma nos lleva a concluir que, dada las facultades reconocidas al titular de los datos, la persona física es la dueña de los datos. Las entidades que los gestionan únicamente pueden hacerlo en respeto de esas facultades.

iii. ¿Qué mecanismos son válidos para acreditar la identidad de una persona?

Conforme la Ley Nicaragüense de Identidad, en su artículo 4, la cédula de identidad es necesaria para acreditar la identidad en los siguientes casos:

> a) Ejercer el voto de acuerdo con los procedimientos establecidos por la Ley Electoral;
> b) tomar posesión de cargos públicos;
> c) celebrar contratos de trabajo;
> ch) obtener o renovar pasaporte, licencia de conducir, carné del Seguro Social, Cédula del Registro Único del Contribuyente y cualquier otro documento de esta naturaleza;
> d) recibir pagos o giros del Estado, de los municipios o de instituciones autónomas;
> e) Realizar operaciones bancarias;
> f) Solicitar inscripciones en los registros del estado civil de las personas, registros públicos de la propiedad inmueble, registros mer-

cantiles y de la propiedad industrial y en cualquier otra Institución Pública;
g) Concurrir ante notario;
h) Contraer matrimonio civil, salvo el caso de que se realice en peligro de muerte;
i) Matricular a los hijos o pupilos en escuelas y/o colegios públicos o privados;
j) Matricularse en colegios, universidades y cualquier otro centro de enseñanza, cuando el solicitante sea mayor de dieciséis años;
k) Iniciar acción judicial y realizar cualquier otra gestión ante los tribunales de justicia y demás organismos estatales, regionales y municipales;
l) Cualquier otra diligencia u operación en las que se deba acreditar la identificación personal.

En lo que hace a los actos privados, el artículo 5 de la citada norma indica que es necesario consignar el número de la cédula de identidad de las partes en el instrumento en cuestión. Fuera de ese requisito, queda en manos de las partes o de las exigencias del negocio en concreto como acreditaran su identidad.

iv. ¿Existen entidades reguladas para brindar servicios de identificación de personas?

Al momento del presente informe no existen en Nicaragua entidades reguladas para brindar servicios de identificación de personas fuera del Registro Central del Estado Civil de las Personas.

v. ¿Qué validez tienen los documentos digitales o electrónicos?

La Ley Nº 729 (la "Ley Nicaragüense de Firma Electrónica") reconoce la existencia de los documentos electrónicos al definir el concepto, pero no contempla ni su normativa reglamentaria ni su validez legal. Con lo cual, es posible concluir que los documentos electrónicos pueden tener efectos legales pero su validez estará sujeta al tipo de firma que tengan insertadas.

vi. ¿Los datos relativos a la identidad deben almacenarse en el país o pueden ser transferidos al exterior?

Conforme la Ley Nicaragüense de Protección de Datos Personales, los datos pueden transferirse a otros países solo con el consentimiento del titular de los mismos, salvo disposición legal en contrario que autorice a hacerlo sin el consentimiento.

0. Panamá

i. ¿Hay una definición legal de identidad?

Aunque la Constitución Política de Panamá no tenga una definición del concepto de identidad, sí existen ciertas normas o artículos que tratan sobre este concepto. En primer lugar, se menciona que todos los panameños tienen derecho a obtener una cédula de identidad personal y que es obligación del Estado proporcionarla, quedando en manos del Tribunal Electoral esta tarea. En segundo lugar, es posible construir una noción de identidad a partir de la protección constitucional de ciertos elementos como la pertenencia a los pueblos originarios o la dignidad de la persona. Por último, Panamá también está sujeta a los instrumentos internacionales de derechos humanos de los cuales es parte y que influyen sobre lo que debe considerarse por identidad.

En línea con lo señalado en el párrafo anterior, la primera norma que interesa es la Ley Nº 31 de 2006 junto con su modificación por la Ley Nº 17 de 2007 (la "Ley Panameña del Registro Civil"), la cual regula el funcionamiento del Registro Civil de este país. Esta entidad tiene a su cargo llevar el registro de la existencia de las personas y de los hechos vitales que afectan a estas. Su artículo 25 prescribe que las actas del registro, sus certificaciones y los documentos que se expidan sobre ellas serán la prueba del estado civil de las personas.

Ahora, para realizar una nueva anotación en las actas del registro será necesario la presentación de la cédula de identidad, conforme el artículo 3 de la normativa reglamentaria de la Ley Panameña del Registro Civil, con excepción de los casos allí consignados. Esto nos lleva a analizar la Ley Nº 68 de 2015 (la "Ley Panameña del Documento de Identidad") donde se establece el funcionamiento de la Dirección Nacional de Cedulación, dependiente del Tribunal Electoral, y la expedición de los documentos de identidad nacional, cuya información básica esta prescripta en el artículo 10.

ii. ¿Quién es el dueño de los datos según la normativa?

Si bien la Ley Panameña de Protección de Datos Personales no lo menciona expresamente, una lectura sistemática de la norma nos lleva a concluir que, dada las facultades reconocidas al titular de los datos, la persona física es la dueña de los datos. Las entidades que los gestionan pueden hacerlo únicamente en respeto de esas facultades.

iii. ¿Qué mecanismos son válidos para acreditar la identidad de una persona?

El documento de identidad personal es el medio probatorio por excelencia para acreditar la identidad (ver punto i). Conforme el artículo 19, el documento de identidad es obligatorio para acreditar la identidad en los siguientes actos:

1. Identificarse ante las autoridades
2. Ejercer el sufragio.
3. Tomar posesión de cargos públicos.
4. Celebrar contratos de cualquier naturaleza.
5. Obtener o renovar pasaporte, licencia de conducir, Registro Único del Contribuyente y cualquier otro documento de naturaleza similar.
6. Recibir pagos o giros del Estado, de los municipios o de instituciones autónomas.
7. Realizar operaciones bancarias.
8. Solicitar inscripciones en los registros del estado civil de las personas, salvo las excepciones que establece la Ley del Registro Civil, para la inscripción de hechos vitales y reconocimiento de paternidad.
9. Concurrir ante notario público.
10. Contraer matrimonio civil, salvo el caso de que se realice en peligro de muerte.
11. Iniciar acción judicial y realizar cualquier otra gestión ante los tribunales de justicia y demás organismos estatales regionales y municipales.

12. Realizar cualquier otra diligencia u operación en la que se deba acreditar la identificación personal.

En el caso de los menores y los extranjeros, rigen disposiciones especiales muy similares a las prescripciones generales para el documento de identidad personal de los mayores de edad que sean ciudadanos panameños en los artículos 14 a 16 y 25 a 28, respectivamente.

iv. ¿Existen entidades reguladas para brindar servicios de identificación de personas?

Al respecto de este punto, la única entidad autorizada para brindar servicios de identificación, conforme el artículo 7 de la Ley Panameña del Documento de Identidad, es el Servicio de Verificación de Identidad del Tribunal Electoral.

v. ¿Qué validez tienen los documentos digitales o electrónicos?

La Ley Nº 51 de 2008 (la "Ley Panameña de Firma Electrónica") establece en su artículo 4 que:

> Cuando la ley requiera que la información conste un documento escrito, se le reconocerá validez, efectos jurídicos y fuerza obligatoria a los actos contratos que hayan sido o adoptados a través de medios electrónicos en documentos electrónicos de conformidad con esta Ley y sus reglamentos.
>
> Lo dispuesto en el presente artículo no será aplicable a los actos para los cuales la ley exige una solemnidad que no sea verificable mediante documento electrónico.

En este sentido, el artículo 7 amplía sobre la admisibilidad y fuerza probatoria de los mismos:

> Los documentos electrónicos serán admisibles como medios de prueba y tendrán la misma fuerza probatoria otorgada a los documentos en el Libro Segundo de Procedimiento Civil del Código Judicial.
>
> En todo caso, al valorar la fuerza probatoria de un documento electrónico se tendrá presente la confiabilidad de la forma en la que se haya generado, archivado o comunicado, y la confiabilidad de la forma en la que se haya conservado la integridad de la información.

vi. ¿Los datos relativos a la identidad deben almacenarse en el país o pueden ser transferidos al exterior?

Conforme la Ley Panameña de Protección de Datos Personales, los datos pueden transferirse a otros países solo con el consentimiento del titular de los mismos, salvo disposición legal en contrario que autorice a hacerlo sin su consentimiento.

p. Paraguay

i. ¿Hay una definición legal de identidad?

Aunque la Constitución Política de Paraguay no tenga una definición del concepto de identidad, existen ciertas normas o artículos que tratan sobre este concepto. En ese sentido, podemos traer a colación los artículos 22, 25, 28, 33 y 135 que tratan sobre diferentes aspectos de este derecho. Por otro lado, Paraguay, al ser parte de los instrumentos internacionales de derechos humanos reseñados en la introducción, debería garantizar el respeto por el derecho a la identidad.

Al margen de estas prescripciones normativas, Paraguay cuenta con un sistema estatal de registración de los ciudadanos bajo la Ley Nº 1.266 (la "Ley Paraguaya del Registro Civil") para llevar un registro con toda la información sobre los ciudadanos y sus hechos vitales de relevancia. Esa información es utilizada por la Policía Nacional de Paraguay para, en ejercicio de las facultades encomendadas por el artículo 6 inciso 11 de la Ley Nº 222 (la "Ley Paraguaya de la Policía", emitir las cédulas de identidad, que serán el instrumento para acreditar la identidad.

En materia de identidad digital, el gobierno paraguayo lanzó una iniciativa de identidad electrónica basada en la identidad proporcionada por el Estado bajo el marco del Decreto 8709/2018 para que los ciudadanos puedan usar en sus interacciones con la administración pública.

ii. ¿Quién es el dueño de los datos según la normativa?

Si bien la Ley Paraguaya de Protección de Datos Personales no lo menciona expresamente, una lectura sistemática de la norma nos lleva a concluir que, dada las facultades reconocidas al titular de los datos, la persona física es la dueña de los mismos. Las entidades que los gestionan únicamente pueden hacerlo en respeto de esas facultades.

iii. ¿Qué mecanismos son válidos para acreditar la identidad de una persona?

Sobre esta cuestión, atento a la falta de una regulación especial, es necesario hacer un análisis acto por acto de la vida jurídica de la persona para determinar cómo tiene que acre-

ditar su identidad en cada caso. Dada la existencia de un documento nacional de identidad otorgado por el Estado, ciertos actos realizados con entidades reguladas, como podría ser una entidad financiera o un sujeto obligado a cumplir con normas de prevención de lavado de activos, requieren presentar este documento para acreditar la identidad.

iv. ¿Existen entidades reguladas para brindar servicios de identificación de personas?

En Paraguay no hay regulación especial para que los privados puedan ofrecer servicios de identificación digital. El único habilitado a la fecha del presente informe es el Estado paraguayo conforme lo reseñado en el punto i.

v. ¿Qué validez tienen los documentos digitales o electrónicos?

La Ley Nº 4.017 así como su modificación por medio de la Ley Nº 4.610 (la "Ley Paraguaya de Firma Electrónica") establecen la validez de los documentos electrónicos y su equivalencia funcional. En tal sentido, el artículo 4 de la citada norma establece que:

> Se reconoce el valor jurídico de los mensajes de datos y no se negarán efectos jurídicos, validez o fuerza obligatoria a la información por la sola razón de que esté en forma de mensaje de datos.
>
> Tampoco se negarán efectos jurídicos, validez ni fuerza obligatoria a la información por la sola razón de que no esté contenida en el mensaje de datos que se supone ha de dar lugar a este efecto jurídico, sino que figure simplemente en el mensaje de datos en forma de remisión.

vi. ¿Los datos relativos a la identidad deben almacenarse en el país o pueden ser transferidos al exterior?

A pesar de la existencia de regulación sobre la identidad y la protección de los datos personales, no hay limitaciones sobre la ubicación geográfica de los datos o su transferencia internacional.

q. Perú

i. ¿Hay una definición legal de identidad?

En Perú fue dictado el Decreto Legislativo Nº 1412 de 13 de septiembre del 2018 (la "Ley Peruana de Identidad Digital") mediante el cual se estableció un concepto de identidad digital. Es importante señalar que este concepto de identidad digital está exclusivamente relacionado con los actos que una persona tenga que hacer con el Estado, no así con los particulares. En ese sentido, el artículo 10 define a esta como:

> 10.1 La identidad digital es aquel conjunto de atributos que individualiza y permite identificar a una persona en entornos digitales.
>
> 10.2 Los atributos de la identidad digital son otorgados por distintas entidades de la Administración Pública que, en su conjunto, caracterizan al individuo.

Esta identidad digital está concentrada en las credenciales, las cuales son usadas para la identificación digital de la persona y están autenticadas por la Administración Pública. La credencial por excelencia es el documento nacional de identidad electrónico.

Al margen de ello, la doctrina peruana[22] considera que la identidad digital de las personas en lo que hace a la actividad privada está dada, principalmente, por los certificados digitales expedidos para ser usados en la Infraestructura Oficial de Firma Electrónica.

ii. ¿Quién es el dueño de los datos según la normativa?

La Ley Peruana de Identidad Digital nada dice sobre la titularidad de los datos que hacen a la identidad digital de la persona. Con lo cual, es posible remitirse a la Ley Peruana de Protección de Datos Personales y, en atención al concepto de titular de los datos previsto en su artículo 2.14, considerar a la persona como el dueño de los mismos.

iii. ¿Qué mecanismos son válidos para acreditar la identidad de una persona?

Conforme la Ley Peruana de Identidad Digital, todas las interacciones de los ciudadanos con el Estado peruano y sus dependencias administrativas tienen que realizar de la forma que dichos organismos fijen al respecto y siempre dentro del Marco de Identidad Digital del Estado Peruano. Por excelencia, ello podrá

22 Cfr. NÚÑEZ PONCE, Julio, "La identidad digital y la identificación en el derecho informático empresarial y en el gobierno electrónico", Revista de Derecho de la Empresa, Nº 12, 2016, Universidad Popular Autónoma del Estado de Puebla, págs. 7 y siguientes.

hacerse mediante el uso del documento nacional de identidad electrónico.

Fuera de esos casos, debe realizarse un análisis caso por caso para determinar si el acto jurídico demanda la acreditación de la identidad de una forma específica.

iv. ¿Existen entidades reguladas para brindar servicios de identificación de personas?

Bajo el paraguas de la Ley Peruana de Identidad Digital, únicamente las administraciones públicas están autorizadas a ofrecer servicios de identificación de los particulares.

v. ¿Qué validez tienen los documentos digitales o electrónicos?

Tanto los documentos digitales como los electrónicos son válidos para instrumentar actos jurídicos, conforme el artículo 141 y 141-A del Código Civil Peruano.

Conforme la Ley Nº 27.269 (la "Ley Peruana de Firma Digital") y el Decreto Supremo Nº 052-2008-PCM (el "Decreto Reglamentario de la Ley Peruana de Firma Digital"), cuando un acto jurídico pida expresamente que sea firmado con una firma manuscrita, ese requisito solo puede satisfacerse con una firma digital.

vi. ¿Los datos relativos a la identidad deben almacenarse en el país o pueden ser transferidos al exterior?

Conforme el artículo 11 de la Ley Peruana de Protección de Datos Personales, los datos personales únicamente podrán salir del país cuando en la jurisdicción de destino se garantice un nivel suficiente de protección de datos, el cual debe ser, como mínimo, equiparable a la normativa peruana. Subsidiariamente, y en el caso de que la jurisdicción de destino no ofrezca ese nivel equiparable de protección de datos, podría suplantar ello mediante el consentimiento del titular de los datos o mediante un instrumento jurídico, como un contrato, entre importador y exportador de datos. En caso de duda, puede requerirse la opinión de la autoridad de aplicación para verificar estas circunstancias, no siendo ello obligatorio.

r. República Dominicana

i. ¿Hay una definición legal de identidad?

La Constitución de la República Dominicana carece de una definición de la noción de identidad, pero el concepto aparece en diferentes apartados con relación a algunas de las aristas que tiene el concepto, a saber: datos de filiación (art. 55 inciso 7), tenencia de documentos públicos que den fe de su estado civil (art. 55 inciso 8), la cultura individual y colectiva a la que se quiere o a la que se pertenece (art. 64 inciso 3), entre otros. En particular, el artículo 212, párrafo II indica que depende de la Junta Central Electoral la emisión de la cédula de identidad, documento que acredita la identidad de los dominicanos y los extranjeros que pueden obtener este documento. Al margen de estas prescripciones, la República Dominicana suscribe a los instrumentos internacionales de derechos humanos reseñados en la introducción por lo que debería garantizar el respeto por el derecho a la identidad en atención a estas normas.

A su vez, la República Dominicana cuenta con la Ley Nº 659 del 17 de julio de 1994 (la "Ley Dominicana del Registro Civil") que crea a los Oficiales del Estado Civil y les encomienda la registración de todos los eventos vitales de los residentes dominicanos. Por su parte, es necesario agregar también a este análisis la Ley Nº 8 del 13 de abril de 1992 y su modificación por la Ley Nº 26 del 1 de febrero de 2001 (la "Ley Dominicana de la Cédula de Identidad"), que dispone la consolidación de todos los documentos de identificación expedidos por el gobierno dominicano en torno a la cédula de identidad, que es el único documento habilitado para el sufragio.

Fuera de estos casos, el gobierno de República Dominicana está trabajando activamente en la digitalización de su administración pública bajo el programa "República Digital", que cuenta con un proyecto de identidad digital a nivel municipal para facilitar los trámites de los usuarios.

ii. ¿Quién es el dueño de los datos según la normativa?

Si bien la Ley Dominicana de Protección de Datos Personales no lo menciona expresamente, una lectura sistemática de la norma nos lleva a concluir que, dada las facultades reconocidas al titular de los datos, la persona física es la dueña de los mismos. Las entidades que los gestionan únicamente pueden hacerlo en respeto de esas facultades.

iii. ¿Qué mecanismos son válidos para acreditar la identidad de una persona?

A diferencia de lo que ocurre en otros ordenamientos, no existe una obligación de acreditar la identidad usando cierto documento en particular, salvo en materia de sufragio por las

consideraciones de la Ley Dominicana de la Cédula de Identidad. Por lo tanto, y ante el silencio normativo, lo prudente es considerar que las partes del acto jurídico tienen plena libertad para acreditar su identidad como estas lo estimen adecuado, salvo que el acto jurídico en cuestión exija que se presente cierto documento o se realicen ciertos actos en concreto.

iv. ¿Existen entidades reguladas para brindar servicios de identificación de personas?

No existen regulaciones que indiquen cómo debería ser prestado un servicio de identificación digital de personas en República Dominicana.

v. ¿Qué validez tienen los documentos digitales o electrónicos?

La Ley Nº 126 del 19 de marzo de 2002 (la "Ley Dominicana de Firma Electrónica") establece en su artículo 4 que no se puede negar efectos jurídicos a la información que esté contenida en un documento digital o mensaje de datos por el mero hecho de estar en ese soporte. Este principio está reforzado por el artículo 5, el cual prescribe que:

> Cuando cualquier norma requiera que la información conste por escrito, dicho requisito quedará satisfecho con un documento digital o mensaje de datos, si la información que este contiene es accesible para su posterior consulta y si el documento digital o mensaje de datos cumple con los requisitos de validez establecidos en la presente ley.

