IDENTIDAD DIGITAL AUTO-SOBERANA

El futuro de la identidad digital: auto-soberanía, billeteras digitales y blockchain

BID BID | LAB LACCHAIN

IDENTIDAD DIGITAL AUTO-SOBERANA

El futuro de la identidad digital: auto-soberanía, billeteras digitales y blockchain

Autor: Marcos Allende López (@marcosallendeL)
Supervisado por: Marcelo Da Silva, Alejandro Pardo Vegezzi

Diseño: .Puntoaparte Editores

Este documento ha sido producido en colaboración con todos los miembros del grupo de trabajo de identidad digital de la Alianza Global LACChain. Sin las aportaciones directas e indirectas de todos y cada uno de los miembros de este grupo esta publicación no existiría. Asimismo, especial reconocimiento para Kenneth Foley, Ignacio Alamillo, Suzana Maranhão, Paula Ventoso, Melissa Julian, Melissa Penteado, Mariano Sturla, María Weisson, Rubén Cessa, Andrea Ortega, Itzel Nava, Daniel Zárate, y para el equipo de .Puntoaparte Editores por sus contribuciones esenciales de distinta índole. Toda la gratitud para con Nuria Simo e Irene Arias por su apoyo fundamental en todo este proyecto. Por último, el documento va especialmente dedicado a Marcelo Da Silva y Alejandro Pardo, con mucho cariño y gran aprecio, por hacerlo posible.

Autor: Marcos Allende López.

Colaboradores: Moisés Menéndez Andrés, Oscar Bazoberry, Ismael Arribas, Albi Rodríguez Jaramillo, David Ammouial, Juan José Miranda, Pelle Braendgaard, Andrew Hughes, Zaira Pérez, Antonio Leal, Adrián Pareja, Sergio Cerón, Diego Lopez, David Peces, Guillermo Villanueva, Pedro Perrotta, Jaime Centellas, Sergio Bazoberry y Jesus Ruiz.

Revisores: Ignacio Alamillo, Pelle Braendgaard, Kenneth Foley, Suzana Maranhão, Moises Menendez y Ismael Arribas.

Supervisado por: Marcelo Da Silva y Alejandro Pardo Vegezzi.

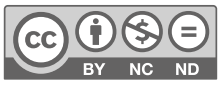


Tabla de contenidos

IDENTIDAD DIGITAL AUTO-SOBERANA

Parte I

El futuro de la identidad

Identidad digital auto-soberana

BID BID | LAB LACCHAIN

Vivimos en un mundo en el que una gran parte de la población tiene acceso a grandes avances tecnológicos que hace unas pocas decenas de años eran impensables pero que hoy son parte de su vida diaria, como poder volar de un lugar a otro cualquiera del planeta en el mismo día o poder comunicarse a distancia con otra persona en una videollamada a tiempo real usando dispositivos inalámbricos. Sin embargo, al mismo tiempo somos también testigos de las deficiencias tecnológicas y el estado mucho menos avanzado de otros campos, como el de los sistemas de identificación y autenticación de personas, tanto presencial como digital, y la desprotección ante el tráfico y el uso de nuestros datos personales en internet.

El mecanismo de identificación y autenticación presencial más confiable que se utiliza hoy en día en la inmensa mayoría de los lugares donde necesitan saber quiénes somos consiste en solicitarnos un documento oficial de identidad con una fotografía y hacer una comparación visual. Muy raramente el verificador cuenta con tecnología que le permita comprobar que el documento de identidad no sea falso, y solamente en lugares muy puntuales se lleva a cabo una verificación biométrica para asegurar que efectivamente somos el dueño o la dueña de ese documento de identidad.

En cuanto a la identificación y autenticación digitales, solamente unos pocos países ofrecen a sus ciudadanos una tarjeta o ID electrónico que les permite acceder a servicios electrónicos de manera autenticada. Sin embargo, incluso en los países más avanzados, estos servicios están generalmente limitados a aquellos que ofrecen la administración pública, no pudiendo usarse estos ID electrónicos para acceder a servicios ofrecidos por entidades privadas.

La falta de tecnología en materia de identidad tiene grandes consecuencias negativas. En el día a día, son frecuentes la indocumentación de personas, la falsificación de documentos de identidad, la usurpación de identidad o la pérdida de documentos de identidad. En poblaciones vulnerables expuestas a catástrofes naturales o forzadas a la migración, la situación es mucho más crítica, pues se cuentan en millones las personas que cada año no solo se quedan sin hogar sino que no disponen los documentos que les permitirían probar quiénes son, de dónde vienen o qué formación y experiencia profesional tienen.

Adicionalmente, el hecho de que los sistemas de identificación y autenticación electrónica de individuos sean casi inexistentes limita la digitalización de muchos servicios, genera monopolios de entidades intermediarias que ofrecen confianza entre las dos partes interactuantes, hace casi imposible la verificación de las fuentes de información y es una traba para la protección de datos y la privacidad de las personas.

En los últimos años se han venido desarrollando un conjunto de estándares, protocolos y tecnologías que buscan ofrecer un nuevo concepto de identidad al alcance de todos, barata, segura y escalable, que pueda solucionar los problemas actuales presentes en

la identificación y autenticación de personas dándole además al individuo un control total sobre su persona digital. Este nuevo modelo de identidad se conoce como identidad digital auto-soberana e incorpora dos elementos tecnológicos innovadores: las billeteras digitales y los registros descentralizados de información.

Dado que su nombre puede dar lugar a confusiones, es importante aclarar que la identidad digital auto-soberana no consiste en que los individuos se certifiquen su propia identidad. Mientras las sociedades sigan organizándose políticamente en sistemas no anárquicos con entidades de gobierno bien definidas que garanticen el desarrollo y cumplimiento de políticas regulatorias y permitan el establecimiento de acuerdos y marcos de confianza públicos y privados, nacionales e internacionales, seguirán siendo las administraciones públicas quienes tengan la soberanía última de la identificación de los ciudadanos.

Por tanto, lo que la identidad auto-soberana propone es una soberanía para el individuo no en la emisión de la identidad sino en su administración y presentación a terceros. En primer lugar, este modelo habilita que los individuos tengan soberanía en la administración y manejo de sus activos y credenciales digitales -como por ejemplo un pasaporte digital, un título académico, un título de propiedad, o divisas como dólares, euros, libras o pesos tokenizados- usando billeteras digitales personales y portables como por ejemplo un aplicativo móvil. En segundo lugar, elimina la necesidad de que la entidad tercera a la que se le presente un activo digital tenga que acudir directamente al emisor para comprobar su veracidad o validez, pues puede hacerlo contra un registro público y descentralizado como son las redes blockchain.

IDENTIDAD DIGITAL AUTO-SOBERANA

Bloque 1
Identidad

1.1. Definición

La identidad de una persona, organización, cosa o proceso es todo aquello que lo caracteriza. En un individuo, la identidad abarca desde características físicas, género, información biométrica o experiencias, hasta pertenencias, diplomas o propiedades. Por lo tanto, podríamos decir que existen infinitos atributos que conforman la identidad de una persona y la mayoría de ellos se encuentran en constante cambio y evolución.

Siendo así, resulta casi imposible recopilar o enlistar todos estos atributos al mismo tiempo o en un único lugar. Sin embargo, sí podemos reunir subconjuntos determinados y acotados de atributos que sean lo suficientemente exclusivos como para ser diferentes de los de cualquier otra persona, lo que los hace únicos. Ser capaces de definir, recopilar, presentar y verificar estos subconjuntos de manera estandarizada permite a los seres humanos no solo tener una identidad, sino también poder probarla ante terceros, es decir, autenticarse.

La autenticación de una persona ante terceros consiste en convencerles de que puede ser reconocida de manera confiable en base a un conjunto de identificadores y/o atributos. Esto se basa generalmente en información recogida en certificados o documentos (por ejemplo, un pasaporte) emitidos o validados por una entidad confiable. Esta entidad es, a menudo, algún tipo de "autoridad" o, al menos, se le atribuye la capacidad reconocer y recordar individuos (por ejemplo, una administración pública).

El concepto de identidad ha sido definido en distintas normas y estándares de manera similar:

"La identidad es la representación de una entidad en forma de uno o más atributos que permiten que la entidad o entidades se distingan suficientemente en su contexto."– UIT (ITU, 2018)

"La identidad es un conjunto de atributos relacionados con una entidad." – ISO/IEC 24760-1 (ISO, 2019)

1.2. La identificación como un derecho humano

De acuerdo con la ISO/IEC 24760-1, "la identificación es el proceso de reconocer una entidad en un dominio particular como distinta de otras entidades" (ISO, 2019). La identificación es esencial para solicitar y otorgar acceso a servicios de todo tipo. Paradójicamente, la Declaración Universal de Derechos Humanos (DUDH) no menciona la palabra identidad ni una sola vez, ni tampoco reconoce explícitamente el derecho a ser identificado. Sin embargo, sí reconoce "el derecho de todo ser humano al reconocimiento de su personalidad jurídica en cualquier lugar" en su Artículo 6, el "derecho a una nacionalidad" en su Artículo 15 y el "derecho a la propiedad privada" en su Artículo 17 (ONU, 1948). Para garantizar los anteriores derechos, las personas han de ser identificables. De ahí que entendamos que el derecho a tener una identidad y a ser identificable se reconoce en la DUDH de forma implícita.

El Grupo Interinstitucional de Expertos sobre los indicadores de los Objetivos de Desarrollo Sostenible (GIE-ODS) publicó en 2016 una lista final de indicadores de los Objetivos de Desarrollo Sostenible como punto de partida práctico para las Naciones Unidas. El objetivo 16.9 de este documento establece que se debe conseguir "de aquí a 2030, proporcionar acceso a una identidad jurídica para todos, en particular mediante el registro de nacimientos". (SDG, 2016)

En la actualidad, en la mayoría de los países y regiones del mundo, los gobiernos son responsables de proporcionarnos nuestro primer identificador de identidad, así como una credencial asociada: el certificado de nacimiento. La acción esencial tras este proceso no es otra que el registro de información en un registro civil que presumiblemente será gestionado y mantenido en el tiempo. Esta información puede incluir nombres, fecha y lugar de nacimiento, nacionalidad, padres, características

físicas, etc. Siendo así, el responsable legal del recién nacido recibe una credencial o certificado que acredita la información presente en el registro.

Posteriormente, a lo largo de nuestra vida, generamos toneladas de información identificable y se nos otorgan credenciales y titulaciones que, al igual que nuestro certificado de nacimiento, nos permiten demostrar quiénes somos frente a los demás. Algunos ejemplos son nuestros documentos de identidad emitidos por gobiernos, nuestros diplomas académicos, nuestros títulos de propiedad o nuestra huella digital, que incluye por ejemplo la información que compartimos en redes sociales.

Según las estimaciones del conjunto de datos identificación para el desarrollo del Banco Mundial, a febrero de 2016 alrededor de mil millones de personas en todo el mundo carecían de prueba de identidad alguna (WB-ID4D, 2018), lo que representa un 14% de la población mundial. Por lo tanto, existe un grave problema con el funcionamiento de la identificación hoy en día, pues no solo se está impidiendo la provisión de un derecho humano a 3 de cada 20 personas en el mundo, sino que de manera indirecta también se están produciendo enormes limitaciones para el desarrollo y la inclusión social y financiera, como veremos en el Bloque 4.

Desde principios del siglo XX, la llegada de Internet tal y como lo conocemos, los teléfonos inteligentes y el Internet de las cosas (IoT por su nombre en inglés) han cambiado el tipo de servicios que consumimos, así como la forma en que socializamos como el resto de los seres humanos. La digitalización de nuestras vidas ha introducido nuevos desafíos y oportunidades para la identificación de individuos y, consecuentemente, la identificación e identidad digital son ahora esenciales en cualquier sociedad.

IDENTIDAD DIGITAL AUTO-SOBERANA

Bloque 2
Identidad digital

2.1. Definición

Como ampliación del concepto de identidad, se puede definir la identidad digital como un conjunto finito de atributos que permite a una persona, animal, cosa o proceso ser identificado como único y probar su identidad frente a terceros electrónicamente. Nuestra persona digital se compone de varias identidades digitales, estando a su vez cada una de estas identidades representada por uno o varios identificadores y atributos que son únicos en un contexto específico.

La verificación de la identidad digital presenta algunos desafíos como, por ejemplo, el hecho de que ya no sea posible comparar visualmente las características físicas de un individuo con las de un documento oficial de identidad para verificar quién es. Sin embargo, al mismo tiempo ofrece enormes ventajas pues nos permite tener acceso a todo tipo de servicios digitales globales, abriéndonos así un amplio abanico de posibilidades, muchas de ellas en materia de inclusión. Por ejemplo, la identidad digital permite prestar servicios de forma remota y en tiempo real a comunidades y poblaciones que no pueden recibirlos en persona por razones diversas.

Según el Banco Mundial, las identidades digitales se crean y utilizan como parte de un ciclo vital que se compone de cuatro etapas: (a) registro, incluyendo inscripción y validación, (b) emisión de documentos o credenciales, (c) autenticación de identidad y (d) autenticación para la prestación de servicios o transacciones. (WB-TS, 2018)

Como hemos mencionado anteriormente, la identidad digital ha sido definida por diferentes agencias y organismos de manera similar:

> "La identidad digital es la representación única de un sujeto involucrado en una transacción en línea. Una identidad digital siempre es única en el contexto de un servicio digital, pero no necesariamente identifica de manera única al sujeto en todos los contextos. En otras palabras, acceder a un servicio digital no significa que se conozca la identidad de la vida real del sujeto". - Instituto Nacional de Estándares y Tecnología – NIST (NIST-IDG, 2017)

> "La identidad digital es la suma de toda la información disponible digitalmente con respecto a un individuo, independientemente de su grado de validez, su forma o su accesibilidad, que comprende datos directos e inferidos (o indirectos)" – OIX (OIX-TOOLS, 2019)

> "La identidad digital es la representación digital de una entidad lo suficientemente detallada como para que el individuo pueda distinguirse dentro de un contexto digital". - UIT (EU-BDID, 2019)

Imagen 1. Ejemplos de información de identidad en tres contextos diferentes.

2.2. Ventajas de la identidad digital

Como hemos discutido en la sección anterior, la identidad digital permite a las personas evitar las limitaciones del mundo físico y posibilita conexiones confiables en todo el mundo, así como transacciones y provisión y recepción de servicios digitales. En un mundo que se está volviendo más digital cada día, unos sistemas de gestión de identidad digital robustos, útiles y escalables son necesarios para permitir la identificación y autenticación electrónica, de manera que podamos saber con quién estamos interactuando y tengamos el control de nuestros datos pudiendo decidir en todo momento con quién, cómo y con qué fin los compartimos.

Según McKensie[1], "una buena identificación digital es aquella identificación verificada y autenticada con un alto grado de confianza sobre canales digitales, única y establecida con consentimiento individual, que protege la privacidad del usuario y garantiza el control sobre sus datos personales". De tal modo que puede "agregar valor promoviendo la inclusión, la formalización y la digitalización. Por ejemplo:

- El 45% de las mujeres mayores de 15 años carecen de identificación en países de ingresos limitados frente a un 30% de hombres.
- 1700 millones de personas podrían obtener acceso a servicios financieros.
- Se podría reducir potencialmente el 90% de los costes de incorporación de clientes.
- La identificación digital podría generar un valor económico de entre el 3 y el 13% del PIB en 2030."

En el Bloque 4 analizaremos en detalle el potencial de la identidad digital, particularmente el de la identidad auto-soberana, en relación con la inclusión financiera y social. En la Tabla 1 presentamos a modo de resumen algunos de los beneficios de la identidad digital para personas individuales, sector público y sector privado.

Tabla 1. Beneficios de la identidad digital.

Beneficios para las personas	Beneficios para el sector público	Beneficios para el sector privado
Conveniencia	Mejor prestación de servicios	Oportunidades comerciales en ciberseguridad
Utilidad	Reducción de costes de personal	Oportunidades comerciales como proveedores de identidad
Reducción de costes	Reducción de costes de procesos en papel y almacenamiento	Mayor accesibilidad de clientes
Inclusión	Reducción de costes de prestación de servicios	Facilitación de procesos de verificación de usuarios
Experiencia de usuario	Datos preparados para el análisis	Reducción de costes por prestación de servicios
	Incremento de la seguridad	

1. https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/infographic-what-is-good-digital-id#

2.3. Problemas presentes en los sistemas actuales de gestión de identidad digital

A medida que surgen nuevas tecnologías, los reguladores adquieren una mayor comprensión del mundo digital, los gobiernos y las entidades privadas encuentran mejores formas de interactuar electrónicamente, y los usuarios se sienten más seguros con el uso de internet para todo tipo de transacciones, se van proponiendo y adoptando soluciones mejores y más robustas de identidad digital. Sin embargo, las soluciones actuales aún presentan diversos problemas que pueden clasificarse en tres categorías: regulación, tecnología, y seguridad.

Como ya señaló la Unión Europea (UE), "sin una manera de identificarnos entre nosotros y nuestras posesiones, difícilmente podríamos construir grandes naciones o crear mercados globales. Desafortunadamente, existen problemas persistentes –y cada vez más serios– con la forma en que funciona la identidad digital. Debido a razones históricas y de otras índoles, la experiencia de identidad digital actual está fragmentada, con pocos estándares o interoperabilidad, y es insegura, como nos recuerdan los informes casi diarios de piratas informáticos y violaciones de datos" (EU-BDID, 2019).

2.3.1. Regulación y estándares

A medida que las sociedades crecen digitalmente, las nuevas formas de conectarse e interactuar entre individuos y organizaciones requieren de una evolución constante de los requisitos de la identidad digital. En primer lugar, es esencial identificar los diferentes contextos de las interacciones electrónicas para que los estándares y las regulaciones puedan adaptarse y apoyarlos si fuese necesario.

Uno de los problemas a los que se enfrentan hoy en día la identificación, la autenticación y la autorización electrónicas es que la regulación sobre transacciones electrónicas, cuando existe, se centra en un uso limitado de la identidad digital para la interacción entre individuos y servicios proporcionados por la administración pública. Faltan contextos o escenarios que permitan que las entidades privadas cualifiquen para ofrecer servicios electrónicos confiables y cualificados para la identificación, autenticación y autorización de tal forma que se garantice por ley el no repudio. Esto hace necesario desarrollar unos estándares para permitir la interoperabilidad y el reconocimiento transfronterizo.

Es en Europa donde podemos encontrar la normativa más avanzada para la identificación electrónica y la protección de datos (Reglamento eIDAS y Reglamento General de Protección de Datos -GDPR-, respectivamente). En la primera de estas normas, la definición del papel del proveedor de servicios de confianza (TSP por sus siglas en inglés) permite a las entidades privadas certificarse para proporcionar servicios como la creación, verificación y validación de firmas electrónicas, sellos electrónicos o sellos de tiempo en los Estados Miembros de la Unión Europea. Estas entidades certificadas se pueden encontrar en la lista oficial de proveedores de servicios[2] y son reconocidas internacionalmente. Sin la existencia de estas regulaciones y marcos de confianza no se podría garantizar la no discriminación en el uso de mecanismos mencionados anteriormente.

2.3.2. Tecnología

La tecnología utilizada hoy en día para la identificación electrónica de las personas dista mucho de ser ideal. En la actualidad, los mecanismos más seguros para acceder a los diferentes servicios electrónicos confidenciales, como por ejemplo las plataformas gubernamentales, son los certificados X.509 y las tarjetas con chip, que normalmente combinan contraseñas e información biométrica. No obstante, ambos mecanismos tienen costes de producción muy altos y la recuperación en caso de pérdida o robo no es sencilla.

2. https://ec.europa.eu/digital-single-market/en/eu-trusted-lists-trust-service-providers

Los certificados X.509 se almacenan generalmente en servidores específicos, lo que los hace no portables. Además, no permiten el uso de seudónimos, ya que la identidad del sujeto se refleja en el propio certificado. Por su parte, las tarjetas con chip normalmente requieren que las personas tengan una combinación de tarjeta y contraseña o biometría para cada servicio al que quieran acceder. Si a esto sumamos que las tarjetas pueden perderse o robarse fácilmente, su uso se convierte en muy poco práctico.

Consideramos que las herramientas tecnológicas y servicios electrónicos para identificación, autenticación y autorización ideales han de reunir siete características:

Escalabilidad: que sean adaptables y replicables.
Interoperabilidad: que permitan acceso a todo tipo de servicios públicos y privados.
Portabilidad: que permitan llevar los identificadores digitales y credenciales a cualquier lugar.
Recuperación: que permitan recuperar claves y credenciales de manera fácil y segura.
Seguridad: que protejan datos e información personal, incluidas claves privadas y credenciales.
Seudónimo: que permitan interactuar sin revelar nuestra identidad real.
Utilidad: que proporcionen valor a las personas y ofrezcan una experiencia de usuario satisfactoria.

Todo lo anterior requiere un cambio completo de paradigma desde la perspectiva tecnológica, evolucionando desde el uso de los certificados X.509 y tarjetas con chip a una realidad nueva y más avanzada. En primer lugar, desde la perspectiva de las credenciales, necesitamos una solución que nos permita interactuar bajo un seudónimo con el mismo nivel de seguridad que otorgan los X.509 y las tarjetas con chip. Por otro lado, en lo relativo al almacenamiento y la administración, necesitamos un método que nos permita administrar nuestras credenciales de una manera sencilla, portable, eficiente y segura, garantizando así la seguridad y la recuperación de datos. En tercer lugar, es igualmente necesario que la combinación de estas nuevas credenciales digitales y los dispositivos de gestión nos permitan acceder a todo tipo de servicios digitales, tanto públicos como privados.

2.3.3. Seguridad

Hoy en día, en general las personas no pueden administrar sus identidades digitales, ya que no tienen el control de sus autenticadores, de sus datos o de sus credenciales digitales. No somos dueños de la información que existe en internet sobre nosotros; ni siquiera aquella información a la que accedemos con nuestro usuario y contraseña (como nuestra información bancaria o nuestros perfiles en redes sociales), pues se almacena en las bases de datos de terceros y son estos quienes nos proporcionan acceso a ella.

Asimismo, estamos obligados a memorizar decenas de contraseñas para acceder a diferentes servicios y plataformas digitales; casi una para cada sitio que requiera autenticación, a menos que confiemos en un tercero como Facebook o Google para administrar nuestras credenciales, si es que el proveedor de servicios lo permite. Bajo esta perspectiva, los derechos de protección de datos como el consentimiento, el derecho al olvido, la portabilidad y el seudónimo, que ya han sido reconocidos por diferentes regulaciones -como veremos en la Sección 6.2-, difícilmente pueden garantizarse.

Básicamente, nuestra interacción electrónica está en manos de proveedores de servicios que nos dan acceso a aquellos datos e información que ellos controlan, así como de proveedores de identidad de terceros que administran nuestros autenticadores y los usan en nuestro nombre. Como es lógico, crear y mantener las infraestructuras necesarias para almacenar y proteger esa información conlleva altos costes. Además, dichas infraestructuras son, en muchas ocasiones, vulnerables a los robos de datos. Según el Informe de incumplimiento de datos del consumidor de EE. UU. de 2019 (ForgeRock, 2019):

- En 2018, se filtraron más de 2.800 millones de registros de datos de consumidores, que supusie-

ron 342 infracciones con un coste total de más de 654.000 millones de dólares.
- El principal tipo de ataque en 2018 fue el acceso no autorizado, representando el 34% de todas las infracciones.
- En el primer trimestre de 2019, las infracciones de los servicios financieros le costaron a la industria 6.200 millones de dólares, superando enormemente los 8 millones de dólares del primer trimestre del año anterior.
- La asistencia sanitaria fue la industria más afectada. Este sector fue víctima del 48% de todas las infracciones.
- La información de identificación personal (IIP) fue, con diferencia, el tipo de hackeo más común en 2018, representando el 97% de todos los hackeos.
- La fecha de nacimiento y/o los números de la Seguridad Social fueron el tipo de información personal identificable más comprometida en 2018, exponiéndose dichos datos en un 54% de las infracciones.

Según Gartner, aunque los sistemas de gestión de identidad actuales vienen ofreciendo mejoras en su utilidad en comparación con los no digitales, aún siguen teniendo muchos puntos débiles (Gartner, 2020):

- Su diseño y mantenimiento es caro.
- No sirven para establecer y mantener una confianza real a través de la prueba de identidad.
- Son propensos a la proliferación de datos y a la violación de privacidad.
- Se deben someter a las normas de privacidad ya que recopilan, almacenan y analizan datos confidenciales.
- Son la causa de un sinfín de problemas de calidad de los datos debido a que existen muchos almacenes de información.
- Son vulnerables a los ataques de seguridad y se exponen en mayor medida a la pérdida de datos (debido a los repositorios centralizados).
- Son susceptibles a hackeos debido a la falta de control del propietario de la identidad.
- Son susceptibles a censura ya que los proveedores de identidad tienen capacidad de suspender las cuentas.

Entendemos que las soluciones de identidad auto-soberana pueden ayudar a mitigar todos estos problemas, como explicaremos en las Secciones 2.5, 3.1 y 4. Para dar un mayor contexto, vamos a revisar primero diferentes sistemas existentes de gestión de identidad digital.

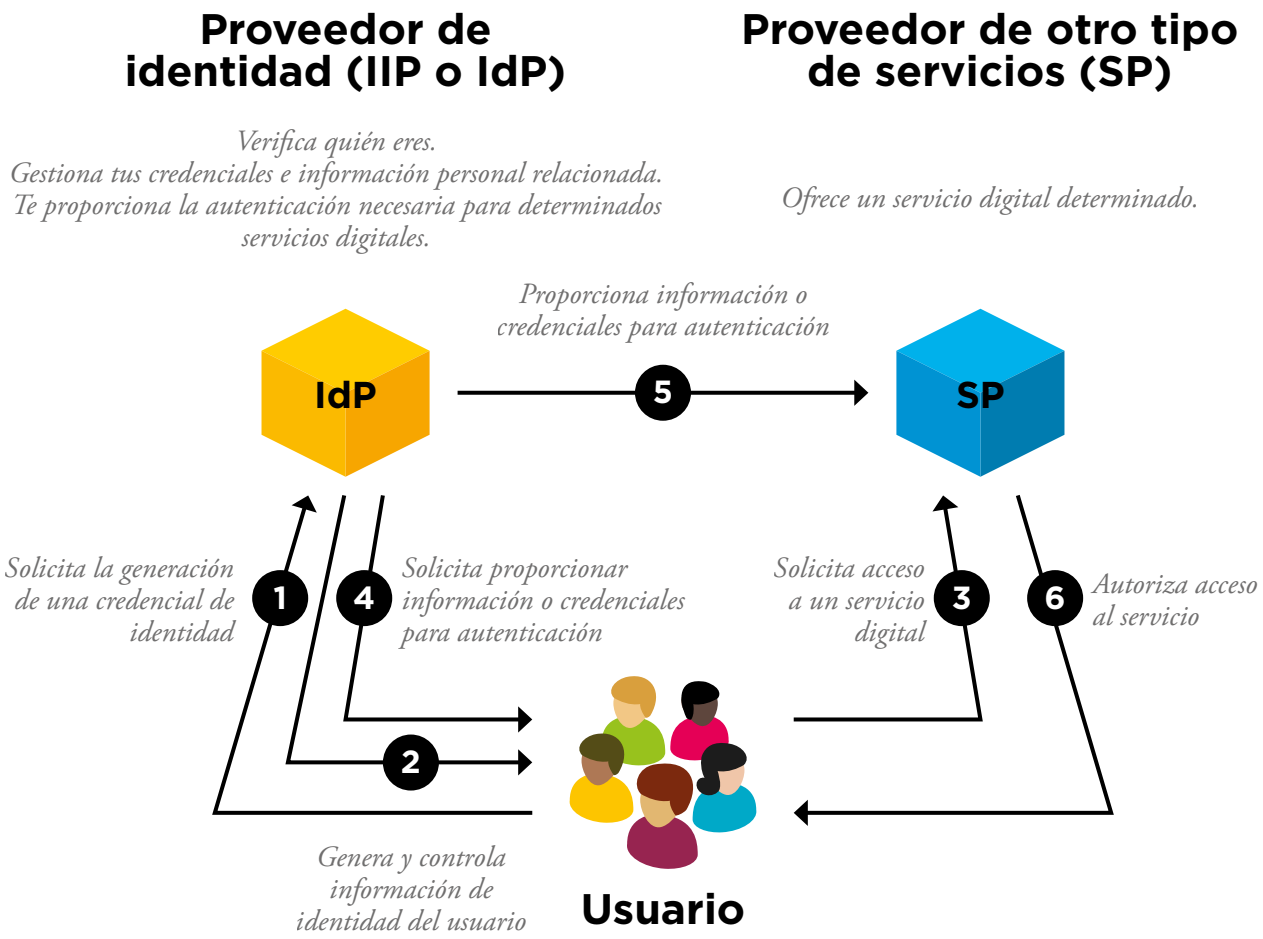
2.4. Descripción general de los sistemas de gestión de la identidad digital

Puede distinguirse cinco modelos diferentes de sistemas de gestión de identidad digital: centralizado, identidad provista por un tercero, federado, centrado en el usuario e identidad auto-soberana. Antes de revisar los cinco modelos, es importante definir los dos conceptos siguientes:

Proveedor de identidad (IIP o IdP por sus siglas en inglés): según la ya mencionada ISO/IEC 24760-1, un proveedor de identidad es "una entidad que proporciona información sobre identidad" (ISO, 2019). Esto incluye la creación de información de identidad, así como el mantenimiento y el manejo de las credenciales en nombre de personas físicas o jurídicas, al tiempo que se proporcionan servicios de autenticación ante proveedores de servicios o aplicaciones de terceros confiables.

Proveedor de otro tipo de servicios cualesquiera (SP por sus siglas en inglés): un proveedor de servicios es cualquier entidad que proporciona un servicio para personas físicas o jurídicas. Esto incluye, como no podía ser de otra forma, a los proveedores de identidad. De este modo un proveedor de identidad es siempre un proveedor de servicios, pero no cualquier proveedor de servicios es necesariamente un proveedor de identidad. Para denominar a aquellas entidades que actúan como proveedoras de servicios cualesquiera que no sean de identidad utilizaremos el concepto de "proveedor de otro tipo de servicios cualesquiera". Por simplicidad, nos referiremos a estos últimos simplemente como proveedor de servicios, entendiendo que en

Imagen 2. Relación entre proveedor de identidad (IdP), proveedor de otro tipo de servicios (SP) y usuario.



el caso de que fuese un servicio de identidad lo denominaríamos proveedor de identidad.

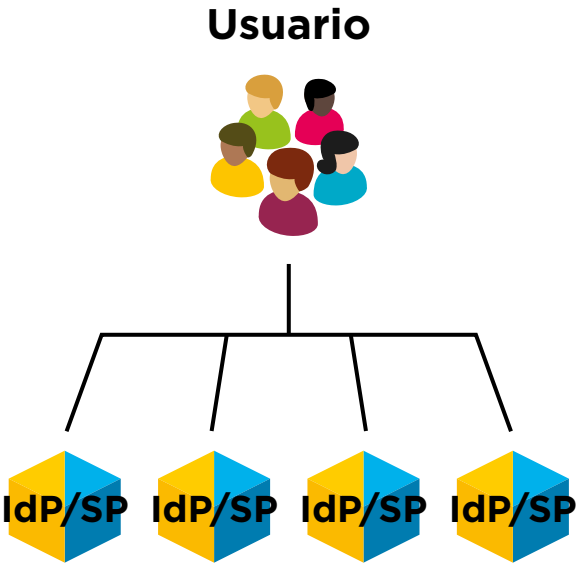
2.4.1. Centralizado

El modelo de identidad centralizado es el más simple y tradicional de todos. En él, cada servicio digital que consumimos está actuando al mismo tiempo como proveedor de identidad y proveedor de servicios. Algunos ejemplos de este modelo son los sitios web en los que iniciamos sesión con el usuario y contraseña que hemos creado previamente al registrarnos (redes sociales, correo electrónico, etc.).

Este modelo presenta varios inconvenientes:

- Los datos se almacenan en bases centralizadas que no siempre están bien protegidas.

Imagen 3. Esquema simplificado del modelo de identidad digital centralizado.



- Los usuarios deben autenticarse de forma independiente para cada organización por lo que deben memorizar o almacenar muchas claves.
- Las organizaciones deben asumir costes muy altos y tener una gran infraestructura de hardware (*on-premise* o en la nube) para mantener seguros los autenticadores, credenciales y datos del usuario.
- Mantener las bases de datos centralizadas es una gran responsabilidad para las organizaciones y empresas.

2.4.2. Identidad provista por un tercero

En el modelo de identidad provista por un tercero, el proveedor de identidad y el proveedor de servicios son entidades diferentes que se comunican entre sí. Cada vez que una persona física o jurídica desea acceder al servicio digital ofrecido por el proveedor del servicios, dicha persona recurre a su proveedor de identidad para autenticarse en su nombre en lugar de autenticarse directamente frente al proveedor de servicios. La comunicación entre el proveedor de identidad y el servicio o recurso se realiza a través de protocolos, estándares y marcos comunes, como SAML (OASIS, 2008), OAuth (IETF, 2012) y OpenID.[3]

La utilización de este modelo se ha incrementado con la llegada de las redes sociales como Facebook y la monopolización de Google como buscador web. Muchas veces, en lugar de iniciar sesión en un sitio web con un nuevo usuario y contraseña específicos, tenemos la opción de autenticarnos con nuestra cuenta de Facebook o Google. Cabe mencionar también a otros proveedores de identidad de terceros como Okta y Azure AD que cada día son más utilizados por organizaciones y empresas para administrar y manejar la identificación, autenticación y autorización de los empleados.