Esta prescripción es completada por el artículo 9 que señala que los documentos digitales y los mensajes de datos tendrán la misma fuerza probatoria que los documentos en papel con firma privada. El artículo 10 por su parte nos da los criterios que deberán ser considerados a la hora de analizar la validez de estos, a saber: la confiabilidad del soporte usado para su generación, así como para su archivo o comunicación, según corresponda; la confiabilidad de los recursos empleados para garantizar su integridad; la confiabilidad del método empleado para identificar al firmante; y cualquier otro criterio de relevancia.

vi. ¿Los datos relativos a la identidad deben almacenarse en el país o pueden ser transferidos al exterior?

Conforme la Ley Dominicana de Protección de Datos Personales, los datos pueden transferirse a otros países solo con el consentimiento del titular de los datos, salvo disposición legal en contrario que autorice a hacerlo sin el consentimiento.

S. Uruguay

i. ¿Hay una definición legal de identidad?

Aunque la Constitución de Uruguay no tenga una definición del concepto de identidad, existen normas y artículos que tratan este concepto. En ese sentido, podemos traer a colación los artículos 7, 29, 39, entre otros que tratan sobre diferentes aspectos de este derecho. Por otro lado, Uruguay, al ser parte de los instrumentos internacionales de derechos humanos reseñados en la introducción, debería garantizar el respeto por el derecho a la identidad.

Los hechos de relevancia del estado civil de las personas deben anotarse en los Registros del Estado Civil, conforme lo señalado por la Ley Nº 1.430 y sus modificatorias (la "Ley Uruguay del Registro Civil"). Actualmente, Uruguay está impulsando un proyecto para la digitalización de los registros civiles de ese país como un objetivo prioritario del plan "Gobierno Digital Uruguay 2020".

Fuera de ello, la Ley Nº 14762 (la "Ley Uruguay de Identificación Civil") establece cómo se realizará la identificación de las personas físicas, así como también de las jurídicas y los empresarios. En lo que hace a las personas físicas, el artículo 2 establece que su identificación se realizará en base a un número conforme se regula en la norma citada; este número se conformará con un conjunto secuencial de cifras y una adicional para un dígito verificador. Con ese número asignado se dispone también la expedición de la cédula de identidad para toda persona nacional o extranjera con residencia permanente en el país. Estas cédulas, según el artículo 9, tienen la siguiente información sobre la identidad de la persona:

> a) Número de identificación;
> b) Apellido paterno, apellido materno, primer nombre y segundo nombre.
> Si se trata de mujer casada se incluirá el apellido del cónyuge, salvo que no lo use habitualmente;
> c) Lugar y fecha de nacimiento, entendiéndose por lugar el político geográfico independiente de los cambios de soberanía que se hubieren operado con ulterioridad;
> d) Firma habitual del interesado;
> e) Impresión dígito pulgar derecha o la que en su lugar se indique;
> (...)
> g) Fotografía del titular; (...)

Esta tarea de entregar las cédulas de identidad es responsabilidad de la Dirección Nacional de Identificación Civil, la cual podrá requerir a otras dependencias información relevante para la confección de estas. Por otro lado, conforme la Resolución Nº 5/2019 de la Unidad de Certificación Electrónica, la cédula de identidad electrónica sirve para acreditar la identidad de la persona con el mismo valor probatorio que su exhibición presencial.

ii. ¿Quién es el dueño de los datos según la normativa?

Si bien la Ley Uruguay de Protección de Datos Personales no lo menciona expresamente, una lectura sistemática de la norma nos lleva a concluir que, dada las facultades reconocidas al titular de los datos, la persona física es la dueña de los mismos. Las entidades que los gestionan únicamente pueden hacerlo en respeto de esas facultades.

iii. ¿Qué mecanismos son válidos para acreditar la identidad de una persona?

Conforme el artículo 16 de la Ley Uruguaya de Identificación Civil, es necesario exhibir la cédula de identidad cuando ello sea requerido por una autoridad. Por otro lado, el artículo 20 señala que:

> Las oficinas públicas, entes paraestatales, bancos oficiales y privados, no darán curso a ninguna petición o gestión de particulares obligados a obtener la cédula de identidad, ni pagarán sueldos, salarios, jornales, jubilaciones, pensiones, retiros, beneficios sociales u operaciones de crédito de cualquier naturaleza, cuando no se tenga constancia del citado documento.

Fuera de estas situaciones, entendemos que queda a criterio de las partes intervinientes, así como también de las regulaciones específicas de cada caso, qué documentos serán necesarios para tener por acreditada la identidad de las partes.

iv. ¿Existen entidades reguladas para brindar servicios de identificación de personas?

Conforme lo prescripto por la Ley Nº 18.600 (la "Ley Uruguaya de Firma Electrónica") y su Decreto Nº 70/18 (el "Decreto Uruguayo de Servicios de Confianza"), en Uruguay existen los terceros de confianza que pueden brindar servicios de identificación de personas. En la Ley Uruguaya de Firma Electrónica, estos servicios están regulados en los artículos 31 y 33. Por su parte, el Decreto Uruguayo de Servicios de Confianza delega en la Unidad de Certificación Electrónica el establecimiento y reglamentación de los niveles de seguridad en la provisión de servicios de identificación digital. Dicha unidad técnica mediante el dictado de la Resolución Nº 5/2018 estableció 4 niveles, del 0 a 3, de estos servicios en la Política de Identificación Digital.

v. ¿Qué validez tienen los documentos digitales o electrónicos?

Conforme el artículo 4 de la Ley Uruguaya de Firma Electrónica, "los documentos electrónicos satisfacen el requerimiento de escritura y tendrán el mismo valor y efectos jurídicos que los documentos escritos, salvo las excepciones legalmente consagradas."

vi. ¿Los datos relativos a la identidad deben almacenarse en el país o pueden ser transferidos al exterior?

Conforme la Ley Uruguay de Protección de Datos Personales, en principio están prohibidas las transferencias de datos personales a una jurisdicción que no sea considerada como adecuada. Si bien existen varios supuestos en el artículo 23 de dicha norma que actúan como excepciones, en caso de que no se caiga en ninguna de ellas, es posible requerir una autorización especial a la Unidad Reguladora y de Control de Protección de Datos Personales, conocida con el nombre de declaración de conformidad, para que se permita la transferencia internacional de datos.

t. Venezuela

i. ¿Hay una definición legal de identidad?

El derecho a la identidad no está atendido de forma directa por la Constitución de la República Bolivariana de Venezuela, pero muchas de sus aristas están contempladas. En ese sentido, es posible destacar los artículos 56, 60, 80, 121, entre otros. Por otro lado, Venezuela, al ser parte de los instrumentos internacionales de derechos humanos reseñados en la introducción, debería garantizar el respeto por el derecho a la identidad.

Al margen de ello, tenemos que considerar también las regulaciones de la Ley publicada en Gaceta Oficial Número 39.264 del 15 de septiembre de 2009 (la "Ley Venezolana del Registro Civil"). Esta norma regula el funcionamiento del Registro Civil, donde se deben inscribir ciertos hechos de relevancia para la vida de las personas que configuran su identidad. Dentro del Registro Civil existe la Oficina Nacional de Supervisión del Registro Civil e Identificación que tiene a su cargo la tarea de identificar a las personas. En este marco, los hechos vitales son registrados en los expedientes civiles únicos; estos están asociados a un número único de identidad, el cual deberá indicarse en todos los documentos de identidad expedidos por el gobierno venezolano.

También es necesario tener en cuenta las consideraciones de la Ley publicada en Gaceta Oficial Nº 38.458 del 14 de junio de 2006 junto con el Decreto N° 1.412 del 13 de noviembre de 2014, con rango, valor y fuerza de Ley de Reforma de la Ley Orgánica de Identificación, publicado en la Gaceta Oficial de la República Bolivariana de Venezuela Nº 6.155 Extraordinario de fecha 19 de noviembre de 2014 (la "Ley Venezolana de Identificación"), la cual define en su artículo 2 a la identificación como "(...) el conjunto de datos básicos que individualizan y diferencian a una persona con respecto a otros individuos y que sirve de fuente de información para su reconocimiento."

Respecto de esos datos básicos, el artículo 4 indica que son los siguientes: "(...) sus nombres, apellidos, sexo, fecha de nacimiento, lugar de nacimiento, los dibujos de sus cestas dactilares y cualquier otro medio de identificación."

La Ley Venezolana de Identificación también regula la llamada cédula de identidad, la cual constituye el documento público por excelencia para acreditar la identidad de las personas. Conforme el artículo 14, toda persona tendrá un único número de cédula en línea con el expediente referido en el punto anterior que la identificará para toda su vida. Sus efectos jurídicos serán analizados en el punto iii. Su contenido, en lo que resulta relevante al concepto de identidad, es el siguiente, conforme el artículo 16:

> 1. Apellidos y nombres.
> 2. Fecha de nacimiento.
> 3. Número Único de Identidad.
> 4. Estado Civil.
> 5. Fotografía a color.
> 6. Firma e impresión dactilar del pulgar derecho de su titular y, en su defecto, del pulgar izquierdo.
> (...)
> 8. Número que se le asigne.
> 9. Nacionalidad y término de permanencia autorizada a su titular en el país, cuando se trate de extranjero o extranjera.
> 10. En el caso de los ciudadanos indígenas, se señalará el pueblo o comunidad a la cual pertenecen. (...)

ii. ¿Quién es el dueño de los datos según la normativa?

Si bien no existe una previsión expresa sobre la titularidad de los datos personales, es posible considerar que la persona física es la titular de los datos ya que el ordenamiento jurídico le reconoce el derecho al titular de los datos de reclamar su protección vía el *habeas data*.

iii. ¿Qué mecanismos son válidos para acreditar la identidad de una persona?

Conforme el artículo 13 de la Ley Venezolana de Identificación:

> "La cédula de identidad constituye el documento principal de identificación, para los actos civiles, mercantiles, administrativos, judiciales y para todos aquellos casos en los cuales su presentación sea exigida por la ley."

Por lo tanto, en atención a la falta de una regulación general sobre la materia, el análisis debería ser caso a caso para determinar qué exigencias tiene el acto en cuestión. Como bien señala el artículo 13, existen casos en los que no será obligatoria la presentación de la cédula de identidad y la identidad podrá acreditarse haciendo uso de los instrumentos que las partes, de común acuerdo, decidan utilizar.

iv. ¿Existen entidades reguladas para brindar servicios de identificación de personas?

A la fecha del presente informe no existen regulaciones sobre servicios de identificación de personas en ámbitos digitales.

v. ¿Qué validez tienen los documentos digitales o electrónicos?

El Decreto N° 1.204 del 10 de febrero de 2001, con Fuerza de Ley de Mensaje de Datos y Firmas Electrónicas, publicada en la Gaceta Oficial de la República Bolivariana de Venezuela Nº 37.148 del 28 de febrero de 2001 (la "Ley Venezolana de Firma Electrónica") regula, en su artículo 4, la validez de los mensajes de datos electrónicos, equivalente del documento electrónico, en los siguientes términos:

> Los Mensajes de Datos tendrán la misma eficacia probatoria que la ley otorga a los documentos escritos, sin perjuicio de lo establecido en la primera parte del artículo 6 de este Decreto-Ley. Su promoción, control, contradicción y evacuación como medio de prueba, se realizará conforme a lo previsto para las pruebas libres en el Código de Procedimiento Civil.
>
> La información contenida en un Mensaje de Datos, reproducida en formato impreso, tendrá la misma eficacia probatoria atribuida en la ley a las copias o reproducciones fotostáticas.

A ello debemos agregar las prescripciones del artículo 8:

> Cuando la ley requiera que la información conste por escrito, ese requisito quedará satisfecho con relación a un Mensaje de Datos, si la información que éste contiene es accesible para su ulterior consulta.

vi. ¿Los datos relativos a la identidad deben almacenarse en el país o pueden ser transferidos al exterior?

A pesar de la existencia de regulación, no hay limitaciones sobre la la ubicación geográfica de los datos.

u. Otros casos con reglamentación especial en materia de identidad digital

Existen varios ejemplos de regulaciones internacionales vigentes que tienen un impacto sobre la construcción de la identidad digital. Aunque existen numerosos proyectos desarrollando soluciones sobre identidad digital, así como también grupos de trabajo abocados a esta problemática, los ejemplos y referencias mencionados a continuación son europeos. Los motivos de ello son dos. En primer lugar, las regulaciones latinoamericanas están alineadas conceptualmente con las normas europeas en materia de identidad y protección de datos personales al reconocer el resguardo de estos conceptos mediante derechos humanos o fundamentales y no permitir la comercialización de los atributos de la personalidad. En segundo lugar, y en línea con esta similitud jurídica, ciertas jurisdicciones latinoamericanas han sido reconocidas por la Comisión Europea como jurisdicciones que brindan una adecuada protección a los datos personales, quedando demostrada así la afinidad entre espíritus y prácticas regulatorias.

En ese sentido, se destaca la normativa de la Unión Europea, principalmente el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, del 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, de aquí en más "RGPD"); y el Reglamento (UE) 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 (el "Reglamento eIDAS").

Al respecto de estos dos instrumentos normativos, el grupo de trabajo de la Unión Europea dedicado a trabajar sobre *blockchain*, el Observatorio y Foro de la Unión Europea sobre Blockchain, ha publicado un informe repasando la aplicación de ambas normas a las soluciones de identidad auto soberanas dado que ambas regulaciones son de aplicación directa en todo el territorio de la Unión Europea[23]. Asimismo, y de forma específica a lo que nos ocupa en este informe, dicho grupo de trabajo ha trabajado un artículo analizando este fenómeno de las identidades digitales descentralizadas en el marco de la normativa europea[24].

En cuanto al RGPD, el informe en cuestión señala que el marco legal europeo, en sí misma, no prohíbe el despliegue de estos sistemas de identidad. También señala que es necesario realizar un fuerte trabajo a nivel técnico para asegurar el cumplimiento de los requisitos de seguridad y ubicación de los datos y así permitir a las autoridades europeas ejercer sus poderes sancionatorios contra aquellas entidades que hagan un uso indebido de los datos. Al mismo tiempo, el informe señala que estas soluciones están alineadas con los principios del RGPD y los derechos que los titulares de los datos tienen sobre estos.

23 Cfr. EU BLOCKCHAIN OBSERVATORY AND FORUM, "Blockchain and the GDPR", 16 de octubre de 2018

24 Cfr. EU BLOCKCHAIN OBSERVATORY AND FORUM, "Blockchain and Digital Identity", 2 de mayo de 2019.

Por otro lado, el Reglamento eIDAS, al ser tecnológicamente neutro, admite el uso de la tecnología *blockchain* dentro del territorio de la Unión Europea. Dado el carácter distribuido de una *blockchain*, será imposible que estas puedan adquirir el carácter de cualificadas para prestar servicios de confianza; en todo caso, los operadores que hagan uso de esta tecnología deberán ser quienes solicitan la autorización a los diferentes estados para prestar servicios de confianza de forma cualificada usando tecnología *blockchain*. Una cuestión no menor es que los documentos de identidad electrónicos expedidos por los estados podrán tener plena validez en el territorio de otros países cuando se realice el procedimiento previsto en el Reglamento eIDAS. Esta cuestión no es menor porque, como hemos visto, existen muchos actos de la vida de las personas donde resulta obligatorio la exhibición de documentos de identidad estatales para acreditar la identidad. Sin embargo, algunas jurisdicciones, como puede ser Estonia, admiten el uso de cualquier tipo de documento en la medida que estos reúnan ciertos requisitos.

La virtud que tienen las normas europeas reseñadas es que tratan sobre los elementos fundamentales de la identidad a efectos legales: por un lado, el RGPD se enfoca sobre el tratamiento de datos personales, mientras que el Reglamento eIDAS enmarca la prestación de servicios de identificación. La creación de un sistema de identidad que cumpla con ambas normas ya garantiza que pueda ser desplegado dentro del continente europeo con éxito. Asimismo, la Unión Europea cumple el rol de permitir los flujos de datos personales hacia jurisdicciones que sean adecuadas y someterlos al cumplimiento de requisitos para aquellas que no lo sean. En cierta medida, Europa ha fijado el piso mínimo para que un tratamiento de datos sea considerado respetuoso con los derechos fundamentales. Es por ello que todas las jurisdicciones están adecuando sus marcos normativos en materia de protección de datos al RGPD. En América Latina, el primero en lograrlo ha sido Brasil, y hay otros países que cuentan con borradores de normativa en sus órganos legislativos.

La mayoría de los estudios que analizan experiencias de soluciones de identidad digital señalan que, para su implementación, es inevitable tener que mirar a cada legislación en particular para determinar si es posible el reemplazo total de la identidad estatal por una identidad auto soberana. Es decir, si basta con acreditar la identidad por medios privados o, en cambio, si se necesita de la identidad que proporciona el Estado. Otras normas internacionales recientes, como la regulación del sistema indio Aadhaar, siguen el mismo esquema de creación de identidades estatales de forma totalmente independiente a los esquemas de prestación de servicios de identificación bajo normas que imitan al Reglamento eIDAS, como es el caso de Argentina y Uruguay. Por lo tanto, hasta el momento no hay una norma que brinda un esquema superador.

Marco normativo aplicable a *blockchain* en América Latina

Además de considerar la definición de identidad en cada jurisdicción, evaluar la posibilidad de implementar una solución de identidad digital auto soberana exige analizar la normativa aplicable a la tecnología *blockchain* en cada país de América Latina. Para facilitar la consulta de este informe, la Tabla 3 resume las características del marco normativo de cada país.

ivo aplicable a
América Lati
ivo aplicable a

Tabla 3

Marco normativo aplicable a blockchain en países de América Latina

País	¿Hay regulación sobre blockchain?	¿Es válido un acto en formato digital?	¿Hay legislación sobre firma digital?	¿Hay regulación sobre contratos inteligentes?	¿Un contrato inteligente es un contrato?*
Argentina	Sí*	Sí	Sí	Sí*	Sí
Bolivia	Sí*	Sí	Sí	No	Sí
Brasil	No*	Sí	Sí	No	Sí
Chile	No	Sí	Sí	No	Sí
Colombia	No	Sí	Sí	No	Sí
Costa Rica	No	Sí	Sí	No	Sí
Cuba	No	Sí *	Sí*	No	Sí
Ecuador	No	Sí	Sí	No	Sí
El Salvador	No	Sí	Sí	No	Sí
Guatemala	No	Sí	Sí	No	Sí
Haití	No	Sí	Sí	No	Sí
Honduras	No	Sí	Sí	No	Sí
México	No	Sí	Sí	No	Sí
Nicaragua	No	Sí	Sí	No	Sí
Panamá	No	Sí	Sí	No	Sí
Paraguay	No	Sí	Sí	No	Sí
Perú	No	Sí	Sí	No	Sí
República Dominicana	No	Sí	Sí	No	Sí
Uruguay	No	Sí	Sí	No	Sí
Venezuela	Sí *	Sí	Sí	No	Sí

* La respuesta proporcionada en este punto no es absoluta y es necesario revisar el análisis realizado del punto para tener un conocimiento pleno de la situación.

a. Argentina

i. ¿Hay regulación en materia de *blockchain*?

Actualmente, no existe una regulación omnicomprensiva sobre la tecnología *blockchain*. La única regulación existente sobre la tecnología está dada por el Decreto 182/2019. Esta norma incluye a los terceros que brinden el servicio de "operación de cadenas de bloques para la conservación de documentos electrónicos, gestión de contratos inteligentes y otros servicios digitales" dentro de la categoría de "prestadores de servicios de confianza", contemplada en el artículo 36 del Anexo. Al respecto, la norma no brinda mayores precisiones y se encuentra pendiente la reglamentación de este apartado.

ii. ¿Son válidos los actos celebrados en forma electrónica?

Sí, en Argentina es posible la instrumentación de actos jurídicos mediante soportes informáticos, tal como mencionamos brevemente en el apartado 3.a.iv.

iii. ¿Qué validez tienen las firmas digitales?

En Argentina se encuentran reguladas las llamadas firmas digitales y las firmas electrónicas conforme la Ley Argentina de Firma Digital, tal como mencionamos brevemente en el apartado 3.a.v. La diferencia entre ambos tipos de firmas es de índole legal y consiste en que las primeras hacen uso de un certificado de firma digital otorgado por un certificador licenciado en Argentina o reconocido por la autoridad de aplicación de la Ley Argentina de Firma Digital. Es decir, firma electrónica es todo aquello que no es firma digital desde el punto de vista jurídico, aun cuando desde la perspectiva técnica sea una firma digital.

La diferencia entre ambos tipos de firmas tiene consecuencias sobre los efectos que tienen en el acto en el cual están involucradas. Por un lado, las firmas digitales, por la redacción del artículo 288 del CCyCN, son las únicas aptas para suplir a las firmas ológrafas, cuando se exigen estas como una formalidad ad solemnitatem, y gozan de las presunciones de autoría e integridad del documento donde son insertadas. Por otro lado, las firmas electrónicas carecen de estas presunciones y solo son aptas para firmar aquellos documentos sin requisitos formales en lo que hacen a la firma.

iv. ¿Hay regulación sobre contratos inteligentes?

El Decreto 182/2019 incluye dentro de los trabajos que pueden realizar los prestadores de servicios de confianza a los servicios de gestión de contratos inteligentes, pero este punto aún carece de normativa reglamentaria para comprender sus alcances. Fuera de esta norma, y en la medida en que los contratos inteligentes pueden ser legales, son de aplicación las previsiones del CCyCN sobre contratos.

v. ¿Son los contratos inteligentes contratos legales?

La doctrina señala que los contratos inteligentes pueden llegar a configurar contratos en el sentido legal en la medida que reúnan los requisitos establecidos para estos. En particular, compete a la forma debido a que los contratos inteligentes hacen uso de firmas electrónicas y no digitales para el sistema jurídico argentino. En el caso de que el contrato inteligente no pueda ser considerado como un contrato, hay tres posibilidades: (i) considerarlo como una promesa de otorgar el contrato legal, conforme lo establecido en el artículo 1018 CCyCN; (ii) considerarlo como una herramienta utilizada por las partes para instrumentar y automatizar ciertos aspectos de la relación jurídica subyacente; o (iii) tomar este contrato inteligente como un principio de prueba instrumental por revestir el mismo carácter, en este caso, de instrumento privado no firmado o firmado, en consonancia con lo prescripto por el artículo 1020 del CCyCN.

b. Bolivia

i. ¿Hay regulación en materia de *blockchain*?

Bolivia cuenta con regulación en materia de *blockchain* al haber prohibido en el año 2014 su principal aplicación: las criptomonedas. Por medio de la Resolución de Directorio Nº 044/2014 del Banco Central Boliviano, las criptomonedas, salvo que sean autorizadas expresamente por dicha entidad, se encuentran prohibidas.

Fuera de esta situación, el resto de los casos de uso de la tecnología están permitidos, aunque no existe una regulación que los contemple expresamente.

ii. ¿Son válidos los actos celebrados en forma electrónica?

En Bolivia son válidos los actos celebrados de forma electrónica. Al respecto, sugerimos revisar los requisitos de validez enumerados en el punto 3.b.v.

iii. ¿Qué validez tienen las firmas digitales?

La firma electrónica no tiene los mismos efectos que la firma digital y, por lo tanto, no es apta para sustituirla (recomendamos revisar el punto 3.b.v. de este informe).

iv. ¿Hay regulación sobre contratos inteligentes?

No existe regulación sobre contratos inteligentes en Bolivia. Por lo tanto, es de aplicación la normativa de fondo, principalmente la Ley Boliviana de TIC y el Código Civil, así como también el Código de Comercio.

v. ¿Son los contratos inteligentes contratos legales?

Sobre este punto aplica el principio de libertad de formas. Esto significa que, si el contrato puede ser celebrado por medios electrónicos, si cumple con los requisitos fijados para que la firma en ese soporte sea válida y también con los requisitos de los contratos, es posible que un contrato inteligente sea válido.

c. Brasil

i. ¿Hay regulación en materia de *blockchain*?

A la fecha del presente informe no hay regulación sobre la tecnología *blockchain* en Brasil.

ii. ¿Son válidos los actos celebrados en forma electrónica?

Los soportes informáticos son aptos para plasmar actos y hechos jurídicos, tal como adelantamos en el punto 3.c.v.

iii. ¿Qué validez tienen las firmas digitales?

El sistema jurídico brasilero reconoce únicamente a las firmas digitales emitidas dentro del sistema de llave pública de Brasil como firmas con pleno alcance legal equivalente a las firmas manuscritas, conforme lo reseñado previamente sobre el artículo 10 del Marco Normativo Brasileño de Firma Digital.

Sin perjuicio de ello, y tal como fuera analizado, las partes pueden optar por usar firmas digitales con certificados no emitidos por entidades dentro del sistema de llave pública de Brasil. Al respecto de ello, es necesario que se pongan de acuerdo con carácter previo sobre la validez de los certificados. Por otra parte, los terceros que no fueron parte de ese acuerdo pueden desconocer la validez de las firmas en cuestión.

iv. ¿Hay regulación sobre contratos inteligentes?

A la fecha del presente informe no hay regulación sobre contratos inteligentes en Brasil.

v. ¿Son los contratos inteligentes contratos legales?

Sobre este punto, aplica el principio de libertad de formas. Con lo cual, si el contrato puede ser celebrado por medios electrónicos, cumple con los requisitos fijados para que la firma en ese soporte sea válida y también con los requisitos de los contratos, es posible que un contrato inteligente sea válido.

d. Chile

i. ¿Hay regulación en materia de *blockchain*?

No existe a la fecha del presente informe regulación especial sobre esta tecnología.

ii. ¿Son válidos los actos celebrados en forma electrónica?

Los actos celebrados en forma electrónica son válidos, en cumplimiento de las prescripciones de la Ley Chilena de Firma Digital (ver punto 3.d.v.).

iii. ¿Qué validez tienen las firmas digitales?

La Ley Chilena de Firma Digital no habla de firmas digitales sino de firmas electrónicas simples y avanzadas. El concepto de firma digital podría asociarse al de firma electrónica avanzada. En tal sentido, ésta goza de una presunción de autoría e integridad frente a la firma electrónica simple.

iv. ¿Hay regulación sobre contratos inteligentes?

No existe regulación especial sobre contratos inteligentes a la fecha del presente informe. Sin perjuicio de ello, aplican las prescripciones de la Ley Chilena de Firma Digital y también los lineamientos del Código Civil y del Código de Comercio de Chile en materia de contratación.

v. ¿Son los contratos inteligentes contratos legales?

En la medida que el contrato inteligente reúna los requisitos fijados para la existencia de un contrato válido y cumpla con las prescripciones de la Ley Chilena de Firma Digital, y ante la ausencia de una norma que prohíba este tipo de contratos, un contrato inteligente debería ser aceptado como legal y válido.

e. Colombia

i. ¿Hay regulación en materia de *blockchain*?

No hay normativa vigente sobre esta materia a la fecha del presente informe.

ii. ¿Son válidos los actos celebrados en forma electrónica?

En Colombia es posible la instrumentación de actos jurídicos usando medios electrónicos (ver punto 3.e.v). En particular, cabe traer a colación el artículo 14 de la Ley Colombiana de Firma Digital:

> En la formación del contrato, salvo acuerdo expreso entre las partes, la oferta y su aceptación podrán ser expresadas por medio de un mensaje de datos. No se negará validez o fuerza obligatoria a un contrato por la sola razón de haberse utilizado en su formación uno o más mensajes de datos.

iii. ¿Qué validez tienen las firmas digitales?

El artículo 7 de la Ley Colombiana de Firma Digital prescribe lo siguiente:

> Cuando cualquier norma exija la presencia de una firma o establezca ciertas consecuencias en ausencia de la misma, en relación con un mensaje de datos, se entenderá satisfecho dicho requerimiento si:
>
> a) Se ha utilizado un método que permita identificar al iniciador de un mensaje de datos y para indicar que el contenido cuenta con su aprobación,
>
> b) Que el método sea tanto confiable como apropiado para el propósito por el cual el mensaje fue generado o comunicado.

En concreto, el artículo 28 indica que una firma digital tendrá el mismo efecto que una firma manuscrita si reúne los siguientes requisitos:

> 1. Es única a la persona que la usa.
> 2. Es susceptible de ser verificada.
> 3. Está bajo el control exclusivo de la persona que la usa.
> 4. Está ligada a la información o mensaje, de tal manera que, si éstos son cambiados, la firma digital es invalidada.
> 5. Está conforme a las reglamentaciones adoptadas por el Gobierno Nacional.

iv. ¿Hay regulación sobre contratos inteligentes?

Si bien no existe regulación especial al respecto, puede considerarse que las prescripciones reseñadas en puntos anteriores de la Ley Colombiana de Firma digital son de aplicación.

v. ¿Son los contratos inteligentes contratos legales?

En línea con la respuesta del punto anterior, si el contrato inteligente da cumplimiento a los requisitos de validez exigidos por la Ley Colombiana de Firma Digital, así como también a los requisitos formales para los contratos en general, podemos afirmar que un contrato inteligente es legal.

f. Costa Rica

i. ¿Hay regulación en materia de *blockchain*?

A la fecha del presente informe no hay regulación en materia de *blockchain* en Costa Rica.

ii. ¿Son válidos los actos celebrados en forma electrónica?

Sí, en tanto la Ley Costarricense de Firma Digital señala en su artículo 5 que un contrato puede ser formalizado usando medios electrónicos. Sin embargo, ello se encuentra limitado en los casos que la ley mande la forma física de forma consustancial.

iii. ¿Qué validez tienen las firmas digitales?

El artículo 9 de la Ley Costarricense de Firma Digital prescribe que:

> Los documentos y las comunicaciones suscritos mediante firma digital, tendrán el mismo valor y la eficacia probatoria de su equivalente firmado en manuscrito. En cualquier norma jurídica que se exija la presencia de una firma, se reconocerá de igual manera tanto la digital como la manuscrita.

Por otro lado, la norma reconoce las llamadas firmas digitales certificadas, para las cuales reserva una serie de presunciones detallas en el artículo 10:

> Todo documento, mensaje electrónico o archivo digital asociado a una firma digital certificada se presumirá, salvo prueba en contrario, de la autoría y responsabilidad del titular del correspondiente certificado digital, vigente en el momento de su emisión.
>
> No obstante, esta presunción no dispensa el cumplimiento de las formalidades adicionales de autenticación, certificación o registro que, desde el punto de vista jurídico, exija la ley para un acto o negocio determinado.

Además de ello, las prescripciones del artículo 10 de la normativa reglamentaria sobre las firmas digitales simples agregan que, a pesar de no poder reemplazar a la firma manuscrita, las firmas digitales son aptas para actuar como "(...) elemento de convicción complementario para establecer la existencia y alcances de un determinado acto o negocio".

iv. ¿Hay regulación sobre contratos inteligentes?

A la fecha de este informe, no existe una regulación especial para los contratos inteligentes. Por lo tanto, aplican las previsiones sobre contratación por medios electrónicos previstas en la Ley Costarricense de Firma Digital así como también en el Código Civil Costarricense y en su Código de Comercio.

v. ¿Son los contratos inteligentes contratos legales?

En la medida que se reúnan los requisitos fijados para los contratos mediante un contrato inteligente y ante la ausencia de una prohibición, los contratos inteligentes son válidos como legal.

g. Cuba

i. ¿Hay regulación en materia de *blockchain*?

No, en Cuba no existe normativa sobre *blockchain*.

ii. ¿Son válidos los actos celebrados en forma electrónica?

El comercio electrónico en Cuba carece de normativa especial, más allá de ciertas iniciativas estatales de realizar pruebas piloto sobre este. Al respecto, el Acuerdo del Consejo de Ministros por el que se aprobaron los lineamientos para el Comercio Electrónico del 26 de diciembre de 2005 establece que, dentro de esta prueba, los Ministerios del Interior y de Justicia tenían la obligación de proponer o dictar todas las normas necesarias para darle validez legal a los actos celebrado en forma electrónica. Sin perjuicio de ello, y fuera del ámbito de esa prueba, no hubo normas dictadas al respecto.

Sin embargo, la Ley Nº 7 del 19 de agosto de 1977 (la "Ley Cubana de Procedimiento Civil, Administrativo y Laboral"), en su reforma de 2006, introdujo el artículo 777, relativo a los procesos de índole económica, que establece que:

> Las pruebas consisten en documentos, comprendidos los electrónicos o digitales, dictámenes de peritos, reconocimiento judicial, y declaraciones de testigos o especialistas, y demás medios que se reconocen y regulan en esta Ley.

Con lo cual, un acto celebrado con medios electrónicos sería válido ya que se pueden aportar elementos que demuestren su existencia como evidencia en un pleito judicial. Estas conclusiones son apoyadas por la doctrina cubana [25] en tanto el Código Civil cubano permite la libertad de formas para los actos sin formalidades fijadas por la ley. De este modo, si el acto en cuestión no exige una formalidad, puede ser realizado por medios informáticos.

iii. ¿Qué validez tienen las firmas digitales?

El Reglamento Cubano sobre el funcionamiento de la infraestructura de llave pública no establece que las firmas digitales son equivalentes a las firmas manuscritas. Siguiendo a la doctrina en la materia mencionada antes, en la medida que sea de aplicación el principio de libertad de formas, será posible considerar equiparable una firma digital a una firma manuscrita.

iv. ¿Hay regulación sobre contratos inteligentes?

No existe regulación sobre contratos inteligentes en Cuba.

v. ¿Son los contratos inteligentes contratos legales?

Al no existir una regulación especial ni una prohibición al respecto, si se reúnen los requisitos legales para tener un contrato mediante la forma de un contrato inteligente, no debería haber obstáculos para que el contrato inteligente sea considerado legal.

25 Cfr. FORMENTÍN ZAYAS, Yanixet Milagro, "Reflexiones sobre el comercio electrónico. un pensamiento analógico en la era digital: el caso de Cuba", *Revista Associação dos Juízes do Rio Grande do Sul*, Vol. 39, Nº 126, 2012, págs. 373 y siguientes, http://www.ajuris.org.br/OJS2/index.php/REVAJURIS/article/viewFile/786/480 (Fecha de consulta 31 de diciembre de 2019)

h. Ecuador

i. ¿Hay regulación en materia de *blockchain*?

En la actualidad Ecuador carece de normativa especial para la tecnología *blockchain*, siendo de aplicación las secciones pertinentes de la Ley Ecuatoriana de E-Commerce.

ii. ¿Son válidos los actos celebrados en forma electrónica?

Conforme lo reseñado en el punto 3.h.v, es posible instrumentar usando documentos electrónicos un acto jurídico. Asimismo, el artículo 44 de la Ley Ecuatoriana de E-Commerce establece lo siguiente:

> Cualquier actividad, transacción mercantil, financiera o de servicios, que se realice con mensajes de datos, a través de redes electrónicas, se someterá a los requisitos y solemnidades establecidos en la ley que las rija, en todo lo que fuere aplicable, y tendrá el mismo valor y los mismos efectos jurídicos que los señalados en dicha ley.

En línea con ello, el artículo 45 y el 46 admiten expresamente el uso de documentos electrónicos para celebrar un acto jurídico y determinar las condiciones para el perfeccionamiento y aceptación de los mismos.

iii. ¿Qué validez tienen las firmas digitales?

Conforme el artículo 14 de la Ley Ecuatoriana de E-Commerce, las firmas electrónicas tienen la misma validez que las firmas manuscritas. En caso de que se use un certificado de firma electrónica debidamente expedido por entidades autorizadas, la firma electrónica tendrá una presunción de autoría sobre el firmante del documento electrónico.

iv. ¿Hay regulación sobre contratos inteligentes?

Sobre este punto, cabe mencionar que actualmente no existen regulaciones en Ecuador sobre contratos inteligentes.

v. ¿Son los contratos inteligentes contratos legales?

En la medida que el contrato instrumentado mediante un contrato inteligente pueda ser ejecutado usando medios electrónicos y se dé cumplimiento a las prescripciones aplicables al contrato de fondo, así como también a la Ley Ecuatoriana de E-Commerce, en lo que sea aplicable, el contrato inteligente será legal.

i. El Salvador

i. ¿Hay regulación en materia de *blockchain*?

En El Salvador no hay regulación sobre *blockchain*. Sin perjuicio de ello, el Banco Central Salvadoreño se ha pronunciado [26] advirtiendo sobre el fenómeno de las ICO de forma negativa.

ii. ¿Son válidos los actos celebrados en forma electrónica?

Los actos celebrados en forma electrónica son válidos en atención a las prescripciones contenidas en la Ley Salvadoreña de Firma Electrónica.

iii. ¿Qué validez tienen las firmas digitales?

La Ley Salvadoreña de Firma Electrónica señala que tanto los documentos firmados con firma electrónica simple como con firma electrónica certificada tienen validez legal y son equiparables a la firma manuscrita, conforme el artículo 1 inciso a; en ese sentido, el artículo 6 indica que

> la firma electrónica simple tendrá la misma validez jurídica que la firma autógrafa. En cuanto a sus efectos jurídicos, la firma electrónica simple no tendrá validez probatoria en los mismos términos a los concedidos por esta Ley a la firma electrónica certificada; sin embargo, podrán constituir un elemento de convicción conforme a las reglas de la sana crítica.

Según el artículo 25, las firmas electrónicas certificadas gozan de las presunciones de autoría e integridad.

iv. ¿Hay regulación sobre contratos inteligentes?

No existe regulación sobre contratos inteligentes en El Salvador.

v. ¿Son los contratos inteligentes contratos legales?

Al no existir una regulación especial ni una prohibición al respecto, no debería haber obstáculos para que el contrato inteligente sea considerado legal si se reúnen los requisitos para tener un contrato mediante la forma de un contrato inteligente.