Cuando accedemos directamente a Facebook o Google con nuestras credenciales de dichos sitios web, estamos utilizando el modelo centralizado que vimos anteriormente. Sin embargo, cuando accedemos a otros servicios con esas mismas credenciales de Facebook y Google (haciendo una suerte de delegación de las mismas) nos encontramos dentro del modelo de identidad provista por un tercero. En ambos casos Facebook y Google son nuestros proveedores de identidad, pero sólo en el primer caso son también proveedores de servicios -según la terminología que hemos introducido al inicio de la Sección 2.4-. Es importante aclarar que, en ambos modelos, nuestra información y datos siguen estando centralizados en el proveedor de identidad.

Existen tres tipos o submodelos de terceros proveedores de identidad, a saber: proveedor de identidad único, múltiples proveedores de identidad y brókers con múltiples proveedores de identidad. Cuando se utilizan estos modelos de identidad digital para servicios públicosrelevantes que requieren el más alto nivel de seguridad en la prueba de identidad, autenticación y autorización, el gobierno siempre está involucrado (véase la Tabla 4).

Cuando solo existe un proveedor de identidad, el propio gobierno es generalmente dicho proveedor. En caso de existir múltiples proveedores de identidad, el gobierno es el responsable de definir los criterios y completar la acreditación de los proveedores de identidad. Finalmente, en el modelo del bróker, el gobierno es no solo responsable de definir los requisitos y proporcionar acreditación a los proveedores de identidad, sino también de actuar como bróker o designar a una entidad para que actúe como tal.

El modelo de identidad provista por un tercero, al igual que el centralizado, presenta varios inconvenientes:

- Los proveedores de identidad deben poder mantener grandes infraestructuras y asumir altos costes para poder proporcionar un almacenamiento seguro, como ocurre en el modelo centralizado.
- Dado que el número de proveedores de identidad es mucho menor que en el modelo

3. https://openid.net/connect/

Imagen 4. Esquema simplificado de los tres modelos de identidad provista por un tercero.

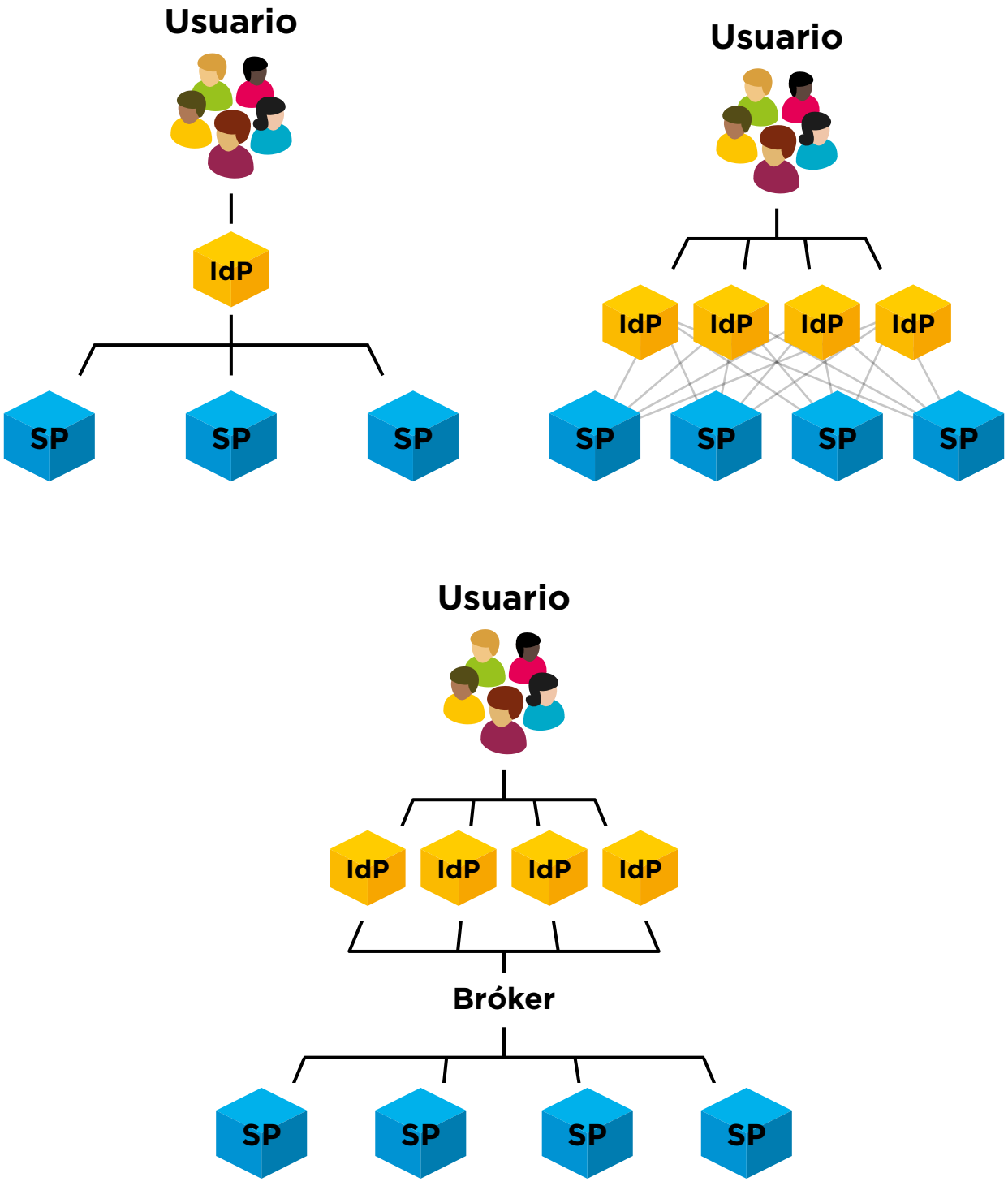


Tabla 2. Ejemplos de los tres sub-modelos de identidad provista por un tercero, según la UIT. (ITU, 2018)

Un único proveedor	Múltiples proveedores de identidad	Bróker/s con múltiples proveedores de identidad
El programa Aadhaar en India (el más grande del mundo). La tarjeta de identificación de Estonia y la identificación móvil para una gran cantidad de servicios. El sistema de autenticación digital para los servicios del gobierno holandés (DigID). La identidad digital emitida por RENIEC en Perú. El Registro de Población de Finlandia, utilizado para elecciones, presentación de impuestos, administración judicial, etc.	El Sistema Público de Identidad Digital (SPID) italiano, para servicios administrativos públicos gestionados por la Agencia de Identidad Digital (AgID).	El programa GOV.UK Verify, un sistema de autenticación externo que permite a los ciudadanos del Reino Unido acceder a diferentes servicios gubernamentales en línea utilizando hasta diez proveedores de identidad diferentes.

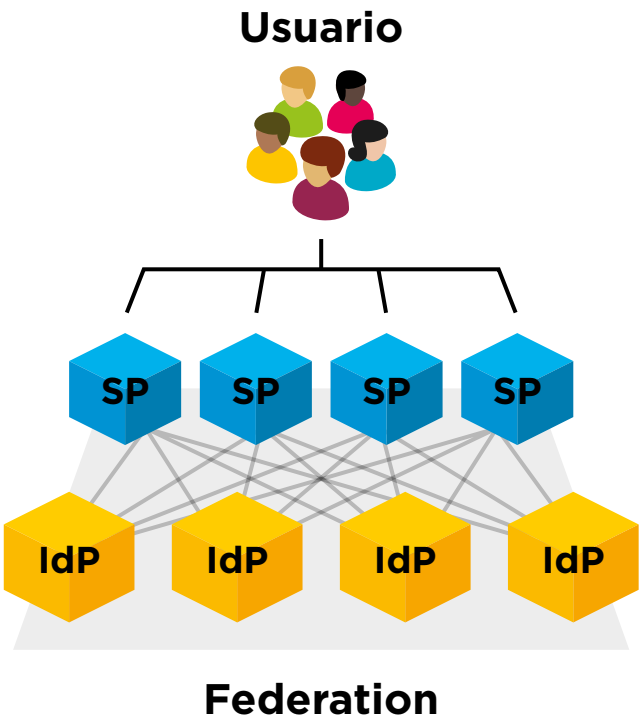
centralizado hay una mayor monopolización, lo que puede afectar a la seguridad y a la confianza.
- Teniendo en cuenta que algunas plataformas como Google o Facebook ya funcionan como proveedores de identidad para muchos servicios digitales (especialmente para aquellos que no requieren altos niveles de seguridad), el modelo de ingresos para otros proveedores de identidad se reduciría únicamente a unos pocos servicios sociales, gubernamentales y financieros.
- Como existen muchas organizaciones involucradas en el manejo de nuestra identidad, datos e información, las personas tenemos cada vez menos control de nuestra identidad, por lo que es muy difícil garantizar los derechos de protección de datos, incluidos en consentimiento, el derecho al olvido, la portabilidad y el seudónimo.

2.4.3. Federado

En el modelo de identidad federado, existen varios proveedores de identidad que han establecido previamente acuerdos entre ellos y operan bajo un marco de confianza común. Este modelo puede ser tanto público y avalado por la regulación (como el eIDAS en la Unión Europea), como privado y habilitado por acuerdos privados entre las partes. De este modo, la información digital de los usuarios se distribuye a través de múltiples proveedores de identidad, en lugar de ser centralizada en un único proveedor. Esta forma de organización de proveedores de identidad suele denominarse federación y, por lo general, las entidades que constituyen la federación comparten un identificador único para cada usuario. La principal diferencia entre este modelo y los centralizados y de identidad provista por un tercero es que el modelo federado es un esquema de gestión de identidad de muchos a muchos, mientras que el modelo centralizado puede verse como de uno a uno, y el tercero como uno a muchos.

En cuanto a las ventajas e inconvenientes podemos aplicar lo mismo que para el modelo de identidad provista por un tercero con múltiples proveedores de identidad, con o sin bróker.

Imagen 5. Esquema simplificado del modelo federado.



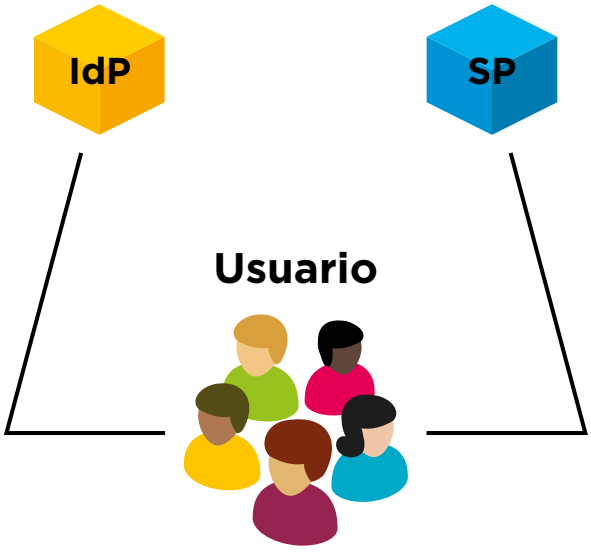
2.4.4. Centrado en el usuario

En este modelo, el usuario almacena en su dispositivo personal autenticadores y credenciales que han sido emitidas por diferentes proveedores de servicios, de tal forma que es el propio usuario quien tiene el control de sus datos. A. Josang y S. Pope presentaron este modelo en 2005 y llamaron dispositivo de autenticación personal al hardware utilizado para almacenar los datos (PAD por sus siglas en inglés) (Josang & Pope, 2005). Según ellos, el PAD podría ser cualquier hardware, con o sin teclado o pantalla, que requeriría algo como así un PIN para que el usuario se pudiese autenticar en él.

No es claro establecer cómo el modelo centrado en el usuario se diferencia o se asemeja al ya mencionado modelo centralizado y al de identidad auto-soberana, en tanto no se formule una propuesta más detallada y precisa del mismo. Por ejemplo, pongamos que un usuario almacena en su PAD claves y autenticadores o tokens para poder acceder a un servicio digital. Podríamos considerar entonces que este modelo centrado en el usuario funciona en realidad como uno centralizado en el que el proveedor de servicios le permite autenticarse con una clave almacenada en un hardware en lugar de con un usuario y una contraseña. Por lo contrario, si el usuario además administra realmente todos los datos en el dispositivo y puede seleccionar qué datos se revelarán a qué proveedor de servicios utilizando diferentes identidades digitales e identificadores para autenticarse en diferentes proveedores de servicios, estaríamos acercándonos mucho a un modelo de identidad auto-soberana.

Con las características actuales de los teléfonos inteligentes parece lógico considerarlos como los dispositivos idóneos para actuar como PADs. En cualquier caso, para poner en práctica el concepto de identidad centrada en el usuario, permitiendo así proporcionar servicios digitales a los usuarios con niveles máximos de seguridad y garantizando a estos últimos el control total de sus autenticadores, credenciales y datos, sigue siendo necesario diseñar un proceso más complejo y detallado, lo que nos lleva al modelo de identidad auto-soberana.

Imagen 6. Esquema simplificado del modelo de identidad centrada en el usuario



2.4.5. Identidad auto-soberana

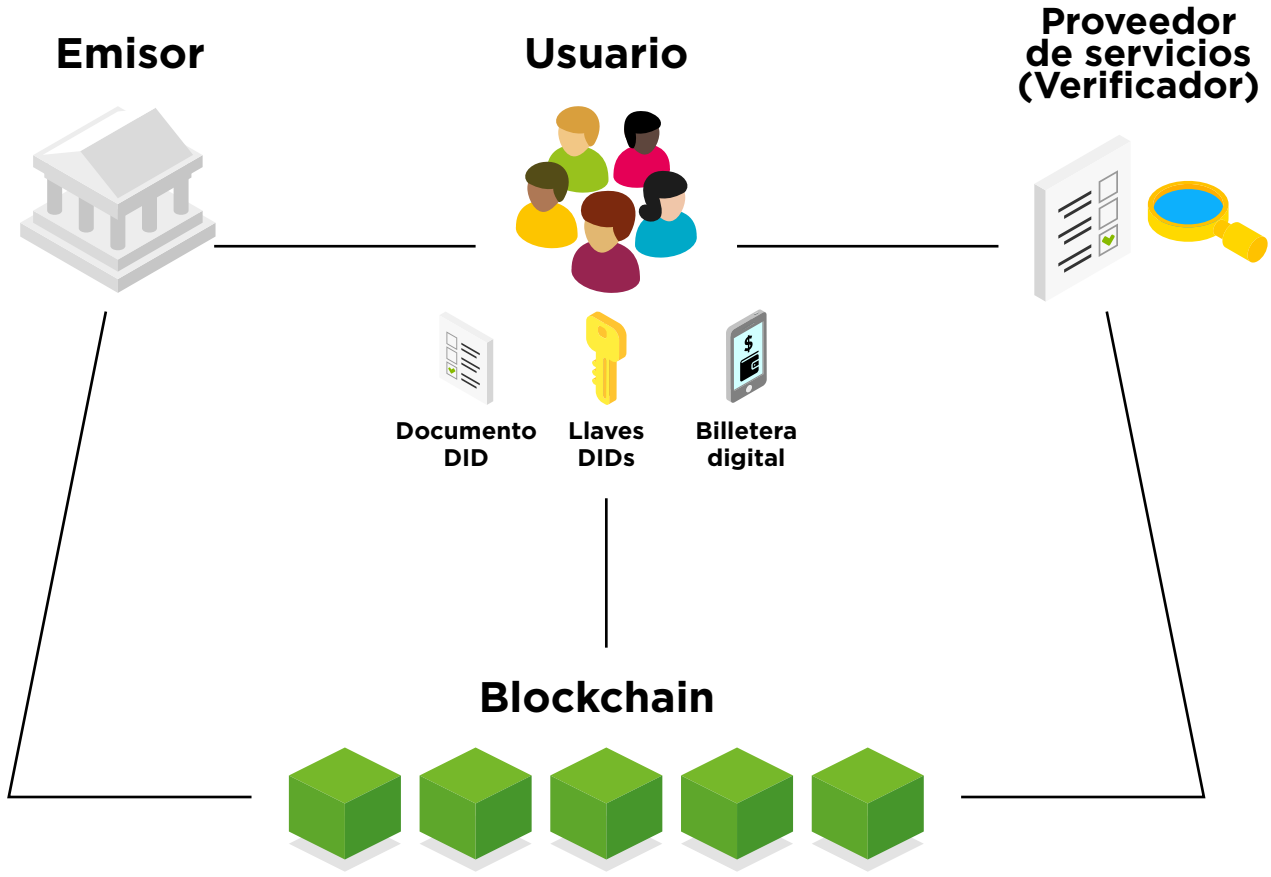
En el modelo de identidad auto-soberana (IAS), el usuario es el administrador central de su identidad, teniendo mucho más control sobre los datos y la

información que se comparte y se conoce sobre él. A diferencia de los modelos centralizados, de identidad provista por un tercero o federados, en el modelo IAS no existe una entidad tercera que realice esta función. Es decir, ni el proveedor de identidad, ni tampoco el proveedor de servicios administra las credenciales y autenticadores de las personas en su nombre, quedando el rol del proveedor de identidad limitado a ser un simple emisor de identidad.

La identidad auto soberana se basa en dos nuevos estándares que están siendo desarrollados por el World Wide Web Consortium: los Identificadores Descentralizados (DID) (W3C-DID, 2019) y las Credenciales Verificables (VC) (W3C-VC, 2019). Los Identificadores Descentralizados (DID) proponen que cada individuo genere sus propios identificadores únicos para interactuar en el mundo digital. Las Credenciales Verificables (VC) son credenciales digitales que contienen información o atributos sobre ellas (por ejemplo, el nombre, la fecha de nacimiento, el lugar de residencia, etc.) y que están siempre bajo el control de los titulares. Estas credenciales pueden ser auto-emitidas o emitidas por terceros. En la Sección 7.3.5 explicaremos en detalle los 6 pasos del Proceso de Verificación de credendiales que hemos elaborado.

La identidad auto-soberana emplea dos elementos esenciales para la gestión de la identidad: los registros descentralizados de información y las billeteras digitales.

Imagen 7. Esquema simplificado del modelo de identidad digital auto-soverana.



Registros descentralizados: el modelo IAS se basa en registros descentralizados de información, donde las pruebas de la propiedad de los identificadores descentralizados y las credenciales verificables se almacenan en una red o registro descentralizado. A diferencia de los modelos centralizados, de terceros y federados en los que la entidad verificadora necesita interactuar de alguna manera con el emisor cuando un sujeto le presenta una credencial para poder verificar su validez, en el modelo IAS el emisor deja todas las pruebas criptográficas necesarias para verificar esa credencial digital (firmas digitales, sellos de tiempo, etc.) en un registro descentralizado público. Esto permite que cualquiera pueda verificar las credenciales digitales sin necesidad de interactuar con el emisor directamente. En la Sección 7.7 daremos más detalles sobre los registros descentralizados.

Billeteras digitales: las billeteras digitales son repositorios personales portables y seguros. Puede ser por ejemplo aplicaciones móviles que nos permiten administrar nuestros identificadores, autenticadores, datos y credenciales verificables en nuestro teléfono, estando éstos completamente protegidos y bajo nuestro control. De este modo, podemos decidir qué información compartimos y con quién, en forma de presentaciones verificables. En la Sección 7.5 hablaremos con más detalle sobre las billeteras digitales.

2.5. Comparación entre diferentes sistemas de gestión de identidad digital

Para comparar los modelos de identidad digital que hemos presentado en la Sección 2.4 hemos elaborado un análisis presentado en la Tabla 5.

Al evaluar las ventajas y desventajas de las diferentes soluciones de identidad digital, es de gran importancia considerar los modelos económicos y financieros de cada una, pues estos son esenciales para garantizar su sostenibilidad. En la Tabla 6 hemos clasificado los costes en cinco categorías:

Prueba de identidad: el emisor de identidad verifica la identidad del sujeto.
Emisión de credenciales: el emisor de identidad genera las credenciales y se las envía al titular.
Gestión de credenciales: el titular almacena y gestiona las credenciales.
Copias de seguridad de claves y credenciales: los autenticadores, las claves privadas y las credenciales tienen copias de seguridad en algún lugar para permitir la recuperación.
Presentación y verificación de credenciales: el titular presenta las credenciales al verificador y éste las verifica.

Tabla 3. Comparación entre los diferentes sistemas de gestión de identidad digital según sus características.

	Centralizado	Identidad provista por tercero/ Federaciones	Centrado en el usuario	Identidad auto-soberana
Los usuarios pueden generar sus identificadores	N	N	N	S
Los usuarios controlan sus autenticadores (p.e. sus claves privadas)	N	N	S	S
Los usuarios pueden controlar sus credenciales digitales y certificados	N	N	S	S
Los usuarios pueden recuperar el control sobre los identificadores en caso de pérdida o robo de sus claves	S	S	N	S
Los usuarios pueden recuperar sus credenciales y certificados en caso de pérdida o robo de sus claves	S	S	N	S
Los usuarios pueden acceder a los datos asociados con su identidad digital	I	I	I	S
Habilitar pruebas de conocimiento cero	N	N	N	S
La información de identificación personal (IIP) se minimiza	N	N	N	S
El derecho al olvido puede garantizarse fácilmente	I	N	N	S
Los repositorios de autenticadores y credenciales son portables*	N	N	S	S
Los proveedores de identidad no mantienen bases de datos centralizadas con los datos del usuario	N	N	N	S
Los proveedores de identidad no tienen acceso a la información sobre el acceso de las personas a los servicios o las interacciones con otros	N	S	S	S
Las implementaciones cumplen con las políticas regulatorias	S	S	S	S
Se desarrollan marcos de confianza para permitir la definición de proveedores de identidad y niveles de garantía	S	S	S	S
La identidad es fácilmente recuperable en caso de catástrofe natural	S	S	N	S
Violaciones de privacidad y datos masivas menos probables	N	N	N	S

S: Si, N: No, I: Indefinido

* Nos estamos refiriendo al estado actual.

Tabla 4. Costes y pagadores en los diferentes sistemas de gestión de identidad digital.

	Centralizado	Identidad provista por tercero/ Federados	Centrado en el usuario	Identidad auto-soberana
Verificación de usuario y autenticación (antes de la emisión)	La compañía actúa como SP[4] =IdP y asume el coste.	Para niveles de garantía más altos, el IdP[5] podría imponer una tarifa a los usuarios.	Igual que la identidad provista por tercero.	Igual que la identidad provista por tercero.
Emisión de credenciales	Es parte del proceso de verificación y autenticación. No hay coste adicional.	Igual que el modelo centralizado.	Igual que el modelo centralizado.	Como la identidad auto-soberana puede requerir DLT, la emisión de credenciales puede incurrir en tarifas de transacción para escribir en esas redes. Los usuarios asumirían esta tarifa.
Gestión de credenciales	Altos costes asumidos por el SP=IdP para proteger las bases de datos centrales.	Igual que el modelo centralizado pero solo por los IdPs que aquí son diferentes de los SPs.	Los usuarios decidirían qué PAD usar para administrar sus credenciales y asumirían los costes.	Los usuarios decidirían con qué billetera digital[6] desean administrar sus credenciales y asumirían los costes.
Copia de seguridad de claves y credenciales	Altos costes asumidos por el SP = IdP para garantizar las copias y la recuperación de la información.	Como el anterior pero los costes son asumidos solo por los IdPs que aquí son diferentes de los SPs.	Los usuarios decidirían qué opciones de respaldo desean (proporcionadas por el proveedor de billetera o externas) y asumirían los costes.	Igual que el modelo centrado en el usuario.
Presentación y verificación de credenciales	No hay más costes ya que las credenciales son controladas por el SP=IdP.	Los acuerdos y conexiones necesarios entre IdPs y SPs pueden suponer costes adicionales para ellos.	La provisión de tecnologías para interactuar con el PAD podría suponer costes para el SP.	La presentación y la verificación no deben suponer coste alguno ya que una implementación adecuada no genera transacciones al verificar las credenciales contra las DLT.

4. Proveedor de servicios.
5. Proveedor de identidad.
6. El modelo de negocio de las billeteras digitales aún no está totalmente definido, pues las primeras soluciones están surgiendo ahora. Algunos de los posibles modelos de monetización podrían ser el cobro por (i) la generación de DID múltiples y no correlativos para diferentes interacciones electrónicas, (ii) la provisión de almacenamiento en la nube para copias de seguridad, (iii) la generación de presentaciones verificables personalizadas a partir de una o varias credenciales, y (iv) la generación de firmas electrónicas cualificadas.

IDENTIDAD DIGITAL AUTO-SOBERANA

Bloque 3 Identidad auto-soberana (IAS)

3.1. Definición

Según Sovrin, "identidad auto-soberana (IAS) es un término utilizado para describir el movimiento digital que reconoce que un individuo debe poseer y controlar su identidad sin la intervención de las autoridades administrativas. La IAS permite a las personas interactuar en el mundo digital con la misma libertad y capacidad de confianza que en el mundo físico". En 2016, Christopher Allen estableció los 10 principios para la identidad auto-soberana que se han convertido en una referencia en el campo[7]. Dichos principios son:

Acceso: los usuarios deben tener acceso a sus propios datos.
Consentimiento: los usuarios deben aceptar previamente el uso de su identidad por terceros.
Control: los usuarios deben poder controlar sus identidades.
Existencia: los usuarios deben tener una existencia independiente.
Interoperabilidad: las identidades deben poder utilizarse ampliamente.
Minimización: la divulgación de reclamaciones debe reducirse.
Persistencia: las identidades deben ser duraderas.
Protección: los derechos de los usuarios deben ser protegidos.
Portabilidad: la información y los servicios sobre identidad deben ser portables.
Transparencia: los sistemas y algoritmos deben ser transparentes.

Consideraremos que la identidad auto-soberana es un modelo de identidad digital siempre que cumpla con los 16 principios de la imagen.

- Las personas pueden generar sus propios identificadores[8] únicos (control, existencia).
- Las personas tienen el control de sus autenticadores[9] (acceso, control, existencia).
- Las personas tienen el control de sus credenciales y certificados digitales[10] (acceso, control, existencia).
- Las personas pueden recuperar las credenciales y certificados en caso de pérdida o robo de sus autenticadores (acceso, control, existencia, persistencia y protección).
- Las personas administran y controlan los datos asociados con su identidad digital (acceso, control).
- Las personas pueden hacer divulgaciones selectivas de datos (consentimiento, control, minimización, protección).
- La información de identificación personal (IIP) de los individuos se minimiza (minimización, protección).
- Las pruebas criptográficas de la propiedad de los identificadores se pueden encontrar en una red pública descentralizada (interoperabilidad, persistencia, transparencia).
- Las pruebas criptográficas de la propiedad y la validez de las credenciales se pueden encontrar en una red pública descentralizada (interoperabilidad, persistencia, transparencia).
- El derecho al olvido está garantizado[11] (protección).
- Las unidades de gestión de identidad[12] (billeteras digitales) son portables (portabilidad).
- Los proveedores de billeteras digitales no tienen acceso a la información sobre el acceso de los individuos a los servicios o las interacciones con otros (acceso, control, protección)
- Las copias de seguridad garantizan los niveles máximos de seguridad y privacidad (persistencia, protección).
- Las implementaciones cumplen con las políticas regulatorias (protección).

7. http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html
8. Por ejemplo, claves públicas.
9. Por ejemplo, claves privadas.
10. Por ejemplo, pasaporte o diploma digital.
11. Con la identidad auto-soberana, los individuos tienen el control de sus identificadores que están vinculados a su información digital, por lo que puede ser más fácil habilitar formas de rastrear dónde está su información digital y quién la tiene, y por lo tanto requerir que se borre.
12. Software, hardware o una combinación de ambos que permite almacenar y administrar claves y credenciales personales.

- Las implementaciones se basan en marcos de confianza públicos y/o privados que definen y especifican proveedores de identidad de confianza y niveles de garantía de la identificación electrónica (persistencia, protección,).

3.2. Visión general de la IAS

La idea general de la identidad auto-soberana se basa en repositorios personales portables en los que podemos almacenar y administrar todas nuestras claves privadas, nuestros autenticadores y nuestros tokens y credenciales digitales de manera segura y confiable. Estos repositorios se conocen como billeteras digitales. Las primeras implementaciones ya están disponible; por ejemplo, ya existen aplicaciones móviles que podemos descargar en nuestros celulares desde los *app stores* que nos permiten ver y administrar todos nuestros tokens y credenciales digitales, pudiendo decidir cuándo los usamos o los compartimos y con quién.

Hay múltiples tipos de tokens digitales. Entre los más relevantes se encuentra la representación electrónica de divisas fiduciarias (como dólares o euros), las criptomonedas o las monedas virtuales. En cuanto a las credenciales digitales, cabe destacar pasaportes digitales, diplomas académicos digitales, títulos de propiedad o acreditaciones corporativas digitales.

Hoy en día, cuando presentamos una credencial o un certificado a un verificador (aquella entidad que intentará comprobar si lo que estamos presentando es válido) o cuando enviamos un token digital a otra persona en una transacción electrónica, el verificador debe determinar si ese certificado o ese token digital es válido. Para ello, generalmente el verificador requiere información complementaria a lo que estamos enviando, que a su vez es certificada por un tercero que desempeña el papel de una autoridad en la que el verificador deposita su confianza.

Por ejemplo, si presentamos un diploma digital (por ejemplo, un PDF) en una entrevista de trabajo, el departamento de recursos humanos de la entidad que tiene esa posición abierta verificará que el certificado sea emitido por una institución académica de confianza. Idealmente, el verificador podría iniciar un proceso electrónico automático para acceder al servicio digital del emisor y realizar así una consulta para comprobar la información presentada por el candidato. Desafortunadamente, no es así como funcionan las cosas en la actualidad y las verificaciones pueden demorarse días, meses o años dependiendo del proceso.

En el modelo IAS no es necesario que el verificador pregunte directamente al emisor de la información, ni tampoco que la confirme con las autoridades de confianza. Esta es, sin duda, una de las principales diferencias y ventajas con respecto al resto de modelos de gestión de identidad. Desde la perspectiva de la auto-soberanía, la validez de todos nuestros activos digitales -incluida la propiedad legítima de dichos activos- se puede verificar contra un registro de información descentralizado y confiable. Esto es gracias a que cada vez que se emiten estos activos (por ejemplo, tokens y credenciales digitales), el emisor registra en esa red descentralizada (por ejemplo, una blockchain) una prueba criptográfica de la emisión, así como el sello de tiempo acreditado con su firma electrónica. El emisor también registra el estado del activo, que puede ser modificado tanto por él mismo o por cualquier entidad autorizada por él en cualquier momento, de acuerdo con determinadas reglas públicas y transparentes.

Estos registros descentralizados en los que se va registrando cada movimiento son también inmutables de manera que, si bien es posible modificar o actualizar información como el estado de una credencial digital (por ejemplo, de activa a revocada) siempre quedará constancia de la alteración, ya que todas las modificaciones son firmadas electrónicamente por la entidad que lo modifica y quedan registradas inmutablemente en el registro descentralizado. Por lo tanto, si se emite una credencial digital que luego se revoca, cualquiera podrá realizar un seguimiento de estos cambios de estado en el registro público al que todos pueden acceder. Los activos digitales pueden "vivir" tanto

Imagen 8. Ejemplo de una presentación de un diploma digital para la aplicación a un puesto de trabajo sin (arriba) y con (abajo) identidad digital auto-soberana.