26 Se trata de un comunicado de prensa del Banco Central Salvadoreño publicado en su cuenta oficial de la red social Twitter, que puede ser consultado en el siguiente enlace: https://twitter.com/bcr_sv/status/927522760888389633 (Fecha de consulta 31 de diciembre de 2019).

j. Guatemala

i. ¿Hay regulación en materia de *blockchain*?

No hay regulación sobre *blockchain* en Guatemala.

ii. ¿Son válidos los actos celebrados en forma electrónica?

El Decreto Guatemalteco de Firma Electrónica en su artículo 33 reconoce la validez de los documentos electrónicos, salvo para disposiciones por causa de muerte y actos jurídicos del derecho de familia. A ello deben sumarse las equiparaciones de los artículos 7, 8 y 9 de los medios electrónicos con los medios físicos.

Por otro lado, el artículo 15 del Decreto Guatemalteco de Firma Electrónica da validez a los contratos celebrados por medios electrónicos de la siguiente manera:

> En la formación de un contrato por particulares o entidades públicas, salvo acuerdo expreso entre las partes, la oferta y su aceptación podrán ser expresadas por medio de una comunicación electrónica. No se negará validez o fuerza obligatoria a un contrato por la sola razón de haberse utilizado en su formación una o más comunicaciones electrónicas.

iii. ¿Qué validez tienen las firmas digitales?

Según el artículo 8 del Decreto Guatemalteco de Firma Electrónica, la firma electrónica es equivalente a la firma manuscrita cuando permite la identificación del firmante y el método utilizado es fiable y apropiado para el medio empleado en la comunicación de la voluntad del firmante.

iv. ¿Hay regulación sobre contratos inteligentes?

No hay regulación sobre contratos inteligentes en Guatemala.

v. ¿Son los contratos inteligentes contratos legales?

Dado que un contrato puede ser instrumentado por medios informáticos, si el contrato inteligente reúne los requisitos establecidos para los contratos, debe ser considerado como un acuerdo con efectos legales entre las partes.

k. Haití

i. ¿Hay regulación en materia de *blockchain*?

No, no existe una regulación especial sobre *blockchain* en Haití.

ii. ¿Son válidos los actos celebrados en forma electrónica?

Conforme la Ley Haitiana de Firma Electrónica, los actos celebrados en forma electrónico tienen plena validez legal.

iii. ¿Qué validez tienen las firmas digitales?

La Ley Haitiana de Firma Electrónico reconoce a las firmas electrónicas la equivalencia con sus contrapartes manuscritas, tal como fue reseñado en el punto 3.k.v.

iv. ¿Hay regulación sobre contratos inteligentes?

No existe una regulación especial sobre contratos inteligentes en Haití. En consecuencia, es de aplicación, si se reúnen los requisitos para tener un contrato tradicional, las normativas generales sobre contratos.

v. ¿Son los contratos inteligentes contratos legales?

Al no existir una regulación especial ni una prohibición al respecto y, como se mencionó anteriormente, si se reúnen los requisitos legales para tener un contrato mediante la forma de un contrato inteligente, no debería haber obstáculos para que el contrato inteligente sea considerado legal.

1. Honduras

i. ¿Hay regulación en materia de *blockchain*?

En Honduras no hay regulación en materia de *blockchain*.

ii. ¿Son válidos los actos celebrados en forma electrónica?

Sí, tal como se ha reseñado en el punto 3.1.v., los actos jurídicos pueden instrumentarse mediante documentos electrónicos.

Al respecto de ello, si el acto tiene que hacerse por instrumento público, solo es posible su ejecución mediante firma electrónica avanzada. Por otro lado, si el acto necesita expresamente firmado o hay consecuencias por su falta de firmado, es necesario que la firma electrónica cumpla con ciertos requisitos previsto en el artículo 8 de la Ley Hondureña de Firma Electrónica.

iii. ¿Qué validez tienen las firmas digitales?

La Ley Hondureña de Firma Electrónica reconoce dos tipos de firmas: las firmas electrónicas simples y las firmas electrónicas avanzadas. La diferencia entre ambos tipos de firmas radica en el uso de un certificado digital emitido por un prestador autorizado por el Estado hondureño; el uso de ese certificado permite resistir los rechazos de autoría e integridad del documento donde esta insertada la firma y, consecuentemente, invertir la carga de la prueba.

iv. ¿Hay regulación sobre contratos inteligentes?

No, no existe regulación especial sobre contratos inteligentes en Honduras.

v. ¿Son los contratos inteligentes contratos legales?

Al no existir una regulación especial ni una prohibición al respecto y, como se mencionó anteriormente, si se reúnen los requisitos legales para tener un contrato mediante la forma de un contrato inteligente, no debería haber obstáculos para que el contrato inteligente sea considerado legal.

m. México

i. ¿Hay regulación en materia de *blockchain*?

No, a la fecha del presente informe no hay regulación sobre la tecnología en México.

ii. ¿Son válidos los actos celebrados en forma electrónica?

Conforme el artículo 4 de la Ley Mexicana de Firma Electrónica, son válidos todos los actos celebrados de forma electrónica excepto que una disposición legal o un dictamen de la Secretaria de la Función Pública dictamine que no es posible otorgar cierto acto haciendo uso de medios electrónicos.

iii. ¿Qué validez tienen las firmas digitales?

La Ley Mexicana de Firma Electrónica solo reconoce la categoría de firma electrónica avanzada. En tal sentido, el artículo 7 de dicha norma prescribe lo siguiente:

> La firma electrónica avanzada podrá ser utilizada en documentos electrónicos y, en su caso, en mensajes de datos.
>
> Los documentos electrónicos y los mensajes de datos que cuenten con firma electrónica avanzada producirán los mismos efectos que los presentados confirma autógrafa y, en consecuencia, tendrán el mismo valor probatorio que las disposiciones aplicables les otorgan a éstos.

Por su parte, el artículo 8 señala que la firma electrónica avanzada deberá cumplir con los siguientes preceptos: equivalencia funcional, autenticidad, integridad, neutralidad tecnológica, no repudio y confidencialidad. Asimismo, según el artículo 9, esa firma electrónica deberá hacer uso de un certificado digital vigente, emitido u homologado bajo el sistema de autorización previsto por la norma, así como también que la clave privada del certificado este bajo exclusivo control del usuario.

iv. ¿Hay regulación sobre contratos inteligentes?

No, no existe regulación especial sobre contratos inteligentes en México.

v. ¿Son los contratos inteligentes contratos legales?

Al no existir una regulación especial ni una prohibición al respecto y, como se mencionó anteriormente, si se reúnen los requisitos legales para tener un contrato mediante la forma de un contrato inteligente, no debería haber obstáculos para que el contrato inteligente sea considerado legal.

n. Nicaragua

i. ¿Hay regulación en materia de *blockchain*?

A la fecha del presente informe no hay regulación especial sobre *blockchain* en Nicaragua.

ii. ¿Son válidos los actos celebrados en forma electrónica?

Los actos celebrados en forma electrónica son válidos en Nicaragua pero deben sujetarse a las prescripciones de la Ley Nicaragüense de Firma Electrónica. En tal sentido, será importante reparar en el tipo de acto jurídico para elegir la firma electrónica apropiada para el mismo.

iii. ¿Qué validez tienen las firmas digitales?

La Ley Nicaragüense de Firma Electrónica reconoce dos tipos de firmas: las firmas electrónicas y las firmas electrónicas certificadas. Las primeras son aptas para exteriorizar la voluntad en todo acto jurídico que no exija una firma manuscrita, sino que simplemente pida que el acto sea firmado o no diga nada al respecto. La normativa reglamentaria de la Ley Nicaragüense de Firma Electrónica en su artículo 4 prescribe que para que la firma electrónica sea válida es necesario que pueda cumplir con lo siguiente:

> a) Los datos de creación de la firma, en el contexto en que son utilizados, corresponden exclusivamente al titular;
> b) Los datos de creación de la firma estaban, en el momento de la firma, bajo el control exclusivo del titular;
> c) Es posible detectar cualquier alteración de la firma electrónica hecha después del momento de la firma; y
> d) Es posible detectar cualquier alteración de esa información hecha después del momento de la firma.

En cambio, solo las firmas electrónicas certificadas son aptas para reemplazar a una firma manuscrita cuando la norma lo pide expresamente, según lo dispuesto en el artículo 6 de la mencionada norma. A pesar de ello, existen ciertos casos donde no es posible usar ni siquiera una firma electrónica certificada, tal como señala el artículo 6. Para que una firma electrónica sea considerada como certificada, conforme el artículo 5, es necesario que se cumpla con los siguientes requisitos:

> 1. Que los datos de creación de firma correspondan exclusivamente al titular;
> 2. Que el certificado reconocido en que se base, haya sido expedido por un proveedor de servicios de certificación acreditado; y
> 3. Cuando el dispositivo seguro de creación de firma provenga de un proveedor de servicios de certificación acreditado.

iv. ¿Hay regulación sobre contratos inteligentes?

No, a la fecha del presente informe no hay regulación sobre contratos inteligentes en Nicaragua.

v. ¿Son los contratos inteligentes contratos legales?

Al no existir una regulación especial ni una prohibición al respecto y, como se mencionó anteriormente, si se reúnen los requisitos legales para tener un contrato mediante la forma de un contrato inteligente, no debería haber obstáculos para que el contrato inteligente sea considerado legal.

0. Panamá

i. ¿Hay regulación en materia de *blockchain*?

No, a la fecha del presente informe no hay regulación sobre *blockchain* en Panamá.

ii. ¿Son válidos los actos celebrados en forma electrónica?

Los documentos electrónicos tienen validez jurídica, con lo cual es posible instrumentar usando medios informáticos un acto jurídico (punto 3.o.v.). Al respecto de ello, la Ley Panameña de Firma Electrónica dispone la modificación de ciertos artículos del Código de Comercio de Panamá para permitir expresamente la contratación electrónica cuando no exista una formalidad especial o incompatible con los medios informáticos.

iii. ¿Qué validez tienen las firmas digitales?

Siguiendo con las prescripciones de la Ley Panameña de Firma Electrónica, esta norma distingue entre las firmas electrónicas y las firmas electrónicas calificadas. La diferencia entre ambas está dada por el uso de un certificado electrónico calificado.

Sobre las primeras, el artículo 8 indica que "La firma electrónica tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel." En el caso de las firmas electrónicas calificadas, las mismas serán necesarias, conforme el artículo 9, cuando:

> Si una disposición legal requiere que una firma relacionada a un documento o a una transacción sea reconocida o hecha bajo la gravedad del juramento, dicho requisito será satisfecho en un documento electrónico si el otorgante utiliza la firma electrónica calificada.
>
> Si una disposición legal requiere que una firma relacionada a un documento o a una transacción, sea notariada, refrendada o hecha bajo la gravedad del juramento ante un notario o funcionario público, dicho requisito será satisfecho en un documento electrónico si a la firma electrónica calificada del otorgante se adiciona la firma electrónica del funcionario autorizado para dar fe pública, siempre que la firma electrónica utilizada por el funcionario cumpla con los requisitos establecidos en esta Ley y en sus reglamentos, para ser considerada una firma electrónica calificada.

iv. ¿Hay regulación sobre contratos inteligentes?

A la fecha del presente informe, no hay regulación especial en Panamá sobre contratos inteligentes.

v. ¿Son los contratos inteligentes contratos legales?

Al no existir una regulación especial ni una prohibición al respecto y, como se mencionó anteriormente, si se reúnen los requisitos legales para tener un contrato mediante la forma de un contrato inteligente, no debería haber obstáculos para que el contrato inteligente sea considerado legal.

p. Paraguay

i. ¿Hay regulación en materia de *blockchain*?

No, a la fecha del presente informe Paraguay no tiene regulación sobre *blockchain*.

ii. ¿Son válidos los actos celebrados en forma electrónica?

La Ley Paraguaya de Firma Electrónica establece la validez de los actos celebrados por medios informáticos: entre los artículos 12 a 14 regula cómo es la emisión y recepción de comunicaciones electrónicas. En lo que hace a la validez del acto en sí mismo cuando se usan medios informáticos, el artículo 5 establece que es posible su uso, sin que tenga que haber un acuerdo previo entre las partes sobre ello, y lo que importa es cumplir con los requisitos formales exigidos para el acto. Si el acto exige que el uso de la forma escrita, el artículo 6 indica lo siguiente:

> Cuando en el ámbito de aplicación de la presente Ley, la normativa vigente requiera que la información conste por escrito o si las normas prevean consecuencias en el caso de que la información no sea presentada o conservada en su forma original; ese requisito quedará satisfecho con un mensaje de datos firmado digitalmente que permita que la información que éste contiene sea accesible para su ulterior consulta.
>
> En caso de que el mensaje de datos no estuviere vinculado con una firma digital, el mismo será considerado válido, en los términos del parágrafo anterior; si fuera posible determinar por algún medio inequívoco su autenticidad e integridad.

Asimismo, es necesario agregar las precisiones del artículo 7:

> Toda información presentada en forma de mensaje de datos gozará de la debida fuerza probatoria, siempre y cuando el mismo tenga una firma digital válida de acuerdo con la presente Ley.
>
> Los actos y contratos suscritos por medio de firma digital, otorgados o celebrados por personas naturales o jurídicas, públicas o privadas en el ámbito de aplicación de la presente Ley, serán válidos de la misma manera y producirán los mismos efectos que los celebrados por escrito y en soporte de papel. Dichos actos y contratos se reputarán como escritos, en los casos en que la ley exija que los mismos consten por escrito, a los efectos de que surtan consecuencias jurídicas.

Conforme el artículo 21, no es viable la instrumentación por medios informáticos de:

> a) las disposiciones de última voluntad;
> b) los actos jurídicos del derecho de familia; y,
> c) los actos que deban ser instrumentados bajo exigencias o formalidades incompatibles con la utilización de la firma digital, como los que requieran de escritura pública y aquellos en los que así se haya determinado por acuerdo de partes.

iii. ¿Qué validez tienen las firmas digitales?

La Ley Paraguaya de Firma Electrónica distingue, como ya hemos esbozado en el punto anterior, dos tipos de firmas: las electrónicas y las digitales. Cada una de estas firmas tiene diferentes alcances. Su diferencia está dada por los requisitos fijados por el artículo 22 que deben ser cumplidos para tener una firma digital. Si falta alguno de ellos, es imposible hablar de firma digital y tendremos una electrónica. En cuanto esos requisitos, son los siguientes:

> a) haber sido creada durante el período de vigencia del certificado digital válido del firmante;
> b) haber sido debidamente verificada la relación entre el firmante y la firma digital, por la referencia a los datos indicados en el certificado digital, según el procedimiento de verificación correspondiente. Se exigirá la presencia física del solicitante del certificado con documento de identidad vigente y válido en la República del Paraguay;
> c) que dicho certificado haya sido emitido por una entidad prestadora de servicios de certificación autorizada por la presente Ley;
> d) que los datos de creación de la firma hayan estado, en el momento de la firma, bajo el control del firmante;
> e) que sea posible detectar cualquier alteración de la firma electrónica hecha después del momento de la firma;
> f) que sea posible detectar cualquier alteración de la información contenida en el mensaje de datos al cual está asociada, hecha después del momento de la firma;
> g) el solicitante es el responsable respecto de la clave privada cuya clave pública correspondiente se consigna en el certificado y todos los usos que a la misma se le dieran;
> h) el solicitante deberá manifestar su total conocimiento y aceptación de la Declaración de Prácticas de Certificación y/o Política de Certificación correspondientes al certificado solicitado.
> Reunidos estos elementos, se logra una firma digital que, según el artículo 23, goza de dos presunciones: autoría e integridad.

iv. ¿Hay regulación sobre contratos inteligentes?

No, Paraguay no tiene regulación especial sobre contratos inteligentes.

v. ¿Son los contratos inteligentes contratos legales?

Al no existir una regulación especial ni una prohibición al respecto y, como se mencionó anteriormente, si se reúnen los requisitos legales para tener un contrato mediante la forma de un contrato inteligente, no debería haber obstáculos para que el contrato inteligente sea considerado legal.

q. Perú

i. ¿Hay regulación en materia de *blockchain*?

A la fecha de este informe no existe en Perú regulación en materia de *blockchain*.

ii. ¿Son válidos los actos celebrados en forma electrónica?

En Perú los actos celebrados mediante medios informáticos son válidos (punto 3.q.v).

iii. ¿Qué validez tienen las firmas digitales?

Una firma digital que usa un certificado digital emitido o reconocido bajo el amparo de la Infraestructura Oficial de Firma Electrónica es equivalente a una manuscrita.

Una firma electrónica es válida y equivalente a una firma manuscrita únicamente cuando el acto jurídico en el cual se la está usando no tiene una formalidad especial en cuanto al tipo de firma exigido.

iv. ¿Hay regulación sobre contratos inteligentes?

No existe regulación especial sobre la materia siendo de aplicación el Código Civil peruano.

v. ¿Son los contratos inteligentes contratos legales?

Dado que, conforme el artículo 1374 del Código Civil peruano, los contratos pueden instrumentarse mediante medios electrónicos, si un contrato inteligente reúne los requisitos exigidos para la existencia de un contrato conforme la normativa peruana, es posible considerar que un contrato inteligente es legal.

r. República Dominicana

i. ¿Hay regulación en materia de *blockchain*?

A la fecha del presente informe no hay regulación sobre *blockchain* en la República Dominicana.

ii. ¿Son válidos los actos celebrados en forma electrónica?

La Ley Dominicana de Firma Electrónica establece la validez de los actos celebrados por medios informáticos: entre los artículos 13 a 28 regula todo lo relativo a los actos jurídicos realizados en soportes electrónicos. Por otro lado, y en cuanto a la validez de los documentos electrónicos, remitimos a las consideraciones realizadas en el punto 3.r.v.

iii. ¿Qué validez tienen las firmas digitales?

En cuanto a este punto, la normativa distingue entre las firmas digitales y las firmas digitales seguras. Las primeras, conforme el artículo 31, deben reunir los siguientes requisitos, a saber:

1. Es única a la persona que la usa
2. Es susceptible de ser verificada;
3. Esta bajo el control exclusivo de la persona que la usa;
4. Está ligada a la información, documento digital o mensaje a la que está asociada, de tal manera que si estos son cambiados, la firma digital es invalidada, y
5. Esta conforme a las reglamentaciones adoptadas por el Poder Ejecutivo.

Esta firma digital goza de las presunciones de autoridad e integridad del documento donde esta insertada. Por otro lado, la firma digital segura, en atención a lo prescripto por el artículo 32, es aquella que puede ser verificada de conformidad con un sistema de procedimiento de seguridad que cumpla con los requisitos fijados por la normativa.

La normativa reglamentaria de la Ley Dominicana de Firma Electrónica introduce la categoría de firma electrónica y la califica como una firma digital que adolece de alguna de sus características.

iv. ¿Hay regulación sobre contratos inteligentes?

A la fecha del presente informe no existe regulación sobre contratos inteligentes en República Dominicana.

v. ¿Son los contratos inteligentes contratos legales?

Al no existir una regulación especial ni una prohibición al respecto y, como se mencionó anteriormente, si se reúnen los requisitos legales para tener un contrato mediante la forma de un contrato inteligente, no debería haber obstáculos para que el contrato inteligente sea considerado legal.