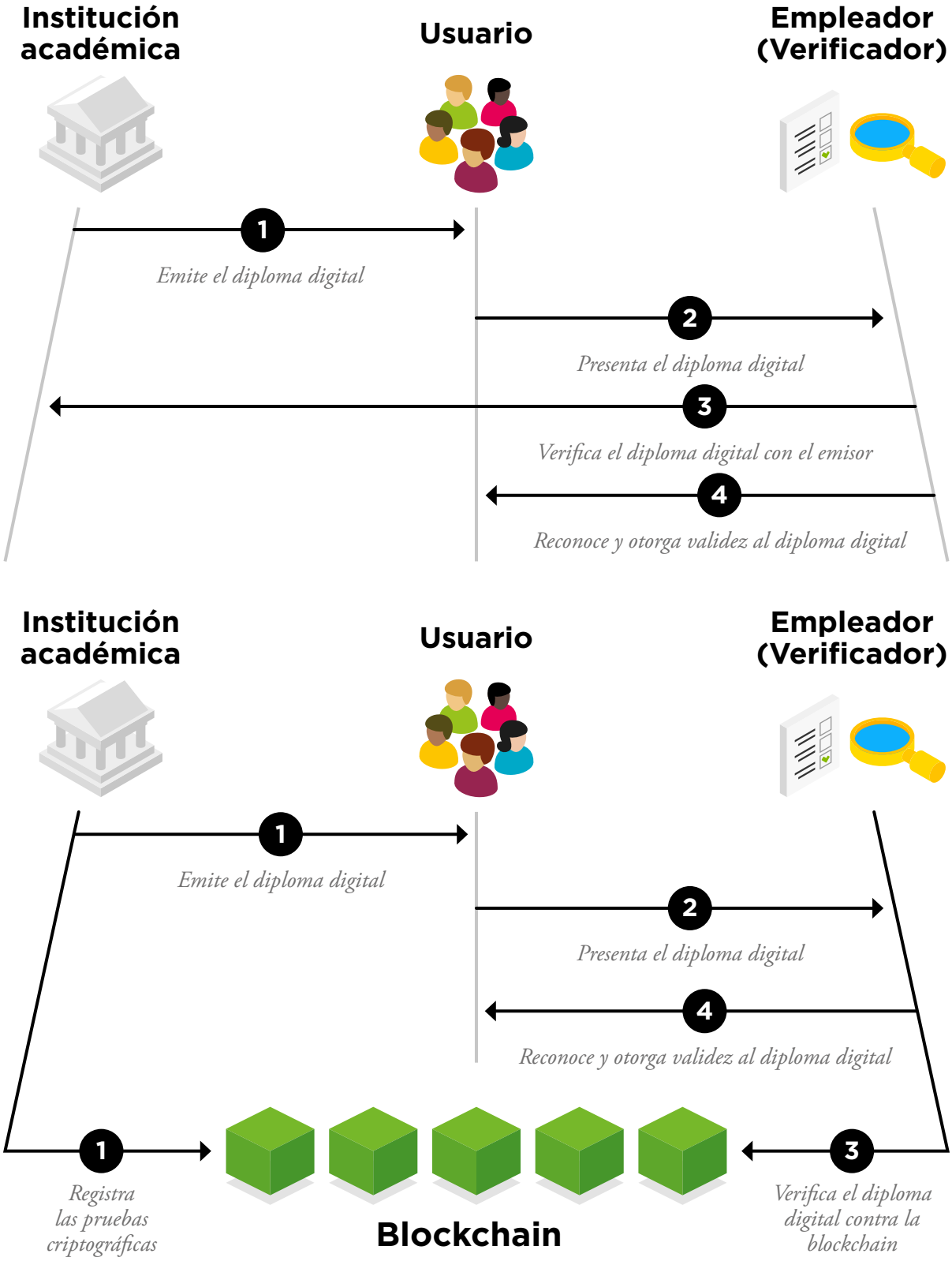
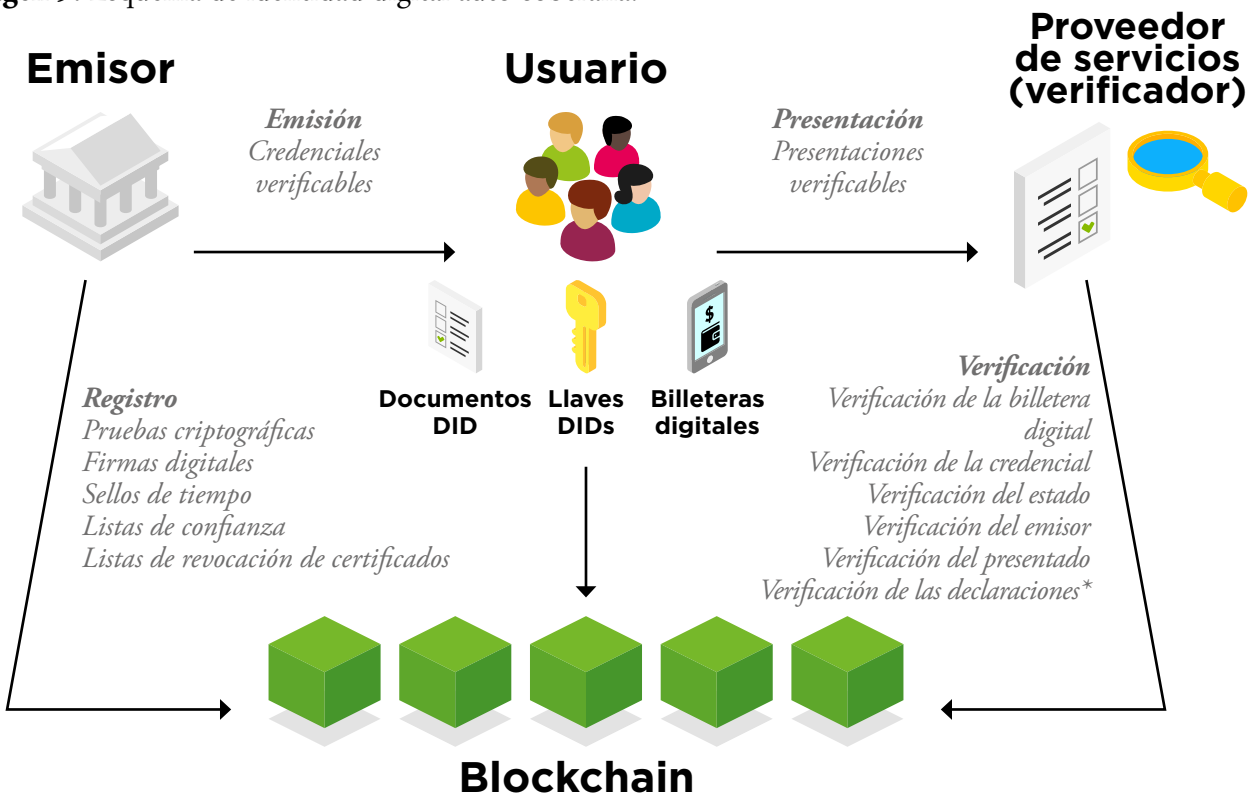


Imagen 9. Esquema de identidad digital auto-soberana.



* Para más información, consultar el Proceso de Verificación de LACChain ID.

en la red como fuera de ella[13], en nuestra billetera digital. En ambos casos, están totalmente bajo nuestro control porque se requiere nuestra firma electrónica para realizar cualquier gestión sobre ellos. En las siguientes secciones presentaremos todos los conceptos necesarios para pasar de la teoría del modelo a su puesta en práctica, y en la Sección 7.3.5 presentaremos un proceso de verificación completo.

3.3. Ventajas de la IAS

Existen diferencias sustanciales entre administrar todos nuestros activos como lo hacemos hoy en día y hacerlo usando una billetera digital móvil bajo el modelo de identidad auto-soberana. Algunas de estas diferencias están relacionadas con los problemas presentados en la Sección 2.3. Estos problemas podrían desaparecer con la IAS. Vamos a ilustrarlo con algunos ejemplos específicos:

Escalabilidad: mediante el uso de estándares y protocolos internacionales, así como tecnologías universales, las soluciones son replicables en distintas sociedades y comunidades. Los registros descentralizados son accesibles desde cualquier parte del mundo -como Internet-, y las billeteras digitales se pueden descargar a cualquier *smartphone*. Obviamente, como veremos en los Bloques 6 y 8, las regulaciones y los marcos de confianza son necesarios para complementar los componentes tecnológicos.

13. Los datos personales o credenciales no deben almacenarse en las redes descentralozadas, ya que estas son generalmente públicas e inmutables. Solo las pruebas criptográficas de la información y los tokens públicos deben guardarse en las redes descentralizadas. Por lo tanto, mientras que los tokens que representan activos pueden "vivir" en redes descentralizadas o blockchain, las credenciales que contienen datos o atributos deben hacerlo *off-chain*.

Interoperabilidad: mediante el uso de tecnología descentralizada y unidades de gestión personales y portables, la adopción de protocolos y estándares globales de IAS permite que entidades públicas y privadas almacenen las pruebas de la información en registros descentralizados, como redes blockchain, comunes. También permite a las personas administrar todas sus credenciales con un único dispositivo seguro y portable, sin importar quién las haya emitido o para qué sirven. Igualmente, en cuanto a la escalabilidad, una regulación adecuada y el establecimiento de marcos de confianza es esencial para complementar las herramientas tecnológicas.

Portabilidad: en la actualidad tenemos que llevar con nosotros diferentes documentos físicos para demostrar quiénes somos, de qué somos propietarios o qué hemos logrado si queremos poder probarlo frente a terceros. Pasaportes, documentos de identidad nacionales, carnés de conducir, escrituras de propiedad, certificados de nacimiento, diplomas, etc. Con la IAS, todos nuestros documentos pueden ser digitales, lo que permite almacenarlos y administrarlos con una billetera digital móvil. Este método es considerablemente más portable que las unidades de administración propuestas en los otros modelos de identidad, que requieren administrar certificados X.509 -almacenados en un computador-, o tarjetas con chip que pueden perderse fácilmente.

Propiedad: hoy en día, nuestro dinero en efectivo nos pertenece. Sin embargo, no se puede decir lo mismo del dinero electrónico en nuestras cuentas bancarias. Cuando deseamos verificar nuestros saldos o transacciones, necesitamos acceder a un portal provisto por nuestro Banco que nos muestra el saldo desde la base de datos del Banco. De modo que, si el banco se declara en quiebra o si el gobierno decide expropiarlo, perderíamos todo ese dinero. Los casos de ¨corralitos¨ son bien conocidos en América Latina. Asimismo, cuando hacemos un pago con nuestra tarjeta de crédito o débito, existen varios intermediarios incluido nuestro proveedor de tarjeta, nuestro banco y el banco del destinatario que se comunican entre sí, realizan validaciones y ejecutan el pago modificando los saldos del remitente y del destinatario en sus bases de datos. En el modelo IAS, nuestro saldo se puede determinar directamente desde la red de blockchain (asegurando la preservación de la privacidad) sin necesidad de validaciones intermedias en las transacciones, ya que sus reglas están automatizadas en la blockchain mediante procesos computacionales llamados contratos inteligentes. Las instituciones financieras siguen siendo esenciales en este esquema, pues son las emisoras de los tokens digitales que representan nuestro dinero electrónico, el cual podemos poseer y transferir sin intermediarios. La diferencia es que ya no desempeñan un papel directo en la transferencia del dinero, sino que lo hacen indirectamente al ser ellos quienes emitieron esos tokens en un principio[14]. La confianza se basa ahora en el libro mayor descentralizado. Más de una docena de bancos centrales ya han piloteado la emisión de divisas digitales de bancos centrales (CBDCs por su nombre en inglés)[15], y Visa ha presentado una patente para solicitar y generar una moneda digital en redes blockchain[16].

Recuperación: en los tiempos que corren, no es difícil perder o que nos roben nuestros documentos físicos o tarjetas con chip. Casi todos hemos

14. Esto permitiría de hecho funcionar electrónicamente de una manera mucho más similar a cómo lo hacemos en el mundo físico. En el mundo físico, las instituciones financieras emiten dinero en efectivo que podemos transferir e intercambiar sin que ninguna institución financiera lo valide explícitamente. En el mundo digital, cada pago electrónico es validado y ejecutado directamente por las instituciones financieras, lo que encarece y realentiza el proceso. Con un libro mayor descentralizado y la IAS, las personas podrán transferir dinero y cualquier otro activo de forma instantánea, de igual a igual y sin comisiones.
15. Algunos de estos proyectos son Jasper (Canadá), Ubin (Singapur), Khokha (Sudáfrica), RTGS RP (Inglaterra), Stella (Japón y Europa), LBChain (Lituania), an initiative by the Central Bank of Brazil (Brazil), Inthanon (Tailandia) o E-Krona (Suecia), entre otros.
16. https://cointelegraph.com/news/visa-files-patent-application-for-digital-currency

Tabla 5. Análisis de los ocho inconvenientes que presentan los sistemas de gestión de identidad tradicionales destacados por Gartner (Gartner 2020) frente al modelo de identidad auto-soberana.

Identidad digital tradicional	Identidad digital auto-soberana
Diseño, creación y mantenimiento caros. Cada sistema centralizado generalmente requiere su propia infraestructura.	Como existe una infraestructura central descentralizada, algunos de los costes son compartidos. Según la billetera digital que elijan para administrar su identidad, las tarifas para los usuarios pueden variar.[17]
No sirven para establecer y mantener una confianza real a través de la prueba de identidad.	Identidad digital verificable más fácil de emitir, administrar y presentar con billeteras digitales. Esto permite una mejor prueba de identidad en todo tipo de servicios, no solo en aquellos provistos por el gobierno y las instituciones financieras, como ocurre actualmente.
Propenso a la proliferación de datos y a la violación de la privacidad.	Como las personas tienen el control de sus datos y se pueden utilizar identificadores y seudónimos diferentes para interactuar con diferentes servicios digitales, la violación de privacidad directa o por correlación es mucho más improbable.
Expuestas a regulaciones de privacidad de datos debido a la recopilación, almacenamiento y análisis de datos confidenciales.	Privacidad por diseño. Los emisores de identidad ya no necesitarán conservar y mostrar los datos de los usuarios, y los proveedores de servicios pueden mantener registros usando identificadores seudónimos. Sin embargo, las regulaciones deben continuar mejorándose y adaptándose, y siempre deben ser respetadas.
Causa de un sinfín de problemas de calidad de los datos debido a la existencia de silos de información.	Los silos desaparecen ya que los usuarios controlan sus identificadores, autenticadores, datos y credenciales.
Vulnerables a los ataques de seguridad y se exponen en mayor medida a la pérdida de datos (debido a los repositorios centralizados).	Los repositorios centralizados se minimizan, y los hackeos contra registros descentralizados mantenidos por cada individuo se vuelven mucho más difíciles.
Susceptibles de registrar robos debido a la falta de control del propietario de la identidad.	El propietario ahora tiene el control y puede revocar fácilmente las credenciales y los identificadores tan pronto como detecte el robo.
Susceptibles a censura ya que los proveedores de identidad tienen la capacidad de suspender las cuentas.	Los emisores de identidad aún pueden revocar las credenciales, pero la trazabilidad de la emisión y la revocación es proporcionada por el registro descentralizado o la red blockchain. Las injusticias pueden ser perseguidas y resueltas.

17. Las billeteras digitales todavía no son productos definitivos y sus modelos de monetización aún no están deninidos. Algunas de las funcionalidades por pago pueden ser la generación de identificadores no correlativos, la firma electrónica avanzada o las copias de seguridad en la nube.

perdido una identificación a lo largo de nuestra vida y sabemos lo difícil y caro que es rehacerlas. Sin embargo, con la IAS, si perdiésemos el control de nuestra billetera digital, podríamos recuperar toda nuestra información de copias de seguridad encriptadas y seguras que se encuentran en la nube. Igualmente, podremos generar y almacenar copias personales discos duros.

Seguridad: las billeteras digitales tienen la capacidad de cumplir con estándares máximos de seguridad. Con diferentes fases de identificación, autenticación y autorización, los protocolos de IAS aseguran que nadie más que el propio usuario pueda acceder y usar su identidad. Además, la criptografía y la inmutabilidad de los registros descentralizados garantizan que las pruebas de la información no puedan ser manipuladas sin dejar rastro. En comparación con los miles de millones de registros de datos pirateados cada año (discutidos en la Sección 2.3.3) debido a silos de información centralizados, el enfoque de la identidad auto-soberana tiene el potencial de dificultar los hackeos al cifrar y proteger los datos personales en los dispositivos personales del propietario.

Seudónimo: en el modelo IAS, los individuos generan sus propios identificadores, siendo posible generar tantos como sea necesario para interactuar con diferentes servicios y personas sin posibilidad de establecer correlaciones. Además, los protocolos de IAS permiten divulgación selectiva de información y pruebas de conocimiento cero de modo que podemos probarle a alguien que tenemos más de 21 años sin revelar nuestra edad real. Hoy en día, sin embargo, para demostrar que somos mayores de una cierta edad, generalmente mostramos un documento de identificación que no solo revela de manera innecesaria nuestra fecha de nacimiento, sino que también revela información adicional no requerida, como nuestro nombre y apellidos, nuestra nacionalidad o los nombres de nuestros padres. En la Sección 7.3.7 abordaremos este tema con mayor profundidad.

Utilidad: la utilidad viene de la mano de la portabilidad, la recuperación, la seguridad, la interoperabilidad y el seudónimo. Obviamente, para que la IAS tenga un propósito, es necesario que cada vez más servicios públicos empiecen a ser accesibles bajo este marco. El estado actual, los principales desafíos y las hojas de ruta para el sector público y privado con respecto a la IAS se discutirán en el Bloque 5.

Recuperando la lista de inconvenientes de los sistemas tradicionales de identidad digital señalados por Gartner que presentamos en la Sección 3.3, podemos ver cómo son resueltos con el modelo de identidad auto-soberana.

Como veremos en el Bloque, la IAS no solo presenta beneficios directos en comparación con otros sistemas de gestión de identidad digital, sino que también tiene un gran potencial de impacto en desarrollo, inclusión social e inclusión financiera.

3.4. Taxonomía, conceptos básicos y aclaraciones

La siguiente lista taxonómica está completamente alineada con la ISO / IEC 24760-1 (ISO, 2019). La mayoría de las definiciones son una fusión entre la taxonomía proporcionada por el World Wide Web Consortium (W3C por su nombre en inglés) (W3C-VC, 2019) y el Instituto Nacional de Estándares en Tecnología (NIST por su nombre en inglés) (NIST-TA, 2020). Esta clasificación no pretende ser normativa, siendo su único propósito el de proporcionar definiciones consistentes y estandarizadas para los conceptos utilizados en este documento.

I. Agente de usuario: programa, como una especie de navegador u otro cliente web, que media la comunicación entre titulares, emisores y verificadores.

II. Atributo: característica de un sujeto.

III. Autenticador: token, como, por ejemplo, una clave privada o información biométrica, utilizada para autenticarse en un servicio digital.

IV. Credencial: representación de una identidad para su uso en autenticación.
Nota 1 a la entrada: una credencial es un conjunto de una o más declaraciones realizadas por un emisor sobre un tema.
Nota 2 a la entrada: las credenciales están asociadas a identificadores.

V. Credencial verificable: credencial a prueba de manipulación que tiene autoría y puede verificarse criptográficamente.

VI. Declaración: exposición o manifestación sobre un sujeto, realizada por un emisor como parte de una credencial.

VII. Divulgación selectiva: capacidad de un presentador para tomar decisiones detalladas sobre qué información compartir.

VIII. Documento de identificador descentralizado: documento accesible mediante un registro de datos verificable que contiene información relacionada con un identificador descentralizado específico.
Nota 1 a la entrada: también denominado documento DID.
Nota 2 a la entrada: la información típica contenida en un documento DID son los mecanismos de autenticación, las llaves públicas y los canales de contacto.

IX. Emisor: entidad que emite una credencial sobre un tema en nombre de un solicitante.

X. Entidad: elemento relevante para el propósito de operación de un dominio que tiene una existencia distinta reconocible.
Nota 1 a la entrada: una entidad puede tener una materialización física o lógica.
Nota 2 a la entrada: una entidad puede ser una persona, organización o dispositivo que desempeña uno o más roles en el ecosistema.

XI. Firma digital: esquema matemático para demostrar la autenticidad de un mensaje digital.

XII. Gráfico: red de información compuesta de sujetos y su relación.

XIII. Identidad: conjunto de atributos relacionados con una entidad.
Nota 1 a la entrada: las identidades digitales permiten la trazabilidad y la personalización de las interacciones de la entidad en contextos digitales, utilizando generalmente identificadores y atributos.
Nota 2 a la entrada: la distribución o el uso involuntario de la información de identidad pueden comprometer la privacidad.
Nota 3 a la entrada: la recopilación y el uso de dicha información debe seguir el principio de minimización de datos.

XIV. Identificador: atributo o conjunto de atributos que caracteriza de forma única una identidad en un contexto.
Nota 1 a la entrada: un identificador puede ser un atributo creado específicamente con un valor asignado para ser único dentro del dominio.
Nota 2 a la entrada: los identificadores son típicamente códigos alfanuméricos únicos asociados a una entidad.
Nota 3 a la entrada: un identificador puede ser una dirección de blockchain.

XV. Identificador descentralizado: identificador portable tipo URL asociado a una entidad.
Nota 1 a la entrada: también conocido como DID.
Nota 2 a la entrada: estos identificadores se usan con mayor frecuencia en una credencial verificable y están asociados con un sujeto de manera que una credencial verificable en sí misma se pueda portar fácilmente de un repositorio a otro sin la necesidad de volver a emitir la credencial.
Nota 3 a la entrada: ejemplo de un DID: 123456abcdef.

XVI. Libro mayor descentralizado: registro de información que se comparte y sincroniza de manera consensuada en múltiples sitios o computadores.

XVII. Minimización de datos: acto de limitar la cantidad de datos compartidos estrictamente al mínimo necesario para lograr con éxito una tarea u objetivo.
Nota 1 a la entrada: un ejemplo de la tarea u objetivo es la provisión de un servicio digital.

XVIII. Parte dependiente: entidad basada en la verificación de la información de identidad de una entidad en particular.

XIX. Predicado derivado: aserción booleana verificable sobre el valor de otro atributo en una credencial verificable.
Nota 1 a la entrada: los predicados derivados son útiles en presentaciones verificables de pruebas de conocimiento cero porque pueden limitar la cantidad de información expuesta.
Nota 2 a la entrada: si una credencial verificable contiene un atributo para expresar una altura específica en centímetros, un predicado derivado podría hacer referencia al atributo de altura en la credencial verificable que demuestre que el emisor da fe de un valor de altura de que el sujeto cumple con el requisito de altura mínima, sin revelar realmente el valor de altura específico. Por ejemplo, el sujeto mide más de 150 centímetros.

XX. Presentación: información derivada de una o más credenciales, emitida por uno o más emisores, que el titular expone a un verificador para comunicar cierta calidad sobre un tema.

XXI. Presentación verificable: presentación a prueba de manipulaciones codificada de tal manera que se pueda confiar en la autoría de los datos después de un proceso de verificación criptográfica.
Nota 1 a la entrada: ciertos tipos de presentaciones verificables pueden contener datos que se sintetizan a partir de, pero no contienen, las credenciales verificables originales (por ejemplo, pruebas de conocimiento cero).

XXII. Presentador: entidad que genera y divulga presentaciones.

XXIII. Propietario del sistema: entidad que posee un sistema de gestión de identidad determinado.

XXIV. Proveedor de identidad: entidad que proporciona información de identidad.
Nota 1 a la entrada: un proveedor de identidad es una entidad y/o un sistema para crear identidad, mantener y administrar credenciales para individuos, mientras proporciona servicios de autenticación a proveedores de servicios o aplicaciones de terceros.

XXV. Registro de datos verificables: rol que un sistema puede desempeñar al mediar la creación y verificación de identificadores, claves y otros datos relevantes.
Nota 1 a la entrada: un ejemplo de datos verificables son contratos inteligentes o redes blockchain.
Nota 2 a la entrada: un ejemplo de un caso de uso es un registro de revocación de certificados (CRL).
Nota 3 a la entrada: algunas configuraciones pueden requerir identificadores correlacionales para los sujetos.
Nota 4 a la entrada: algunos registros, como los de los UUID y las claves públicas, podrían actuar como espacios de nombres para los identificadores.

XXVI. Repositorio: lugar de almacenamiento de credenciales digitales.

XXVII. Solicitante: entidad que hace una solicitud a un emisor para emitir una credencial que contenga declaraciones sobre un tema[18].

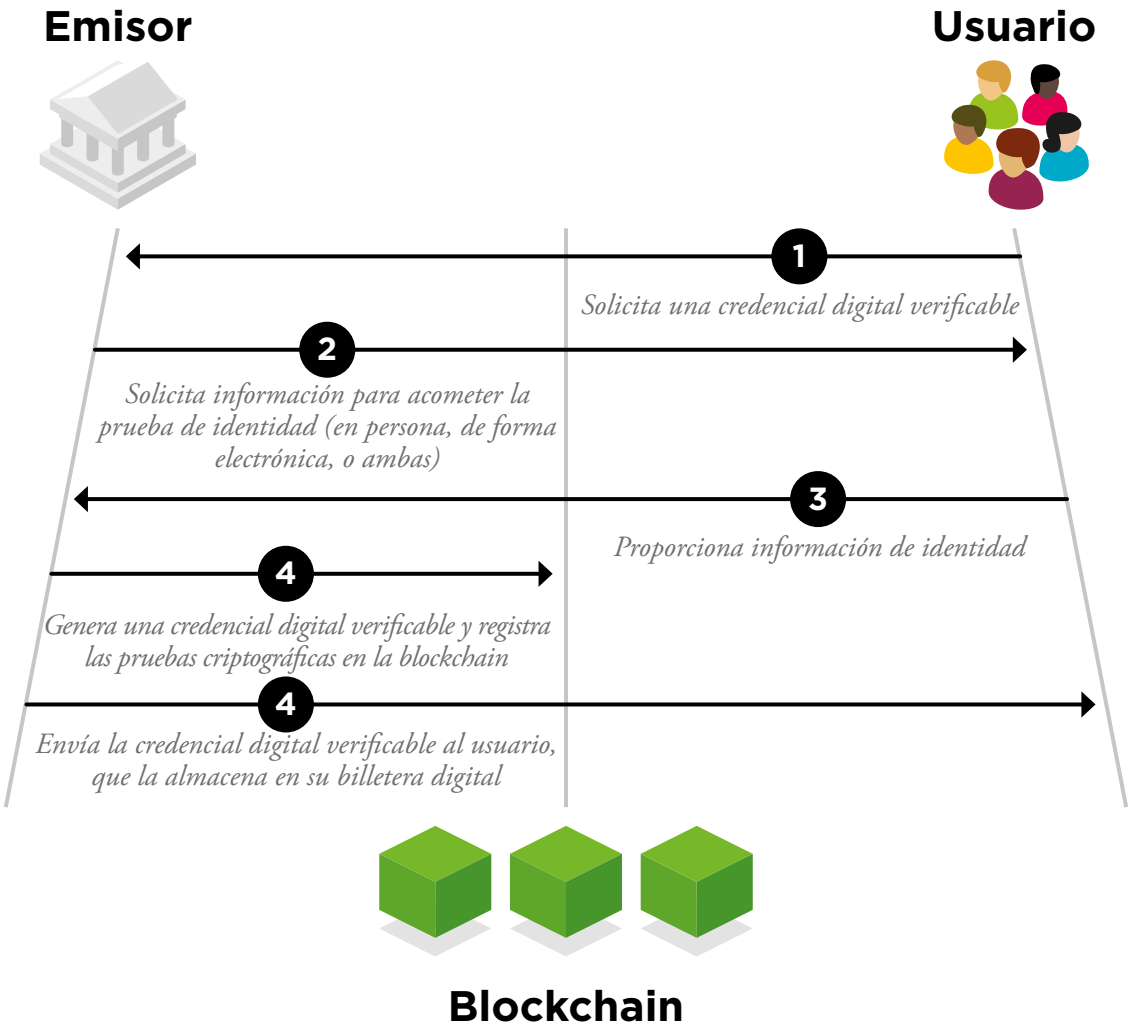
XXVIII. Sujeto: entidad cuya información de identidad se almacena y gestiona mediante un sistema de gestión de identidad.
Nota 1 a la entrada: en la IAS, los sistemas de administración de identidad son típicamente billeteras digitales personales.

XXIX. Titular: función que una entidad podría desempeñar al poseer una o más credenciales verificables y generar presentaciones a partir de ellas.
Nota 1 a la entrada: un titular suele ser, aunque no siempre, el sujeto de las credenciales verificables que posee. Los titulares almacenan sus credenciales en repositorios de credenciales.

XXX. UUID: identificador, tal como se define en [RFC4122].

18. El solicitante, el sujeto y el titular pueden ser la misma entidad, dos entidades diferentes o incluso tres entidades diferentes. Por ejemplo, cuando una entidad solicita credenciales sobre sí misma y luego las administra, es solicitante, titular y sujeto al mismo tiempo. Cuando una entidad, como por ejemplo una escuela, le pide al gobierno que emita un diploma digital para uno de sus estudiantes, y esta credencial debe ser administrada por los padres porque el estudiante es menor de edad, entonces el solicitante es la escuela, el sujeto es el estudiante y el titular es el padre.

Imagen 10. Solicitud de una credencial digital verificable.



XXXI. URI: identificador uniforme de recursos, según lo definido por [RFC3986].

XXXII. Validación: garantía de verificación.
Nota 1 a la entrada: un ejemplo es la garantía de que una credencial verificable o una presentación verificable satisface las necesidades de un verificador y otras partes interesadas dependientes.

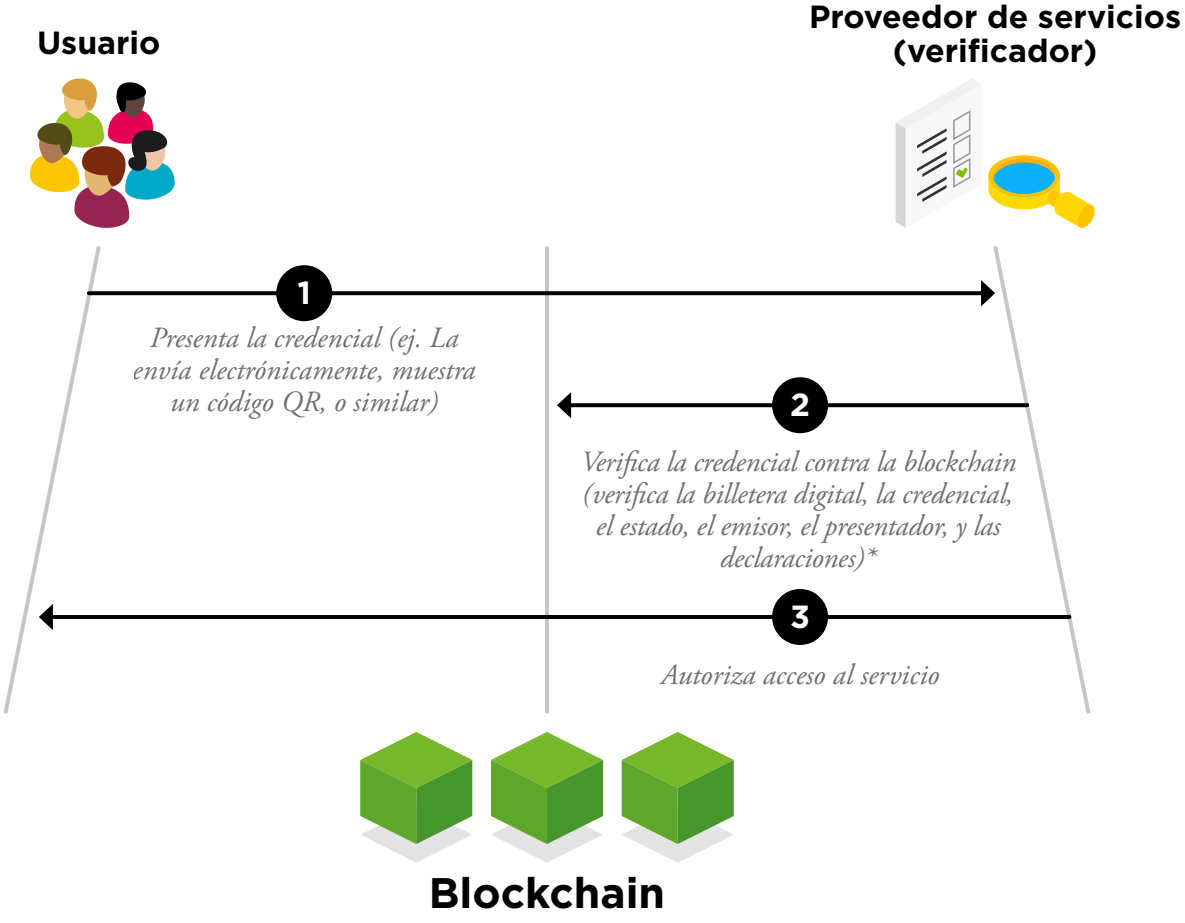
XXXIII. Verificación: proceso de establecer que la información de identidad asociada con una entidad particular es correcta.
Nota 1 a la entrada: esta definición ISO se centra más en la identidad digital tradicional. La IAS es más amplia que los sistemas de identidad digital tradicionales pues incluye no solo la capa de información de identidad sino también otros atributos que no son información de identidad como tal (por ejemplo, un diploma universitario).
Nota 2 a la entrada: esto también incluye la evaluación de si una credencial verificable o una presentación verificable es una declaración auténtica y oportuna del emisor o presentador, respectivamente.
Nota 3 a la entrada: la verificación de una credencial incluye validar que: la credencial (o presentación) se ajusta al formato; el mecanismo de prueba se satisface; el presentador está autorizado; y, si corresponde, la verificación de estado tiene éxito.

XXXIV. Verificador: entidad que realiza la verificación.
Nota 1 a la entrada: por ejemplo, una entidad que comprueba la validez de una presentación (puede ser en nombre de una parte confiable).

Con el fin de que esta taxonomía no resulte demasiado compleja, es importante aclarar y resaltar algunos conceptos:

- Como ya dijimos en la Sección 2.4.5, los proveedores de identidad ya no existen como tal en el modelo de identidad auto-soberana. En el esquema IAS, las entidades que emiten credenciales digitales ya no son las mismas que las administran en nombre de las personas para proporcionar autenticación a los proveedores de servicios o aplicaciones de terceros de confianza. Ahora, los proveedores de identidad o IdPs se han convertido en entidades que únicamente emiten la identidad, por lo que se les ha dado el nombre de emisores de identidad en lugar de proveedores.
- En el modelo IAS, los usuarios administran sus credenciales, generalmente usando billeteras digitales, y los proveedores de servicios pueden verificar las credenciales criptográficamente cuando les son presentadas.
- En los modelos centralizados y de terceros proveedores, los proveedores de identidad siempre actúan como los titulares. Sin embargo, en el modelo de identidad auto-soberana, los titulares son los individuos, sujetos de esa identidad.
- Un atributo será una declaración cuando se manifiesta en una credencial o una presentación.
- Esta taxonomía no se limita a esquemas de identidad digital para las personas. Los sujetos también pueden ser animales, plantas, cosas o procesos.

Imagen 11. Presentación y verificación de una credencial digital.



* Para más información, consultar el Proceso de Verificación de LACChain ID.

3.5. IAS y la tecnología blockchain

La tecnología blockchain y la identidad auto-soberana se complementan formando una simbiosis perfecta. Las soluciones de IAS necesitan registros de información descentralizados e inmutables para poder almacenar las pruebas de la propiedad de los identificadores únicos y la validez de las credenciales digitales. Estos registros también son útiles para almacenar listas de identificadores descentralizados, autoridades de certificación (CA por sun nombre en inglés) y otras listas de confianza públicas necesarios en el modelo de identidad auto-soberana. A la inversa, la identidad es necesaria[19] para poder crear redes de blockchain donde cualquier activo físico pueda ser digitalizado e intercambiado. De no ser así, la mayoría de las aplicaciones basadas en blockchain en áreas como cadena de suministro, comercio, notarización, registros de tierras o diplomas digitales, entre muchos otros, nunca serían aceptadas legalmente. Algunos de los beneficios de las redes blockchain para el modelo de IAS son los siguientes:

Billeteras digitales como repositorios: las billeteras digitales no dejan de ser repositorios digitales que permiten no solo almacenar y administrar claves, sino también generar presentaciones verificables y compartirlas con otros. Existen diferentes tipos de billeteras que se pueden conectar fácilmente a registros de blockchain, como veremos en la Sección 7.5.

Delegación automatizada: los contratos inteligentes se pueden utilizar para establecer fechas que permitan una transferencia automática de responsabilidad. Por ejemplo, cuando un menor de edad se vuelve legalmente responsable.

Direcciones de blockchain como DID: las direcciones de blockchain son códigos alfanuméricos únicos que se pueden usar de manera natura como identificadores descentralizados, como veremos en la Sección 7.1.3.