S. Uruguay

i. ¿Hay regulación en materia de *blockchain*?

A la fecha del presente informe no hay regulación sobre blockchain en Uruguay.

ii. ¿Son válidos los actos celebrados en forma electrónica?

Es posible instrumentar actos jurídicos en soportes informáticos, conforme lo reseñado en el punto 3.s.v.

iii. ¿Qué validez tienen las firmas digitales?

La Ley Uruguaya de Firma Electrónica reconoce dos tipos de firmas: las firmas electrónicas y las firmas electrónicas avanzadas. Conforme el artículo 5, la firma electrónica:

> (...) tendrá eficacia jurídica cuando fuese admitida como válida por las partes que la utilizan o haya sido aceptada por la persona ante quien se oponga el documento firmado electrónicamente.
>
> Se respetará la libertad de las partes para concertar de común acuerdo las condiciones en que aceptarán las firmas electrónicas, conforme a la presente normativa.
>
> En caso de ser desconocida la firma electrónica por una de las partes, corresponde a la otra parte probar su validez.

Por otro lado, según el artículo 6, la firma electrónica avanzada:

> (...) tendrá idéntica validez y eficacia que la firma autógrafa consignada en documento público o en documento privado con firmas certificadas, siempre que esté debidamente autenticada por claves u otros procedimientos seguros que:
>
> A) garanticen que la firma electrónica avanzada se corresponde con el certificado reconocido emitido por un prestador de servicios de certificación acreditado, que lo asocia con la identificación del signatario;
>
> B) aseguren que la firma electrónica avanzada se corresponde con el documento respectivo y que el mismo no fue alterado ni pueda ser repudiado; y
>
> C) garanticen que la firma electrónica avanzada ha sido creada usando medios que el signatario mantiene bajo su exclusivo control y durante la vigencia del certificado reconocido.
>
> El documento electrónico suscripto con firma electrónica avanzada tendrá idéntico valor probatorio al documento público o al documento privado con firmas certificadas en

soporte papel. El documento electrónico no hará fe respecto de su fecha, a menos que ésta conste a través de un fechado electrónico otorgado por un prestador de servicios de certificación acreditado.

Es decir, la firma electrónica avanzada es aquella que cumple con los siguientes requisitos:

1) Requerir información de exclusivo conocimiento del firmante, permitiendo su identificación unívoca;
2) ser creada por medios que el firmante pueda mantener bajo su exclusivo control;
3) ser susceptible de verificación por terceros;
4) estar vinculada a un documento electrónico de tal modo que cualquier alteración subsiguiente en el mismo sea detectable; y
5) haber sido creada utilizando un dispositivo de creación de firma técnicamente seguro y confiable y estar basada en un certificado reconocido válido al momento de la firma.

Respecto del uso de la firma electrónica o firma electrónica avanzada para los notarios, la Administración Pública y la administración de justicia, la Ley Uruguaya de Firma Electrónica establece su régimen entre los artículos 7 a 11.

iv. ¿Hay regulación sobre contratos inteligentes?

A la fecha del presente informe no existe regulación sobre contratos inteligentes en Uruguay.

v. ¿Son los contratos inteligentes contratos legales?

Al no existir una regulación especial ni una prohibición al respecto y, como se mencionó anteriormente, si se reúnen los requisitos legales para tener un contrato mediante la forma de un contrato inteligente, no debería haber obstáculos para que el contrato inteligente sea considerado legal.

t. Venezuela

i. ¿Hay regulación en materia de *blockchain*?

Sí, en la actualidad existe regulación en esta materia pero vinculada al mundo de las criptomonedas, conforme se detallará en el punto 5.t.

ii. ¿Son válidos los actos celebrados en forma electrónica?

La Ley Venezolana de Firma Electrónica establece la validez de los actos celebrados por medios informáticos: entre los artículos 9 a 15 regula todo lo relativo a los actos jurídicos realizados en soportes electrónicos. Por otro lado, y en cuanto a la validez de los documentos electrónicos, remitimos a las consideraciones realizadas en el punto 3.t.v.

iii. ¿Qué validez tienen las firmas digitales?

La Ley Venezolana de Firma Electrónica reconoce únicamente la categoría de firma electrónica, conforme el artículo 16, el cual establece lo siguiente:

> (...) tendrá la misma validez y eficacia probatoria que la ley otorga a la firma autógrafa. A tal efecto, salvo que las partes dispongan otra cosa, la Firma Electrónica deberá llenar los siguientes aspectos:
> 1. Garantizar que los datos utilizados para su generación puedan producirse sólo una vez, y asegurar, razonablemente, su confidencialidad.
> 2. Ofrecer seguridad suficiente de que no pueda ser falsificada con la tecnología existente en cada momento.
> 3. No alterar la integridad del Mensaje de Datos.

A su vez, y conforme el artículo 18, la firma electrónica debe hacer uso de un certificado proporcionado por un proveedor de servicios de certificación para que pueda ser considerada como tal.

En el caso de las firmas electrónicas que no reúnan estos requisitos o no hagan uso de un certificado válido, el artículo 17 indica que "(...) no tendrá los efectos jurídicos que se le atribuyen en el presente Capítulo, sin embargo, podrá constituir un elemento de convicción valorable conforme a las reglas de la sana crítica".

iv. ¿Hay regulación sobre contratos inteligentes?

A la fecha del presente informe no hay regulación especial sobre contratos inteligentes. Sin perjuicio de ello, el Decreto Constituyente sobre el Sistema Integral de Criptoactivos publicado en la Gaceta Oficial de la República Bolivariana de Venezuela Nº 41.575 del 30 de enero de 2019 (el "Decreto Venezolano del Sistema Integral de Criptoactivos") señala que es competencia del Consejo Ejecutivo de Intendentes de la Superintendencia Nacional de Criptoactivos y Actividades Conexas aprobar las directrices que regulen, entre otros temas, a los contratos inteligentes.

v. ¿Son los contratos inteligentes contratos legales?

Conforme la situación normativa actual, al no existir una regulación especial ni una prohibición al respecto y, como se mencionó anteriormente, si se reúnen los requisitos legales para tener un contrato mediante la forma de un contrato inteligente, no debería haber obstáculos para que el contrato inteligente sea considerado legal, teniendo en especial consideración a las regulaciones reseñadas en el punto ii.

u. Otros casos con reglamentación especial en materia de *blockchain*

En cuanto a los casos de regulación internacional más allá de Latinoamérica en materia de *blockchain*, podemos decir que existen dos grandes tendencias: la visión estadounidense y la visión europea. Esta última está dada por el uso de los marcos normativos generales pre-existentes y su aplicación a la tecnología *blockchain*. Al igual que en la sección anterior, estos son temas que han sido tratados por el Observatorio y Foro *Blockchain* de la Unión Europea en un informe especial[27]. Esta posición encuentra su razón de ser en que las regulaciones que podrían ser aplicables son tecnológicamente neutrales, es decir regulan actividades o conductas y no tecnologías. Por lo tanto, es posible su aplicación a diferentes infraestructuras o soluciones en la medida que realicen lo mismo. La principal regulación de interés es el Reglamento eIDAS, que contiene las regulaciones para la provisión de servicios de identificación y también permite brindar servicios de certificados digitales y de sellado de tiempo bajo la figura de los prestadores de servicios de confianza. Estos últimos son elementos fundamentales para la realización de actos jurídicos con medios informáticos.

Sin perjuicio de ello, existen varias jurisdicciones europeas que han creado marcos normativos especiales para favorecer la instalación de proyectos *blockchain* en sus fronteras y, quebrando la postura europea, han dictado normativa especial aplicable a ciertas infraestructuras o soluciones tecnológicas, en este caso *blockchain* o tecnologías de registro distribuido, en lugar de regular actividades o conductas. En ese sentido, podemos mencionar los casos de Malta y Gibraltar.

Del otro lado del Atlántico, en los Estados Unidos de América, se adoptó la postura de reconocer la validez legal expresa de los actos celebrados usando tecnología *blockchain* en ciertas jurisdicciones mediante el dictado de una normativa especial[28]. Esto es posible dado que se trata de una materia que no ha sido delegada al gobierno federal, la potestad para legislar sobre la validez de esta tecnología recae en cada uno de los Estados. Sin perjuicio de ello, existen iniciativas que buscan la creación de una normativa similar en cada jurisdicción para unificar los efectos legales de la tecnología[29].

A pesar de las diferencias, el común denominador, salvo ciertas excepciones, es seguir la lógica de autorización y certificación bajo un marco normativo creado por el Estado. Sin esa aprobación, los actos realizados en estas plataformas tecnológicas carecen de validez legal o su validez debe ser demostrada en caso de cuestionamiento.

27 Cfr. EU BLOCKCHAIN OBSERVATORY AND FORUM, "Legal and regulatory framework of blockchains and smart contracts", 27 de septiembre de 2019.

28 Cfr. KOHEN, Matthew E. – WALES, Justin S., "State Regulations on Virtual Currency and Blockchain Technologies", 29 de agosto de 2019, https://www.carltonfields.com/insights/publications/2018/state-regulations-on-virtual-currency-and-blockchain-technologies (Fecha de consulta 31 de diciembre de 2019).

29 Cfr. Smith, Edwin, "The Uniform Commercial Code and Digital Assets: Legislative Initiatives", 13 de marzo de 2019, https://www.uniformlaws.org/blogs/edwin-smith/2019/03/13/ucc-and-digital-assets-legislative-initiatives (Fecha de consulta 31 de diciembre de 2019).

Marco normativo aplicable a las criptomonedas

6 Marco normativo aplicable a las criptomonedas

Una tercera y última dimensión que resulta necesario considerar para evaluar la posibilidad de implementar una solución de identidad digital auto soberana en los países de América Latina que incluya una billetera digital capaz de almacenar la información transaccional de los usuarios como parte de su identidad, es la normativa aplicable a las criptomonedas en cada país. Para facilitar la consulta de este informe, la Tabla 4 resume las características del marco normativo de cada país.

ivo aplicable a
s Marco norm
s criptomoned

Tabla 4

Marco normativo aplicable a las criptomonedas en países de América Latina

País	¿Hay regulación sobre criptomonedas?	¿Las criptomonedas son dinero?	¿Las criptomonedas tienen curso legal?	¿Un criptoactivo de moneda local es dinero electrónico?*
Argentina	Sí	No	No	No
Bolivia	Sí	No	No	Sí
Brasil	Sí*	No	No	Sí
Chile	Sí*	No	No	Sí
Colombia	Sí	No	No	Sí
Costa Rica	No*	No	No	No
Cuba	No	No	No	No
Ecuador	No*	No	No	Sí
El Salvador	No	No	No	Sí
Guatemala	No	No	No	No
Haití	No	No	No	No
Honduras	No	No	No	Sí
México	Sí	No	No	Sí
Nicaragua	No	No	No	Sí
Panamá	No*	No	No	Sí
Paraguay	No*	No	No	Sí
Perú	No*	No	No	Sí
República Dominicana	No*	No	No	Sí
Uruguay	No	No	No	Sí
Venezuela	Sí	No	No	Sí

* La respuesta proporcionada en este punto no es absoluta y es necesario revisar el análisis realizado del punto para tener un conocimiento pleno de la situación.

a. Argentina

i. ¿Hay regulación en materia de criptomonedas?

En Argentina existen diferentes regulaciones sobre criptomonedas. Como comentario previo, es importante indicar que en las normas existentes no hay una coherencia sobre la terminología empleada: en ciertas regulaciones se emplea el término criptoactivo mientas que en otras se habla de monedas digitales. A efectos de la presente investigación, se empleará el término criptomoneda para referirse de forma unívoca a todas las realidades alcanzadas por las normas.

La primera norma dictada sobre la materia fue en el ámbito de la prevención de lavado de activos y financiamiento del terrorismo: la Resolución Nº 300/2014 de la Unidad de Información Financiera. Tras dicha norma, en la reforma al impuesto a las ganancias del año 2017 se dispuso la inclusión de las ganancias generadas por la enajenación de criptomonedas. Esta regulación está discutida por la doctrina[30] en cuanto a sus alcances reales y, a la fecha de este informe, no hay opinión formal del fisco local sobre la aplicabilidad de la misma. Recientemente, la Administración Federal de Ingresos Públicos ha obligado a ciertos actores de la industria *blockchain* de Argentina, principalmente exchanges[31], a informar las operaciones de sus clientes. Por último, el Banco Central de la República Argentina dictó la Comunicación "A" 6823 que limitó el monto que puede comprarse de criptomonedas a una entidad del exterior del país usando tarjeta de crédito.

ii. ¿Cómo están categorizadas jurídicamente las criptomonedas?

Conforme la Resolución Nº 300/2014, las criptomonedas, como parte de las monedas virtuales, pueden ser definidas como la

> representación digital de valor que puede ser objeto de comercio digital y cuyas funciones son la de constituir un medio de intercambio, y/o una unidad de cuenta, y/o una reserva de valor, pero que no tienen curso legal, ni se emiten, ni se encuentran garantizadas por ningún país o jurisdicción.

Fuera de esta definición, no hay una clasificación general de los criptoactivos a la cual podamos recurrir, lo cual no contribuye a unificar y clarificar los diferentes términos usados por la normativa. Ante ello, y dado que las criptomonedas no podrían ser subsumidas en el concepto de moneda, ni nacional ni extranjera, corresponde su calificación como bienes inmateriales, en atención al artículo 16 del CCyCN, dado que tienen un valor patrimonial.

iii. ¿Puede ser considerado un medio de pago?

En atención a la definición proporcionada por la Resolución Nº 300/2014, sería posible considerar a las criptomonedas como medios de pago en las operaciones comerciales de las personas de aceptación voluntaria.

iv. ¿Qué calificación jurídica merece un criptoactivo derivado de una moneda local?

Sin perjuicio que actualmente no existen regulaciones en Argentina sobre el dinero electrónico, un criptoactivo emitido a partir de la entrega de pesos argentinos puede ser considerado dinero electrónico. Este criptoactivo estará regido por los contratos que las partes del sistema de dinero electrónico celebren entre sí.

30 Cfr. MIHURA ESTRADA, Ricardo. "Las "monedas digitales" y el Bitcoin en el nuevo impuesto a las rentas financieras". *Doctrina Tributaria*, 456 (marzo de 2018), pág. 233.

31 Se refiere a las plataformas donde se realizan los intercambios de criptomonedas a cambio de dinero fiat o de otras criptomonedas.

b. Bolivia

i. ¿Hay regulación en materia de criptomonedas?

Sí, al respecto de ello remitimos a la respuesta dada en el punto 4.b.i.

ii. ¿Cómo están categorizadas jurídicamente las criptomonedas?

Siguiendo la lógica brindada por el Banco Central Boliviano en la normativa antes referida, cabe concluir que las criptomonedas son monedas privadas equivalentes a las monedas fiduciarias, ya sean nacionales o extranjeras.

iii. ¿Puede ser considerado un medio de pago?

En la medida que la criptomoneda sea admitida como válida por el Banco Central Boliviano, la misma podría constituir un medio de pago válido.

iv. ¿Qué calificación jurídica merece un criptoactivo derivado de una moneda local?

Bolivia cuenta con un marco normativo para la emisión de dinero electrónico dentro de su sistema nacional de pagos por parte de instituciones de intermediación financiera y empresas proveedoras de servicios de pago. Este se compone principalmente por el Reglamento de Servicios de Pago, Instrumentos Electrónicos de Pago, Compensación y Liquidación -la Resolución de Directorio Nº 134/2015 del Banco Central Boliviano- junto con su modificación -la Resolución de Directorio Nº 166/2015 del Banco Central Boliviano- (el "Marco Normativo Boliviano de Dinero Electrónico"). Por lo tanto, el criptoactivo podría ser emitido en Bolivia ajustado a los requisitos fijados al momento de iniciar la actividad por parte de la Autoridad de Supervisión del Sistema Financiero.

c. Brasil

i. ¿Hay regulación en materia de criptomonedas?

A la fecha del presente informe no hay regulación sobre criptomonedas en Brasil. Sin perjuicio de ello, varios reguladores con facultades para sus respectivas áreas han emitido pronunciamientos sobre la aplicabilidad de ciertas partes del ordenamiento jurídico brasileño a las criptomonedas. En tal sentido, es posible traer a colación: el Comunicado Nº 25.306 del 19 de febrero de 2014 y el Comunicado Nº 31.379 del 16 de noviembre de 2017 del Banco Central de Brasil, la Circular Nº 1/2018 de la Comisión de Valores Negociables de Brasil, la Guía para el Pago del Impuesto a la Renta del año 2017 y la Instrucción Normativa 1.888/2019. Por último, es necesario señalar que, a efectos contables del Banco Central de Brasil, las criptomonedas son consideradas como productos no financieros, conforme la clasificación del Fondo Monetario Internacional.

ii. ¿Cómo están categorizadas jurídicamente las criptomonedas?

En cuanto a los comunicados del Banco Central de Brasil, las criptomonedas no son monedas extranjeras ni son dinero electrónico. De ambos comunicados, podemos concluir que el Banco Central de Brasil concibe a las criptomonedas como bienes inmateriales. En lo que hace a la Comisión de Valores Negociables de Brasil, esta entidad considera que las criptomonedas no pueden ser calificadas como activos financieros, alineándose por lo tanto bajo las mismas conclusiones que el Banco Central de Brasil. Sin embargo, la guía de la Agencia Tributaria de Brasil concluye en su punto 447 que las criptomonedas pueden ser asimiladas, en el tratamiento fiscal, a los activos financieros. Si bien no es una norma jurídica, en una nota al pie del comunicado de prensa de agosto del 2019 sobre las estadísticas del sector externo del balance del Banco Central de Brasil, se ha señalado que las operaciones de compraventa de criptomonedas entre particulares constituye un contrato de cambio de divisas, dando cabida a la posibilidad de considerar a las criptomonedas como una moneda más.

iii. ¿Puede ser considerado un medio de pago?

De la lectura de todos los documentos que hemos consultado, no encontramos motivo para considerar que las criptomonedas no puedan ser usadas como medio de pago de aceptación voluntaria.

iv. ¿Qué calificación jurídica merece un criptoactivo derivado de una moneda local?

Los comunicados del Banco Central de Brasil sostienen que todo instrumento digital que este denominado en reales debe ser considerado como dinero electrónico y, por lo tanto, sujeto a la Ley Nº 12.865 (la "Ley Brasileña de Dinero Electrónico").

d. Chile

i. ¿Hay regulación en materia de criptomonedas?

Si bien no existe regulación formal sobre criptomonedas, el Servicio de Impuestos Internos de Chile ha dictado dos opiniones, los Oficios Nº 963/2018 y 1371/2019, mediante los cuales brinda una calificación impositiva en materia de criptomonedas.

ii. ¿Cómo están categorizadas jurídicamente las criptomonedas?

En línea con lo reseñado en el punto anterior, es posible considerar a las criptomonedas como "un activo digital o virtual, soportado en un registro digital único denominado *blockchain*, desregulado, desintermediado y no controlado por un emisor central, cuyo precio está determinado por la oferta y la demanda". Asimismo, las opiniones emitidas por el Servicio de Impuestos Internos de Chile agregan que "ni el bitcoin, ni ningún otro activo digital o también llamados criptomonedas, se consideran en Chile como monedas de curso legal o como monedas extranjeras o divisas".

iii. ¿Puede ser considerado un medio de pago?

No existe una prohibición para usar criptomonedas como medio de pago en Chile aunque, en consideración de las opiniones dictadas por el Servicio de impuestos Internos, ello puede no ser lo más eficiente desde la perspectiva impositiva.

iv. ¿Qué calificación jurídica merece un criptoactivo derivado de una moneda local?

El criptoactivo derivado de un peso chileno podría ser calificado como un medio de pago bajo la Ley Nº 20.950 (la "Ley Chilena de Autorización a la Emisión y Operación de Medios de Pago con Provisión de Fondos por Entidades No Bancarias"). En consecuencia, correspondería que la emisión del criptoactivo sea realizado bajo el alcance de esta norma y siguiendo los lineamientos fijados por el Banco Central de Chile.

e. Colombia

i. ¿Hay regulación en materia de criptomonedas?

En Colombia existen ciertas normas relacionadas con criptomonedas. En tal sentido, podemos mencionar: (i) la Carta Circular 29 de 2014 de la Superintendencia Financiera de Colombia; (ii) el Concepto Nº 20348 de 2016 del Banco de la República; (iii) el Concepto Nº 20436 de 2017 de la Dirección de Impuestos y Aduana Nacionales; y (iv) el Concepto Nº 977 de 2017 del Consejo Técnico de la Contaduría Pública en Colombia.

ii. ¿Cómo están categorizadas jurídicamente las criptomonedas?

En cuanto a la naturaleza jurídica de las criptomonedas, la respuesta es diferente en atención al organismo que se consulte. La Superintendencia Financiera de Colombia y el Banco de la República parecen coincidir en que no se trata de una divisa, pero no determinan su calificación legal. Por su parte, la Dirección de Impuestos y Aduana Nacionales, junto con el Consejo Técnico de la Contaduría Pública en Colombia, coinciden en que se trata un activo inmaterial que debería ser computado, impositivamente, como un commodity.

iii. ¿Puede ser considerado un medio de pago?

Tanto la Superintendencia Financiera de Colombia como el Banco de la República consideran que las criptomonedas no son medios de pagos con poder cancelatorio. Sin perjuicio de ello, y por aplicación de la autonomía de la voluntad, las criptomonedas pueden ser aceptadas voluntariamente por las partes y se les puede otorgar poder cancelatorio de las obligaciones frente a las cuales se comprometió su entrega, tal como reseña la doctrina[32].

iv. ¿Qué calificación jurídica merece un criptoactivo derivado de una moneda local?

El dinero electrónico se encuentra regulado en Colombia por la Ley Nº 1735 de 2014 (la "Ley Colombiana de Dinero Electrónico"). Conforme el artículo 1 de dicha norma, la entidad que recolecte fondos del público y ponga a disposición de los titulares de aquellos depósitos mecanismos, conforme las prescripciones dictadas por el Estado colombiano, para hacer uso de esos depósitos. En atención a ello, el criptoactivo debería ajustarse a los lineamientos de la Ley Colombia de Dinero Electrónico y la entidad que expide el criptoactivo debería cumplir con los requisitos allí fijados.

32 CABALLERO MARTINEZ, Jhon, "Las criptomonedas y su marco normativo en Colombia", Blog del Departamento de Derecho Informático de la Universidad Externado de Colombia, 7 de mayo de 2019, https://derinformatico.uexternado.edu.co/las-criptomonedas-y-su-marco-normativo-en-colombia/ (Fecha de consulta 31 de diciembre de 2019).

f. Costa Rica

i. ¿Hay regulación en materia de criptomonedas?

El Banco Central de Costa Rica y sus Órganos de Desconcentración Máxima fijaron su posición en 2017 sobre las criptomonedas en un comunicado de prensa al público general; esta constituye la única posición oficial de un regulador sobre la materia en este país[33].

ii. ¿Cómo están categorizadas jurídicamente las criptomonedas?

Conforme el comunicado de prensa referenciado en el punto anterior, las criptomonedas no son consideradas como divisas nacionales ni extranjeras y, en cambio, deben ser estimadas como activos digitales inmateriales o bienes inmateriales.

iii. ¿Puede ser considerado un medio de pago?

Al respecto de ello, y siguiendo el comunicado de prensa, las criptomonedas no son medios de pago oficiales. Sin perjuicio de ello, se reconoce en el comunicado de prensa que las partes de una transacción pueden voluntariamente aceptar las mismas como medio de pago, estando a su pleno riesgo el uso de estas.

iv. ¿Qué calificación jurídica merece un criptoactivo derivado de una moneda local?

Costa Rica carece de regulación sobre dinero electrónico. A pesar de ello, existen referencias a este concepto pero únicamente dentro del sistema bancario. Por lo tanto, la doctrina[34] [35] coincide en que el dinero electrónico es un derecho originado por un contrato entre emisor y depositario de fondos. Por lo tanto, un criptoactivo derivado de una moneda local debería ser entendido como un derecho crediticio cuyo respeto recae sobre el emisor del criptoactivo.

33 El texto completo del aviso puede ser consultado en el siguiente enlace: https://www.bccr.fi.cr/seccion-noticias/Noticia/Posicion_bccr_criptomonedas.aspx (Fecha de consulta 31 de diciembre de 2019).

34 GÓMEZ DUARTE, Adriana, "El dinero electrónico como sustituto parcial del efectivo y posible mecanismo para masificar el acceso a los servicios financieros. Análisis de la normativa costarricense y la comparada", tesis de Licenciatura en Derecho, Facultad de Derecho, Universidad de Costa Rica, San José, Costa Rica, 2012.

35 SALAS GUZMÁN, Michael - SEGURA ROJAS, Michael, "La Comisión del Delito de Legitimación de Capitales, a través del uso del dinero electrónico en Costa Rica y su posible regulación", Tesis de Licenciatura en Derecho, Facultad de Derecho, Universidad de Costa Rica, San José, Costa Rica, 2015.

g. Cuba

i. ¿Hay regulación en materia de criptomonedas?

No, no existen regulaciones en torno a las criptomonedas.

ii. ¿Cómo están categorizadas jurídicamente las criptomonedas?

Ante la ausencia normativa, las criptomonedas podrían ser calificadas como parte del patrimonio de una persona por su valor conforme el artículo 45.1 del Código Civil cubano.

iii. ¿Puede ser considerado un medio de pago?

Al no existir una norma que prohíba su uso como medio de pago, las criptomonedas pueden ser consideradas como un medio de pago voluntario.

iv. ¿Qué calificación jurídica merece un criptoactivo derivado de una moneda local?

Si bien no existe normativa que regule el dinero electrónico en Cuba, es posible considerar al criptoactivo generado a partir de moneda local como dinero electrónico, el cual se encontrará regulado por las prescripciones que fije su emisor cuando proceda a la recolección de los fondos. Dado que no hay emisión de nueva moneda, sino simplemente una reconversión del soporte del dinero ya emitido por el Banco de Cuba, no se estaría incurriendo en la emisión original de moneda, potestad reservada a esta entidad por el Decreto Ley Nº 361.

h. Ecuador

i. ¿Hay regulación en materia de criptomonedas?

Si bien no hay regulación expresa sobre las criptomonedas, el Código Orgánico Monetario y Financiero de Ecuador contiene disposiciones que afectan el encuadre normativo de las criptomonedas, así como también el Banco Central de Ecuador ha señalado en varias oportunidades la calificación legal de las criptomonedas.

ii. ¿Cómo están categorizadas jurídicamente las criptomonedas?

Las criptomonedas están consideradas como dinero electrónico y, en atención al artículo 101 del Código Orgánico Monetario y Financiero de Ecuador, se considera que las mismas están prohibidas en el territorio de ese país a efectos de su uso como medio de pago. Al respecto, la doctrina considera que si se obtienen criptomonedas, solo pueden usarse en Ecuador con fines especulativos[36].

iii. ¿Puede ser considerado un medio de pago?

En Ecuador las criptomonedas no pueden considerarse un medio de pago. Conforme los artículos 94, 99 y 100 del Código Orgánico Monetario y Financiero de Ecuador los únicos medios de pago habilitados son el dólar estadounidense, los cheques, las transferencias por medios electrónicos o digitales, las tarjetas de crédito y débito y otros de similar naturaleza que oportunamente el regulador autorice.

iv. ¿Qué calificación jurídica merece un criptoactivo derivado de una moneda local?

Este criptoactivo podría ser considerado un medio de pago electrónico, en los términos del artículo 101 del Código Orgánico Monetario y Financiero de Ecuador reformando por la Ley Orgánica para la Reactivación de la Economía, Fortalecimiento de la dolarización y Modernización de la Gestión Financiera. Por lo tanto, es necesario la intervención de una entidad del sistema financiero para el despliegue del criptoactivo.

36 Cfr. SIMONE, Juan Francisco, "La legalidad de las bitcoins en Ecuador", *Gestión Digital*, Sección Análisis, 2 de enero de 2018, disponible en https://revistagestion.ec/economia-y-finanzas-analisis/la-legalidad-de-las-bitcoins-en-ecuador (Fecha de consulta 31 de diciembre de 2019).

i. El Salvador

i. ¿Hay regulación en materia de criptomonedas?

No, no hay regulación sobre criptomonedas en El Salvador, con excepción del comunicado de prensa mencionado anteriormente. Si bien el uso de criptomonedas no está prohibido, queda a exclusivo riesgo de los usuarios.

ii. ¿Cómo están categorizadas jurídicamente las criptomonedas?

Dado que las criptomonedas tienen un valor patrimonial y carecen de regulación especial, pueden ser consideradas como derechos personales, en atención al artículo 567 del Código Civil Salvadoreño.

iii. ¿Puede ser considerado un medio de pago?

Al no existir una norma que prohíba su uso como medio de pago, las criptomonedas pueden ser consideradas como un medio de pago voluntario.

iv. ¿Qué calificación jurídica merece un criptoactivo derivado de una moneda local?

Podría ser considerado como dinero electrónico bajo los términos del artículo 5 de la Ley Nº 72 del 13 de agosto de 2015 (la "Ley Salvadoreña de Dinero Electrónico").

j. Guatemala

i. ¿Hay regulación en materia de criptomonedas?

No, no hay regulación sobre criptomonedas en Guatemala.

ii. ¿Cómo están categorizadas jurídicamente las criptomonedas?

Ante la ausencia de regulación en la materia, es necesario recurrir a las reflexiones de la doctrina en esta materia. En ese sentido, la doctrina concluye que las criptomonedas pueden ser consideradas como bienes incorpóreos[37].

iii. ¿Puede ser considerado un medio de pago?

Al no existir una norma que prohíba su uso como medio de pago, las criptomonedas pueden ser consideradas como un medio de pago voluntario.

iv. ¿Qué calificación jurídica merece un criptoactivo derivado de una moneda local?

Si bien no existe normativa que regule el dinero electrónico en Guatemala, es posible considerar al criptoactivo generado a partir de moneda local como dinero electrónico, el cual se encontrará regulado por las prescripciones que fije su emisor cuando proceda a la recolección de los fondos. Dado que no hay emisión de nueva moneda, sino simplemente una reconversión del soporte del dinero ya emitido por el Banco de Guatemala, no se estaría incurriendo en la emisión original de moneda, potestad reservada a esta entidad por el Decreto Nº 17-2002.

37 Cfr. RAMÍREZ MONZÓN, Darío Alejandro, "Las monedas criptográficas en Guatemala (análisis técnico y jurídico)", *Documentos de Trabajo del Banco de Guatemala*, Nº 137, 2016, pág. 26, http://www.banguat.gob.gt/Publica/Investigaciones_Ec/Working%20Paper_No137.pdf (Fecha de consulta 31 de diciembre de 2019)

k. Haití

i. ¿Hay regulación en materia de criptomonedas?

En la actualidad, no existen normas dictadas en materia de criptomonedas.

ii. ¿Cómo están categorizadas jurídicamente las criptomonedas?

Dada la inexistencia de normativa al respecto, y siguiendo la categorización genérica que se propone en este informe cuando no existe una regulación especial, las criptomonedas deben ser consideradas como bienes conforme el Código Civil de Haití.

iii. ¿Puede ser considerado un medio de pago?

Ante la inexistencia de una prohibición, una criptomoneda puede ser considerada un medio de pago de aceptación voluntaria entre las partes de una determinada transacción.

iv. ¿Qué calificación jurídica merece un criptoactivo derivado de una moneda local?

Debido a la inexistencia de normativa sobre dinero electrónico en este país, el criptoactivo podría ser calificado como un derecho crediticio que el tenedor del mismo tiene contra el emisor de estos que recibe la moneda local en contraprestación.

1. Honduras

i. ¿Hay regulación en materia de criptomonedas?

No hay regulación especial sobre criptomonedas en Honduras. Sin perjuicio de ello, el Banco Central de Honduras dispuso un comunicado donde señala que las criptomonedas no forman parte del sistema financiero bajo su control y que, por lo tanto, los usuarios asumen los riesgos de uso [38].

ii. ¿Cómo están categorizadas jurídicamente las criptomonedas?

Dada la inexistencia de normativa al respecto, las criptomonedas deben ser consideradas como bienes inmateriales.

iii. ¿Puede ser considerado un medio de pago?

A diferencia de lo que ocurre en algunos países de la región, no hay prohibición alguna para usar las criptomonedas como medio de pago en Honduras. Sin perjuicio de ello, se tratará de un medio de pago de aceptación voluntaria, quedando en manos de la parte que debe pagar la posibilidad de cancelar la obligación en moneda de curso legal.

iv. ¿Qué calificación jurídica merece un criptoactivo derivado de una moneda local?

No hay dudas que un criptoactivo derivado de una moneda local será dinero electrónico. Sin perjuicio de ello, la solución tendrá un marco normativo diferente en atención a quién sea el emisor del criptoactivo.

Si se trata de una institución del sistema financiero será de aplicación el artículo 50 del Decreto Nº 129-2004 (la "Ley Hondureña del Sistema Financiero").

Por otro lado, el Decreto Nº 46-2015 (la "Ley Hondureña del Sistema de Pago y Liquidación de Valores") regula las transacciones por medio de dispositivos móviles de dinero electrónico. En este caso, será de aplicación la normativa reglamentaria prevista por el Banco Central de Honduras, principalmente el Acuerdo Nº 1-2016. Para la operación de un sistema de pagos, como podría ser este criptoactivo, es necesario contar con autorización del Banco Central de Honduras, salvo que la iniciativa sea impulsada por ciertos organismos públicos. En el marco de norma se define al dinero electrónico, en su artículo 2.8, como:

> Valor monetario exigible de conformidad al monto pagado que reúne las características siguientes:
> 1) Almacenado en una billetera electrónica;
> 2) Aceptado como facilitador de pago por personas naturales o jurídicas;
> 3) Emitido por un valor igual a los fondos requeridos;
> 4) Convertible en dinero en efectivo en cualquier momento;
> 5) No constituye depósito; y,
> 6) No genera intereses.

38 El texto completo del aviso puede ser consultado en el siguiente enlace: https://www.bch.hn/download/boletines_prensa/2018/boletin_otro_01_18.pdf (Fecha de consulta 31 de diciembre de 2019).

m. México

i. ¿Hay regulación en materia de criptomonedas?

Sí. La ley publicada en el Diario Oficial de la Federación el 9 de marzo de 2018 (la "Ley Mexicana Fintech") contiene normas aplicables a las criptomonedas, principalmente los artículos 30 a 34. Además, el Banco de México, en ejercicio de las facultades reglamentarias que la Ley Fintech de México le concede, dictó la Circular 4/2019 (la "Reglamentación Mexicana de Criptoactivos") que contiene provisiones generales sobre la operatoria con criptoactivos.

ii. ¿Cómo están categorizadas jurídicamente las criptomonedas?

Conforme el artículo 30, las criptomonedas están dentro del concepto de activo virtual, el cual es definido de la siguiente manera:

> (...) se considera activo virtual la representación de valor registrada electrónicamente y utilizada entre el público como medio de pago para todo tipo de actos jurídicos y cuya transferencia únicamente puede llevarse a cabo a través de medios electrónicos. En ningún caso se entenderá como activo virtual la moneda de curso legal en territorio nacional, las divisas ni cualquier otro activo denominado en moneda de curso legal o en divisas.

Por su parte, el artículo 4.a. de la Reglamentación Mexicana de Criptoactivos indica que los activos virtuales deben reunir las siguientes características:

> I. Ser unidades de información, unívocamente identificables, incluso de manera fraccional, registradas electrónicamente, que no representen la titularidad o derechos de un activo subyacente o bien, que representen dicha titularidad o derechos por un valor inferior a estos;
> II. Tener controles de emisión definidos mediante Protocolos determinados y a los que se pueden suscribir terceros, y
> III. Contar con Protocolos que impidan que las réplicas de las unidades de información o sus fracciones se encuentren disponibles para ser transmitidas más de una vez en un mismo momento.

iii. ¿Puede ser considerado un medio de pago?

Conforme el artículo 34, las instituciones que operan con activos virtuales tienen que informar a sus clientes, entre otras cosas, que estos no tienen curso legal; es decir, que carecen del poder cancelatorio compulsivo que tiene la moneda nacional. Sin embargo, el artículo 30 señala que el Banco de México tomará como elemento para autorizar el uso de un ac-

tivo virtual en territorio mexicano, entre otras cuestiones, el uso como medio de cambio del activo virtual, es decir que reconoce que pueden ser usadas como medios de pagos voluntarios, no así con curso legal. Por lo tanto, se sostiene que las criptomonedas solo son medios de pago cuando las partes así lo acuerden.

iv. ¿Qué calificación jurídica merece un criptoactivo derivado de una moneda local?

A pesar de la existencia de regulación especial sobre criptoactivos, un criptoactivo derivado de una moneda local, a los efectos de la Ley Fintech de México, debe ser considerado como un fondo de pago electrónico, cuyas características están establecidas en el artículo 22, a saber:

> (...) aquellos fondos que estén contabilizados en un registro electrónico de cuentas transaccionales que, al efecto lleve una institución de fondos de pago electrónico y que:
> I. Queden referidos a:
> a) Un valor monetario equivalente a una cantidad determinada de dinero, en moneda nacional o, previa autorización del Banco de México, moneda extranjera, o
> b) Un número determinado de unidades de un activo virtual determinado por el Banco de México, conforme a lo establecido en el Capítulo III del Título II de esta Ley;
> II. Correspondan a una obligación de pago a cargo de su emisor, por la misma cantidad de dinero o de unidades de activos virtuales a que se refiere la fracción I de este artículo;
> III. Sean emitidos contra la recepción de la cantidad de dinero o de activos virtuales a que se refiere la fracción I de este artículo, con el propósito de abonar, transferir o retirar dichos fondos, total o parcialmente, mediante la instrucción que, para esos efectos, dé el respectivo tenedor de los fondos de pago electrónico, y
> IV. Sean aceptados por un tercero como recepción de la cantidad de dinero o de activos virtuales respectiva.