Fuente de verificación criptográfica: en el modelo IAS, los DID y las credenciales digitales deben verificarse criptográficamente. Debido a su inmutabilidad y descentralización, las redes blockchain son ideales para almacenar las pruebas criptográficas necesarias para estas verificaciones.

Listas de confianza: los marcos de confianza especifican quiénes puede emitir qué credenciales para cumplir con un cierto nivel de garantía en la identificación electrónica. Los contratos inteligentes también pueden ser utilizados por las entidades autorizadas para mantener listas de confianza. En la actualidad, las autoridades de certificación (CA) y las administraciones públicas mantienen las listas de confianza (TL) para los certificados digitales de manera centralizada, como veremos en la Sección 8.2.

Listas de revocación de certificados: en lugar de que cada emisor de identidad mantenga listas centralizadas de revocación de certificados, se pueden utilizar para este propósito los contratos inteligentes implementados, controlados y mantenidos por ellos mismos en la blockchain, lo que hace que sea más fácil, rápido y económico verificar, por ejemplo, si se revocó una credencial, como veremos en la Sección 7.2.6.

Notarización de credenciales: las redes blockchain permiten que cualquier credencial sea notarizada[20], lo que significa que la existencia de evidencia digital se pueda probar debidamente en cualquier momento posterior.

19. Lograr esto es, precisamente, el objetivo del programa LACChain. En la Arquitectura Blockchain de LACChain, reconocida por la UIT como una de las catorce arquitecturas de referencia de blockchain en el mundo (ITU, 2019), la IAS es una capa nativa de la infraestructura (capa 2), que complementa la red de blockchain con permiso público (capa 1) y habilita la emisión de electrónico basado en blockchain (capa 3).

20. Por notarización entendemos el registro del hash de una credencial.

Registros de DIDs: los contratos inteligentes son softwares implementados en una red blockchain que se puede usar de manera natural como registros de DID, como veremos en la Sección 7.1.3.

El enorme potencial de la tecnología blockchain o, extensiblemente, de los registros descentralizados, para complementar el modelo de identidad auto-soberana, ha sido ya ampliamente reconocido por entidades internacionales de renombre:

"Para las aplicaciones de identidad digital, existe un mayor uso de registros descentralizados autorizados entre entidades que confían unas en otras, pues proporciona mayor velocidad en la transaccionabilidad y mejora la privacidad de los datos. Muchos de los sistemas de identidad digital respaldados por blockchain que se han propuesto hasta la fecha son ejemplos de acumulación de IDs, por lo que la tecnología blockchain se puede utilizar para registrar transacciones entre un individuo (en principio sin otro documento de identidad digital formal) y un proveedor de servicios o una autoridad" - OIX (OIX-TOOLS, 2019)

"Gracias a una combinación de avances en hardware, que incluyen la creciente sofisticación de los teléfonos inteligentes, así como avances en criptografía y la llegada de blockchain, es posible construir nuevos marcos de identidad basados en el concepto de identidades descentralizadas, potencialmente incluyendo un interesante subconjunto de identidad descentralizada conocida como identidad auto-soberana" - UE (EU-BDID, 2019)

"La tecnología blockchain tiene el potencial de soportar nuevos modelos de propiedad de datos y gobierno con mecanismos integrados de control y consentimiento, que pueden beneficiar tanto a los usuarios como a las empresas al aliviar estas preocupaciones; como resultado, los IDMS basados en blockchain están comenzando a proliferar" – NIST (NIST-TA, 2020)

"Los registros descentralizados pueden representar alternativa futura de arquitectura para la gestión de identidad, y ciertamente es digna de evaluación por parte de los gobiernos que buscan establecer un marco nacional de identidad digital. Esta arquitectura acomoda a múltiples proveedores de identidad que interactúan con múltiples proveedores de servicios, como en otros modelos de arquitectura. La diferencia radica en lo que se llama el proceso de "certificación de identidad". En la práctica, esto significa que las credenciales de identidad son certificadas por usuarios y terceros a través de una base de datos descentralizada" - UIT (ITU, 2018)

"Es común implementar el tejido de confianza de identidad (ITF por sus nombre en inglés) utilizando una tecnología de contabilidad distribuida, que generalmente se basa en una plataforma blockchain (véase "Orientación para evaluar las plataformas blockchain"), para habilitar una red de identidad descentralizada. De hecho, ITF es la representación digital del marco de gobierno descentralizado que abarca las reglas del ecosistema de identidad descentralizado. Si bien algunos argumentan que ITF se puede implementar utilizando una tecnología DBMS centralizada, Gartner cree que blockchain es una opción más viable debido a su propiedad descentralizada" – Gartner (Garner, 2020)

IDENTIDAD DIGITAL AUTO-SOBERANA

Bloque 4

Potencial para la inclusión social y financiera

El desarrollo e implementación de soluciones de IAS sostenibles abre un nuevo mundo de posibilidades y usos prácticos. A continuación presentamos algunos ejemplos con gran potencial en el desarrollo y la inclusión social y financiera.

Acceso a la primera identidad: según las estimaciones del ID4D Dataset del Banco Mundial, en 2018 alrededor de mil millones de personas en todo el mundo carecían de prueba de identidad (WB-ID4D, 2018). El número reducido de puntos físicos de registro y las dificultades para llegar a ellos desde zonas rurales y sin recursos son dos de las principales causas por las que no se ha registrado, de media, el nacimiento de 1 de cada 10 niños entre 0 y 4 años en América Latina y el Caribe (IDB, 2013). Poder disponer de billeteras de identidad portables en posesión de los individuos permitiría a los gobiernos desarrollar programas en los que los representantes que actúen como notarios o certificadores oficiales de nacimientos puedan viajar a zonas rurales y poblaciones vulnerables para emitir certificados de identidad digital que se manejarían con estas billeteras. Si bien puede pensarse que de este modo no se garantizan los niveles más altos de garantía en la identificación, sería más que suficiente para identificar a las personas de estas poblaciones rurales y/o vulnerables con un grado mínimo de precisión que permitiese proporcionarles todo tipo de servicios, como educación o atención médica.

Catástrofes naturales: los desastres naturales son también una amenaza para la información esencial de las entidades y las personas. La digitalización de documentos (de identidad, médicos, diplomas, etc.) puede ser de gran utilidad para reducir el impacto de los desastres naturales en la pérdida de información. Sin embargo, es importante encontrar la manera más conveniente de llevar a cabo esa digitalización. Dado que los registros centralizados de información digital también pueden resultar dañados en los desastres naturales, la utilización de registros descentralizados y soluciones de IAS que permitan a los usuarios controlar sus identificadores y documentos digitales y recuperarlos fácilmente en caso de pérdida o robo puede ser en muchos casos la mejor opción para mitigar el daño que una catástrofe puede causar en cuanto a la pérdida de información. En 2015, la Agencia Federal para el Manejo de Emergencias (FEMA) de EE. UU. comenzó una iniciativa para transformar la forma en la que administraban las subvenciones y ayudas en casos de desastre natural. Afirmaron que "además de la validación de activos, FEMA puede usar la gestión de identidad de blockchain para emitir identidades electrónicas a personas que buscan ayuda y asistencia. Una identidad electrónica de blockchain puede ayudar a garantizar que FEMA tenga un registro único de cada persona y emitir pagos de alivio de manera segura y transparente". (FEMA, 2019)

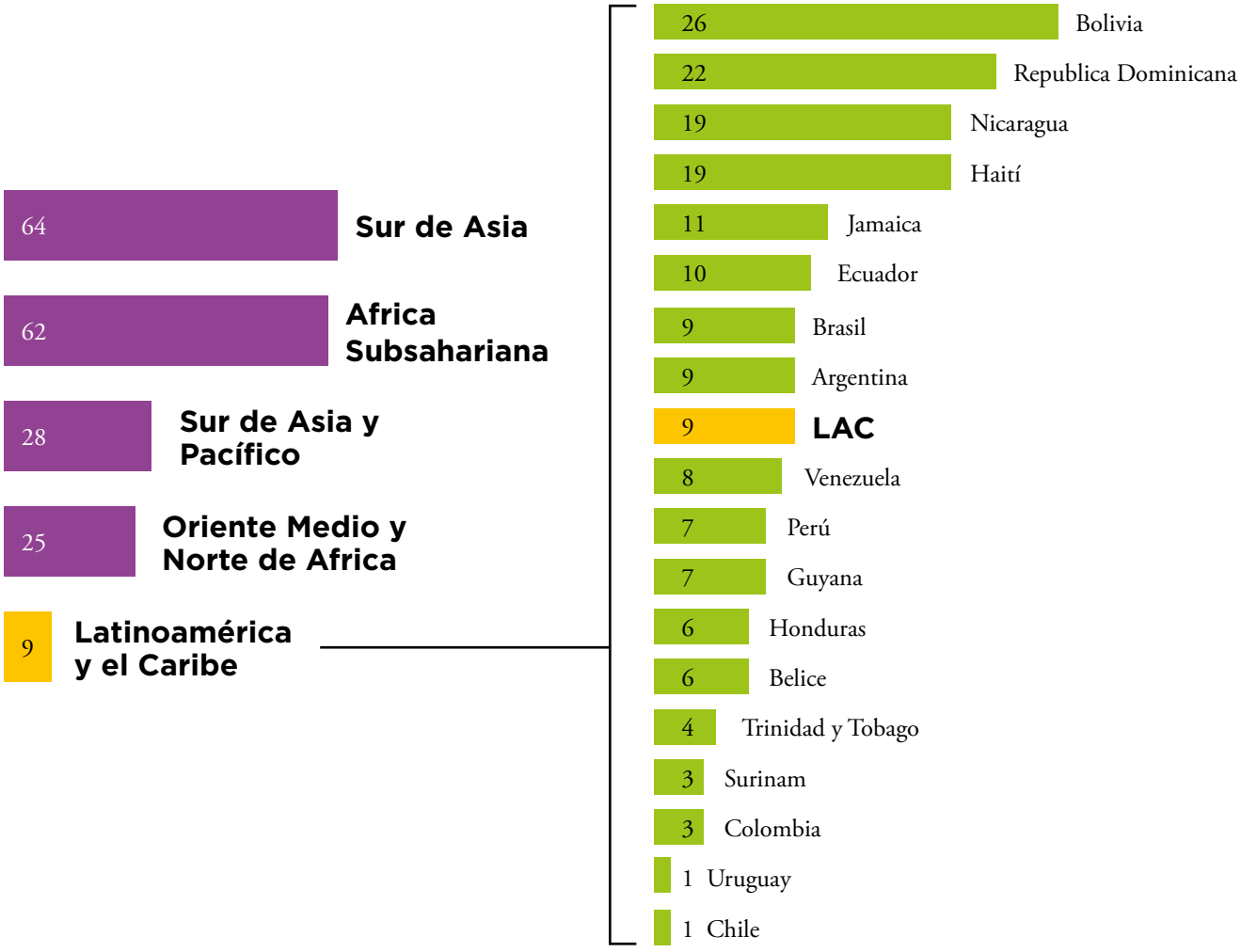
Diplomas digitales: la emisión, gestión, traducción y verificación de diplomas es un gran problema en todo el mundo. Muchos países pueden tardar dos, tres o incluso más años en emitir un diploma oficial de educación secundaria o universitario. Para poder presentarlos en el extranjero, generalmente se nos requiere llevar físicamente o bien las versiones originales o bien copias certificadas de los diplomas, además de las traducciones pertinentes. Por supuesto, cuando perdemos o nos roban los diplomas, la re-emisión puede resultar imposible. Además, no es solamente un problema de tiempo sino también de coste ya que los precios que debemos pagar si queremos recuperar estos documentos son muy elevados. Es innegable que todas estas trabas tienen que ver no sólo con los procesos y la tecnología, sino también con la normalización y la estandarización. La IAS fomenta la emisión de credenciales verificables digitales que no necesitan traducción, son portables, siguen estándares internacionales y pueden verificarse criptográficamente en tiempo real. Los tiempos de emisión también se pueden reducir, ya que no es necesario imprimir copias físicas y esperar a que las firmen las diferentes instituciones; los diplomas pueden emitirse digitalmente y ser firmados en el mismo instante. Podría incluso digitalizarse el historial académico de los estudiantes con las pruebas criptográficas almacenadas en la blockchain, y se podrían desarrollar contratos inteligentes para generar diplomas de manera automática firmadas

por los profesores o las entidades académicas tras completar los estudios.[21]

Educación: según un estudio del BID, los niños no registrados en América Latina y el Caribe tienen hasta un 17.7% menos de posibilidades de inscribirse en la escuela que aquellos que sí están documentados. Esto hace que tengan hasta un 25.3% menos de opciones de tener acceso a la educación primaria y hasta un 19.5% menos de tener acceso a la educación secundaria (IDB, 2013). Con un acceso más fácil a la identidad y una gestión más fácil de la identificación y autenticación proporcionada por la IAS se podría reducir considerablemente estos números.

Inclusión financiera: según informes del BID, en 2015 alrededor de 185 millones de personas en América Latina y el Caribe no tenían acceso a servicios financieros. En países como Bolivia,

Imagen 12. Porcentaje de niños sin registrar entre 0 y 4 años de 2000 a 2012. (IDB, 2013)



21. Un ejemplo muy ilustrativo de un proyecto que aprovecha la identidad auto-soberana para emitir diplomas digitales es el liderado por el Consejo de Exámenes del Caribe (CXC) y el Banco Interamericano de Desarrollo. Este proyecto emitió diplomas digitales a 24.000 estudiantes en una primera fase piloto, y ahora está desarrollando una segunda fase utilizando la Red LACChain Blockchain para emitir diplomas digitales en los países de Barbados, Jamaica y Trinidad y Tobago.

Colombia, El Salvador, Honduras, México, Nicaragua, Panamá y Perú, el acceso a estos servicios desde poblaciones en zonas rurales es inferior al 40%, debido en parte a que el desarrollo de plataformas digitales sostenibles y escalables ha sido escaso. En 2015, a pesar de que había 37 servicios de dinero móvil en 19 países de América Latina y el Caribe, éstos sólo representaban alrededor de 15 millones de cuentas con un 60% de inactividad (IDB, 2015). Las soluciones de IAS están llamadas a permitir una digitalización y bancarización más fácil, rápida y barata, al proporcionar información más confiable para los procesos KYC y AML. Además, la IAS auto-soberana no sólo contribuye a la inclusión financiera directamente, sino que también lo hace de manera indirecta, pues al habilitar la prestación de diversos servicios digitales como los descritos en esta sección generan incentivos para que las personas utilicen servicios financieros electrónicos y generen así un historial crediticio. Según entrevistas a la población estadounidense que no tiene cuentas bancarias, el 30.2% argumenta que no confía en los bancos, el 28.2% dice que les preocupa su privacidad y el 13.1% reconoce que no tiene interés en los servicios prestados (FDIC, 2017). Es muy probable que estas razones y muchas otras sean también aplicables tanto en América Latina y el Caribe como en el resto del mundo y podrían enfrentarse con las soluciones que propone la IAS.

Inmigrantes y refugiados: la IAS tiene potencial para facilitar el trabajo de las organizaciones multilaterales y de las ONG que se dedican a ayudar y proteger a refugiados e inmigrantes forzosos. Según estudios de las Naciones Unidas, en la actualidad hay 30 millones de refugiados en todo el mundo[22]. Muchos de ellos no solo no pueden demostrar su identidad, sino que tampoco pueden demostrar su capacidad o experiencia profesional. Tener soluciones de IAS y redes blockchain descentralizadas e inmutables proporciona nuevos mecanismos para que las ONG y los organismos multilaterales puedan emitir credenciales de identidad y certificaciones profesionales digitales y verificables[23].

Privacidad de los datos: como ya se analizó en la Tabla 7, la identidad auto-soberana mitiga los riesgos de abuso de la privacidad mediante la agregación de datos, elimina los silos de información, aumenta la dificultad de los ataques ya que los depósitos centralizados ya no son necesarios y permite realizar un seguimiento de la emisión y revocación de credenciales, de tal manera que los usuarios pueden reclamar y probar los abusos. Una implementación perfecta de la IAS permitiría también garantizar el consentimiento, el derecho al olvido, el derecho al seudónimo, la portabilidad de los datos y la minimización de la IIP, como veremos en la Sección 6.2.

Remesas: en 2014, un trabajo de investigación mostró que cada año entran más de 60 mil millones en concepto de remesas a América Latina y el Caribe (FOMIN-I, 2014). En países como Haití, Honduras, El Salvador, Jamaica, Guatemala y Nicaragua, los ingresos por remesas representaron entre el 10% y 34% de su PIB en 2017 (IDB-REM, 2017). Una parte importante del coste total de las remesas se genera en la última milla, ya que la mayoría de los receptores no tienen cuentas bancarias. Adicionalmente, la investigación realizada por FOMIN muestra que los remitentes envían mayores cantidades de dinero y con más frecuencia cuando los destinatarios tienen cuentas bancarias (FOMIN-II, 2014). Por lo expuesto en los párrafos anteriores, donde se presentaron algunas de las ventajas que la IAS ofrecer en términos de bancarización e inclusión financiera, este nuevo modelo de identidad tiene potencial para facilitar las transferencias y reducir el precio de las remesas. Combinado con

22. https://www.un.org/es/sections/issues-depth/refugees/index.html

23. UNICEF ha estado explorando aplicaciones de tecnologías blockchain desde 2015 https://www.unicefusa.org/stories/unicef-expands-use-blockchain-help-deliver-children/36473.

la tecnología blockchain, la identidad auto-soberana permitirá transferir dinero digital de una identidad digital a otra en tiempo real, reduciendo los tiempos y los costes de las remesas, puesto que por un lado se facilita la bancarización y se fomenta la inclusión financiera de personas en situaciones de pobreza, y por otro lado se reduce el número de entidades financieras intermediarias necesarias para pagos trasfronterizos.

Sanidad: sin duda el de la salud es uno de los sectores que más se beneficiará de la existencia de la identidad auto-soberana. Como ya explicamos en la Sección 2.3.3, la atención médica fue la industria más afectada por las violaciones de datos, habiendo sido el sector víctima del 48% del total de los hackeos en 2018. La fecha de nacimiento y/o los números de la Seguridad Social fueron los datos personales más comprometidos en 2018, exponiéndose en el 54% de las infracciones. La posibilidad de otorgar a las personas el control sobre sus registros médicos cambiaría esta situación, pues los centros médicos podrían minimizar la IIP que almacenan de sus usuarios, pasando de identificar a las personas con sus identificadores seudónimos, incluso a borrar completamente los registros médicos de sus bases de datos, para que los médicos tengan acceso a sus registros solo cuando los pacientes les permitan autenticarse con sus autenticadores auto-gestionados. La IAS también ha hecho posible incrementar el número de personas identificadas para que puedan proporcionárseles servicios sanitarios como, por ejemplo, las vacunas. En la actualidad, en América Latina y el Caribe, a los niños sin certificado de nacimiento se les administra, de media, un 13.9% menos de vacunas contra enfermedades peligrosas o potencialmente mortales en comparación con su aquellos que sí están documentados (IDB, 2013).

Seguridad pública e igualdad de género: tener una identidad auto-soberana y redes de blockchain inmutables puede ayudar a aumentar la seguridad pública mediante la notificación en tiempo real de infracciones de la ley, violencia o abusos personales. En el caso de mujeres maltratadas, los protocolos de acción podrían implementarse mediante contratos inteligentes, de manera que se activen tan pronto como se notifique un abuso[24].

Servicios gubernamentales: existen algunos países en el mundo que ya cuentan con sistemas nacionales de identificación digital que permiten acceder a diferentes tipos de servicios gubernamentales. El ejemplo de país más conocido y presentado generalmente como referencia es Estonia. Según la información proporcionada por el gobierno, el 98% de los 1.3 millones de estonios tienen una tarjeta de identificación y la usan para viajar, acceder a cuentas bancarias, generar firmas digitales, verificar registros médicos o votar electrónicamente.[25] La labor de Estonia es muy útil para mostrar que son las muchas ventajas de tener una identificación nacional emitida por el gobierno. Sin embargo, incluso las mejores implementaciones de identificaciones nacionales respaldadas por el gobierno tienen limitaciones importantes debido al modelo de identidad digital que está detrás y que es en general centralizado, como veremos en la Sección 5.3. La identidad digital auto-soberna permitirá a los gobiernos que ya cuentan con soluciones nacionales de identificación digital actualizarlas con un planteamiento más seguro y escalable, y supondrá una gran oportunidad para aquellos países que aún no la tienen pues les permitirá pasar de una situación de retraso en cuanto desarrollo y digitalización a colocarse a la cabeza de estos en este campo.

Transferencias monetarias condicionadas: desde la década de los noventa, la mayoría de los países de América Latina y el Caribe han desarrollado programas de transferencias monetarias condicionadas. En 2015, estos programas ya beneficiaban al 88.2% de la población de Uruguay y al 76.9% en Bolivia (IDB, 2016). Dichos programas enfrentan hoy muchos desafíos: la identificación y verificación de la población objetivo, la entrega de las transfe-

24. LACChain ha lanzado el desafío "Blockchangels", una llamada de ayuda para buscar soluciones de cara a enfrentar la violencia, el acoso y el abuso a mujeres, niños y ancianos. https://blockchangel.webintra.net/.
25. https://e-estonia.com/solutions/e-identity/id-card/

rencias condicionadas y la trazabilidad del dinero para verificar que se utilizó para su el propósito al que se había condicionado su entrega, entre otros (IDB, 2017). La IAS permite a las personas tener billeteras digitales donde pueden almacenar credenciales de identidad y dinero electrónico. Esto permite, a su vez, la verificación en tiempo real y sin coste alguno de la población objetivo (siempre y cuando se haya llevado a cabo un proceso previo de identificación digital), el envío en tiempo real y sin coste de transferencias monetarias, y la trazabilidad total del uso de las transferencias gracias a la red inmutable de blockchain, que también se puede aprovechar para crear contratos inteligentes con reglas que solo permitan gastar dinero para los fines condicionados.

Violaciones de datos: como vimos en la Sección 2.3.3, solo en el año 2018 más de 2.800 millones de registros de datos del consumidor fueron expuestos en un total de 342 infracciones, lo que supuso un coste de más de 654.000 millones de dólares (ForgeRock, 2019). Las violaciones de datos ocurren porque la información está centralizada en proveedores de identidad y proveedores de servicios, y no cuenta con medidas de protección suficientes. Con la nueva perspectiva de la IAS, los proveedores de identidad ya no administran las credenciales de los usuarios, sino que se convierten en meros emisores. Esto elimina la posibilidad de hackear información directamente de dichos proveedores. Con respecto a los proveedores de servicios, aún necesitan mantener cierta información de sus clientes. Sin embargo, como los sujetos se identifican mediante identificadores seudónimos en el modelo IAS, los proveedores de servicios pueden mantener información seudónima, minimizando así la cantidad de IIP. En un contexto ideal, en el que cada individuo es el único administrador de sus credenciales y datos personales, los hackeos son solo posibles de manera individual, lo que aumenta exponencialmente el tiempo y los esfuerzos necesarios para que los hackers pudieran obtener información privada.

IDENTIDAD DIGITAL AUTO-SOBERANA

Bloque 5

El camino hacia la adopción

5.1. Estado actual de la IAS

En la actualidad, la identidad auto-soberana todavía se encuentra en un estado prematuro. No obstante, su potencial ha sido ya reconocido ampliamente, como puede inferirse de la lectura de las citas de la Unidad Internacional de Telecomunicaciones (UIT), el Instituto Nacional de Estándares y Tecnología (NIST), la Unión Europea (UE) o el Open Identity Exchange (OIX) que hemos ido presentando en las secciones anteriores de este documento. Para que el modelo de IAS alcance un cierto grado de madurez que permita el desarrollo de soluciones de referencia tanto públicas como privadas, es necesario que se siga avanzando en la consolidación de las tres capas del marco tecno-legal que veremos en el segundo bloque de esta publicación, a saber, regulación, tecnología y marcos de confianza. El objetivo de esta sección es presentar un análisis general y a alto nivel del estado actual de estas tres capas.

Cualquier servicio electrónico confiable debe cumplir con la regulación. En el caso de la identidad digital auto-soberana, las dos grandes áreas regulatorias de interés son las regulaciones de firma y transacciones electrónicas, y las leyes de protección de datos. La firma electrónica, que constituye un elemento esencial del modelo IAS, pues constituye la base de confianza en el mundo digital, ya se encuentra regulada en un gran número de estados, incluyendo la mayoría de los países de América Latina y el Caribe. Sin embargo, no se puede decir lo mismo de las regulaciones en materia de protección de datos, ya que el número de países que carecen de ese tipo de políticas es muy superior, también en América Latina y el Caribe. Regulación actualizada sobre protección de datos es necesaria para garantizar que las soluciones y servicios digitales respeten los datos, los derechos y la privacidad de las personas. Las políticas regulatorias más reconocidas sobre firma electrónica y protección de datos proceden de la Unión Europea: Identificación electrónica, autenticación y servicios de confianza (eIDAS) y Reglamento general de protección de datos (GDPR), respectivamente. En las secciones 6.1.1 y 6.2.1 analizaremos la normativa actual sobre firmas electrónicas y protección de datos en América Latina y el Caribe, y en las Secciones 6.1.2 y 6.2.2 exploramos cómo se aplican eIDAS y GDPR a la identidad auto-soberana.

En lo que respecta a la tecnología, diferentes grupos de trabajo y agencias de estandarización han estado trabajando durante los últimos años en el desarrollo de nuevos estándares y protocolos que han constituido la base del modelo IAS. Algunos de estos esfuerzos proceden de Alastria, la Fundación de Identidad Descentralizada (DIF), la Fundación OpenID (ODIF), el Grupo de Trabajo de Ingeniería de Internet (IETF), la Infraestructura Europea de Servicios de Blockchain (EBSI), LACChain, NIST, OASIS, Sovrin o el World Wide Web Consortium (W3C). Hay dos estándares principales para la identidad auto-soberana: los identificadores descentralizados (DID) y las credenciales verificables (VC). Ambos se encuentran aún en su versión 1.0 y proponen, respectivamente, un modelo de datos para identificadores únicos en soluciones auto-soberanas, y un modelo de datos para la emisión, almacenamiento, presentación y verificación de credenciales digitales. También existen soluciones en el mercado que están aprovechando los nuevos estándares y protocolos para IAS como por ejemplo Evernym, Hyperledger Indy, KayTrust (por Everis), Rem (por World Data), Sovrin y uPort. Más adelante, concretamente en el Bloque 8 de este documento, cubriremos en detalle las diferentes capas de componentes tecnológicos que consideramos necesarios para el éxito de las soluciones de identidad auto-soberana.

Los marcos de confianza consisten en una serie de especificaciones, reglas y acuerdos legalmente aplicables que rigen un sistema multipartito establecido para un propósito común, en este caso el de habilitar interacciones electrónicas confiables utilizando esquemas de identidad digital auto-soberana para la identificación, autenticación y autorización de personas. Los marcos de confianza pueden ser públicos o privados, y pueden tener un alcance local, nacional, o regional. Desafortunadamente, apenas

existen hoy en día marcos de confianza hechos a medida para la IAS. Sin embargo, en la Unión Europea sí cuentan con un gran marco de confianza regional para la identificación electrónica: eIDAS. El Reglamento eIDAS organiza y normaliza la definición de órganos de gobierno y el mantenimiento de listas de confianza a nivel nacional para los países miembros de la Unión Europea. Igualmente, establece normas y canales estandarizados y seguros para la comunicación de información entre países, como las autoridades de certificación, los emisores de identidad y las listas de revocación de certificados. También obliga al no repudio de credenciales por parte de entidades públicas de los diferentes países miembros cuando dichas credenciales se han emitido cumpliendo con la normativa. En el resto del mundo, como por ejemplo en América Latina y el Caribe, no existe tal marco de confianza regional, y muchos países ni siquiera tienen uno nacional, como veremos en la sección 8.3 al discutir los enfoques de OIX, eIDAS y Sovrin.

5.2. Desafíos

Existen varios desafíos que la identidad auto-soberana debe enfrentar antes de que su uso pueda ser generalizado, habiendo sido algunos de ellos mencionados indirectamente en la sección anterior. Los presentamos a continuación:

Adaptación la infraestructura y modelos de datos digitales: la infraestructura de sistemas actual necesita una transición para permitir la emisión y verificación de credenciales de IAS para así poder acceder a los servicios digitales.

Análisis y comprensión de la tecnología por juristas, notarios y reguladores: una comprensión clara de la tecnología por parte de juristas, notarios y reguladores es necesaria para que la regulación se vaya actualizando al ritmo que la tecnología avanza.

Billeteras digitales: las billeteras digitales son una interfaz esencial entre los usuarios finales y la infraestructura descentralizada de IAS, y desempeñan un rol esencial para la identificación, autenticación y autorización de usuarios. Si bien ya están disponibles las primeras billeteras digitales, aún tienen mucho que mejorar en cuanto a seudonimización, experiencia de usuario, o recuperación de claves y credenciales. Existe por tanto una necesidad, que es al mismo tiempo una oportunidad, de crear un ecosistema de billeteras más grande y competitivo.

Captación de usuarios: es necesario proponer soluciones fáciles de usar, de carácter tanto público como privado, para atraer el interés de usuarios, de modo que la IAS sea ampliamente adoptada. También es muy importante desarrollar un mercado de aplicaciones donde se pueda usar la identidad auto-soberana para dar un propósito a estas soluciones.

Copias de seguridad: se precisa de una integración flexible entre billeteras digitales y servicios de respaldo de información para poder garantizar la recuperación de las credenciales y la información en control de los usuarios.

Derecho al olvido: debe poder garantizarse el derecho al olvido. Como se define en el Artículo 17 del RGPD[26], "el interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan" bajo ciertas condiciones. El enfoque de identidad auto-soberana puede facilitar la consecución de este derecho, ya que las personas tienen el control de sus identificadores, vinculados a su información digital, por lo que puede ser más fácil habilitar formas de rastrear dónde está la información digital y quién la tiene, y por lo tanto solicitar que se borre. Sin embargo, el hecho de que redes inmutables de blockchain se usen para almacenar pruebas criptográficas de la información también puede presentar grandes riesgos siendo necesario garantizar que se evite el registro de datos personales o IIP en estos registros descentralizados.

Marcos de confianza: marcos de confianza públicos y privados que permitan la definición de niveles de garantía en la identificación, autenticación y

26. https://gdpr-info.eu/art-17-gdpr/

autorización electrónica, y la creación de proveedores de identidad digital certificados dentro de un contexto determinado son necesarios, como por ejemplo eIDAS en la Unión Europea.

Participación de los gobiernos: los gobiernos deberán proceder a la transición hacia un esquema de IAS para la provisión de documentos de identificación nacionales y el establecimiento de marcos tecno-legales.

Políticas regulatorias: es necesario poder contar regulaciones de firmas y transacciones electrónicas, lo cual no ocurre en todos los países. También es preciso que las credenciales verificables se reconozcan como documentos electrónicos, y los registros descentralizados como registros electrónicos de confianza.

Privacidad: la identidad auto-soberana pude representar una solución para la privacidad si se tienen en cuenta las consideraciones pertinentes, pero también puede ponerla en riesgo en caso de desobedecerlas. Como ya hemos discutido, la IAS utiliza registros descentralizados de información para almacenar las pruebas criptográficas de los identificadores y las credenciales digitales; sin embargo, si en lugar de almacenar solamente las pruebas criptográficas en estos registros públicos e inmutables se registran también las credenciales en sí mismas que generalmente contienen datos confidenciales o información sensible, se estará violando la privacidad de los sujetos.

Protección de datos: es esencial poder contar con leyes de protección de datos más estrictas y modernas para garantizar derechos de privacidad en el tratamiento digital de la información.

Pruebas de conocimiento cero: las soluciones de prueba de conocimiento cero todavía están en una etapa de desarrollo y necesitan más tiempo para seguir evolucionando.

Reconocimiento de estándares: los estándares como los DID y las VC deben seguir evolucionando y madurando para ser aceptados y reconocidos por las Organizaciones de Desarrollo de Estándares (SDO por su nombre en inglés) como IEEE, ISO, UIT o NIST.

Recuperación de claves: la recuperación de claves no es lo suficientemente independiente, rápida y robusta en las soluciones disponibles en la actualidad por lo que se necesita más trabajo en esta área.

Registros descentralizados maduros: registros descentralizados de información maduros y sólidos en lo tecnológico y con un marco regulatorio robusto, y la capacidad de procesar grandes volúmenes de transacciones por segundo para generar y registrar identificadores y pruebas criptográficas de credenciales son necesarios para que las soluciones de IAS sean escalables. Sin embargo, el ecosistema fragmentado actual de redes blockchain no interoperables, no reguladas y con una baja capacidad transaccional está lejos de ser ideal. Los esfuerzos regionales para desarrollar redes público-permisionadas, como EBSI en Europa o LACChain en América Latina y el Caribe, han sido reconocidos como opciones muy prometedoras.

Seudónimo: el uso de registros de información públicos, descentralizados e inmutables exige un esfuerzo adicional para poder garantizar el seudónimo de la información y los identificadores. Estos registros no deben contener IIP.

Uso de la biometría: el uso de la biometría en la identidad auto-soberana para la prueba de identidad y la autenticación tiene un enorme potencial y requiere ser explorado en profundidad.

Todos estos desafíos son superables y no deben resultar desalentadores. La identidad auto-soberana presenta un gran cambio de paradigma y es por tanto natural que surjan algunos obstáculos que, sin duda, vale la pena enfrentar. La IAS traerá consigo mejoras en conveniencia, utilidad, reducción de costes, inclusión, seguridad, experiencia del usuario, prestación de servicios, oportunidades comerciales, accesibilidad y verificación, entre muchos otros. Del mismo modo, permitirá múltiples soluciones dirigidas a la inclusión social y financiera, como vimos en el Bloque 4.