En consecuencia, será necesario contar con intervención de una institución de fondos de pago electrónico, que será una persona jurídica autorizada por la Comisión Nacional Bancaria y de Valores de México para operar como tal.

n. Nicaragua

i. ¿Hay regulación en materia de criptomonedas?

A la fecha del presente informe no hay regulación especial sobre criptomonedas.

ii. ¿Cómo están categorizadas jurídicamente las criptomonedas?

Dada la inexistencia de normativa al respecto, las criptomonedas deben ser consideradas como bienes inmateriales.

iii. ¿Puede ser considerado un medio de pago?

A diferencia de lo que ocurre en algunos países de la región, no hay prohibición alguna para usar las criptomonedas como medio de pago. Sin perjuicio de ello, se tratará de un medio de pago de aceptación voluntaria, quedando en manos de la parte que debe pagar la posibilidad de cancelar la obligación en moneda de curso legal.

iv. ¿Qué calificación jurídica merece un criptoactivo derivado de una moneda local?

Podría considerarse que un criptoactivo es dinero electrónico en los términos de la Resolución N° CD-SIBOIF-725-1-ABR26-2012 del 26 de abril de 2012 (el "Marco Normativo Nicaragüense de Dinero Electrónico") por reunir los requisitos fijados en su definición, a saber:

> Anotación en cuenta o registro contable del valor monetario de un crédito exigible a su emisor, que reúne las siguientes características: i) es almacenado en un dispositivo móvil; ii) es aceptado como un facilitador de pago por personas naturales o jurídicas distintas del emisor; iii) es emitido por un valor igual a los fondos requeridos; iv) es convertible a dinero en efectivo en cualquier momento; v) no constituye depósito; vi) es registrado en los pasivos del emisor; y vii) no genera intereses.

La particularidad que tiene el criptoactivo es que debe ser emitido por una institución financiera regulada por el gobierno nicaragüense y ajustarse a las prescripciones del Marco Normativo Nicaragüense de Dinero Electrónico.

0. Panamá

i. ¿Hay regulación en materia de criptomonedas?

A la fecha del presente informe no hay una regulación especial sobre criptomonedas en Panamá. Sin perjuicio de ello, la Superintendencia de Bancos de Panamá dispuso un aviso al público donde resalta el carácter descentralizado de las criptomonedas e indica que no están bajo su potestad regulatoria salvo en lo que hace a la actividad de las entidades financieras con estos instrumentos[39]. Asimismo, la Superintendencia del Mercado de Valores de Panamá realizó una advertencia similar y ha dictado, al menos, una resolución -la Opinión Nº 7/2018 del 15 de noviembre de 2018[40]- ratificando la postura de la inexistencia de regulación en la materia.

ii. ¿Cómo están categorizadas jurídicamente las criptomonedas?

Dada la inexistencia de normativa al respecto, las criptomonedas deben ser consideradas como bienes inmateriales.

iii. ¿Puede ser considerado un medio de pago?

A diferencia de lo que ocurre en algunos países de la región, no hay prohibición alguna para usar las criptomonedas como medio de pago. Sin perjuicio de ello, se tratará de un medio de pago de aceptación voluntaria, quedando en manos de la parte que debe pagar la posibilidad de cancelar la obligación en moneda de curso legal.

iv. ¿Qué calificación jurídica merece un criptoactivo derivado de una moneda local?

En Panamá no existe una regulación sobre dinero electrónico con lo cual todo criptoactivo derivado de una moneda local está reglado por el contrato entre el emisor del dinero electrónico y el depositante de los fondos.

Sin perjuicio de ello, las emisoras de dinero electrónico están alcanzadas por las normas de prevención de lavado de activos y financiamiento del terrorismo dictadas por la Superintendencia de Bancos de Panamá.

39 El texto completo del aviso puede ser consultado en el siguiente enlace: https://www.superbancos.gob.pa/superbancos/documentos/leyes_y_regulaciones/comunicados/2018/aviso5-2018.pdf (Fecha de consulta 31 de diciembre de 2019).

40 El texto completo del aviso puede ser consultado en el siguiente enlace: http://www.supervalores.gob.pa/reglamentacion/opiniones/opiniones-2018/1912-opinion-07-2018/file (Fecha de consulta 31 de diciembre de 2019).

p. Paraguay

i. ¿Hay regulación en materia de criptomonedas?

Sin perjuicio de la inexistencia de regulación formal, el Banco Central de Paraguay ha dictado un comunicado de prensa donde pone de manifiesto que las criptomonedas no son emitidas ni controladas por este ni otro país, haciendo énfasis en que los usuarios corren con todo el riesgo de la operatoria con estos instrumentos [41].

ii. ¿Cómo están categorizadas jurídicamente las criptomonedas?

Dada la inexistencia de normativa al respecto, las criptomonedas deben ser consideradas como bienes inmateriales.

iii. ¿Puede ser considerado un medio de pago?

A diferencia de lo que ocurre en algunos países de la región, no hay prohibición alguna para usar las criptomonedas como medio de pago. Sin perjuicio de ello, se tratará de un medio de pago de aceptación voluntaria, quedando en manos de la parte que debe pagar la posibilidad de cancelar la obligación en moneda de curso legal.

iv. ¿Qué calificación jurídica merece un criptoactivo derivado de una moneda local?

Un criptoactivo con estas características podría ser considerado como dinero electrónico bajo los términos de la Resolución Nº 6/2014 del Banco Central del Paraguay (el "Marco Normativo Paraguayo de Dinero Electrónico"). El dinero electrónico en Paraguay tiene las siguientes características:

a) Es generado y almacenado en un dispositivo electrónico o en un sistema informático y es utilizable a través de servicios de telecomunicaciones tales como: teléfono móvil, internet u otros dispositivos de acceso o equipos similares.
b) Es aceptado como medio de pago por personas físicas o jurídicas distintas a la EMPE y por esta misma.
c) Es proveído por un importe igual al de los fondos recibidos, deducidas las comisiones y otros cargos legalmente aplicables.
d) Es reconvertible a dinero en efectivo por la EMPE en cualquier momento, según el valor almacenado electrónicamente.
e) No constituye depósito bancario y no genera intereses.

Al respecto de ello, el emisor del dinero electrónico deberá solicitar autorización al Banco Central del Paraguay y asegurarse de cumplir con lo requerido en la normativa citada.

41 El texto completo del aviso puede ser consultado en el siguiente enlace: https://www.bcp.gov.py/comunicado-del-bcp-sobre-monedas-virtuales-o-criptomonedas-n1153 (Fecha de consulta 31 de diciembre de 2019).

q. Perú

i. ¿Hay regulación en materia de criptomonedas?

No existen regulaciones sobre criptomonedas en Perú, más allá de advertencias que han realizados ciertas autoridades nacionales de ese país[42].

ii. ¿Cómo están categorizadas jurídicamente las criptomonedas?

Dado que no existe regulación sobre la materia, es pertinente recurrir a los criterios de la doctrina peruana. En ese sentido, se las puede considerar como bienes incorporables cuyo régimen jurídico debe ser asimilado al de los bienes muebles por aplicación de una ficción legal ad hoc en virtud del comportamiento de las criptomonedas[43].

iii. ¿Puede ser considerado un medio de pago?

En idéntico sentido, dada la inexistencia de regulaciones al respecto, es necesario recurrir a la doctrina para contestar esta pregunta. Siguiendo a esta, las criptomonedas son aptas para funcionar como medios de pago legales en la medida que sean aceptadas de forma voluntaria por las partes[44].

iv. ¿Qué calificación jurídica merece un criptoactivo derivado de una moneda local?

Perú cuenta con normativa en materia de dinero electrónico, a saber, la Ley Nº 29985 (la "Ley Peruana de Dinero Electrónico") junto con el Decreto Supremo Nº 090-2013-EF (el "Decreto Reglamentario de la Ley Peruana de Dinero Electrónico"), y, por lo tanto, siguiendo la definición prevista para este, es posible considerar a estos criptoactivos como dinero electrónico según la normativa mencionada.

42 Se trata de un comunicado de prensa del Banco Central de Reserva del Perú publicado en su cuenta oficial de la red social Twitter, que puede ser consultado en el siguiente enlace https://twitter.com/bcrpoficial/status/1063504017505116160 (Fecha de consulta 31 de diciembre de 2019).

43 Cfr. GUTIÉRREZ, Omar - MORENO, Abraham, "El bitcoin: consideraciones financieras y legales sobre su naturaleza y propuesta para su regulación", *Universidad ESAN*, Lima, 2017, págs. 56 y 57.

44 Cfr. Ibidem, pág. 54.

r. República Dominicana

i. ¿Hay regulación en materia de criptomonedas?

A la fecha del presente informe, no hay regulación formal en materia de criptomonedas en la República Dominicana. Sin perjuicio de ello, el Banco Central de la República Dominicana ha dispuesto un comunicado donde ha brindado una advertencia al público general sobre los riesgos asociados al uso de criptomonedas y ha dejado en claro que ellos no son los encargados de regular el uso y funcionamiento de estas unidades de intercambio[45].

ii. ¿Cómo están categorizadas jurídicamente las criptomonedas?

Dada la inexistencia de normativa al respecto, las criptomonedas deben ser consideradas como bienes inmateriales.

iii. ¿Puede ser considerado un medio de pago?

Siguiendo con las consideraciones del Banco Central de la República Dominicana, el uso de las criptomonedas como medio de pago queda a exclusivo riesgo de las personas que voluntariamente las toman como tal. Es por ello que carecen de curso legal, quedando a decisión de los particulares su aceptación para cancelar obligaciones.

iv. ¿Qué calificación jurídica merece un criptoactivo derivado de una moneda local?

El dinero electrónico está regulado por la Primera Resolución del 18 de diciembre de 2014 de la Junta Monetaria del Banco Central de la República Dominicana (la "Regulación Dominicana del Sistema Nacional de Pagos"). Al respecto de ello, el dinero electrónico se define, conforme el artículo 4 inciso j, como:

> "el valor monetario representado por un crédito exigible a su emisor, expresado en unidades de moneda, con su registro correspondiente y almacenado en medios electrónicos o magnéticos, que permite realizar operaciones de pago"

Al respecto del dinero electrónico en particular, la normativa citada carece de mayores detalles sobre el proceso de emisión y quienes están formalmente autorizados a emitir y gestionar este. Sin perjuicio de ello, considerando que el dinero electrónico forma parte del Sistema Nacional de Pagos, es prudente concluir que solo las entidades autorizadas por la Regulación Dominicana del Sistema Nacional de Pagos a operar en ese sistema son quienes pueden emitir el dinero electrónico. Por lo tanto, este criptoactivo debería ajustarse a estas regulaciones.

45 El texto completo del aviso puede ser consultado en el siguiente enlace: https://cdn.bancentral.gov.do/documents/sala-de-prensa/documents/cronica2017-06.pdf?v=1569542400127 (Fecha de consulta 31 de diciembre de 2019).

S. Uruguay

i. ¿Hay regulación en materia de criptomonedas?

A la fecha del presente informe no hay regulación sobre criptomonedas en Uruguay.

ii. ¿Cómo están categorizadas jurídicamente las criptomonedas?

Dada la inexistencia de normativa al respecto, las criptomonedas deben ser consideradas como bienes inmateriales.

iii. ¿Puede ser considerado un medio de pago?

Ante la ausencia de regulación y pronunciamientos de las autoridades con competencia en la materia, es posible considerar a las criptomonedas como medios de pago de aceptación voluntaria.

iv. ¿Qué calificación jurídica merece un criptoactivo derivado de una moneda local?

El dinero electrónico se encuentra regulado en Uruguay por medio de la Ley Nº 19210 (la "Ley Uruguaya de Dinero Electrónico"). En tal sentido, el artículo 2 de la citada norma define al dinero electrónico como:

> Se entenderá por dinero electrónico los instrumentos representativos de un valor monetario exigible a su emisor, tales como tarjetas prepagas, billeteras electrónicas u otros instrumentos análogos, de acuerdo a lo que establezca la reglamentación, con las siguientes características:
> A) El valor monetario es almacenado en medios electrónicos, tales como un chip en una tarjeta, un teléfono móvil, un disco duro de una computadora o un servidor.
> B) Es aceptado como medio de pago por entidades o personas distintas del emisor y tiene efecto cancelatorio.
> C) Es emitido por un valor igual a los fondos recibidos por el emisor contra su entrega.
> D) Es convertible a efectivo a solicitud del titular, según el importe monetario del instrumento de dinero electrónico emitido no utilizado.
> E) No genera intereses.
> (...)
> Podrán emitir dinero electrónico las instituciones de intermediación financiera y las instituciones emisoras de dinero electrónico, habilitadas a tales efectos por el Banco Central del Uruguay.

Al respecto de ello, el Banco Central de Uruguay reglamentó la actividad de las empresas emisoras de dinero electrónico por medio de la Circular Nº 2198.

t. Venezuela

i. ¿Hay regulación en materia de criptomonedas?

Sí. Tal como señalamos antes, existe el Decreto Constituyente sobre el Sistema Integral de Criptoactivos. Agregado a esta norma, la Providencia Nº 008-2019 del 4 de febrero de 2019 regula el Registro Integral de Servicios en Criptoactivos (RISEC), publicada en la Gaceta Oficial de la República Bolivariana de Venezuela N° 41.578 de esa misma fecha (la "Providencia Venezolana sobre el RISEC"); la Providencia Administrativa Nº 009-2019 del 5 de febrero de 2019, mediante la cual se establecen los requisitos y trámites para el envío y recepción de Remesas en criptoactivos a personas naturales en el territorio de la República Bolivariana de Venezuela, publicada en la Gaceta Oficial de la República Bolivariana de Venezuela N° 41.581 del 7 de febrero de 2019 (la "Providencia Venezolana sobre remesas en criptoactivos"), y la Providencia Administrativa Nº 012-2019 del 29 de marzo de 2019, mediante la cual se regula la operatividad de las Casas de Intercambio en el Sistema Integral de Criptoactivos, publicada en la Gaceta Oficial de la República Bolivariana de Venezuela N° 41.609 del 3 de abril de 2019 (la "Providencia Venezolana sobre Exchanges").

ii. ¿Cómo están categorizadas jurídicamente las criptomonedas?

Conforme el artículo 5 del Decreto Venezolano del Sistema Integral de Criptoactivos, se distinguen dos tipos de criptoactivos: los simples y los soberanos. Los primeros son activos digitales que usan criptografía y sistemas de registro descentralizados mientras que los segundos son activos digitales emitidos por la República Bolivariana de Venezuela.

Al margen de las definiciones generales del marco normativo venezolano, la Providencia Venezolana sobre Exchanges brinda una definición especial sobre criptomonedas en su artículo 3, a saber:

> Es un activo digital que es principalmente utilizado como medio de intercambio, el cual se vale de la criptografía para otorgarle seguridad a sus transacciones, controlar la creación de nuevas unidades y verificar su transferencia, en sede del sistema de base de datos con seguridad bajo el cual éstas operan y por virtud del cual se hace el seguimiento y verificación de pagos (cadena de bloques o *Blockchain*). Los criptoactivos podrán cumplir, entre otras, funciones como medio de transferencia de valor, medio de pago, propiedad de almacenamiento de valor y programación de contratos inteligentes.

De la lectura de las normas podría, por lo tanto, reconocerse que las criptomonedas son monedas en Venezuela. Sin embargo, están sujetas a fuertes regulaciones, que incluyen la obligatoriedad de declarar ante el Estado venezolano toda adquisición y uso de criptomonedas en el Registro Integral de Servicios en Criptoactivos.

iii. ¿Puede ser considerado un medio de pago?

Sí, conforme las definiciones brindadas en el punto ii., es posible considerar a las criptomonedas como medios de pago, aunque no surge del texto legal analizado si tienen curso legal o no.

iv. ¿Qué calificación jurídica merece un criptoactivo derivado de una moneda local?

Este criptoactivo estaría encuadrado en las normas reseñadas en el punto ii. Por lo tanto, se deberá dar cumplimiento a la normativa reseñada en el punto i.

u. Otros casos con reglamentación especial en materia de criptomonedas

Con relación a lo que han realizado otras jurisdicciones en materia de criptomonedas, consideramos que todas van en la misma dirección, aunque con distintos matices. La postura universal que se ha adoptado es la de no tratar a las criptomonedas como monedas, ya sean nacionales o extranjeras. Sin embargo, hay diferencias en su calificación como medio de pago y, consecuentemente, su situación tributaria. En ese sentido, la legislación se divide en dos grandes grupos: los que admiten a las criptomonedas como medios de pago y, por lo tanto, les dan tratamiento fiscal apropiado para evitar situaciones que puedan resultar perjudiciales para su uso como tales; y, por el otro lado, las jurisdicciones donde las criptomonedas son simplemente activos.

Conclusiones 7 Conclusiones

El presente informe ha recorrido la regulación existente y de aplicación en relación a tres grandes ejes temáticos: identidades, *blockchain* y criptomonedas. Este acercamiento a la regulación pretendía esclarecer aquellos aspectos que intervienen en la implementación de una solución digital de identidad auto soberana sobre *blockchain*, y la posibilidad de incorporar una billetera digital para la gestión de criptoactivos, como la que propone el proyecto DIDI, llevado a cabo por la Asociación Civil DECODES y BID Lab.

El análisis llevado a cabo en el presente documento revela que los países latinoamericanos no se encontrarían en condiciones de dar apoyo normativo a un proyecto que incluya estos tres componentes y, por lo tanto, sería conveniente avanzar en estrategias que aseguren las condiciones para avanzar en su implementación, ya sea incluyendo todos sus componentes, o algunos de ellos. Dentro de las estrategias posibles, se propone: (i) realizar una actividad de interpretación normativa y de diseño de estructuras legales que permita la realización de un proyecto para el desarrollo de identidad digital auto soberana; y (ii) introducir un paquete normativo específico para apoyar este tipo de proyectos. Esta segunda alternativa resulta más compleja dado que requiere de regulaciones federales o nacionales, según el país, y en consecuencia puede ser dificultoso obtener su aprobación. De todas formas, este informe contiene una propuesta de principios que podría orientar la elaboración de dicha regulación. Por este motivo, resulta conveniente y recomendable avanzar en la primera actividad propuesta, la cual comprende la interpretación de las normas en juego para el diseño y ejecución de las estructuras legales pertinentes con apoyo legal local.

La identidad es el componente que menor interpretación normativa requiere para desplegar una solución de identidad digital auto soberana de forma exitosa y en cumplimiento

Conclusiones
siones Conclu

con la normativa de cada país. Al respecto, durante la preparación de este informe fue posible la identificación de dos etapas: la etapa de creación o construcción de la identidad; y la etapa de uso de la identidad. Cada etapa presenta sus particularidades y demanda diferentes esfuerzos interpretativos dentro de los actuales marcos normativos.

Todas las regulaciones en América Latina consideran a la persona como el titular de los datos y como la única que está en condiciones de determinar cómo serán tratados. Esto se alinea con el espíritu de los proyectos de identidad digital auto soberana sobre *blockchain*, en tanto proponen construir una identidad digital que certifique y valide datos sociales, cívicos y económicos, a través de la emisión de credenciales verificables, a partir de información certificada por terceros (instituciones o individuos) y que garantice los requisitos de i) privacidad, ii) control, y iii) portabilidad, eliminando el control externo centralizado bajo el dominio de múltiples instituciones privadas vigente hasta ahora (Tobin & Reed, 2016)[46].