5.3. Pasos para la adopción

Algunas entidades como la UIT (ITU, 2018), FATF (FATF, 2020), la Unión Europea (UE, 2018) y OIX (OIX, 2019) han desarrollado en los últimos años guías y pautas para el desarrollo de marcos de identidad digital nacionales liderados por gobiernos. A pesar de que estos no son específicos de la identidad soberana, son perfectamente aplicables a ella.

Los marcos y las soluciones de identidad se pueden clasificar en tres grupos o niveles según OIX (OIX, 2014), en función del marco normativo que rige la responsabilidad. En el nivel uno, el esquema de identidad digital se basa en el derecho público general que se aplica a todas las soluciones de identidad digital y a todas las personas físicas y jurídicas. El nivel dos también se basa en el derecho público pero, en este caso, solo aplica a jurisdicciones específicas. El nivel tres se consiste en reglas basadas en contratos privados que varias entidades acuerdan cumplir (derecho privado entre particulares). Resulta muy interesante analizar por separado cómo se aplica el enfoque de identidad auto-soberana a las soluciones basadas en marcos públicos y a las soluciones basadas en acuerdos privados, evaluando el potencial y la hoja de ruta para su adopción.

5.3.1. Oportunidades para los gobiernos.

Algunos gobiernos ya han habilitado esquemas de identidad digital nacional para que los ciudadanos de sus países puedan acceder a diferentes servicios electrónicos ofrecidos por la administración pública. Estonia es uno de los países de referencia con un sistema de tarjetas de identificación nacional obligatorio, adoptado por el 98% de la población[27], que habilita el acceso a todos los servicios electrónicos ofrecidos por la administración pública. En América Latina y el Caribe, una de las tarjetas de identificación electrónicas nacionales más avanzadas

Tabla 6. Tipos de esquemas de identidad digital dependiendo de la fuente normativa que rige la responsabilidad, según OIX.

Fuente normativa	Derecho común	Normativa de identidad digital	Contratos privados
Nivel	1	2	3
Ordenamiento jurídico	Derecho público	Derecho público	Derecho privado
Aplicación	A toda la jurisdicción	Participantes del sistema de identificación en la jurisdicción cubierta por el estatuto	Entidades parte del contrato

27. https://e-estonia.com/solutions/e-identity/id-card/

(DNIe, por su nombre en español) es la peruana, emitida por el Registro Nacional de Identificación y Estado Civil (RENIEC). En contraste con estos dos ejemplos, la mayoría de los países del mundo, incluidos la gran mayoría de América Latina y el Caribe, carecen de esquemas nacionales de identidad digital. Cada tipo de servicio electrónico requiere un nivel de garantía específico en la identificación electrónica (LOA por su nombre en inglés), y habilitar identidades digitales con un LOA equivalente al de un pasaporte físico requiere un esfuerzo normativo, regulatorio y tecnológico considerable. Además, incluso en aquellos países que cuentan con esquemas nacionales de identidad digital, en general su alcance se limita a proporcionar acceso a algunos servicios gubernamentales, pero no puede ser utilizada para acceder a servicios ofrecidos por entidades privadas. Por lo tanto, no existen contextos en los que un ciudadano pueda acceder a una amplia variedad de servicios digitales públicos y privados con su identidad digital.

Una de las principales razones por las que las soluciones de identidad digital ciudadana proporcionadas por las administraciones públicas tienen un alcance limitado son los sistemas de gestión de identidad digital existentes tras ellas. Estos esquemas de identidad tienen o bien a los propios gobiernos o bien a entidades designadas por ellos como proveedores de identidad; es decir, corresponden al modelo de identidad digital centralizado presentado en la Sección 2.4.1. Esto quiere decir que los autenticadores y los datos de los usuarios están centralizados directa o indirectamente en la infraestructura del gobierno. Este modelo funciona bien siempre y cuando los servicios a los que se accede sean proporcionados por gobierno. Por lo contrario, al plantear el uso de estas identificaciones digitales para acceder a servicios proporcionados por entidades distintas del gobierno la situación se vuelve menos favorable.

Sin embargo, creemos que el modelo de identidad auto-soberana tiene potencial para permitir a los gobiernos emitir credenciales digitales de identidad que puedan utilizarse para acceder a cualquier tipo de servicio digital (ya sea público o privado) sin necesidad de asumir grandes costos y esfuerzos en infraestructura ni responsabilidad adicional. En el enfoque de identidad auto-soberana, los gobiernos emiten credenciales de identidad cuyas pruebas se registran en una red de blockchain, así como listas de confianza, y aquella entidad tercera que desee verificar una identidad digital de un individuo ya no le pregunta directamente al gobierno, sino que va contra el registro descentralizado y público de información. Esto cambia totalmente la situación, pues en primer lugar el gobierno no necesita ofrecer ningún tipo de servicio para poder autenticar a los ciudadanos ante terceros, sino que se limitan a emitir credenciales digitales que están en posesión de los ciudadanos y que se verifica no contra un sistema del gobierno sino contra un registro público y descentralizado que el gobierno no tiene necesidad de mantener (aunque naturalmente pueda hacerlo si lo desea), lo que elimina la necesidad de un costo adicional de infraestructura. Por otro lado, al estar ahora las credenciales en posesión del ciudadano y ser el ciudadano quien las comparte con terceros para obtener acceso a sus servicios, es el ciudadano quien asume toda la responsabilidad sobre a quién le comparte información y datos personales. Con respecto a la responsabilidad ante los proveedores de servicios, dado que estos ya no van directamente contra la administración pública o el gobierno para que les garantice que una persona es quien dice ser sino que lo que hacen es verificar de manera indirecta una credencial emitida por el gobierno pero contra un registro público y descentralizado, puede entenderse que el gobierno ya no está ofreciendo un servicio de autenticación y por tanto no tiene responsabilidad sobre si el tercero decide confiar en sus credenciales para poder autorizar acceso a servicios a un individuo en particular.

Para aquellos gobiernos que ya cuentan con esquemas nacionales de identidad digital y que ya tienen un marco construido, la transición a la identidad auto-soberana podría ser sencilla, aunque implicaría posiblemente modificaciones en el reglamento, como veremos en el Bloque 7, y seguramente la incorporación de algunos elementos tecnológicos, como analizaremos en el Bloque 8. Para aquellos países sin un esquema

de identidad digital, existe una gran oportunidad para adentrarse en la IAS y colocarse a la cabeza de la identificación y autenticación electrónica del futuro. La UIT destaca cuatro áreas en las que centrarse cuando se trata de desarrollar modelos de identidad digital nacionales: el modelo de gobernanza, los enfoques para fomentar la adopción, el modelo arquitectónico y el modelo de sostenibilidad (ITU, 2018). En la Sección 8.1 presentamos una revisión desagregada de las diferentes capas que requieren los modelos de gobernanza en un modelo de identidad auto-soberana.

5.3.2. Oportunidades para el sector privado

El intercambio de información de identidad de ciudadanos o empresas es habitual entre entidades privadas. En general, cada pareja o conjunto de entidades que intercambia información sensible sobre sus clientes lo hace bajo un acuerdo privado multilateral, y en muchos casos estos intercambios son inseguros e ineficientes. Los estándares y protocolos de identidad digital auto-soberana abren la puerta a un intercambio de información de identidad mucho más estandarizado, seguro, y eficiente, que de lugar al desarrollo de plataformas y servicios digitales privados mucho más interoperables, seguros y confiables, en cumplimiento con regulaciones nacionales e internacionales.

Como vimos anteriormente en las secciones 2.3 y 2.4, algunas de las desventajas de los modelos de identidad digital centralizados y de identidad provista por un tercero son los silos de información, las bases de datos centralizadas, la existencia de diferentes tipos de identificadores para los mismos usuarios o la falta de estándares, protocolos, regulaciones y normas de protección de datos. Todos estos inconvenientes hacen muy difícil que las diferentes partes puedan desarrollar marcos privados comunes para soluciones de identidad digital. Por lo tanto, para que un grupo de entidades del mismo sector como por ejemplo aduanas, instituciones financieras o compañías de automóviles, puedan desarrollar plataformas comunes óptimas que requieran la identificación de individuos, como ventanas únicas o redes de liquidación, estos problemas han de ser abordados. La identidad auto-soberana proporciona una nueva forma de identificación y autenticación digital pues propone el uso de registros de información comunes, públicos y descentralizados; el uso de identificadores descentralizados siguiendo las mismas reglas para todos los usuarios; y el uso de estándares y protocolos comunes para la emisión, almacenamiento, presentación y verificación de credenciales digitales, entre muchas otras ventajas.

El hecho de tener un registro único y confiable, como una red blockchain regional, y seguir los protocolos y estándares comunes -identificadores descentralizados y credenciales verificables-, sería un gran primer paso para el desarrollo de marcos y acuerdos privados escalables, seguros y robustos, a un precio menor y con menos esfuerzo. Un ejemplo exitoso de este enfoque se puede encontrar en las aduanas de Chile, Colombia, Costa Rica, México y Perú. En el contexto del Proyecto Cadena, financiado por el Banco Interamericano de Desarrollo, estas cinco aduanas desarrollaron e implementaron una solución conjunta para usar la red regional blockchain de LACChain para poder intercambiar información confidencial. Con este fin, actualizaron sus acuerdos bilaterales de reconocimiento mutuo (ARM) para que se reconocieran las identidades auto emitidas de cada uno en la red blockchain y, por lo tanto, la información firmada electrónicamente por ellos en forma de transacciones blockchain.

Lo anterior, junto con las reglas de privacidad definidas a nivel de blockchain -que limitan la visualización de información confidencial a las agencias personalizadas que forman parte del ARM-, permitió que cinco aduanas de cinco países diferentes de América Latina y el Caribe, que no tienen siquiera regulaciones comunes de firma electrónica o protección de datos, creasen una solución común basada en una implementación privada del esquema de identidad auto-soberana para intercambiar información segura y confiable en tiempo real, y sin tener que mantener una plataforma centralizada, interconectar bases de datos centralizadas o integrar silos de información. En el

caso de las aduanas, hasta la creación de este proyecto, resultaba impensable construir una plataforma común con datos compartidos, accesos, esquemas de autenticación, integraciones, mantenimiento y muchos otros requisitos que permitiesen un intercambio alternativo eficiente de información con tecnología tradicional.

La identidad auto-soberana abre la puerta a un nuevo ecosistema de identidad, independiente de la supervisión y aprobación directa de los gobiernos. Las ONG, las instituciones financieras, los organismos multilaterales, las compañías de seguros privadas y otras grandes instituciones podrían convertirse en emisores de identidad y proporcionar credenciales digitales a las personas que ya hoy en día tienen capacidad de identificar, pudiendo desarrollar un modelo de negocio alrededor. Estas credenciales estarían bajo el control de los usuarios, permitiéndoles presentarlas electrónicamente ante cualquier persona o entidad que podría a su vez verificarlas contra un registro público. Diferentes tipos de entidades confiarían en la validez de estas credenciales al haber sido emitidas por grandes instituciones de su confianza.

5.3.3. Comparación según una mayor o menor participación del gobierno

Los pasos necesarios para desarrollar un ecosistema de identidad auto-soberano completo, escalable y funcional pueden ser similares en cuanto a sus objetivos, pero son diferentes en términos de gobernanza, roles y responsabilidades, dependiendo de cuánto se involucre el gobierno. En la Tabla 9 presentamos una visión hipotética de dos enfoques que cuentan, respectivamente, con un gobierno completamente involucrado y un gobierno que no se involucra en absoluto. Este análisis no pretende ser tomado como guía, sino que solamente se presenta a modo ilustrativo y parte de la base de una regulación completa y de la disponibilidad de la tecnología.

El primer paso para implementar cualquier solución de IAS es elegir una red descentralizada que sirva como registro de confianza. Hay dos redes regionales de blockchain, una en Europa y el otra en América Latina y el Caribe, que se están posicionando para servir como referencias estas regiones.

La Infraestructura Europea de Servicios Blockchain (EBSI por sus siglas en inglés) es una "iniciativa conjunta de la Comisión Europea y la Asociación Europea de Blockchain (EBP por su nombre inglés) para ofrecer servicios públicos transfronterizos en toda la UE utilizando la tecnología blockchain. La EBSI se materializará como una red de nodos distribuidos en toda Europa (blockchain), aprovechando un número creciente de aplicaciones centradas en casos de uso específicos. En 2020, EBSI se convertirá en un componente básico de CEF[28], proporcionando software, especificaciones y servicios reutilizables para apoyar la adopción por las instituciones de la UE y las administraciones públicas europeas"[29]. Los gobiernos europeos aprovecharán esta infraestructura de blockchain para probar cuatro usos prácticos en 2020: notarización, diplomas, identidad auto-soberana e intercambio de datos. Éste es el único esfuerzo regional liderado por entidades de gobierno para desarrollar una solución de identidad auto soberana que se conoce en el mundo. El UE está aplicando normativa europea como el eIDAS y el GDPR para construir una infraestructura regional de blockchain que habilite la IAS.

El SSI eIDAS bridge, un piloto que busca proporcionar una solución de identidad transfronteriza que cumpla con el marco de confianza del Reglamento eIDAS, describe tres escenarios a corto, medio y largo plazo. En el corto plazo sugiere algunas recomendaciones en las que no es necesario realizar cambios en el Reglamento. Para el medio y el largo plazo, indica los principales cambios necesarios en el Reglamento para cumplir con los principios de diseño[30] de la IAS, como analizaremos más pormenorizadamente en la Sección 6.1.2.

28. CEF stands for "common European framework".
29. https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI
30. https://joinup.ec.europa.eu/collection/ssi-eidas-bridge/document/ssi-eidas-legal-report-flyer

Tabla 7. Dos marcos hipotéticos según la implicación del gobierno.

	Gobierno involucrado	Gobierno no involucrado
Desarrollo de un registro fiable	El gobierno podría desarrollar y mantener un registro público y descentralizado. En el caso de una red blockchain, también definiría las reglas para permitir que otros formasen parte de la red.	Las entidades privadas, generalmente consorcios, desarrollarían y mantendrían las redes.
Desarrollo de billeteras digitales confiables	El gobierno podría designar ciertos proveedores de servicios para convertirse en proveedores autorizados de billeteras digitales.	Sería necesario un mercado de billeteras digitales en el que los usuarios puedan confiar para administrar sus autenticadores y credenciales, proporcionando seudónimos, seguridad y garantías de recuperación. Diferentes proveedores competirían para posicionarse en el mercado.
Atraer a los usuarios	El gobierno podría obligar a los ciudadanos a utilizar una identificación digital para los servicios gubernamentales.	Sería necesario presentar aplicaciones interesantes para promover el uso de billeteras digitales para generar y administrar DID. El desarrollo de un mercado de proveedores de servicios que acepten IAS sería fundamental.
Generación de DIDs	El gobierno podría desarrollar o elegir un método DID existente, y exigir a los proveedores de billeteras que lo usen.	La comunidad seguiría contribuyendo proponiendo métodos DID más seguros y escalables. Diferentes proveedores de billeteras elegirán qué método/s usar.
Reconocimiento de normas o estándares	Para ser aceptados e implementados en todo el mundo, estándares como los identificadores descentralizados y credenciales verificables deben ser reconocidos por agencias internacionales de estándares, como IEEE, ISO, UIT o NIST.	Para ser aceptados e implementados en todo el mundo, estándares como los identificadores descentralizados y credenciales verificables deben ser reconocidos por agencias internacionales de estándares, como IEEE, ISO, UIT o NIST.
Emisión de credenciales verificables	El gobierno podría desarrollar la infraestructura y protocolos necesarios para emitir credenciales verificables como documentos de identificación digital (por ejemplo, un pasaporte digital).	Las organizaciones necesitarían desarrollar mecanismos para emitir credenciales digitales basadas en IAS, de manera que se genere un mercado de emisores de identidad.
Aceptación por parte de los proveedores de servicios	Para los proveedores de servicios, la IAS con identidades digitales generadas por gobiernos es muy conveniente, ya que les proporciona una mayor accesibilidad a los usuarios, permitiéndoles verificar su identidad con un mayor nivel de garantía antes de proporcionarles el servicio digital.	Los proveedores de servicios deberían comenzar a aceptar soluciones IAS para autenticarse en sus servicios. Probablemente, algunos proveedores de servicios serían los primeros en convertirse en emisores de identidad de credenciales verificables digitales alineadas con el modelo IAS, que sus clientes podrían usar para autenticarse en sus servicios.

En América Latina y el Caribe, el programa LACChain dirigido por el BID Lab está ya permitiendo el despliegue de soluciones de identidad auto-soberana al proporcionar una red gratuita con estándares y protocolos internacionales, soporte técnico y un gran grupo de expertos y asesores internacionales. Esta red sido reconocida como una de las catorce arquitecturas de referencia en el mundo por la Unión Internacional de Telecomunicaciones (ITU, 2019). A diferencia del enfoque EBSI, en esta iniciativa no hay un gobierno o un conjunto de gobiernos que mantengan la infraestructura, siendo en cambio el BID y sus aliados quienes se encargan de su mantenimiento. Sin embargo, LACChain también está recomendando a los gobiernos que usen su infraestructura, protocolos y estándares o que construyan los suyos, permitiendo así un enfoque complementario basado en la intervención de los gobiernos. Cabe mencionar que LACChain ya ha conseguido implementaciones reales de identidad auto-soberana como, por ejemplo, el Proyecto Cadena comentado en la sección anterior[31].

31. La red blockchain LACChain y la red blockchain de EBSI usan la misma tecnología, estándares y protocolos, por lo que estas dos infraestructuras podrían llegar a interoperar eventualmente. Las dos iniciativas están inspiradas y colaboran también con Alastria, un esfuerzo pionero liderado por una gran comunidad de entidades asociadas en España.

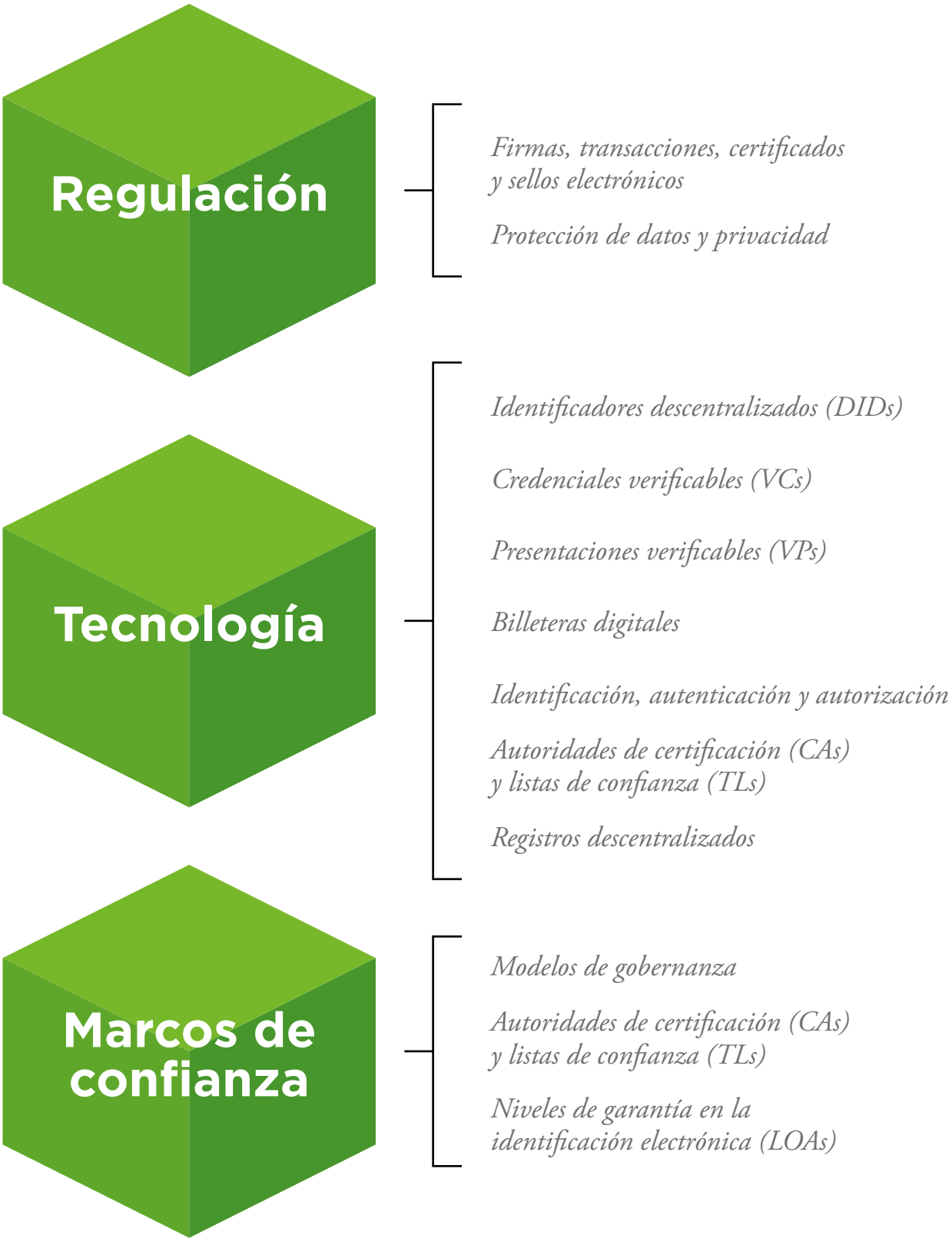
IDENTIDAD DIGITAL AUTO-SOBERANA

Capítulo II

Las tres capas necesarias para la identidad auto-soberana

Regulación, tecnología y marcos de confianza

BID BID | LAB LACCHAIN


Regulación
Firmas, transacciones, certificados y sellos electrónicos
Protección de datos y privacidad
Tecnología
Identificadores descentralizados (DIDs)
Credenciales verificables (VCs)
Presentaciones verificables (VPs)
Billeteras digitales
Identificación, autenticación y autorización
Autoridades de certificación (CAs) y listas de confianza (TLs)
Registros descentralizados
Marcos de confianza
Modelos de gobernanza
Autoridades de certificación (CAs) y listas de confianza (TLs)
Niveles de garantía en la identificación electrónica (LOAs)

Para poder de desarrollar soluciones de identidad digital auto-soberana robustas, escalables y que cumplan con la regulación, entendemos que hay tres capas complementarias que deben ser consideradas.

La primera capa es la regulatoria. El modelo de identidad auto-soberana se basa en la criptografía de las redes blockchain inmutables y descentralizadas, la firma electrónica de transacciones y certificados digitales, y como los sellos de tiempo. Además, para garantizar la protección de los datos y la información de las personas, también se requiere una regulación moderna en materia de protección de datos. Desafortunadamente, algunos países carecen de regulación de ningún tipo sobre firmas y transacciones electrónicas, y un mayor número no cuenta con regulación en materia de protección de datos y privacidad.

La segunda capa es la tecnológica. En la actualidad, están emergiendo nuevas tecnologías, conceptos, estándares y protocolos que son necesarios para diseñar y desarrollar soluciones de identidad auto-soberana. En primer lugar, el modelo IAS requiere de registros de información descentralizados. En segundo lugar, necesita de la existencia de nuevos estándares para generar identificadores únicos, credenciales digitales verificables y presentaciones digitales verificables. En tercer lugar, precisa una nueva generación de repositorios digitales para permitir a las personas almacenar, administrar, presentar y recuperar datos personales de manera sencilla y segura. Por último, pero no por ello menos importante, todos lo anterior exige que se creen nuevos protocolos de identificación, autenticación y autorización electrónica.

La tercera capa son los marcos de confianza. En un contexto de identidad digital, sea de auto-soberanía o no, un marco de confianza define el modelo de gobernanza, las autoridades de certificación, los proveedores de identidad, los niveles de garantía y los canales de comunicación, entre otros, permitiendo así establecer cadenas de certificación, listas de confianza, listados de revocación de certificados y muchos otros elementos confiables necesarios para el reconocimiento de las identidades y la autorización para poder acceder a servicios e información.

IDENTIDAD DIGITAL AUTO-SOBERANA

Bloque 6
Regulación

La regulación es la primera capa en cualquier modelo de identidad, digital o no. Para poder proporcionar IAS de manera confiable y escalable a las personas de todo el mundo, es necesario revisar las regulaciones en materia de firma electrónica y leyes de protección de datos, pues son varios los gobiernos que aún no han regulado el uso de la firma electrónica y son aún muchos más los que no tienen regulaciones actualizadas en materia de protección de datos.

6.1. Políticas regulatorias

El modelo de identidad auto-soberana se basa en la criptografía de los registros inmutables y descentralizados, la firma digital de transacciones y certificados digitales, y los sellos de tiempo electrónicos. Afortunadamente, estos temas no suponen una novedad para muchos países desde una perspectiva regulatoria o legislativa. Sin embargo, el desarrollo de la identidad auto-soberana está condicionado al reconocimiento del valor legal de elementos como las redes blockchain, los identificadores descentralizados, las credenciales verificables o las billeteras digitales, que cubriremos en El bloque 7. Los pasos a seguir para poder modernizar las regulaciones existentes en materia de identificación y autenticación electrónica convirtiéndolas en versiones actualizadas que reconozcan, ya sea explícita o implícitamente, los nuevos elementos introducidos por la IAS, deben analizarse de forma individualizada para cada región. Por otro lado, los países que carecen de cualquier tipo de política regulatoria tienen ahora una gran oportunidad de dar un paso al frente y avanzar en este campo.

Además, estos nuevos elementos traen consigo varios retos, pues las tecnologías descentralizadas no han sido utilizadas anteriormente de manera general para la gestión de identidad. Además, el registro de datos en redes internacionales también precisa de la existencia de marcos de confianza basados en las distintas regulaciones nacionales, como veremos en el Bloque 8. Es por ello que algunas preguntas como las que expondremos a continuación requieren ser abordadas por primera vez:

- Si una entidad difunde una transacción en una red blockchain que podría violar la ley y los otros nodos blockchain incorporan esta transacción a su copia de la red, ¿están también violando la ley? ¿Recae alguna responsabilidad sobre los generadores de bloques pese a que solo apliquen las reglas lógicas para la validación de las transacciones, que generalmente no incluyen la revisión de su contenido de datos?
- ¿Cuáles son los requisitos aplicables para cumplir con la ley para una entidad que brinda servicios en uno o varios países y registra datos en una red descentralizada donde algunas de las copias se mantienen en otro conjunto de países, cuando todos estos países tienen políticas reguladoras diferentes?
- ¿Es el hash de un dato personal también un dato personal?

La finalidad de este documento no es responder a estas preguntas, sino mostrar el estado actual de la regulación, así como resaltar la necesidad y motivar el desarrollo de políticas reguladoras modernas para soluciones de identidad auto-soberana que garanticen la escalabilidad, la interoperabilidad y la privacidad de los datos.

6.1.1. Regulación de transacciones electrónicas, firmas y documentos en América Latina y el Caribe.

Desde 1999, la mayoría de los países de América Latina y el Caribe han aprobado leyes y reglamentos sobre transacciones, firmas y documentos electrónicos. La Tabla 15 recoge información actualizada sobre el estado actual de la regulación de firma electrónica de los 42 países de América Latina y el Caribe. Una lista basada en la Corporación Andina de fomento (CAF) se presenta en la Tabla 12 (CAF, 2012). En la Sección Referencias se pueden encontrar los enlaces a la versión digital de estas regulaciones.

Del análisis de la Tabla 15 se deduce que la mayoría de los países de la región de América Latina y el Caribe ya tienen algún tipo de regulación sobre firmas y transacciones electrónicas. Los 7 países de América Central y México cuentan con regulación.

Tabla 8. Regulaciones nacionales de transacciones, firmas y documentos electrónicos en América Latina y el Caribe.

País	Región	Regulación	Año
Antigua and Barbuda	Caribe	Acta de transacciones electrónicas (modificación).	2006
Argentina	América del Sur	Ley 25506.	2001
Aruba	Caribe	-	-
Bahamas	Caribe	Acta de Comunicaciones y Transacciones Electrónicas.	2003
Barbados	Caribe	Acta de transacciones electrónicas (modificación).	2014
Belice	América Central	Acta de transacciones electrónicas (modificación).	2003
Bolivia	América del Sur	Ley No. 164.	2011
Brasil	América del Sur	Ley No. 25506.	2001
Chile	América del Sur	Law No. 19.799	2002
Colombia	América del Sur	Ley No. 527.	1999
Costa Rica	América Central	Ley No. 8454.	2005
Cuba	Caribe	No hay leyes, diferente normativa segregada.	-
Dominica	Caribe	No hay precedentes legales.	-
Ecuador	América del Sur	Ley No 2002-67 (2002) y Decreto No. 3496 (2018)	2018
El Salvador	América Central	Decreto No.133.	2015
Granada	Caribe	Acta de transacciones electrónicas.	2008
Guadalupe	Caribe	No hay precedentes legales.	-
Guatemala	América Central	Decreto No. 47-2008.	2008
Guyana	América del Sur	No hay precedentes legales.	-
Guyana Francesa	América del Sur	No hay precedentes legales.	-
Haití	Caribe	Proyecto de ley sobre firma electrónica.	2014
Honduras	América Central	Ley No. 35217.	2020
Islas Caimán	Caribe	Ley No 4.	2000
Islas Turcas y Caicos	Caribe	-	-
Islas Vírgenes	Caribe	-	-
Jamaica	Caribe	Acta de transacciones electrónicas.	2007

Country	Region	Regulation	Year
Martinica	Caribe	-	-
México	América del Norte	Ley de firma electrónica avanzada.	2012
Nicaragua	América Central	Ley No 729.	2011
Panamá	América Central	Law No. 51 (2008) Law No. 82 (2012)	2012
Paraguay	América del Sur	Law No. 4017/10 Decree 7369	2001
Perú	América del Sur	Ley No. 27269.	2000
Puerto Rico	Caribe	Ley No. 148 (2006) Ley No. 155 (2010) Ley No. 75 (2019)	2019
República Dominicana	Caribe	Ley No. 126.	2002
San Bartolomé	Caribe	-	-
San Cristóbal y Nieves	Caribe	-	-
San Vicente y las Granadinas	Caribe	Acta de Transacciones Electrónicas.	2007
Santa Lucía	Caribe	Acta de Transacciones Electrónicas.	2007
Surinam	América del Sur	Anteproyecto de ley de transacciones electrónicas.	2017
Trinidad y Tobago	Caribe	Acta de transacciones electrónicas.	2011
Uruguay	América del Sur	Ley No. 18600.	2009
Venezuela	América del Sur	Ley de mensajes de datos y firmas electrónicas.	2014

Los 13 países de Sudamérica excepto Guyana y la Guyana Francesa también aprueban. Solo en el Caribe encontramos un elevado número de países, muchos de ellos islas pequeñas, sin regulación en materia de firmas y transacciones electrónicas, siendo 9 de 21 los que no cuentan con ella. En total, 31 de los 42 países de América Latina y el Caribe los que cuentan con políticas regulatorias en esta materia, lo que representa un 74%.

Este es el primer paso necesario para poder proporcionar un marco regulatorio adecuado para esquemas de identidad digital, y en particular para esquemas de identidad auto-soberana. Si se desease determinar qué modificaciones tendrían que llevarse a cabo -si es que hubiese que hacerlas- para habilitar soluciones de IAS que estén totalmente respaldadas por la ley sería necesario un análisis de cada una de estas regulaciones.

Para que las soluciones nacionales existentes y futuras de identidad digital sean escalables e interoperables en la región, es esencial contar con una marco regulatorio regional para transacciones, firmas y

documentos electrónicos, así como estándares y protocolos comunes que permitan el reconocimiento mutuo. La identidad digital soberana, con su propuesta de descentralización y la interoperabilidad, tiene potencial para facilitar la conciliación de los diferentes esquemas de identidad nacionales.

6.1.2. Reglamento eIDAS, IAS y blockchain

La Unión Europea cuenta con la regulación más avanzada y reconocida a nivel mundial en materia de transacciones, firmas y documentos electrónicos, a saber, el Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo de 23 de Julio de 2014[32], relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior interno y por el que se deroga la Directiva 1999/93/CE, también conocido como eIDAS. Este Reglamento se propone "reforzar la confianza en las transacciones electrónicas en el mercado interior proporcionando una base común para lograr interacciones electrónicas seguras entre los ciudadanos, las empresas y las administraciones públicas[33] e incrementando, en consecuencia, la eficacia de los servicios en línea públicos y privados, los negocios electrónicos y el comercio electrónico en la Unión". A tal fin, el Reglamento eIDAS (UE, 2019):

- Asegura que las personas y las empresas puedan usar sus propios esquemas nacionales de identificación electrónica (eIDs) para acceder a los servicios públicos en otros países de la UE donde también estén disponibles los eIDs.
- Crea un mercado interior interno europeo para los servicios de confianza electrónica al garantizar que funcionarán más allá de las fronteras y tendrán el mismo estatus legal que los procesos tradicionales basados en papel.

El eIDAS reconoce en su Artículo 3 varios elementos relacionados con la identidad digital, de los cuales nos interesan especialmente los cinco siguientes:

Documento electrónico: todo contenido almacenado en formato electrónico, en particular, texto o registro sonoro, visual o audiovisual.

Firma electrónica: datos en formato electrónico ligados o asociados de manera lógica a otros datos en formato electrónico que utiliza el firmante para firmar.

Identificación electrónica: el proceso de utilizar los datos de identificación de una persona en formato electrónico que representan de manera única a una persona física o jurídica o a una persona física que representa a una persona jurídica.

Sello de tiempo electrónico: datos en formato electrónico que vinculan otros datos en formato electrónico a un instante concreto, estableciendo evidencia de que estos últimos datos existían en ese instante.

Sello electrónico: datos en formato electrónico ligados a otros datos en formato electrónico, o asociados de manera lógica con ellos, para garantizar el origen y la integridad de estos últimos.