En lo que respecta a la fase de uso de los datos que conforman la identidad, los usuarios de DIDI estarían protegidos por las normas de protección de datos personales. En este sentido, todo uso de los datos de identidad almacenados en la solución propuesta por DIDI (ai·di *app*) por parte de un tercero que tiene una relación con el usuario debe cumplir con las obligaciones que le impone esas reglas. Es decir, y siguiendo las recomendaciones de la Unión Europea, las interacciones que los usuarios de ai·di mantengan con terceros seguirán siendo relaciones "titular de los datos – responsable del tratamiento", aunque con un mayor nivel de control por parte de los usuarios gracias a la infraestructura de DIDI.

46 Cfr. TOBIN, A. & REED, D. (2016) "The Inevitable Rise of Self-Sovereign Identity", en Evernym White papers, https://www.evernym.com/wp-content/uploads/2017/07/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf

Es importante destacar que el sistema de identidad auto soberana propuesto por DIDI se encuentra en las fases finales de desarrollo e iniciales de implementación, y que la experiencia seguramente proporcione mayores herramientas y conclusiones para futuras implementaciones. En todo caso, el objetivo de estos sistemas es poner al usuario en control real de su identidad. Si la cantidad de interacciones que demandan la atención del usuario se vuelven excesivas, al punto que el sistema pierde su sentido original, será crucial disponer medidas regulatorias para proteger a la persona y resguardarse de potenciales abusos por parte de los responsables del tratamiento de los datos pretendidos con la información del individuo. Es así que las interacciones que el usuario mantenga con terceros deberían ser diseñadas poniendo el foco en la minimización de la recolección de datos y estructurando las operaciones que hagan uso de los datos del usuario para resguardar su privacidad en todo momento.

El mayor desafío de los sistemas de identidad digital está dado por la etapa de construcción de la identidad. Tal como se ha mencionado, el mayor interrogante está puesto sobre si los usuarios pueden ser considerados como responsables del tratamiento de esta etapa. La respuesta a esta pregunta configura como serán las relaciones entre el usuario de ai·di y los terceros que intervengan durante los primeros pasos de la identidad digital de la persona, en particular en lo que hace a la base legal para tratar esos datos personales, así como también quien tiene que informar sobre las características del tratamiento al usuario. En este sentido, la determinación de potestades al momento de diseñar un sistema de identidad digital auto soberana es crucial; mientras más facultades de organización queden en cabeza de quienes ponen en funcionamiento estas soluciones informáticas, habrá más elementos para sostener que el usuario no es el responsable del tratamiento y que esos desarrolladores podrían estar actuando como responsables. De la misma manera, mientras menos obligaciones asuman quienes pongan en funcionamiento estos sistemas, menos tendrán elementos para sostener que estos son quiénes definen cómo y para qué se usan los datos.

En lo que hace al uso de la tecnología *blockchain*, es importante señalar que no debería ser analizada en forma aislada y abstracta, sino que debería tomarse en consideración su uso efectivo y los efectos jurídicos perseguidos con la operación para la cual se usa. En ese sentido, dentro del modelo de identidad digital auto soberana de DIDI, la tecnología se utiliza para firmar la emisión, revocación o validación, según el caso, de documentos o credenciales; es decir, se utiliza la tecnología *blockchain* para firmar expresiones o declaraciones digitales por parte del usuario sobre ciertos hechos, o para que una entidad emisora certifique que una persona es portadora de ciertos atributos que tienen que ver con su identidad. Por lo tanto, en este punto será necesario una mayor tarea interpretativa para darle efectos jurídicos plenos a los actos que se pretendan realizar desde el software a ser desplegado. Esto se resolvería mediante una modificación a las normativas de firma electrónica para permitir que, una vez validada la identidad, toda firma realizada desde el software que acredite la misma sea equiparada a una firma manuscrita.

Finalmente, en caso de que se decida avanzar en la emisión de criptoactivos a favor de las personas a partir de la entrega de dinero fiduciario, los mismos pueden ser calificados, a falta de regulación expresa sobre este tipo de criptoactivos, como dinero electrónico por su similitud jurídica con este tipo de bienes. Dado que se trata de una situación ampliamente reglada en el derecho, sería pertinente dar lugar a la aplicación de aquellas normas para tutelar y proteger a los particulares.

rincipios para ación 8 Propue para una posib

8 Propuesta de principios para una posible regulación en materia de identidad digital autosoberana

Como parte de las conclusiones del presente informe, se adjuntan a continuación recomendaciones generales que deberían ser tenidas en cuenta para la adaptación del marco normativo o, en aquellos casos donde sea necesario crearlo, para darle cobertura normativa expresa a un proyecto de identidad digital auto soberana mediante la utilización de tecnología *blockchain*.

Estas recomendaciones podrían sufrir modificaciones en función de la experiencia recogida en la práctica y de los avances en el estado del arte. Es decir, hasta la actualización final de este reporte no debe considerarse a este documento como la propuesta final sino como una invitación a la reflexión y el debate en torno a las soluciones de identidad digital auto soberana y gestión de criptoactivos.

a una posible r
esta de princip
ble regulación

Recomendaciones de áreas de acción normativa para los sistemas de inclusion social mediante la implentacion de sistemas de identidad digital auto soberana

1. Todo sistema de identidad digital basado en tecnología *blockchain* o de registros distribuidos debería anteponer los intereses del titular de los datos personales por sobre los intereses que terceros pudieran tener sobre ellos.
2. La participación en sistemas de identidad digital no debiera ser obligatoria sino voluntaria: en todo momento, el usuario debería ser capaz de eliminar su perfil de forma plena. De lo contrario, se vulneraría la base misma sobre la cual se construye la idea de identidad digital auto soberana.
3. La base legal para todo tratamiento de datos que se haga a partir de información que forme parte del perfil del usuario debería contar con su consentimiento expreso e informado, conforme sea establecido en la normativa aplicable de protección de datos personales.
4. El uso de los datos de la persona por parte de terceros debería estar precedido por la provisión clara y sencilla sobre qué datos pretenden usarse, cómo serán usados y qué terceros tendrán acceso a ellos.
5. La información y solicitud de consentimiento deberían hacerse de forma que no resulte en un agotamiento de la atención del usuario, debiendo, antes que todo, hacer un ejercicio de minimización de los datos que pretenden usarse antes de la efectiva recolección.
6. La seguridad informática de los sistemas de identidad digital auto soberana es de crucial importancia. Los desarrollos realizados deberían seguir el estado del arte, tanto al momento de su creación como durante su vida.
7. El software sobre el que funciona el sistema de identidad auto soberana debería ser claro en relación a qué puede hacer el usuario con el sistema y cómo lo puede hacer.
8. Los desarrolladores del software deberían estructurar los sistemas de identidad de forma que la privacidad de los usuarios se encuentre resguardada por defecto, es decir, el software debería ser diseñado usando como criterio rector la privacidad de las personas.
9. Todo marco regulatorio en torno a estos desarrollos debería ser tecnológicamente neutro para permitir el desarrollo de soluciones usando tecnologías presentes y futuras.

Glosario

AAIP: Agencia de Acceso a la Información Pública de la República Argentina, autoridad de control de la Ley Argentina de Protección de Datos Personales.

BID: Banco Interamericano de Desarrollo.

CDN: Convención sobre los Derechos de los Niños, aprobada como tratado internacional de derechos humanos el 20 de noviembre de 1989.

CCyCN: el Código Civil y Comercial de la Nación de la República Argentina.

Código Salvadoreño de Familia: Decreto Nº 677 del 11 de octubre de 1993.

Decreto Colombiano del Estatuto del Registro del Estado Civil de las Persona: el Decreto Nº 1260 de 1970

Decreto Guatemalteco de Firma Electrónica: Decreto Nº 47/2008.

Decreto Reglamentario de la Ley Salvadoreña del Registro Nacional de las Personas Naturales: el Decreto Nº 34 del 23 de mayo de 2000.

Decreto Reglamentario de la Ley Peruana de Dinero Electrónico: Decreto Supremo Nº 090-2013-EF.

Decreto Reglamentario de la Ley Peruana de Firma Digital: Decreto Supremo Nº 052-2008-PCM.

Decreto Salvadoreño Reglamentario de la Ley Salvadoreña del Registro Nacional de las Personas Naturales: Decreto Nº 34 del 23 de mayo de 2000.

Decreto Uruguayo de Servicios de Confianza: Decreto Nº 70/18.

DUDH: la Declaración Universal de Derechos Humanos de Naciones Unidas, adoptada y proclamada por la Asamblea General en su resolución 217 A (III), de 10 de diciembre de 1948.

Decreto Venezolano del Sistema Integral de Criptoactivos: Decreto Constituyente sobre el Sistema Integral de Criptoactivos publicada en la Gaceta Oficial de la República Bolivariana de Venezuela Nº 41.575 de fecha 30 de enero de 2019.

Ley Argentina de Firma Digital: la Ley Nº 25.506.

Ley Argentina de Protección de Datos Personales: Ley Nº 25.326 con sus modificaciones y normativa complementaria.

Ley Brasileña de Dinero Electrónico: Ley Nº 12.865.

Ley Brasilera de Protección de Datos Personales: Ley Nº 13.709 de 14 agosto de 2018.

Ley Brasilera del Registro Civil: Ley Nº 6015 del 31 de septiembre de 1973.

Ley Brasilera sobre Identifiación Civil Nacional: Ley Nº 13444 del 11 de mayo de 2017.

Ley Boliviana de TICs: Ley Nº 164, de 8 de agosto de 2011, General de Telecomunicaciones, Tecnologías de la Información y Comunicación.

Ley Boliviana del SEGIP: Ley del Servicio General de Identificación Personal y del Servicio General de Licencias Para Conducir 27 de junio de 2011.

Ley Chilena de Autorización a la Emisión y Operación de Medios de Pago con Provisión de Fondos por Entidades No Bancarias: Ley Nº 20.950

Ley Chilena de Firma Digital: Ley Nº 19.799

Ley Chilena de Protección de Datos Personales: la Ley Nº 19.628.

Ley Chilena del Registro Civil: Ley Nº 19.477

Ley Colombiana de Dinero Electrónico: Ley Nº 1735 de 2014.

Ley Colombiana de Firma Digital: Ley Nº 527 de 1999.

Ley Colombia de Protección de Datos Personales: la Ley Nº 1581 de 17 de octubre de 2012 junto con el Decreto Nº 1377/2013.

Ley Colombia del Documento Nacional: Ley Nº 39 de 1961.

Ley Costarricense de Firma Digital: Ley Nº 8454.

Ley Costarricense de Protección de Datos Personales: la Ley Nº 8968.

Ley Costarricense del Registro Civil: Ley Nº 3504.

Ley Cubana de Procedimiento Civil, Administrativo y Laboral: Ley Nº 7 del 19 de agosto de 1977 junto con su reforma de 2006.

Ley Cubana del Sistema de Identificación Cubana: Decreto-Ley 248.

Ley Dominicana de Firma Electrónica: Ley Nº 126 de 19 de marzo de 2002

Ley Dominicana de la Cédula de Identidad: Ley Nº 8 del 13 de abril de 1992 y su modificación por la Ley Nº 26 del 1 de febrero de 2001

Ley Dominicana de Protección de Datos: La Ley Nº 172-13.

Ley Dominicana del Registro Civil: Ley Nº 659 del 17 de julio de 1994

Ley Ecuatoriana de E-Commerce: la Ley Nº 67, de 17 de Abril del 2002, de Comercio Electrónico, Firmas y Mensajes de Datos.

Ley Ecuatoriana de Identidad: Ley Orgánica de Gestión de la Identidad y Datos Civiles publicada en el Segundo Suplemento al Registro Oficial No. 684 de febrero 4 de 2016.

Ley Guatemalteca del Registro Nacional de las Personas: Decreto 90/2005.

Ley Haitiana de Firma Electrónica: la ley sobre firmas electrónicas del 17 de Marzo de 2017.

Ley Hondureña de Firma Electrónica: Decreto Nº 149-2013.

Ley Hondureña del Registro Nacional de las Personas: el Decreto Nº 62/2004, junto con sus modificaciones del Decreto Nº 108/2007 y Nº 20/2009.

Ley Hondureña del Sistema de Pago y Liquidación de Valores: Decreto Nº 46-2015.

Ley Hondureña del Sistema Financiero: Decreto Nº 129-2004.

Ley Mexicana de Firma Electrónica: Ley publicada en el Diario Oficial de la Federación el 11 de enero de 2012.

Ley Mexicana Fintech: Ley publicada en el Diario Oficial de la Federación el 9 de marzo de 2018.

Ley Mexicana General de Población: Ley publicada en el Diario Oficial de la Federación el 7 de enero de 1974 y su última reforma publicada en el Diario Oficial de la Federación el 12 de julio de 2018.

Ley Nicaragüeña de Identidad: la Ley Nº 152.

Ley Nicaragüense de Protección de Datos: la Ley Nº 787.

Ley Panameña de Firma Electrónica: Ley Nº 51 de 2008.

Ley Panameña de Protección de Datos: la Ley Nº 81 de 26 de marzo de 2019.

Ley Panameña del Documento de Identidad: Ley Nº 68 de 2015

Ley Panameña del Registro Civil: Ley Nº 31 de 2006 junto con su modificación por la Ley Nº 17 de 2007.

Ley Paraguaya de Firma Electrónica: Ley Nº 4610.

Ley Paraguaya de la Policía: Ley Nº 222.

Ley Paraguaya de Protección de Datos: la Ley Nº 1682 con su modificación por la Ley Nº 1969.

Ley Paraguaya del Registro Civil: Ley Nº 1266.

Ley Peruana de Dinero Electrónico: la Ley Nº 29985.

Ley Peruana de Firma Digital: la Ley Nº 27.269

Ley Peruana de Identidad Digital: el Decreto Legislativo Nº 1412 de 13 de Septiembre del 2018.

Ley Peruana de Protección de Datos: la Ley Nº 29.733.

Glosario

Ley Salvadoreña de Dinero Electrónico: Ley Nº 72 del 13 de agosto de 2015.

Ley Salvadoreña de Firma Electrónica: el Decreto Nº 133 del 1 de octubre de 2015.

Ley Salvadoreña del Registro Nacional de las Personas Naturales: la Ley Nº 552 del 21 de diciembre de 1995.

Ley Salvadoreña Reguladora de la Emisión del Documento Único de Identidad: la Ley Nº 581 del 18 de octubre de 2001.

Ley Uruguaya de Dinero Electrónico: Ley Nº 19210.

Ley Uruguaya de Firma Electrónica: Ley Nº 18.600.

Ley Uruguay de Identificación Civil: Ley Nº 14762.

Ley Uruguaya de Protección de Datos: la Ley Nº 18.331.

Ley Uruguay del Registro Civil: Ley Nº 1430 y sus modificatorias.

Ley Venezolana de Firma Electrónica: Decreto N° 1.204 de fecha 10 de febrero de 2001, con Fuerza de Ley de Mensaje de Datos y Firmas Electrónicas, publicada en la Gaceta Oficial de la República Bolivariana de Venezuela Nº 37.148 de fecha 28 de febrero de 2001.

Ley Venezolana de Identificación: Ley publicada en Gaceta Oficial Nº 38.458 de fecha 14 de Junio del 2006 junto con el Decreto N° 1.412 de fecha 13 de noviembre de 2014, con Rango, Valor y Fuerza de Ley de Reforma de la Ley Orgánica de Identificación, publicado en la Gaceta Oficial de la República Bolivariana de Venezuela Nº 6.155 Extraordinario de fecha 19 de noviembre de 2014.

Ley Venezolana del Registro Civil: Ley publicada en Gaceta Oficial Número 39.264 de fecha martes 15 de septiembre de 2009.

Marco Normativo Brasileño de Firma Digital: Medida Provisional Nº 2.200-2 de 24 de agosto de 2001.

Marco Normativo Boliviano de Dinero Electrónico: Resolución de Directorio Nº 134/2015 junto con la Resolución de Directorio Nº 166/2015, ambas del Banco Central Boliviano.

Marco Normativo Nicaragüense de Dinero Electrónico: Resolución N° CD-SIBOIF-725-1-ABR26-2012 de fecha 26 de abril de 2012.

Marco Normativo Paraguayo de Dinero Electrónico: Resolución Nº 6/2014 del Banco Central del Paraguay.

ONG Bitcoin Argentina: Asociación Civil para el Desarrollo de Ecosistemas Descentralizados. (DECODES)

Pacto San Jose de Costa Rica: la Convención Americana Sobre Derechos Humanos suscrita en la conferencia especializada interamericana sobre derechos humanos (B-32) en San José de Costa Rica el 7 al 22 de noviembre de 1969.

PIDCP: el Pacto Internacional de Derechos Civiles y Políticos, adoptado y abierto a la firma, ratificación y adhesión por la Asamblea General en su resolución 2200 A (XXI), de 16 de diciembre de 1966.

Providencia Venezolana sobre el RISEC: Providencia Nº 008-2019 de fecha 4 de febrero de 2019, mediante la cual se regula el Registro Integral de Servicios en Criptoactivos, publicada en la Gaceta Oficial de la República Bolivariana de Venezuela N° 41.578 de esa misma fecha.

Providencia Venezolana sobre Exchanges: Providencia Administrativa Nº 012-2019 de fecha 29 de marzo de 2019, mediante la cual se regula la operatividad de las Casas de Intercambio en el Sistema Integral de Criptoactivos, publicada en la Gaceta Oficial de la República Bolivariana de Venezuela N° 41.609 de fecha 3 de abril de 2019.

Providencia Venezolana sobre remesas en criptoactivos: Providencia Administrativa Nº 009-2019 de fecha 5 de febrero de 2019, mediante la cual se establecen los requisitos y trámites para el envío y recepción de Remesas en criptoactivos a personas naturales en el territorio de la República Bolivariana de Venezuela, publicada en la Gaceta Oficial de la República Bolivariana de Venezuela N° 41.581 de fecha 7 de febrero de 2019.

Reglamento Cubano sobre el funcionamiento de la Infraestructura de Llave Pública: Resolución Nº 2/2016 del Ministerio del Interior cubano.

Reglamento eIDAS: 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.

Regulación Dominicana del Sistema Nacional de Pagos: Primera Resolución del 18 de diciembre de 2014 de la Junta Monetaria del Banco Central de la República Dominicana.

RISEC: Registro Integral de Servicios en Criptoactivos.

RGPD: Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

Reglamentación Mexicana de Criptoactivos: Circular 4/2019.

SEGIP: el Servicio General de Identificación Personal.

Realizado por: A. Chomczyk, J. Madariaga, E. Molina, M Allende.
Editado en el mes de octubre de 2020 en Buenos Aires, Argentina.

Regulación bl
blockchain id
identidad digi
digital Améric
América Latin
atina Regulac
ción blockcha
identidad digi
digital Améric
tina Regulació