32. https://www.boe.es/doue/2014/257/L00073-00114.pdf
33. El Reglamento eIDAS supervisa la identificación electrónica y los servicios de confianza para transacciones electrónicas en el mercado interior de la Unión Europea; regula las firmas electrónicas, las transacciones electrónicas, los organismos involucrados y sus procesos de integración para proporcionar una forma segura para que los usuarios realicen negocios en línea, como transferencias electrónicas de fondos o transacciones con servicios públicos. Esto permite que tanto el firmante como el destinatario puedan tener más comodidad y seguridad en las transacciones electrónicas. En lugar de depender de los métodos tradicionales, como el correo o el fax, o presentarse en persona para aportar documentos en papel, ahora pueden realizar transacciones transfronterizas digitalmente. El reglamento eIDAS ha definido los estándares para los que las firmas electrónicas, los certificados digitales cualificados, los sellos electrónicos, las sellos de tiempo y otros mecanismos de prueba de autenticación permiten transacciones electrónicas con la misma validez legal que el papel.

El eIDAS también diferencia tres niveles o grados de confianza:

- Simple/Ordinario.
- Avanzado.
- Cualificado.

Con respecto a su efecto legal, cualquier firma o sello electrónico, independientemente de su clasificación como "ordinario" o "simple", "avanzado" o "cualificado", persigue un mismo objetivo: atribuir el contenido del documento a una persona física o jurídica y por ello todos son potencialmente válidos y, según el caso, perfectamente aceptables. (Alamillo, 2020)

Los nuevos elementos tecnológicos que introduce la IAS no deben considerarse ajenos a los elementos electrónicos ya definidos y regulados por eIDAS, sino que han de clasificarse usando la taxonomía existente. Por ejemplo, los contratos inteligentes y las credenciales verificables podrían ser tratados como documentos electrónicos y las firmas de transacciones en redes blockchain podrían ser tratadas como firmas electrónicas, con todas las implicaciones legales que eso conlleva.

En este contexto, la pregunta que surge de manera natural es: ¿Es el Reglamento eIDAS, la regulación más avanzada sobre transacciones electrónicas, firmas y documentos, ideal para la IAS y la tecnología blockchain? El eIDAS Bridge[34] -una iniciativa para promover eIDAS como un marco de confianza para la IAS- y EBSI ESSIF[35] -el marco europeo de identidad auto-soberana- han identificado consideraciones y escenarios legales con respecto a la IAS y eIDAS[36]:

Escenarios a muy corto plazo - no sería necesario realizar cambios legales en el eIDAS.

- Uso de medios eIDAS eID notificados y certificados calificados para emitir credenciales verificables
- eIDASBridge: aumentar el valor legal de las credenciales verificables y el reconocimiento transfronterizo.
- Uso de los nodos de eID actuales para emitir una aserción SAML basada en credenciales/presentaciones verificables.

Escenarios a corto plazo - interpretación tecnológica neutral y ligeras modificaciones del eIDAS.

- Uso de identificaciones verificables como medios de identificación electrónica eIDAS.
- Emisión de certificados calificados basados en un método DID específico y credencial verificable.

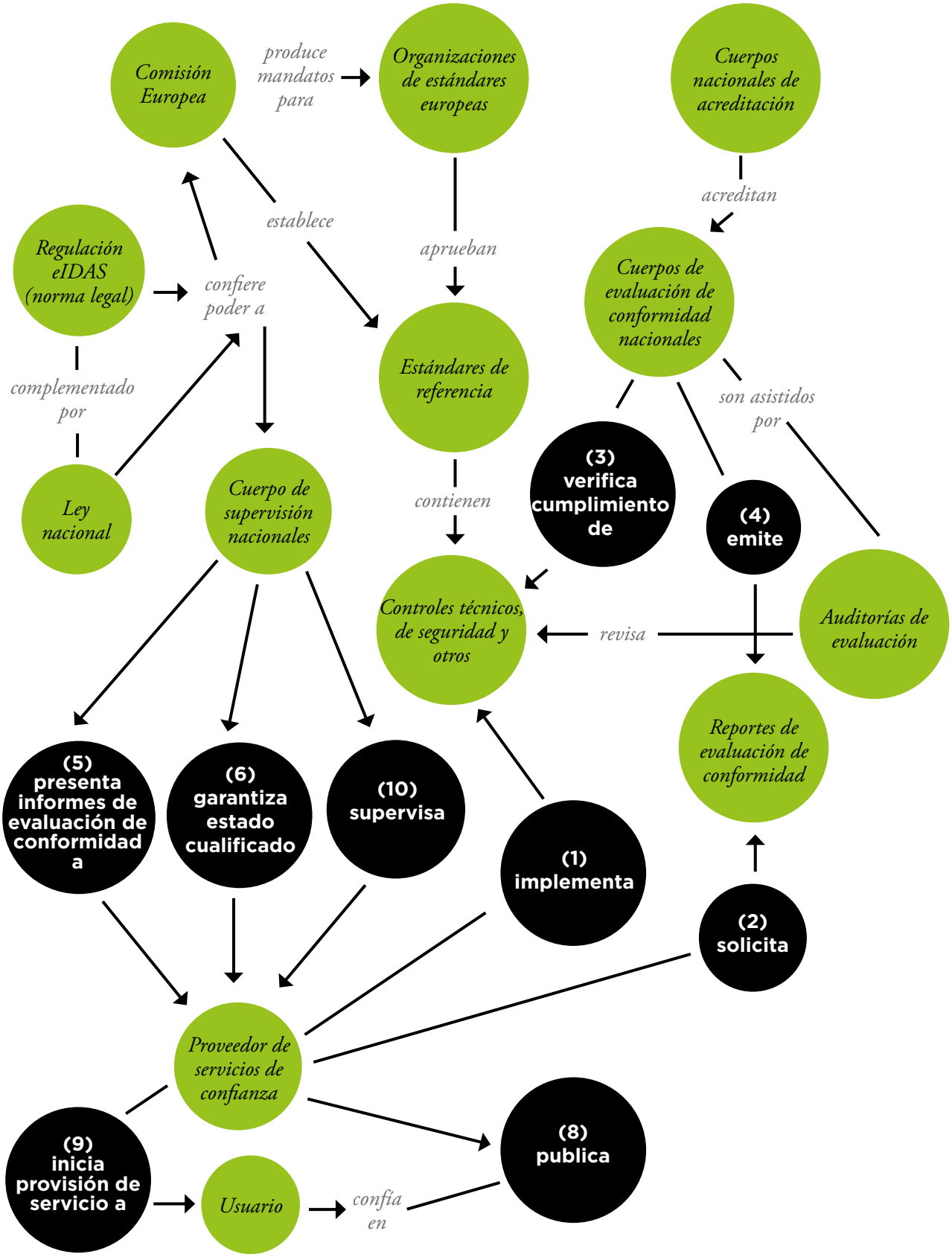
Escenarios a medio y largo plazo - modificación importante del eIDAS.

- Extender el mecanismo de notificación eIDAS a Atestaciones Verificables: gestión mejorada de Emisores Confiables
- Regular la emisión de Atestaciones Verificables como un nuevo servicio de confianza.
- Regular Hubs de identidad como un nuevo servicio de confianza, en apoyo de TOOP basado en IAS.
- Regular la administración de claves delegadas como un servicio de confianza independiente.
- Regular un tipo específico de DLT/nodo como un servicio de confianza.

Por tanto, sí será necesaria una modificación de eIDAS para poder convertirse en el marco legal y de confianza de la identidad digital auto-soberana en la Unión Europea. Esta conclusión es razonable, pues el Reglamento eIDAS se creó como un marco legal para un marco de identidad digital basado en un sistema de autenticación delegada, que resulta más limitado que el enfoque auto-soberano que

34. https://joinup.ec.europa.eu/collection/ssi-eidas-bridge/about
35. https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/2019/12/16/EBSI+-+ESSIF+-+Stakeholder+meeting
36. https://joinup.ec.europa.eu/collection/ssi-eidas-bridge/document/ssi-eidas-legal-report-flyer

Imagen 13. Modelo conceptual de la Regulación eIDAS. (Alamillo, 2019).



permite, entre otras cosas, el seudónimo y los mecanismos de divulgación selectiva que veremos en la Sección 7.3.7 de este documento. Además, también será necesario un trabajo tanto desde el lado de los reguladores como desde el lado de los desarrolladores para que servicios como las redes y nodos blockchain o billeteras digitales también puedan llegar a cualificar y ser certificados como servicios de confianza.

En esta línea, después de analizar la compatibilidad entre el eIDAS y las credenciales verificables, Alamillo hace referencia a dos puntos clave (Alamillo, 2020)[37]:

- Las credenciales verificables deben considerarse documentos electrónicos y, por lo tanto, no se les negará efecto probatorio en los procedimientos legales, prohibiéndose su denegación solo por estar en forma electrónica.
- Podría haber clases definidas de credenciales verificables con una semántica bien definida, posiblemente de acuerdo con un marco de gobierno específico (por ejemplo, una identificación verificable o un diploma verificable). Esto permitiría el reconocimiento específico para propósitos particulares.

Como marco de confianza, el Reglamento eIDAS también establece canales de comunicación que han demostrado ser vulnerables y que podrían ser reemplazados por redes blockchain, como discutiremos en la Sección 8.3.2.

6.2. Protección de datos

En un mundo que se vuelve más digital cada día, es esencial proteger los datos y la privacidad de las personas, y la mejor manera de hacerlo es mediante regulación. Desafortunadamente, muchos países en el mundo carecen de normativa en materia de protección de datos o, si la tienen, está desactualizada. Esto incluye a la mayoría de los países de América Latina y el Caribe.

6.2.1. Normativa de protección de datos en América Latina y el Caribe

La Tabla 16 muestra que la mayoría de los países de América Latina y el Caribe no cuentan con regulaciones en materia de protección de datos. De acuerdo con nuestra investigación, Sudamérica es la región más avanzada con regulación en 8 de 13 países. En América Central solamente 3 de 7 se cuentan en positivo, lo que contrasta con el análisis de regulación en materia de firma y transacciones electrónicas, que mostraba que todos los países de América Central cuentan con legislación, como se ilustró en la Sección 6.1.1. En América del Norte, México también cuenta con regulación. En el Caribe, la región menos avanzada en este campo, solamente 5 de los 21 países tienen leyes de protección de datos. En total, son 17 de los 42 países los que cuentan con estas políticas regulatorias, lo que representa solamente un 40%.

6.2.2. Reglamento General de Protección de Datos (GDPR) y blockchain

La regulación más avanzada en materia de protección de datos es el REGLAMENTO (UE) 2016/679 Del Parlamento Europeo y del Consejo de 27 de abril de 2016[38], 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), también conocido como GDPR. Esta regulación comienza a aplicarse en todos los Estados miembros a partir del 25 de mayo de 2018 (según reza su Artículo 99) para "armonizar las leyes de privacidad de datos en toda Europa" (EU-GDPR, 2016). El GDPR ha sido reconocido en todo el mundo por muchas razones:

37. Esta publicación de Nacho Alamillo, uno de los mayores expertos en la Regulación eIDAS y la IAS que asesora a la Comisión Europea, es una lectura obligatoria en materia de IAS y regulación.

38. https://www.boe.es/doue/2016/119/L00001-00088.pdf

Tabla 9. Leyes de protección de datos en América Latina y el Caribe.

País	Región	Regulación	Última modificación
Antigua y Barbuda	Caribe	Acta de Protección de datos.	2013
Argentina	América del Sur	Ley No. 25325.	2000
Aruba	Caribe	-	-
Bahamas	Caribe	Acta de Protección de datos.	2008
Barbados	Caribe	Proyecto de ley de Protección de datos.	2019
Belice	América Central	Falta de regulación por el acta de libertad de información (2000).	-
Bolivia	América del Sur	Falta de regulación. Derecho constitucional a la privacidad de las comunicaciones personales. Anteproyecto de ley No.185-2019.	-
Brasil	América del Sur	Ley NO. 13709/2018 (LGPD).	2018
Chile	América del Sur	Leyes No. 19628 (1999) y 20575 (2012).	2012
Colombia	América del Sur	Ley No. 1581 (2017).	2017
Costa Rica	América Central	Ley No. 8968.	2011
Cuba	Caribe	Falta de regulación. La nueva Constitución reconoce los derechos de datos personales en sus artículos 48 y 97 (2019).	-
Dominica	Caribe	-	-
República Dominicana	Caribe	Ley No. 172-13.	2013
Ecuador	América del Sur	Proyecto de ley de privacidad y protección de datos	2016
El Salvador	América Central	En desarrollo (2020).	-
Granada	Caribe	-	-
Guadalupe	Caribe	-	-
Guatemala	América Central	-	-
Guyana	América del Sur	-	-
Guyana Francesa	América del Sur	-	-
Haití	Caribe	-	-
Honduras	América Central	En desarrollo	-
Islas Caimán	Caribe	-	-
Islas Turcas y Caicos	Caribe	-	-

País	Región	Regulación	Última modificación
Islas Vírgenes	Caribe	-	-
Jamaica	Caribe	Acta de protección de datos.	2017
Martinica	Caribe	-	-
México	América del Norte	Ley Federal Mexicana de Protección de Datos Personales en posesión de los particulares.	2010
Nicaragua	América Central	Ley No. 787.	2012
Panamá	América Central	Ley No. 81 de 2019.	2019
Paraguay	América del Sur	Ley No. 1862/01 y Ley 1969/02.	2001
Perú	América del Sur	Ley No.29733.	2011
Puerto Rico	Caribe	-	-
San Bartolomé	Caribe	-	-
San Cristóbal y Nieves	Caribe	-	-
San Vicente y las Granadinas	Caribe	-	-
Santa Lucía	Caribe	-	-
Surinam	América del Sur	-	-
Trinidad y Tobago	Caribe	-	-
Uruguay	América del Sur	Ley No. 18331.	2008
Venezuela	América del Sur	-	-

- Ser la regulación más avanzada y completa sobre protección de datos hasta la fecha.
- Tener impacto global, ya que también se aplica a entidades externas a la UE que tratan datos de ciudadanos europeos, lo que puede verse como una motivación para que los países no europeos desarrollen regulaciones que cumplan con el GDPR y habiliten el intercambio de datos con países europeos.
- Ser un esfuerzo regional único en el mundo. Por ejemplo, en los Estados Unidos no existe una regulación común sobre protección de datos para todos los estados; más bien, hay varias leyes a nivel federal y estatal. La más popular es la de California: la Ley de Privacidad del Consumidor de California (California, 2018).

Humildemente creemos que, si las soluciones de IAS se implementasen de acuerdo con las recomendaciones formuladas en este documento, cumplirían totalmente con el GDPR. Para defender esta declaración, nos centraremos en seis de las principales áreas de convergencia entre GDPR e IAS:

Consentimiento: la IAS, como ya vimos en la Sección 2.4.5, representa un cambio de paradigma en la identidad digital. En los esquemas de identidad tradicionales, como el centralizado o el de identidad provista por un tercero, el sujeto de una identidad no tiene el control de las claves, las credenciales o los datos. En el modelo IAS, el sujeto de la identidad tiene el control de todos esos datos y decide cuándo compartirlo con otros en forma de presentaciones verificables que definiremos en la Sección 7.3. Por tanto, desarrollar soluciones que cumplan con el consentimiento del titular no solo es posible, sino que sería más fácil porque (i) no es necesario que terceros intercambien información sobre los sujetos, y (ii) es mucho más sencillo contactar y solicitar el consentimiento al propio sujeto o al titular.

Derecho al olvido: este derecho es siempre un desafío, ya que implica (i) saber exactamente dónde están los datos, (ii) poder demostrar quiénes somos a quienes poseen nuestros datos para poder solicitar su eliminación y (iii) no tener datos personales en registros inmutables y descentralizados. La IAS permite lograr los dos primeros requisitos de forma sencilla, sin embargo, el tercero debe ser cuidadosamente atendido. Las malas implementaciones de IAS y blockchain podrían vulnerar la privacidad de los datos muy fácilmente. No obstante, siguiendo las pautas de este documento, dichas violaciones pueden ser evitadas. Además, las billeteras digitales deben proporcionar formas sencillas de rastrear dónde se han utilizado los identificadores y para qué, y también permitirnos solicitar su eliminación. Del lado de los proveedores de servicios, el mecanismo para garantizar el derecho al olvido también se desarrollará de manera proactiva.

Portabilidad de datos: las billeteras digitales permiten que la información personal digital sea portable. En ellas se almacenan claves, credenciales y datos. Como veremos en la Sección 7.5.2, las billeteras móviles y en la nube son las opciones más atractivas hoy en día.

Protección de datos por diseño y por defecto: todas las piezas del modelo IAS presentadas en este documento que incluyen DID, credenciales verificables, presentaciones verificables, identificación, autenticación y autorización, repositorios y billeteras digitales, así como un registro descentralizado y están diseñados para proteger los datos por defecto.

Registros de actividades de procesamiento: en la medida que los datos están conectados a sus identificadores y el usuario es responsable de compartir sus credenciales, la billetera digital debe poder mantener un registro privado de las actividades de procesamiento, como veremos en la Sección 7.5. Además, tener registros blockchain públicos y descentralizados permite tener datos mucho más rastreables que al mismo tiempo son seudónimos, pues nadie debería poder relacionar los diferentes identificadores si se desarrollan soluciones adecuadas, como veremos en las Secciones 7.1.3 y 7.1.4. En todo caso, se debe preservar la privacidad de los datos, incluida la IIP que podría derivarse de los intercambios y verificaciones.

Seudonimización: la seudonimización es uno de los beneficios directos de la IAS, como se destaca en la Sección 3.3. Para garantizarlo, es importante utilizar registros DID y métodos DID adecuados, como veremos en las Secciones 7.1.3 y 7.1.4. Esto permitirá que un titular de identidad tenga y administre tantos identificadores seudónimos como desee, para que pueda interactuar con diferentes servicios de forma segura y autenticada, pero sin revelar más datos o IIP de los deseados. El seudónimo es también una de las principales ventajas de los documentos DID y las presentaciones verificables sobre el certificado X.509 tradicional para identificación electrónica. Además, el modelo IAS permite funcionalidades como los mecanismos de divulgación selectiva y las pruebas de conocimiento cero que serán presentados en la Sección 7.3.7.

IDENTIDAD DIGITAL AUTO-SOBERANA

Bloque 7
Componentes tecnológicos

El modelo de identidad auto-soberana demanda el desarrollo de nuevos componentes tecnológicos, estándares y protocolos. En la actualidad, estos tres elementos están siendo desarrollados y se encuentran en diferentes estados de madurez. En esta sección hemos clasificado los componentes tecnológicos en siete categorías: identificadores descentralizados (DID); credenciales verificables (VP); presentaciones verificables (VP); identificación, y, autorización; billeteras digitales; autoridades de certificación (CA) y listas de confianza (TL); y tecnología de registros distribuidos (DLT).

7.1. Identificadores descentralizados (DIDs)

7.1.1. Definición

Un grupo de trabajo del World Wide Web Consortium (W3C) ha venido desarrollando el estándar de Identificadores Descentralizados (DID) (W3C-DID, 2019). Un DID es "un nuevo tipo de identificador que permite una identidad digital verificable y descentralizada. Un DID identifica cualquier sujeto (por ejemplo, una persona, organización, cosa, modelo de datos, entidad abstracta, etc.) que el controlador del DID decide que identifique". Las diferentes realizaciones del estándar DID se denominan métodos DID.

7.1.2. Documentos DID

Típicamente, un identificador descentralizado apunta a un documento DID que contiene información sobre dicho DID. Según ha establecido el Instituto Nacional de Estándares y Tecnología (NIST), un documento DID se compone de los siguientes elementos estándar (NIST-TA, 2020):

- Un identificador de resolución uniforme (URI por su nombre en inglés) para identificar de forma unívoca la terminología y los protocolos que permiten a las partes leer el documento DID.
- Un DID que identifica al sujeto del documento DID.
- Un conjunto de autenticadores (en general claves públicas) utilizados para los mecanismos de autenticación, autorización y comunicación.
- Un conjunto de métodos de autenticación utilizados que permiten al sujeto del DID demostrar estar en control del mismo.
- Un conjunto de métodos de autorización y delegación que permiten que otras entidades operen en nombre del sujeto DID (es decir, titulares diferentes del sujeto).
- Un conjunto de puntos de contacto electrónicos que describen dónde y cómo interactuar con el sujeto DID.
- Un sello de tiempo para indicar cuándo se creó el documento.
- Un sello de tiempo para indicar la última actualización del documento.
- Prueba de identidad criptográfica (por ejemplo, firma digital).

Además de lo anterior, consideramos que los documentos DID deberían contener un elemento adicional que indique el estado de dicho documento (activo, suspendido, o revocado), de manera que el o los titulares puedan revocarlo en caso de que ya no deseen usarlo más, propiciando que aquellos documentos digitales asociados a ese DID ya no podrán completar el proceso de verificación pues fallarán en la verificación del sujeto.

En el modelo más básico, un DID puede ser una clave pública generada a partir de una clave privada o semilla utilizando algoritmos criptográficos asimétricos como RSA, curvas elípticas (ECC) o logaritmos discretos (DLL). Como en el caso de las claves públicas simples, en este modelo básico el mecanismo de autenticación podría requerir resolver un desafío criptográfico con la clave privada asociada a la clave pública que se usó para la generación del propio DID. Sin embargo, esto debe evitarse por razones de seguridad y privacidad. Los documentos DID deben contener más de un mecanismo de autenticación cada uno involucrando una clave diferente, y la clave privada utilizada para generar el DID no ha de ser utilizada para ninguno de ellos, como veremos con más detalle en la Sección 7.1.4.

Imagen 14. Ejemplo de un documento DID básico (W3C-VC, 2019).

EXAMPLE 14: Authentication field containing three verification methods

```
{
  "@context": "https://www.w3.org/ns/did/v1",
  "id": "did:example:123456789abcdefghi",
  ...
  "authentication": [
    // this method can be used to authenticate as did:...fghi
    "did:example:123456789abcdefghi#keys-1",
    // this method can be used to authenticate as did:...fghi
    "did:example:123456789abcdefghi#biometric-1",
    // this method is *only* authorized for authentication, it may not
    // be used for any other proof purpose, so its full description is
    // embedded here rather than using only a reference
    {
      "id": "did:example:123456789abcdefghi#keys-2",
      "type": "Ed25519VerificationKey2018",
      "controller": "did:example:123456789abcdefghi",
      "publicKeyBase58": "H3C2AVvLMv6gmMNam3uVAjZpfkcJCwDwnZn6z3wXmqPV"
    }
  ],
  ...
}
```

La curva elíptica y la función hash más adoptadas en el espacio DLT son, respectivamente, la secp256r1 y la keccak-256. Desafortunadamente, ninguna de ellas está respaldada por SP 800-186 (NIST-ECDM, 2019) y FIPS 186-5 (NIST-DSS, 2019). Un esfuerzo conjunto entre Consensys, la Fundación de Identidad Descentralizada (DIF por su nombre en inglés), Enterprise Ethereum Alliance (EEA), el Grupo Comunitario de Credenciales del World Wide Web Consortium (W3C), Hyperledger y empresas individuales miembros del W3C han solicitado al NIST "incluir la curva secp256k1 como parte de los esquemas ECDSA aceptados, y el uso de keccak-256 en los esquemas de firma secp256k1" argumentando que "no hay diferencias de seguridad significativas entre, por ejemplo, la secp256r1 apoyada por el NIST y la secp256r1 o entre el la función hash sha3-256 y el keccak- 256" y afirmando que así "se minimizaría el daño que la diferencia de estándares entre el NIST y el resto del mundo está causando a la innovación y a los mercados" (Consensys et al, 2019).

Como ya recalcamos en el Bloque 5 de este documento, es extremadamente importante que los protocolos y estándares utilizados en blockchain y en IAS sean reconocidos por las agencias internacionales de estándares, lo que incluye los algoritmos criptográficos. Además, es esencial que la comunidad no siga ignorando la necesidad de comenzar a probar algoritmos de criptografía post-cuántica, puesto que cuando los computadores cuánticos sean lo suficientemente potentes tendrán la capacidad de romper la criptografía RSA, de curvas elípticas y de logaritmos discretos, como ya alertaron NSA (NSA, 2016), NIST (NIST-Q, 2016) y ETSI (ETSI, 2015), en 2015 y 2016.

El DIF mantiene una interfaz para aplicaciones JavaScript para resolver documentos DID de identificadores descentralizados[39] y LACChain también tiene ofrece un servicio de resolución[40].

7.1.3. Registros de DIDs

En la sección 3.5 hemos analizado algunos de los beneficios prácticos de la tecnología blockchain para IAS. Algunos de ellos son no solo beneficios

39. https://uniresolver.io/
40. https://didresolver.lacchain.net/

Tabla 10. Tipos de registros DID en redes blockchain basadas en Ethereum (NIST-TA, 2020).

		Descripción	Estándares	Pros	Contras
En la cadena	**Registro de credenciales que actúa como identificador**	Cada identificador tiene un contrato inteligente.	ERC-725 (Cuenta Proxy) ERC-734 (Gestor de claves).	Descentralización: muy descentralizada Mantenimiento y soberanía: fácil de mantener (modificar la lógica, actualizar o destruir).	Escalabilidad: Muy costoso en cuanto a número de transacciones.
	Registro de identificadores globales	Un único contrato inteligente monolítico, o conjunto de contratos integrados, actúa como un registro global para almacenar y administrar todos los identificadores.	Hyperledger Fabric.	Escalabilidad: Más barato en materia de transacciones.	Mantenimiento: un reto para definir modelos de gobernanza confiables. Lugar central de ataque y vulnerabilidad
	Registro de anclajes	Un único contrato inteligente monolítico actúa como un registro global que almacena los hashes de las operaciones de gestión de identificadores que se agrupan en paquetes o "anclajes".	DID:elemento[40].	Interoperabilidad: sistemas de almacenamiento externo. Escalabilidad: Barato en materia de transacciones. Protección de datos: los metadatos del documento DID no están registrados en la blockchain. Solo el hash.	Integridad: si una de las dos capas se ve comprometida, podría ser difícil de reconciliar.
Off-chain	**Traen su propia dirección de blockchain.**	Cualquier dirección de blockchain es un identificador válido y puede usarse de inmediato sin tener que registrarse previamente.	ERC-1056 Identidad ligera.	Escalabilidad: la creación del identificador se realiza sin conexión y sin ningún controlador de acceso, y sin coste alguno. Privacidad: los DID no son identificables por defecto.	La lógica en cadena puede ser necesaria para implementar funcionalidades adicionales como la gestión de identificadores y las capacidades de verificación.

41. https://github.com/decentralized-identity/element

sino también requisitos necesarios para conseguir implementaciones robustas y escalables de DIDs. Por ejemplo, cuando se trabaja con identificadores descentralizados es necesario tener registros de DIDs. Como cualquier entidad puede generar sus propios DIDs, usar bases de datos centralizadas e independientes como registros no escalaría bien. Teniendo en cuenta que se desea que los DID sirvan como identificadores digitales para diversas aplicaciones, y que cada una de estas aplicaciones debe poder saber dónde está el registro y cómo resolver y verificar la propiedad del DID contra él, que cada DID estuviese en un registro diferente sería poco práctico y volveríamos a encontrarnos con algunos de los problemas del modelo de identidad centralizado. Con los registros centralizados seguiríamos dependiendo de entidades centrales que los mantienen, lo que facilitaría los hackeos y ataques, y limitaría la accesibilidad y la escalabilidad. En cambio, las redes blockchain descentralizados, que todas las entidades pueden conocer y de los que pueden tener una copia, se postulan como los registros más adecuados para los registros DID.

NIST ha elaborado una clasificación de los diferentes tipos de registros de DIDs usando redes blockchain, específicamente basadas en Ethereum, lo que permite aprovechar las funcionalidades de los contratos inteligentes (NIST-TA, 2020). La Tabla 10 describe cada uno de los tipos e indica, a su vez, los estándares e implementaciones relacionadas, así como los pros y contras.

En el caso del registro de identificadores globales, los modelos de gobernanza pueden abarcar desde casos en los que la entidad que implementa el contrato tenga el control completo del sistema, hasta casos en los que tenga un control limitado o que no tenga control en absoluto. En el caso de que no tenga control, la gobernanza del contrato correrá a cargo de los usuarios participantes (por ejemplo, con un DAO).

En el caso del registro de anclajes, la agrupación de operaciones de gestión de identificadores se ejecuta mediante un protocolo de segunda capa que se encuentra en la parte superior de la blockchain en la que se encuentra el registro de anclajes. Después, el protocolo agrega los hashes de esos anclajes en el registro y utiliza sistemas de almacenamiento descentralizados, como el sistema de archivos interplanetarios (IPFS por su nombre en inglés)".

En el caso de traer una dirección propia de blockchain, la creación y el almacenamiento del identificador generalmente se realiza localmente en la billetera de identidad. Resolver un DID en su documento DID consiste en iterar sobre las operaciones DID que pueden haberse publicado.

7.1.4. Métodos DID

Las realizaciones del estándar DID se denominan métodos DID. Estos métodos pueden variar en el mecanismo propuesto para la generación de DIDs, los métodos de autenticación o los registros de DIDs. No hay una lista oficial de métodos DID. Sin embargo, el W3C[42] y el DIF[43] mantienen listas informales.

Los métodos DID deben cumplir con los siguientes requisitos:

- Permitir el uso responsable de biometría (por las billeteras y las aplicaciones que se utilizan para operar DIDs).
- Contener todos los elementos enumerados en la Sección 7.1.2, incluido el estado del documento DID.
- Tener más de un método de autenticación (es decir, RSA, EC, criptografía post-cuánticas o biometría).
- Utilizar criptografía resistente a la computación cuántica para los métodos de autenticación, encriptación y firma.
- Destruir la "semilla" del DID para que un hacker no pueda volver a generarlo en caso de robo.
- No divulgar ningún dato personal o información en los documentos DID.

42. https://w3c-ccg.github.io/did-method-registry/
43. https://github.com/decentralized-identity/universal-resolver/

- Garantizar privacidad y seudónimo en el uso de los DIDs.
- Tener más de un autenticador para cada método de autenticación (por ejemplo, varias claves públicas RSA).
- Si el DID se generó a partir de una clave privada, no utilizar la clave pública asociada para autenticación, encriptación o firma.
- Registrar los DID en un contrato inteligente con un gobierno bien definido (generando un registro de DIDs en la red).
- Ser suficiente escalable a nivel económico y transaccional para permitir la generación de la cantidad de DIDs necesaria para un caso de uso especifico en la red escogida.
- Establecer diferentes funcionalidades para las diferentes claves, de modo que algunas claves primarias se puedan usar para la autenticación, algunas claves secundarias se puedan usar para delegación temporal, y algunas claves terciarias se puedan usar para recuperar claves primarias y secundarias.
- Almacenar los documentos DID en la blockchain, de manera que los emisores o verificadores que requieran resolver un DID específico puedan encontrarlos fácilmente.

La estandarización de esta estructura básica supone un cambio de paradigma. Como se presentó en las Secciones 2.4.5 y 3.1, el modelo de identidad auto-soberana comienza con identificadores únicos que las entidades pueden autogenerar y administrar, así como demostrar su propiedad, y es de gran importancia que las reglas para su uso sean establecidas y se reconozcan globalmente

Se podría argumentar que los estándares tradicionales como los certificados X.509 podrían desempeñar el papel de un documento DID en el modelo IAS. Sin embargo, estos no cumplen con los requisitos mínimos necesarios para soluciones escalables, confiables y que garanticen la privacidad de los datos. En el modelo IAS, los certificados X.509 son reemplazados por la combinación de un identificador descentralizado y una credencial digital verificable emitida por una entidad confiable. No obstante, es muy posible que los certificados X.509 existentes se utilicen, a corto plazo, para generar credenciales verificables.

7.2. Credenciales verificables (VCs)

7.2.1. Definición

Para construir o diseñar una solución de identidad auto-soberana, el siguiente paso tras generar identificadores únicos es tener emisores confiables que emitan credenciales verificables que tengan por sujeto esos identificadores. Una credencial verificable es un archivo digital que contiene una o más declaraciones de valor (por ejemplo, fecha de nacimiento, nombre, calificaciones, género, ciudadanía, etc.) sobre una entidad denominada sujeto, emitida por otra entidad denominada emisor, y que es verificable por cualquier entidad denominada verificador.

Un grupo de trabajo en el W3C ha venido trabajando en la definición del estándar de credenciales verificables (VC). Una credencial verificable contiene declaraciones, metadatos y pruebas, siendo estas últimas las que permiten verificar la credencial. La especificación de VC de W3C no aplica un algoritmo de prueba específico, pero describe la articulación entre una credencial y un mecanismo de prueba específico. Los implementadores son libres de proponer su propio mecanismo de prueba o seguir el de otra persona.

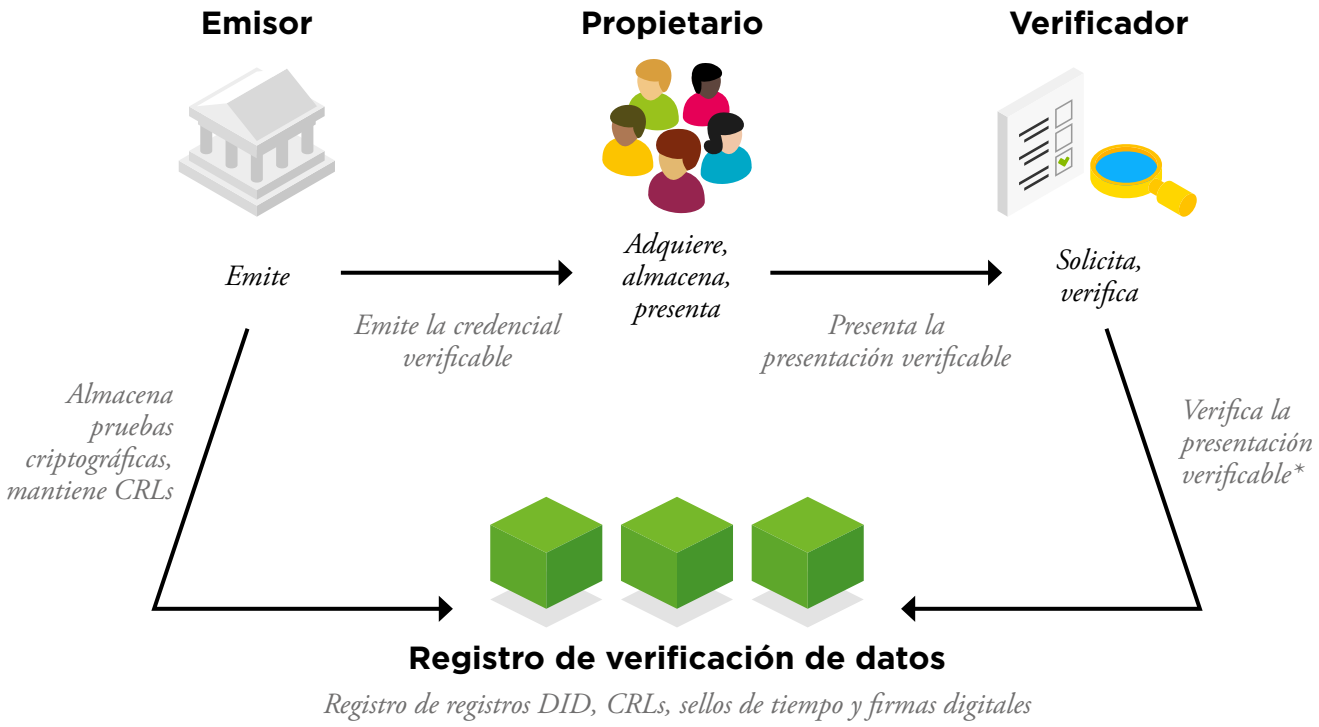
El sujeto de una credencial verificable es el identificador descentralizado de la entidad de a la que corresponden los atributos en la credencial. El verificador siempre puede decidir si confía en el emisor de la credencial o no.

7.2.2. Estructura y formato

Como apunta NIST, una Credencial verificable es un archivo que se compone de los siguientes elementos estándar (NIST-TA, 2020):

- URI para identificar de forma exclusiva la credencial y/o el asunto de la credencial (por ejemplo, un DID).
- URI para identificar al emisor (por ejemplo, un DID).

Imagen 15. Esquema simplificado del flujo de una credencial verificable.



* Para más información, consultar el Proceso de Verificación de LACChain ID.

- URI para identificar el tipo de credencial.
- URI para identificar la terminología y los protocolos que permiten a las partes leer la credencial.
- Prueba criptográfica del emisor.
- Declaraciones de datos o metadatos.
- Fecha de emisión.
- Condiciones de expiración.
- Ubicación de la información estado de la credencial (por ejemplo, un contrato inteligente en una red blockchain).

Además, recomendamos que:

- El DID del sujeto y el emisor puedan encontrarse y resolverse en la blockchain.
- Las declaraciones de datos o metadatos de la credencial nunca sean registrados en la blockchain.
- Las condiciones de exploración se puedan verificar automáticamente desde la credencial.
- El estado de la credencial se pueda verificar contra un contrato inteligente en la blockchain, y nadie más que el emisor pueda modificarlo[44].

Algunos de los formatos preferidos son JWT, JWS y JSON-LD.

7.2.3. Registro

NIST ha elaborado una clasificación de los tipos de registros de credenciales cuando se utilizan redes blockchain que permiten implementar contratos inteligentes (NIST-TA, 2020). La Tabla 13 describe cada tipo y analiza sus ventajas e inconvenientes.

44. Esto elimina la necesidad de un CRL externo y/o centralizado.

Tabla 11. Distintos tipos de registros de credenciales en las redes blockchain, según NIST (NIST-TA, 2019).

		Descripción	Pros	Contras
En la cadena	**Registro de credenciales por identificador**	Cada identificador cuenta con un contrario inteligente en el que se almacenan y administran las credenciales	-	Escalabilidad: muy costoso en términos de transacciones y almacenamiento. Privacidad de datos: muy difícil garantizar los requisitos de privacidad de datos.
	Registro global de credenciales	Todas las credenciales correspondientes a diferentes entidades se registran y administran como entradas en un solo contrato inteligente.	-	Escalabilidad: muy costoso en términos de transacciones. Privacidad de datos: muy difícil garantizar los requisitos de privacidad de datos. Gobernanza: la propiedad del contrato inteligente pertenece a la entidad que lo desplegó
	Registro de tokens no fungibles	Las credenciales adoptan la forma de un token no fungible (NFT)[45]. La acuñación y la administración de los tokens se realizan a través de un contrato inteligente NFT (que actúa como un registro que administra los NFT).	-	Escalabilidad: muy costoso en términos de transacciones. Privacidad de datos: muy difícil garantizar los requisitos de privacidad de datos. Gobernanza: gestión muy centralizada del contrato inteligente NFT.
	Titularidad de un token no fungible mantenible por el usuario.	La credencial toma la forma de un derecho para permitir que un usuario acuñe un NFT predefinido y preasignado en una fecha o condición futura.	-	Escalabilidad: muy costoso en términos de transacciones. Privacidad de datos: muy difícil garantizar los requisitos de privacidad de datos. Gobernanza: gestión muy centralizada del contrato inteligente NFT.
Off-chain	**Objetos *off-chain***	Las credenciales toman la forma de un objeto *off-chain* que actúa como un vehículo autónomo para transmitir información directamente entre las partes.	Escalable: barato en términos de transacciones. Almacenamiento: no se utiliza almacenamiento blockchain. Privacidad de datos: puede cumplir con los requisitos de privacidad de datos ya que la emisión, el almacenamiento y la verificación son *off-chain*. Verificación: la verificación es contra la blockchain, pero no necesariamente genera transacciones.	Trazabilidad: baja trazabilidad, lo que también podría ser una ventaja.

45. Un NFT es un token único, no intercambiable, propiedad de una persona física o jurídica y que puede ser administrado y comercializado.

Solo la opción *off-chain* para el almacenamiento de credenciales es recomendada, pues es la única que escalable en cuanto a número de transacciones y almacenamiento, y permite cumplir con las normas de protección de datos. Cuando se elige esta opción *off-chain*, se consulta la blockchain para verificar las credenciales. En la mayoría de las redes blockchain, estas consultas no generan transacciones y por lo tanto no dejan ningún rastro ni consumen ningún recurso blockchain. En una implementación ideal:

- El DID del sujeto y el emisor se pueden encontrar en los registros de blockchain.
- Las declaraciones de datos o metadatos de la credencial nunca se registran en la blockchain de forma legible.
- Las condiciones de expiración se pueden verificar automáticamente desde la credencial y contra la blockchain.
- El estado de la credencial se puede verificar contra un contrato inteligente que "vive" en la blockchain, y nadie más que el emisor podrá cambiarlo. Esto elimina la necesidad de un CRL u OCSP externo y/o centralizado.

7.2.4. Almacenamiento

Como se introdujo en la Sección 3.1, los titulares usan repositorios privados para almacenar y administrar credenciales. Estos repositorios suelen ser billeteras digitales que también permiten generar presentaciones verificables y compartirlas con otros. En el modelo *off-chain* que acabamos de presentar, las credenciales son almacenadas y protegidas por el software y/o hardware elegido por el usuario. El uso de aplicaciones móviles como billeteras digitales parece la opción más razonable en términos de seguridad y conveniencia. En las secciones 7.4 y 7.5 ofreceremos pautas para repositorios relacionados con identificación, autenticación, autorización, seguridad y recuperación de claves, entre otros.

7.2.5. Intercambio

Existen al menos tres tipos de intercambio de credenciales:

Emisión: la credencial se envía de un emisor al solicitante, titular o sujeto.

Delegación/Transferencia: la credencial se intercambia entre solicitante, titular y sujeto.

Presentación: la credencial se envía de un titular a un verificador.

Para todos los tipos de intercambio de credenciales, los canales digitales entre el repositorio donde se almacena la credencial (por ejemplo, la billetera digital) y el servicio que genera o consume la credencial deben ser seguros y estar protegidos.

7.2.6. Revocación

En la Sección 7.2.2 establecimos como requisito obligatorio que las credenciales debían tener un campo que indique su estado. Esto también implica que el estado de la credencial debe poder cambiarse entre activo, suspendido y revocado. Es por ello por lo que se deben definir reglas claras de revocación para cada credencial de modo que quede claro quién y bajo qué condiciones puede cambiar su estado. Algunos ejemplos son:

- El estado se define como activo automáticamente cuando el emisor emite la credencial.
- Los emisores pueden cambiar el estado a revocado cuando el sujeto deja de cumplir con las declaraciones que figuran en la credencial.
- Los emisores pueden cambiar el estado a suspendido cuando el sujeto informa de que la credencial, los autenticadores o las pruebas asociadas han sido comprometidos.
- Los emisores pueden cambiar el estado a revocado cuando el usuario informa de que ya no desea usar la credencial.
- El sujeto o el titular pueden cambiar el estado a suspendido cuando la credencial o sus claves se hayan visto comprometidas.
- El sujeto o el titular pueden cambiar el estado a revocado cuando ya no desean usar la credencial.
- El estado de la credencial cambia automáticamente después de la fecha de vencimiento.

Para registrar el estado de la credencial, proponemos el uso de contratos inteligentes. En un contrato inteligente, el emisor registra el URI de la credencial cuando la emite. Posteriormente, según las reglas de revocación, las entidades autorizadas pueden cambiar el estado directamente en el contrato inteligente. La credencial deberá contener la dirección del contrato inteligente que contiene la información sobre su estado, de manera que este se pueda comprobar de forma sencilla y automática contra la blockchain según requiere el Paso 2 del Proceso de verificación que veremos en la Sección 7.3.5.

7.3. Presentaciones verificables (VPs)

7.3.1. Definición

El W3C introduce en la especificación de Credenciales Verificables el concepto de Presentaciones Verificables (VP) (W3C-VC, 2019). Como se indica en la especificación, "una presentación verificable expresa datos de una o más credenciales verificables, y se empaqueta de tal manera que la autoría de los datos es verificable. Si las credenciales verificables se presentan directamente[46], se convierten en presentaciones verificables".

7.3.2. Estructura y formato.

Todas las presentaciones verificables deben incluir los siguientes campos[47]:

- URI para identificar de forma exclusiva la presentación.
- URI para identificar de forma exclusiva el tipo de objeto.
- Una o más credenciales verificables o declaraciones derivados de ellas.
- URI para identificar la entidad que genera la presentación (por ejemplo, un DID).
- Prueba criptográfica del sujeto (por ejemplo, una firma digital).

Las presentaciones verificables también pueden incluir Información sobre la audiencia o el verificador para el que se emitió la credencial.

Algunos de los formatos preferidos son JWT, JWS y JSON-LD.

7.3.3. Almacenamiento

Se aplica lo mismo que para las credenciales verificables, descrito en la Sección 7.2.4.

7.3.4. Intercambio

Se aplica lo mismo que para las credenciales verificables, descrito en la Sección 7.2.5.

7.3.5. Proceso de verificación

La verificación de una credencial digital es un proceso que no está estandarizado y que en la mayoría de las ocasiones no es suficientemente riguroso. Es por eso que hemos definido el Proceso de Verificación que se presenta a continuación, que cualquier entidad actuando como un verificador de una credencial debería acometer cuando el titular de la misma se la presenta electrónicamente.

46. Por directamente se entiende que se toma la credencial tal como fue emitida por el emisor y se presenta sin ninguna modificación o combinación con otras credenciales.
47. Esta lista de requisitos supone que la presentación verificable es una encapsulación de diferentes credenciales verificables. Esta es la razón por la cual los campos tales como la prueba criptográfica del emisor, las condiciones de vencimiento y el estado no se indican como campos requeridos en las presentaciones verificables porque se supone que están presentes en las credenciales que las presentaciones están encapsulando. Como se indica en la Sección 7.2.2, estos campos son obligatorios en las credenciales verificables. Si una presentación verificable era una credencial verificable, los requisitos para las credenciales verificables se especifican en la Sección 7.2.2 son suficientes tanto para la credencial como para la presentación de la misma.

En toda interacción electrónica existen dos tipos de verificaciones: la verificación de la información electrónica que se intercambia o presenta digitalmente, y la verificación de las personas físicas detrás de las personas digitales que están tomando parte de esa interacción electrónica. En el modelo de IAS, los individuos almacenan sus credenciales en billeteras digitales que también utilizan para administrarlas y presentarlas a terceros. Generalmente, cuando se presenta una credencial electrónicamente a un tercero, se establece un canal de comunicación entre la billetera digital y el servicio digital de este (por ejemplo, https).

Cuando el verificador recibe la credencial, es capaz de verificar toda la información electrónica de la misma (validez, estado, emisor, presentador o sujeto, y contenido) contra el registro descentralizado en el que el emisor mantiene las pruebas criptográficas, tal y como se indica en los pasos 2 a 6 de este Proceso de Verificación. Sin embargo, el verificador no puede verificar de manera directa que la persona en control del dispositivo que está enviando la credencial electrónica es verdaderamente el sujeto o el titular de la misma. Para ello, el verificador ha de confiar en que la billetera digital lleve a cabo un proceso de autenticación de usuarios para acceder a estas billeteras privadas que garantice que nadie salvo el verdadero sujeto o titular pueda completarlo. Es por eso que el Paso 1 de nuestro Proceso de Verificación consiste en la verificación de la billetera como servicio de confianza.

Algunos marcos regulatorios, como eIDAS en la Unión Europea, definen el concepto de servicio electrónicos de confianza que permite que aquellos servicios electrónicos que cumplan con una serie de requisitos de confianza puedan ser certificados y reconocidos con un grado de garantía determinado para la provisión de servicios relacionados con la identificación electrónica. Consideramos que para que las billeteras puedan ser confiables para las entidades jugando el rol de verificadores de credenciales en el proceso de autenticación de usuarios, de manera que nadie pueda acceder a credenciales que no sean suyas y presentarlas a terceros sin autorización, es esencial que las billeteras puedan ser certificadas como servicios de confianza en los diferentes marcos regulatorios, lo que también requiere de una actualización de estos. La certificación de billeteras digitales como servicios de confianza para la autenticación electrónica de titulares de credenciales digitales es un paso esencial para la escalabilidad del modelo de identidad auto-soberana.

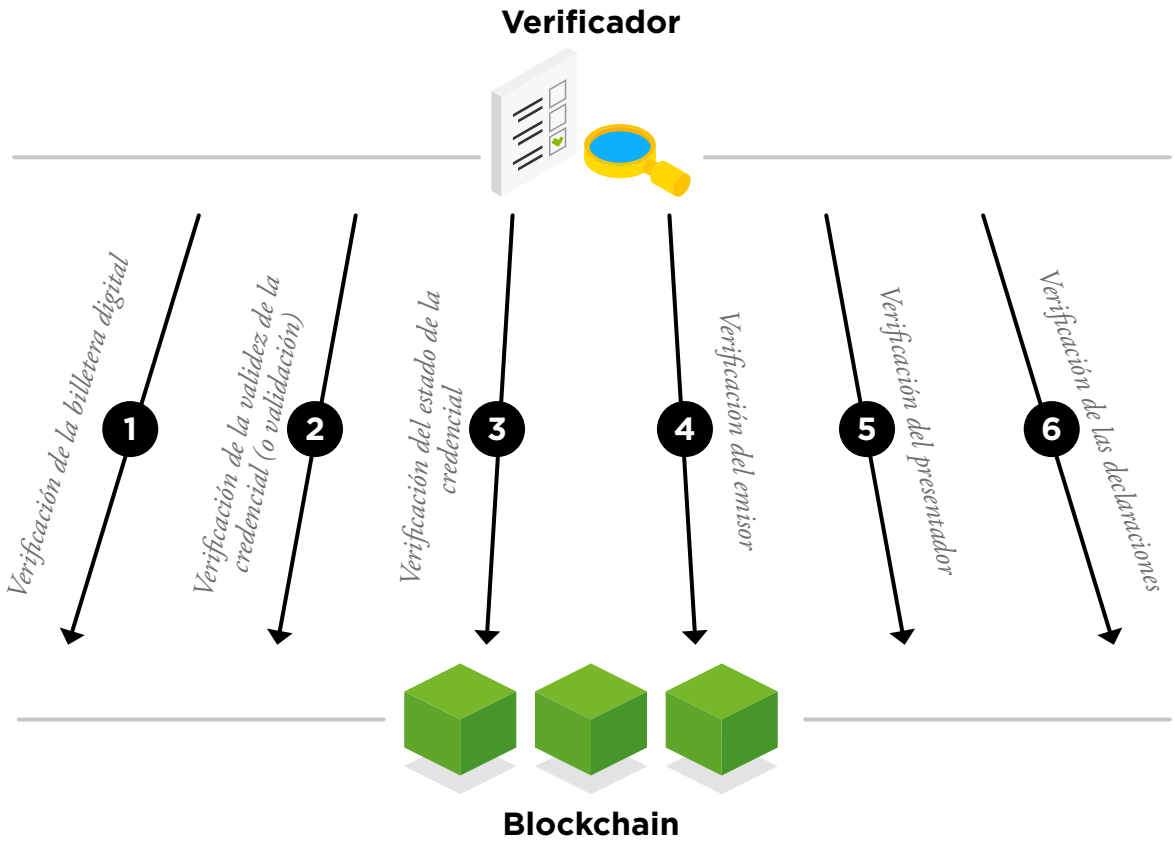
Paso 1. Verificación de la billetera digital: el proveedor de billetera digital garantiza que el titular que presenta la credencial ha sido autenticado en su acceso a la billetera con un nivel de garantía determinado, y asume una responsabilidad en esa garantía.

Paso 2. Verificación de la validez de la credencial (o validación): el verificador comprueba que la estructura, el formato y el contexto de la credencial son correctos. Toda esta información está contenida en la credencial y puede ser verificada automáticamente por el servicio de verificación. La estandarización de la estructura, el formato y el contexto permitirán el reconocimiento internacional de estas, como ocurre con los pasaportes digitales, diplomas digitales o títulos de propiedad digital.

Paso 3. Verificación del estado de la credencial: el verificador comprueba que la credencial tenga un estado activo. Como se describe en la Sección 7.2.6, para este propósito promovemos el uso de contratos inteligentes como CRL mantenidas por los emisores de credenciales. En este caso, las credenciales contendrían un campo que indicaría la dirección del contrato inteligente donde el identificador de la credencial está asociado con un estado dinámico que puede cambiar entre activo, suspendido o revocado. Solo cuando el estado esté activo, el Paso 2 de la verificación deberá considerarse exitoso[48].

48. En la actualidad, a veces, como por ejemplo para entrar a algunos países, se requiere que las personas tengan un pasaporte que no solo sea válido sino que no caduque en los próximos seis meses. Estas condiciones no serían necesarias en un modelo de IAS donde la emisión, presentación, verificación y revocación de credenciales puede ocurrir en tiempo real con mucha mayor facilidad. Sin embargo, si fuese necesario, esta información podría agregarse fácilmente como una condición adicional del proceso de verificación.

Imagen 16. Proceso de Verificación de LACChain ID.



Paso 4. Verificación del emisor: el verificador comprueba la identidad (es decir, la firma digital) del emisor y la cadena de confianza tras de su identidad, si corresponde. Para confiar en el emisor, el verificador necesitará conocer su identidad real. En principio, la credencial presentada por el titular solo contiene el DID y la firma digital del emisor, pero no información adicional sobre su identidad. Es posible que el verificador desconozca o no confíe en esa firma digital. En ese caso, para verificar la identidad real del emisor, ha de ser posible que el verificador sepa cómo acceder a la raíz de confianza detrás de él. Eso requiere raíces de confianza que terminen en una autoridad de certificación inicial (CA) en la que el verificador confíe.[49] En la sección 7.6 veremos un enfoque basado en blockchain para autoridades de certificación, listas de confianza y listas de revocación. Además, en el Bloque 8 analizaremos la tercera capa del modelo de identidad, que consiste en los marcos de confianza que establecen las reglas y los modelos de gobierno para los elementos anteriores. Recomendamos el uso de contratos inteligentes para DNS que vivan dentro de la red.

Paso 5. Verificación del presentador: el verificador comprueba que el presentador esté autorizado para presentar esa credencial, bien sea porque es el sujeto o porque ha sido autorizado para ello por el sujeto. En el primer caso, el presentador podrá demostrar que tiene el control del DID, resolvien-

49. Para poder verificar la cadena de confianza tras un DID, idealmente buscamos llegar a un DID correspondiente a una CA raiz que está registrada en un DNS *on-chain*, que sería un contrato inteligente conocido y reconocido por los miembros de la red. LACChain ha habilitado un DNS *on-chain* donde el Comité Permisionador de LACChain asume la responsabilidad de validar la identidad de entidades emisores y mantener el DNS.

do un desafío asociado a uno de los métodos de autenticación. En el segundo caso, hay al menos dos opciones. Una opción es que el presentador tenga también alguna de las claves privadas asociadas a mecanismos de autenticación del DID, y por tanto pueda resolver retos criptográficos para probar control del mismo. Otra opción es que en la credencial verificable se indique un segundo DID titular, que fuese el de este presentador autorizado, de manera que pudiese resolver retos criptográficos asociados a su propio DID.

Paso 6. Verificación de las reclamaciones: si todos los pasos anteriores se completan con éxito, el verificador finalmente obtiene la información reclamada en la credencial verificable, la procesa y confía en ella.

7.3.6. Revocación

Se aplica lo mismo que para las credenciales verificables, descrito en la Sección 7.2.6.

7.3.7. Mecanismos de divulgación selectiva y pruebas de conocimiento cero (ZKP)

En los esquemas de identidad auto-soberana, los individuos tienen el control de sus datos y sus credenciales, pudiendo decidir cuándo, cómo y a quién desean presentarlos. Las personas también tienen la capacidad decidir cuánta información desean dar a conocer. Pueden, por ejemplo, tener varias credenciales verificables emitidas por diferentes emisores y crear una presentación única con declaraciones específicas parciales de esas credenciales, de tal manera que no se revele ninguna otra declaración que se haga en ellos. Por ejemplo, hoy en día, en el mundo físico, cuando se nos pide que demostremos que tenemos más de cierta edad, generalmente mostramos un documento de identidad que no solo contiene información sobre nuestra edad, sino que también revela una gran cantidad de información no solicitada, como nuestro nombre, el nombre de nuestros padres, la nacionalidad, nuestro género, nuestra fecha de nacimiento, etc. Otro ejemplo es cuando se nos pide que demostremos que nuestros ingresos superan una cierta cantidad, por ejemplo, para poder aplicar a un contrato de alquiler, y para ello debemos mostrar documentos que revelan innecesariamente nuestro salario exacto.

En el mundo digital, cuando trabajamos con elementos como registros blockchain y firmas digitales, existe una forma más sofisticada de demostrar que algo es cierto sin necesidad de revelar ninguna otra información adicional. Estas afirmaciones se conocen como pruebas de conocimiento cero (ZKP por su nombre en inglés). Según el NIST, los principales tipos de declaraciones son los siguientes (NIST-TA, 2020):

- **Igualdad o no igualdad:** el valor de una magnitud es igual o no a un valor dado.
- **Desigualdad:** el valor de una magnitud es mayor o menor que un valor dado.
- **Membresía:** un sujeto está contenido en una lista.
- **Rango:** el valor de una magnitud está dentro de un intervalo dado [a, b] o no lo está.

En el contexto de tener un probador (la entidad que intenta probar la veracidad de la declaración) y un verificador (la entidad que intenta verificar si un reclamo es verdadero), las pruebas de conocimiento cero deben satisfacer las siguientes tres propiedades:

- **Integridad:** si la declaración es verdadera, un verificador honesto podrá convencerse de ello.
- **Solidez:** si la declaración es falsa, un probador deshonesto no podrá convencer al verificador.
- **Conocimiento cero:** si el reclamo es verdadero, el verificador no obtiene ninguna información adicional al hecho de que lo es.

También existen dos tipos de procesos de prueba de conocimiento cero, según la clase de interacción entre el probador y el verificador:

- **Interactivo:** el probador y el verificador participan en diferentes rondas, en las cuales el verificador requiere que el probador resuelva los desafíos.
- **No interactivo:** el verificador puede comprobar la veracidad de la declaración sin ninguna interacción adicional con el probador una vez que se presente la prueba.

Tabla 12. Definición y ejemplos de las pruebas de conocimiento cero.

	Definición	Ejemplo
Igualdad y no igualdad	El valor de una magnitud es igual o no igual a un valor dado.	Una persona de cierta edad.
Desigualdad	El valor de una magnitud es mayor o menor que un valor dado.	El saldo de una cuenta supera una cierta cantidad.
Membresía	El sujeto aparece en una lista.	Una persona es miembro de un club.
Rango	El valor de una magnitud está o no dentro de un intervalo dado [a, b].	El número de personas de una determinada población es de entre 1 y 2 millones.

En algunos casos, se requieren compromisos previos o supuestos de cálculo adicionales. (Lum et al, 1988) (Wu y Hang, 2014).

7.3.8. Trazabilidad y monitorización

Cuando se adopta el almacenamiento de credenciales *off-chain* visto en las Secciones 7.2.3 y 7.2.4:

- El intercambio de credenciales es también *off-chain*, por lo que no deja ningún rastro en el registro.
- La verificación de credenciales consulta el registro, pero sin generar transacciones, por lo que no hay trazabilidad.

Esto ayuda a cumplir con los requisitos de privacidad de datos. Sin embargo, podría darse el caso de que el intercambio y la verificación de las credenciales pretenda conocerse para poder medir el impacto y proporcionar respuestas para la solución. En este caso:

- Deben diseñarse enfoques escalables para cada solución, si se quieren poder registrar transacciones en el libro mayor cuando se presentan y verifican las credenciales.
- Se preservará la privacidad de los datos, incluida la IIP que puede derivarse de intercambios y verificaciones. Solo se registrarán datos cuantitativos en el libro mayor y se recopilarán datos agregados.

7.4. Repositorios digitales y billeteras

7.4.1. Definición

En el contexto de la identidad soberana, una billetera digital es un repositorio privado que permite a su propietario almacenar, administrar y presentar claves y credenciales de identidad. Una billetera digital debe:

- Estar certificada y/o auditada para ser reconocida como servicio de confianza.
- Estar conectada a las redes descentralizadas donde se almacenan los registros de DID, las listas de confianza y las pruebas criptográficas de los documentos DID y las credenciales digitales verificables.

- Garantizar la encriptación robusta de datos.
- Habilitar la recuperación de claves y credenciales.
- Proporcionar mecanismos para que el sujeto borre todos los datos asociados asociados a un identificador en su propiedad.
- Proporcionar mecanismos para que sujetos y emisores puedan modificar el estatus de las credenciales.
- Proporcionar un acceso seguro al titular, garantizando que ningún usuario no autorizado podrá autenticarse.

Una billetera digital podría:

- Mantener información transaccional sobre las entidades, si está autorizada para ello.
- Proporcionar mecanismos para reducir la IIP de las actividades y de las entidades combinando el uso de diferentes DID para diferentes interacciones.
- Proporcionar métricas de actividad.

7.4.2. Tipos

Puede haber diferentes tipos de billeteras digitales:

- Billeteras de escritorio (instaladas en un computador particular).
- Billeteras de hardware (dispositivos físicos como un disco duro o un USB).
- Billeteras móviles (aplicaciones móviles).
- Billeteras de navegador (extensiones de navegador instaladas en un computador particular).
- Billeteras en la nube (basadas en el almacenamiento en la nube).

Las billeteras móviles y en la nube son las opciones más portables.

7.4.3. Recuperación de claves

La primera capa de la identidad digital la conforman nuestras claves privadas y autenticadores, pues nos permiten probar la propiedad de nuestros identificadores y credenciales. Por tanto, es esencial que las billeteras digitales dispongan de mecanismos clave de recuperación en caso de pérdida o robo de las billeteras digitales.

Como se dijo en la Sección 7.1.4, los métodos DID robustos especificarán diferentes tipos de claves de manera que, si una de las claves principales se ve comprometida, se pueda utilizar una clave secundaria para revocarla y/o recuperar el control sobre la identidad. La ausencia de esta funcionalidad es uno de las grandes lacras del mundo de las criptomonedas que viven en redes blockchain públicas no permisionadas, pues muchos usuarios han perdido millones de dólares en criptoactivos al perder la clave privada asociada a su cuenta. Cuando la recuperación de claves no es posible, si un usuario pierde sus llaves privadas nunca más tendrá acceso a su cuenta, no podrá iniciar acciones legales contra el ladrón y tampoco reclamar las divisas y credenciales perdidas, pues no podrá probar que alguna vez poseyó esa cuenta.

Hay dos tipos de sistemas de administración de claves que se pueden utilizarse para la recuperación de claves.

7.4.3.1. Sistemas centralizados de gestión de claves (CKMS)

Es posible y recomendable utilizar sistemas centralizados complementarios para gestión de claves (CKMS por sus siglas en inglés) que permitan hacer copias de seguridad de claves privadas y certificados digitales de manera que puedan ser recuperados en caso de pérdida o robo. Una primera opción de respaldo centralizada es el uso de repositorios privados en la nube que las billeteras proporcionarían a sus usuarios. Una segunda opción son las copias de seguridad off-line, como USB o discos duros, a los que las billeteras permitirían exportar los respaldos de llaves privadas y credenciales digitales verificables.

Los proveedores de billeteras de identidad deben definir reglas claras e informar a las entidades sobre cómo y bajo qué circunstancias pueden recuperar sus claves y credenciales. La recuperación de claves debe encontrar un equilibro entre la utilidad y la seguridad.

7.4.3.2. Sistemas descentralizados de gestión de claves (DKMS)

Los sistemas descentralizados de gestión de claves (DKMS por sus siglas en inglés) consisten en

confiar en varias entidades, personas o nodos para que almacenen las claves privadas o "semillas" de claves privadas de un individuo. Un algoritmo generalmente utilizado para este enfoque es el protocolo Shamir Secret Sharing (SSS), que permite generar m semillas de una clave de manera que con solamente n semillas, siempre que $n<m$, sea posible recuperar la clave. Existen diferentes alternativas para su protección, como:

- **Recuperación de claves sociales:** las m semillas se almacenan en repositorios privados que pertenecen a amigos y familiares.
- **Registros descentralizados:** las m semillas se almacenan en nodos IFPS o en nodos de redes blockchain. Estos nodos deben garantizar disponibilidad.

7.4.4. Recuperación de credenciales

Dado que las billeteras digitales son el repositorio privado de los individuos para almacenar sus credenciales digitales, es esencial que existan mecanismos de recuperación en caso de que la billetera se pierda o se vea comprometida. Como en el caso de las llaves privadas discutidos en la sección anterior, las billeteras digitales han de permitir hacer copias de seguridad de las credenciales tanto en la nube como en dispositivos de hardware off-line.

En el caso de copias de seguridad en la nube o cualquier otra copia de seguridad facilitada por el proveedor de billetera, han de definirse reglas claras y se informará a las entidades sobre cómo y bajo qué circunstancias pueden recuperar sus credenciales. La recuperación de credenciales debe encontrar un equilibrio la utilidad y la seguridad.

Además de la recuperación de credenciales proporcionada por el proveedor de billetera digital podría ser posible recuperar las credenciales pidiéndole al emisor que las emita de nuevo. Como los emisores necesitarían conservar los datos originales de la generación de credenciales para sus propios registros, podrían volver a emitir una credencial a un sujeto cuando el original se pierda o sea robado. Sin embargo, esto requeriría que el sujeto se comunique y autentique contra cada una de las entidades que han emitido sus credenciales, lo que podría suponer altos costes de tiempo y dinero.

7.5. Prueba de identidad, autenticación y autorización

La prueba de identidad, la autenticación y la autorización están presentes en cada prestación electrónica de servicios por parte de un proveedor de servicios a un solicitante. La prueba de identidad consiste en verificar que el solicitante es quien dice ser. La autenticación consiste en asegurar que el servicio electrónico se brinda y consume de manera segura. La autorización consiste en comprobar que el solicitante está autorizado para consumir el servicio y darle acceso.

7.5.1. Prueba de identidad

El proceso que sigue la prueba de identidad es el siguiente:

1. La entidad solicitante solicita la emisión de credenciales de identidad.
2. El emisor de identidad comprueba la identidad real del sujeto.
3. El emisor de identidad emite las credenciales de identidad digital y las envía al titular[50].
4. El titular almacena las credenciales de identidad en un repositorio.

Se pueden distinguir tres niveles en la prueba de identidad (NIST-IDGa, 2017):

IP1: no hay ningún requisito para vincular al solicitante con una identidad específica de la vida real. Las reclamaciones pueden auto-firmarse y las credenciales auto-emitirse o ser emitidas por terceros

50. El titular y el sujeto pueden ser la misma entidad. Titular, tal como se presentó en la Sección 3.4, es un término más general que permite referirse a la entidad que controla la credencial, ya sea que sea el sujeto o no.

que no cumplan con ningún requisito específico. Esto es útil para acceder a servicios digitales como sitios web que solo requieren que tengas un perfil seudónimo. En este caso, se omitiría el paso 2.

IP2: el emisor de identidad verifica la identidad real de la entidad. La verificación puede ser digital. Los emisores deben cumplir con requisitos específicos, como tener un nivel de prueba de identidad IP2 o IP3. Esto es útil para acceder a servicios digitales como redes sociales, como por ejemplo Facebook o LinkedIn, que requieren que los usuarios sean personas reales e identificadas.

IP3: el emisor verifica la identidad real de la entidad con el máximo nivel de garantía. La verificación requiere presencia física. Los emisores se identifican con credenciales que siguen una raíz de confianza donde la CA principal es una entidad confiable y reconocida a nivel local, nacional, regional o internacional. Este nivel es necesario para acceder a los servicios digitales que tienen el máximo nivel de seguridad, como los servicios gubernamentales o financieros.

7.5.2. Autenticación

La autenticación se basa siempre en tres tipos de factores:

- Algo que sabes (por ejemplo, una contraseña).
- Algo que tienes (por ejemplo, un teléfono móvil, una credencial de identificación recibida tras pasar una prueba de identidad, o una clave criptográfica).
- Algo que eres (por ejemplo, una huella digital u otro dato biométrico).

Para acceder a servicios digitales con las credenciales que almacenamos en nuestras billeteras digitales, necesitamos autenticarnos primero en la billetera digital para acceder a nuestra identidad digital y después al servicio digital.

7.5.2.1. Autenticación de los usuarios en las billeteras digitales

En el modelo IAS, los individuos almacenan sus claves y credenciales en repositorios administrados por ellos mismos. Estos repositorios se conocen como billeteras digitales y es fundamental evitar que los usuarios no autorizados accedan a ellas. Si un usuario no autorizado tiene acceso a la billetera digital de otro, podrá controlar sus credenciales de identidad, dinero digital, criptomonedas, diplomas digitales, escrituras de propiedad digitales, etc. Con el fin de crear soluciones de identidad auto-soberana confiables y seguras, la autenticación contra la billetera digital debe ser extremadamente segura.

En una implementación robusta de la IAS, las billeteras son, con diferencia, el punto más sensible ante hackeos. Los proveedores de billeteras deben desarrollar soluciones que no requieran ningún conocimientos técnicos o tecnológicos por parte del usuario para utilizarlas y garantizar su protección. Para ello, es necesario que los proveedores de billeteras desarrollen diferentes mecanismos para autenticar al usuario en el momento de acceder a su billetera digital, en el momento de acceder a su credenciales y en el momento de presentar sus credenciales ante terceros.

1. **Registrarse en la billetera digital:** la billetera digital debe requerir un conjunto mínimo de factores de autenticación al usuario. Una vez que el usuario complete el proceso de registro, puede comenzar a crear DID, generar y recibir credenciales verificables y presentar información a otros (por ejemplo, para acceder a servicios digitales o físicos de estos de manera autenticada).
2. **Iniciar sesión en la billetera digital:** las billeteras digitales se deben asegurar de que los factores de autenticación permitan la verificación de la identidad del usuario con un alto nivel de seguridad, combinando cosas que los usuarios saben, tienen y son.
3. **Acceso a las credenciales digitales en la billetera digital:** una vez que el usuario ha iniciado sesión, la billetera digital podrá restringir la información confidencial de su propio usuario, como el acceso a sus credenciales digitales, y solicitar verificaciones adicionales en tiempo real, tales como biometría o preguntas de seguridad.
4. **Presentar las credenciales a terceros:** de manera similar al acceso a la información confidencial,

las billeteras digitales también deberán requerir a los usuarios que pasen verificaciones adicionales cuando intenten compartir información confidencial con otros o usarla para acceder a servicios de terceros. En algunos casos, el propio proveedor de servicios podría indicarle a la billetera que su servicio requiere un alto nivel de seguridad y garantía en la verificación electrónica. Por ejemplo, cuando se utiliza un pasaporte digital para acceder a los servicios de alto nivel de seguridad, como tomar un vuelo o realizar una operación financiera.

Como vimos en la Sección 7.3.5, cuando una persona intenta usar una credencial digital de su billetera digital para acceder a un servicio digital, el primer paso del proceso de verificación será la verificación de la billetera digital desde donde se presenta la credencial. Si el proveedor de servicios no confía en la billetera digital, entonces no autorizará el acceso. Los proveedores de servicios confiarán en las billeteras digitales siempre que conozcan y confíen en los mecanismos que utilizan para autenticar a las personas. Se espera que las billeteras digitales más avanzadas se certifiquen como servicios de confianza en diferentes regulaciones para así ser reconocidas y confiables nacional e internacionalmente.

7.5.2.2. Autenticación del usuario en servicios digitales

Para acceder a un servicio digital, el titular presenta una credencial de su billetera digital al servicio proporcionado por un proveedor de servicios. Al recibir la credencial verificable, el servicio provisto debe ser capaz de cumplir con el proceso de verificación descrito en la Sección 7.3.5. Esto incluye la verificación de la billetera digital; la estructura, formato y contexto de la credencial; el estado de la credencial; el emisor; el presentador; y las declaraciones.

Si el proveedor de servicios no puede verificar todo lo anterior, el proceso de autenticación fallará y el individuo no tendrá autorización para acceder al servicio. En principio, el proveedor del servicio no podrá reconocer una credencial como válida si no confía en la billetera digital desde la que se presenta la credencial, si no reconoce la sintaxis de la credencial o si no confía en el emisor. Sin embargo, en un ecosistema auto-soberano completamente alineado con las políticas reguladoras, podría imponerse por regulación la validez de ciertas autenticaciones que provienen de billeteras digitales cualificadas y que presentan credenciales estandarizadas que fueron emitidas por emisores confiables cualificados (por ejemplo, un pasaporte digital emitido por un gobierno).

7.5.3. Autorización

Como adelantamos al explicar el proceso de verificación presentado en la Sección 7.3.5, cuando se presenta la credencial para recibir un servicio (digital o físico), el proveedor del servicio verifica que la billetera digital que presenta la credencial (si corresponde) es confiable, la credencial es válida, el emisor es conocido y quien la presenta está autorizado a presentar esa credencial. Como veremos a continuación, existen dos tipos de autorizaciones que pueden verificarse cuando se presenta una credencial verificable.

7.5.3.1. Autorización del presentador

Cuando se presenta una credencial, en el Paso 5 del Proceso de Verificación el verificador comprueba que el presentador esté autorizado para presentar esa credencial, bien sea porque él es el sujeto o porque ha sido autorizado para ello. En el primer caso, el presentador podrá demostrar que tiene el control del DID, resolviendo un desafío de uno de los métodos de autenticación. En el segundo caso, hay al menos dos opciones. Una opción es que el presentador tenga también alguna de las claves privadas asociadas a mecanismos de autenticación del DID, y por tanto pueda resolver retos criptográficos para probar control del mismo. Otra opción es que en la credencial verificable se indique un segundo DID titular, que fuese el de este presentador autorizado, de manera que pudiese resolver retos criptográficos asociados a su propio DID

Si los documentos DID tienen diferentes tipos de métodos de autenticación, como se introdujo en la Sección 7.1.4, estos pueden ser utilizados para diferentes propósitos (por ejemplo, control total, delegación temporal, recuperación de claves, etc.) de manera que la entidad que controla el DID puede compartir con otras entidades algunas claves privadas asociadas a algunos de los métodos de autenticación. Este sujeto podrá, por tanto, generar credenciales verificables en las que se indique que solo se puede usar un conjunto específico de las claves públicas del DID para probar la propiedad de esa credencial específica.

También podría suceder que el sujeto de la credencial sea menor de edad y, por lo tanto, no esté autorizado para presentar la credencial sin la aprobación de un representante legal. En este caso, el verificador no aceptará la credencial a menos que cuente con la aprobación de su representante (por ejemplo, al firmar la presentación con su firma digital o al emitir una credencial de consentimiento adicional). Esto puede lograrse con esquemas multi-firma.

7.5.3.2. Autorización del propósito

En el momento de emisión de la credencial, el emisor podría restringir el uso de la misma para un propósito o servicio específico (por ejemplo, una credencial de identidad académica para autenticar al sujeto a la hora de acceder a servicios digitales proporcionados por un grupo de universidades que tengan acuerdos privados para el reconocimiento de esa credencial). En este caso, la credencial incluiría un campo específico especificando dicho propósito.

7.6. Autoridades de certificación (CAs) y listas de confianza (TLs)

En un modelo de identidad digital basado en PKI, las autoridades de certificación (CA) son aquellas entidades que emiten credenciales de identidad que otros reconocen con cierto grado de garantía. Como se explicó en el Bloque 5, en las soluciones en las que interviene el gobierno, éste designa las CA raíz. Sin embargo, en las soluciones no gubernamentales, que tienen el potencial de proliferar mucho más rápido en el modelo IAS a corto plazo, hay una gran oportunidad para que diferentes entidades privadas y multilaterales se conviertan en CAs confiables.

Hay al menos dos de listas de confianza (TLs por su nombre en inglés) esenciales. La primera lista de confianza es la de proveedores de identidad o CA designadas por una autoridad. Una segunda lista es la de certificados que cada CA ha emitido a otras entidades y su estado (activo, suspendido o revocado). Esto permite crear cadenas de confianza para verificar si un certificado digital emitido por una entidad que no conocemos o en la que no confiamos está certificado por una entidad en la que sí confiamos.

En la actualidad, cada navegador tiene un agente fiable que reconoce las firmas de algunas autoridades de certificación raíz reconocidas internacionalmente. Por lo tanto, cuando cualquier servicio o sitio nos presenta un certificado X.509, nuestro navegador es capaz de rastrear la cadena de certificados que hay detrás de él y verificar en tiempo real si termina en una CA raíz que el navegador conoce y en la que confía. Para la identidad auto-soberana, el mecanismo será exactamente el mismo, pero con modificaciones mínimas de los protocolos que permitan, entre otras cosas, reemplazar los certificados X.509 actuales por credenciales digitales verificables.

Hoy en día, las CA mantienen listas de confianza y listas de revocación de certificados (CRLs), y se aplican protocolos como el protocolo de estado de certificados en línea (OCSP por su nombre en inglés) para verificar si un certificado es válido. La tecnología blockchain permite usar contratos inteligentes para mantener listas de confianza públicas y descentralizada, y CRLs. Con blockchain, en lugar de que cada CA tenga que mantener bases de datos externas que no están interconectadas, las autoridades de certificación simplemente pueden desplegar un contrato inteligente en una red de blockchain y registrar el URI de cada certificado que emiten, jun-

to con su estado y metadatos adicionales de interés. Como vimos en la Sección 7.2.2, las credenciales verificables digitales deben contener un campo que especifique en qué contrato inteligente se encuentra la información sobre el estado de la credencial de manera que cuando se presenta la credencial a terceros, estos pueden verificar automáticamente si la credencial está activa. Como sucede hoy con los certificados X.509, la verificación no es manual, sino que cada aplicación o servicio tendrá un agente la realice automáticamente.

Esto reduce los costes que las autoridades y las CA deben asumir hoy para mantener y exponer bases de datos centralizadas de listas de confianza y CRLs; agrega transparencia al proceso, ya que cada cambio en la lista de confianza o en el estado de la credencial se registra en la blockchain; y proporciona más accesibilidad a la información porque está en cada copia de la blockchain que tiene cada nodo. También garantiza la disponibilidad incluso si la infraestructura tecnológica de la CA se cae o la CA desaparece, porque las listas de confianza y de revocación permanecen en la red de blockchain y no en un repositorio digital centralizado mantenido y expuesto por la CA.

A corto plazo, esperamos una combinación de los certificados electrónicos actuales y la tecnología blockchain, donde los X.509 tradicionales serán utilizados para firmar transacciones en la blockchain. A medio plazo, prevemos una nueva generación de credenciales que siguen el modelo IAS con DIDs, credenciales verificables, presentaciones verificables y billeteras digitales que sustituirán a los certificados X.509 y los repositorios centralizados actuales.

7.7. Tecnología de registro distribuido (DLT)

Como se ha señalado en secciones anteriores, y analizado pormenorizadamente en la Sección 3.6, es esencial que la IAS utilice registros descentralizados para almacenar las pruebas criptográficas de los DIDs, el estado de las credenciales y presentaciones verificables, las claves públicas de las autoridades de certificación y las listas de confianza, entre otros. Las redes blockchain son un tipo específico de registros descentralizados caracterizados por disponer de contratos inteligentes para la automatización procesos y digitalización de activos, y aplicar protocolos de consenso para generar nuevos bloques de forma que todos los nodos mantengan la misma copia de la información. Las redes blockchain son más adecuadas para la IAS que otros registros descentralizados dado que permiten usar direcciones blockchain como DID, permiten también usar contratos inteligentes para listas de confianza y no hay diferentes versiones o silos de información entre diferentes entidades en la red.

Según la Organización Internacional de Normalización (ISO), existen tres tipos de redes blockchain (ISO, 2018):

No permisionadas: son aquellas a las que cualquiera puede unirse en cualquier momento, como Bitcoin o Ethereum. La mayoría de estas redes están asociadas a una criptomoneda. Pese a que son abiertas y transparentes, generalmente tienen tarifas muy altas de transacción, no disponen de privacidad[51], y todos los usuarios son seudónimos. Además, como los participantes no están identificados, es difícil poder obligar a que las transacciones y las aplicaciones cumplan la normativa, y perseguir a aquellos que no lo hagan.

Permisionadas privadas: son aquellas en las que una agrupación bien definida de entidades implementa, ejecuta y mantiene todos los nodos. En general, estas redes son desarrolladas e incluso mantenidas por un proveedor de servicios de blockchain. Las redes privadas, en general, no tienen

51. Las redes no permisionadas no son privadas en el sentido estricto de la palabra, ya que toda la información registrada en ellas es pública. Sin embargo, en principio no es posible saber quién está detrás de cada transacción porque las cuentas son seudónimas. En la práctica, el seudónimo no garantiza la privacidad, ya que la identidad se puede revelar de diferentes maneras.

costos de transacción (aunque podría haber un precio fijo establecido por el proveedor del servicio, si existiera), y también permiten la privacidad. Sin embargo, estas redes no son descentralizadas ni transparentes, la escalabilidad es muy limitada y generalmente están diseñadas para un solo uso o aplicación. Ejemplos de estas redes son IBM FoodTrust[52] y la red blockchain de Energy Web Chain por el grupo Energy Web Foundation (EWF) (EWF, 2018).

Permisionadas públicas: son aquellas en las que un consorcio o agrupación inicia una red y permite que cualquiera se una siempre que cumpla una serie de requisitos, como estar autenticados y cumplir con la regulación. En estas redes, el consorcio es autosuficiente y no necesita depender de un proveedor. Las redes públicas autorizadas son abiertas, transparentes, descentralizadas y, en general, sin costo por transacción. Al mismo tiempo, se identifica a cada participante, de modo que se habilita la privacidad y el cumplimiento de la regulación. Ejemplos de estas redes son Alastria en España, liderada por una asociación de más de 500 miembros; EBSI en Europa liderado por la Unión Europea; y LACChain en América Latina y el Caribe, liderado por el Banco Interamericano de Desarrollo y sus aliados en el programa.

El modelo de identidad auto-soberana puede emplear diferentes tipos de redes blockchain e incluso otros libros mayores descentralizados. Sin embargo, las redes públicas autorizadas son las más adecuadas, pues las redes no permisionadas están diseñadas para ser anónimas y las redes permisionadas privadas son pequeñas están limitadas a usos específicos y pruebas de concepto. Por el contrario, las redes permisionadas públicas tienen costos de transacción nulos, cumplen con la regulación y están diseñadas para ser multipropósito, siendo el complemento perfecto para las registros descentralizados que necesita la identidad auto-soberana. No es una coincidencia que las tres redes público-permisionadas mencionadas en el párrafo anterior estén liderando las iniciativas de referencia en identidad auto-soberana en sus regiones: Alastria ID, el pasaporte digital europeo basado en blockchain y LACChain ID, respectivamente.

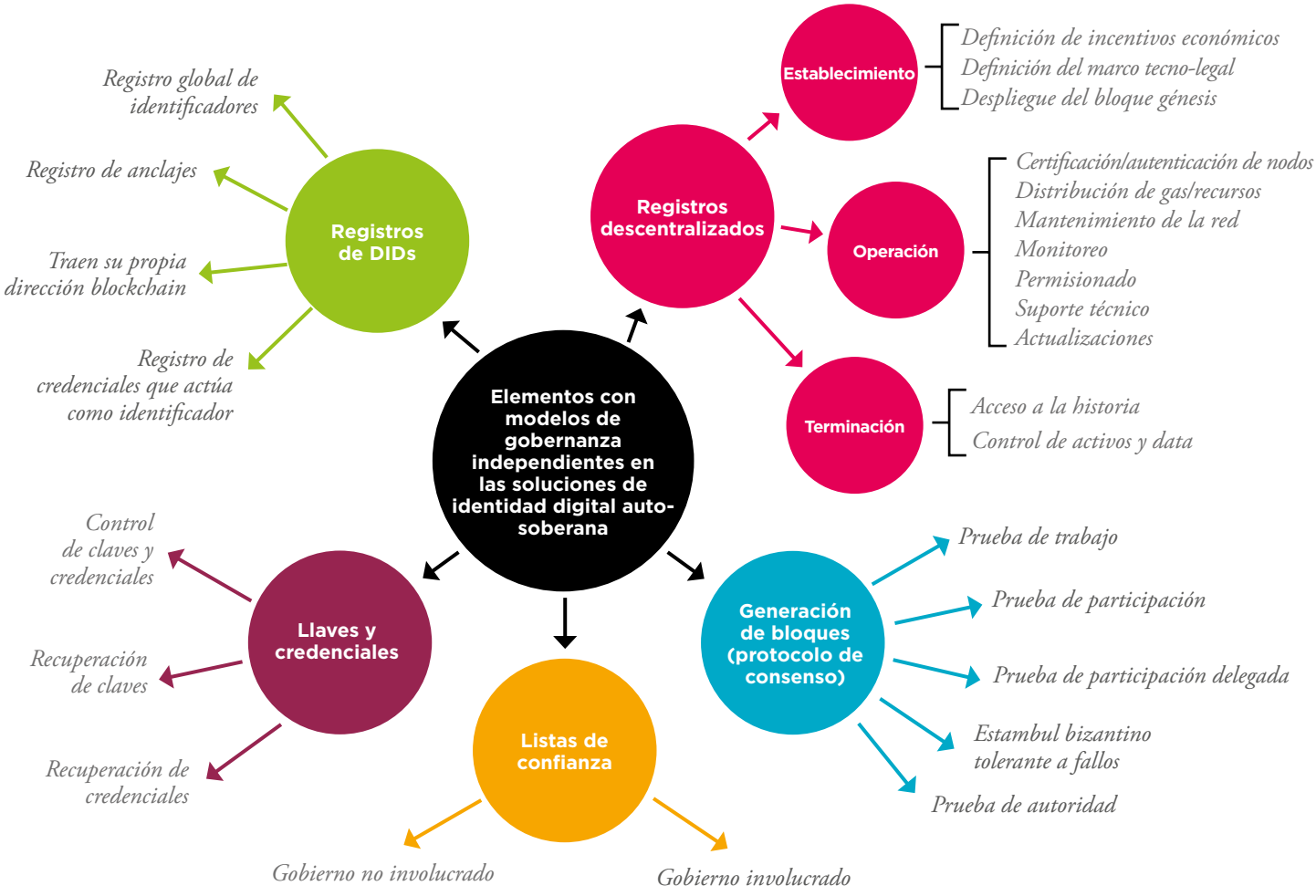
52. https://www.ibm.com/blockchain/solutions/food-trust

IDENTIDAD DIGITAL AUTO-SOBERANA

Block 8

Marcos de confianza

Imagen 17. Elementos con modelos de gobernanza independientes en las soluciones de identidad digital auto-soberana.



Un marco de confianza es el "término genérico que se utiliza a menudo para describir un conjunto de especificaciones, reglas y acuerdos legalmente aplicables que rigen un sistema multipartito establecido para un propósito común, diseñado para realizar tipos específicos de transacciones entre una comunidad de participantes, y obligado por un conjunto común de requisitos. […] Se les conoce como reglamentos operativos, reglas de esquemas o políticas operativas en contextos diferentes a la identidad digital", de acuerdo con Open Identity Exchange (OIX), una referencia internacional en la materia. (OIX-TF, 2010)

El alcance de un marco de confianza[53] puede ser muy amplio, desde un reconocimiento dentro de una sola organización o grupo de entidades, hasta un acuerdo regional, sectorial o internacional. Algunos ejemplos de marcos de confianza nacionales son los que establecen la soberanía del gobierno para la emisión de credenciales de identidad (por ejemplo, los documentos de identificación nacionales). Un ejemplo de marco regional sería el reconocimiento casi global de los pasaportes nacionales que siguen los estándares dictados por la Organización de Aviación Civil Internacional (OACI). Como ejemplos de marcos sectoriales cabe mencionar los acuerdos de reconocimiento mutuo (ARM) entre aduanas, las

53. Hay una publicación muy recomendable de NIST que puede ser obtenida de https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8149.pdf

redes de liquidación entre instituciones financieras o el reconocimiento de certificaciones entre universidades.

En un ecosistema de identidad digital, ya sea auto-soberana o no, los marcos de confianza definen el modelo de gobernanza, las autoridades de certificación,[54] los proveedores de identidad, los niveles de garantía de la identificación electrónica y los canales de comunicación -entre otros-, que permiten establecer raíces confiables, listas de confianza, listas de revocación de certificados y muchos otros elementos de confianza necesarios.

8.1. Modelos de gobernanza

Un modelo de gobernanza establece principios, políticas, terminología, estándares y responsabilidades. Como ejemplo metafórico, los marcos de confianza establecen los acuerdos y las reglas del juego, mientras que los modelos de gobernanza definen los roles y responsabilidades de los jugadores. En las implementaciones actuales de los esquemas de identidad digital, el modelo de gobernanza establece quién determina las autoridades de certificación, quiénes son las autoridades de certificación y dónde se pueden encontrar las listas de confianza y las litas de revocación de certificados. En la identidad auto-soberana, el modelo de gobernanza es más complejo puesto que hay nuevos elementos para gobernar, como el registro descentralizado o red blockchain. Como no hemos encontrado ninguna clasificación ya existente de elementos de gobernanza independientes particularizados a la IAS, hemos propuesto estructurarla como se presenta en la figura 4 y se desglosa en las siguientes secciones.

8.1.1. Gobernanza de registros descentralizados y redes blockchain

De acuerdo con ISO/TC, "la gobernanza de los sistemas DLT y blockchain es un enfoque que comprende elementos de los derechos decisorios centralizados y descentralizados, donde la responsabilidad se encuentra dentro de la red y en la cual se brindan incentivos para llegar a un consenso [...]. La gobernanza de sistemas DLT y blockchain comprende varias funciones clave durante la etapa operativa del sistema DLT y blockchain, como la inscripción de derechos de participación para los participantes en el sistema DLT y blockchain y las reglas de contratación asociadas con la participación en el sistema DLT y blockchain. Todos los sistemas DLT y blockchain operarán dentro del contexto más amplio de marcos legales y regulatorios externos; en algunos casos, los sistemas DLT y blockchain pueden proporcionar orientación y mecanismos sobre la red para gestionar la operación [...]. La vista del ciclo de vida de gobernanza de los sistemas DLT y blockchain aborda tanto los riesgos inherentes como los intereses de los participantes DLT y las partes interesadas más amplias durante el establecimiento, operación y finalización del sistema DLT" (ISO, 2020).

Para nosotros, las tareas esenciales que comprende la gobernanza de un registro descentralizado o una red blockchain se pueden dividir en las tres fases de su "ciclo vital": establecimiento, operación y finalización. Dichas tareas son:

Establecimiento

Definición de los incentivos económicos: definición de incentivos económicos para garantizar la sostenibilidad de la blockchain.

Definición del marco tecno-legal: definición del marco tecno-legal que permita establecer la base legal y la arquitectura técnica de la blockchain, así como los diferentes órganos necesarios.

Despliegue del bloque de génesis: diseño y despliegue del primer bloque de la red que contiene reglas blandas (por ejemplo, los nodos de validación iniciales) y duras (por ejemplo, el protocolo de consenso). Despliegue de los primeros nodos.

Operación

Certificación/autenticación de nodos: acometer verificación de identidad y certificación de nodos

54. El concepto de autoridad de certificación es equivalente al de proveedor de credenciales como servicio.

Tabla 13. Comparación de gobernanza en los tres tipos de redes blockchain vistos en la Sección 7.7.

	No Permisionadas	Permisionadas privadas	Permisionadas públicas
Definición de los incentivos económicos	Comunidad abierta	Consorcio	Entidad neutral gestora de la infraestructura
Definición del marco tecno-legal	Puede ser provisto por el diseñador del software	Consorcio	Entidad neutral gestora de la infraestructura
Despliegue del bloque génesis	Comunidad abierta	Consorcio	Entidad neutral gestora de la infraestructura
Certificación / autenticación	No aplica	Nadie	Entidad neutral gestora de la infraestructura
Distribución de gas/recursos	Consorcio	Consorcio	Entidad neutral gestora de la infraestructura
Mantenimiento	Comunidad abierta	Consorcio	Entidad neutral gestora de la infraestructura
Monitorización	Comunidad abierta	Consorcio	Entidad neutral gestora de la infraestructura
Permisionado	No se aplica	Consorcio	Entidad neutral gestora de la infraestructura
Soporte técnico	Comunidad abierta	Distribuidor/Proveedor de tecnología	Entidad neutral gestora de la infraestructura
Actualizaciones	Comunidad abierta	Distribuidor/Proveedor de tecnología	Entidad neutral gestora de la infraestructura
Acceso al historial después de la terminación	Cualquier entidad que tuviese un nodo	Consorcio	Cualquier entidad que tuviese un nodo
Gestión de datos y activos después de la terminación	Proveedores de servicios y aplicaciones	Consorcio	Proveedores de servicios y aplicaciones

en la red de manera que pueda ser confiable para todos los participantes.

Distribución de gas/recursos: gestión de la distribución de recursos en la red entre los usuarios garantizando que siempre opera bajo un nivel de estrés determinado.

Mantenimiento de la red: mantenimiento de la red para garantizar que corre sin problemas y no falla, colapsa o muere.

Monitorización: desarrollo y mantenimiento de herramientas de monitorización y monitoreo de la red.

Permisionado: autorización y desautorización de nodos y cuentas para su participación en la red (por ejemplo, las listas blancas y listas negras)[55].

Soporte técnico: brindar asistencia técnica en caso de que algo falle en la implementación o el

55. Las condiciones bajo las cuales un usuario tiene acceso a una red blockchain (en redes permisionadas) se basan en la aceptación de los términos de uso de la red. Estas reglas de acceso están determinadas por una entidad gestora neutral de la infraestructura. Todas las partes detrás del sistema son conocidas e identificables.

rendimiento de nodos o aplicaciones en la parte superior de la red.

Actualizaciones: investigación proactiva y desarrollos en la red para mejorar la seguridad, la eficiencia, la escalabilidad, el rendimiento y la interoperabilidad.

Terminación

Acceso al historial: garantizar acceso al historial de las transacciones.

Gestión de activos y datos: determinación de cómo se transfieren, destruyen o eliminan los datos o activos (por ejemplo, contratos inteligentes, tokens y pruebas de certificados).

Dependiendo del tipo de registro descentralizado o red blockchain en cuestión, algunas de estas tareas las realizan diferentes y otras no se aplican. En la Tabla 17 mostramos una visión general[56].

8.1.2. Gobierno de la generación de bloques (protocolo de consenso)

El proceso de generación de bloques en una red blockchain se conoce como protocolo de consenso y su gobernanza es independiente de la gobernanza de la red que incluye todo lo presentado en la sección anterior. Por ejemplo, en Bitcoin, la comunidad abierta es responsable de la gobernanza de la red, pero solo un pequeño número de entidades se encarga de la generación de bloques, y por tanto tiene el gobierno de este proceso. En las redes permisionadas, un vehículo legal de organización (representando a un consorcio) podría gobernar la red, pero cualquier entidad podría participar en el protocolo de consenso[57], sean o no parte del vehículo legal. Algunos de los protocolos de consenso más conocidos y usados son:

Prueba de trabajo: cualquier nodo en la red puede competir con poder computacional para ganar una "lotería" que les permita generar el nuevo bloque (lo que se conoce como minar) y ser recompensado por él, generalmente con una criptomoneda nativa de la red. Aunque en teoría pueda parecer muy descentralizado, en la práctica, en la red más grande con prueba de trabajo, que es Bitcoin, un pequeño grupo de cuatro grupos mineros genera el 58.7% de los bloques, y un grupo un poco más grande de trece grupos mineros genera 97.6 % de los bloques[58]. Además, la cantidad de energía consumida por los mineros en Bitcoin es mayor que el consumo de energía en países como Suiza, Grecia, Israel o Irlanda. Este protocolo de consenso se usa con frecuencia en redes no permisionadas[59].

Prueba de participación: la probabilidad de que un nodo sea seleccionado para la generación del siguiente bloque es proporcional a valor de los activos que ese nodo tiene en la red. El razonamiento que aplica es que, a mayor cantidad de activos en la red, mayor interés en el funcionamiento correcto

56. Entendemos que la transferencia de todos los contratos inteligentes, tokens, pruebas de certificados y cualquier otro dato registrado en blockchain es responsabilidad de la entidad que los registró. Por lo tanto, también será su responsabilidad garantizar su disponibilidad transfiriéndola a una red diferente si una blockchain muere. Sin embargo, en el caso de redes autorizadas por el público, la entidad gestora neutral de la infraestructura. se comprometerá a notificar con anticipación la terminación de la red para que las entidades tomen las medidas adecuadas.

57. Los bloques son siempre generados por los nodos validadores, que escuchan constantemente las nuevas transacciones emitidas por cualquier nodo de la red. Después de un determinado tiempo, que puede variar de segundos a minutos según la red, se selecciona uno de los nodos validadores para generar un nuevo bloque que contiene las transacciones de las que ha estado escuchando. Este nodo luego verifica las transacciones, firma el bloque y lo transmite a la red. El protocolo de consenso establece las reglas para seleccionar un nodo validador para cada nuevo bloque. Existen muchos protocolos de consenso diferentes.

58. https://www.buybitcoinworldwide.com/mining/pools/

59. https://www.forbes.com/sites/niallmccarthy/2019/07/08/bitcoin-devours-more-electricity-than-switzerland-infographic/#550986c121c0

de la misma, por lo que no intentarán manipularla introduciendo bloques corruptos. Este protocolo de consenso no necesita de grandes cantidades de energía computacional, ya que no hay una competencia que implique gastarla. Se utiliza tanto en redes permisionadas como no permisionadas.

Prueba de participación delegada: la capacidad de generar nuevos bloques se delega a un número específico de nodos, en los que el resto deposita su confianza para esa tarea. Entre esos nodos se aplica el protocolo de prueba de participación. Este protocolo de consenso se usa tanto en redes permisionadas como no permisionadas.

Estambul bizantino tolerante a fallos: los nodos validadores se turnan para generar los nuevos bloques. Se aplica un algoritmo que minimiza la posibilidad de manipulación de bloques por parte de un conjunto de nodos corruptos. Este protocolo de consenso se utiliza en algunas redes permisionadas.

Prueba de autoridad: la capacidad de generar nuevos bloques corresponde a un grupo seleccionado de nodos autorizados y los demás confían en estos nodos para realizar la tarea. Este protocolo de consenso se usa tanto en redes permisionadas como no permisionadas.

8.1.3. Gobernanza de los registros de DIDs

Como vimos en la Sección 7.1.3, existen al menos cuatro tipos de registros para los identificadores descentralizados. Los registros DID pueden estar tanto *on-chain* como *off-chain*. En ambos casos, se requieren interacciones con un registro descentralizado o red blockchain para su resolución. Por lo tanto, los modelos de gobernanza para el libro mayor (o cadena) y la generación de bloques presentados en las Secciones 8.1.1 y 8.1.2 están conectados con el modelo de gobernanza de los registros de DIDs. Cada uno de los tipos de registros de DID tiene un modelo de gobierno diferente:

Registro de identificadores globales: al implementarse en el libro mayor un único contrato inteligente monolítico para actuar como un registro global, la gobernanza del contrato inteligente es la gobernanza del registro DID. Hay varias opciones: ser administrado por una entidad centralizada, por un número limitado de cuentas o por un DAO.

Registro de anclajes: aplica lo mismo que para el registro de identificadores globales.

Traen su propia dirección de blockchain: en este caso no existe un registro DID *on-chain*,. La gestión y el almacenamiento de los DID se realiza *off-chain* por el sujeto y/o el titular, y la resolución de un DID se realiza iterando sus registros (transacciones) contra la red.

Registro de credenciales que actúa como identificador: cada sujeto implementa un contrato inteligente dedicado a registrar el DID. El sujeto tiene el control completo del contrato inteligente.

8.1.4. Gobernanza de las listas de confianza (TLs)

La determinación de qué entidades serán responsables de mantener las listas de confianza (TLs por su nombre en inglés) corresponde al marco de confianza. En consonancia con el Bloque 5, podemos clasificar la gobernanza de las listas de confianza en dos tipos, dependiendo de si el gobierno está desempeñando el papel principal en el marco de confianza o no.

Gobierno involucrado: un gobierno es la CA raíz o designa una lista de CA raíz. El gobierno también establece las reglas sobre quién y cómo se pueden emitir certificados cualificados.

Gobierno no involucrado: el gobierno no es la CA raíz y, a través de acuerdos privados, surge un marco de confianza para que diferentes entidades decidan confiar en otras entidades como CA raíz.

8.1.5. Gobernanza de las claves y credenciales

En el modelo de identidad auto-soberana, las billeteras digitales son los repositorios para almacenar,

administrar y presentar credenciales. Idealmente, los sujetos tienen el control total de las billeteras, ya que dichas billeteras deberían ser un hardware en su poder o un software instalado en uno de sus dispositivos personales. Por lo tanto, el sujeto de una identidad digital controla su identidad, y decide con quién la comparte o a quién la delega. Esto es precisamente lo que le da nombre a este modelo de identidad digital auto-soberana. Soberanía, en este contexto, significa que el usuario tiene el control de sus autenticadores, credenciales y datos. La gobernanza de las claves y credenciales incluye al menos:

- Quién puede tener acceso a las claves y credenciales de un sujeto.
- Quién puede presentar una credencial a otros y en qué condiciones.
- Dónde están las copias de seguridad.
- Quién puede facilitar la recuperación de la clave a un sujeto.
- Quién es responsable de una pérdida o robo de claves y credenciales.

8.2. Autoridades de certificación (CAs), listas de confianza (TLs), y niveles de garantía de la identificación electrónica (LOAs)

En un modelo de identidad digital, las autoridades de certificación (CAs) son aquellas entidades que emiten credenciales de identidad reconocidas por terceros con un cierto nivel de garantía. Como ya vimos en el Bloque 5, existen dos tipos de marcos de confianza dependiendo de si el gobierno juega un papel principal o no. En las soluciones en las que el gobierno se implica, éste desempeña el papel de la CA raíz o designa una entidad para ello. En cambio, en las soluciones en las que el gobierno no se involucra -que pueden proliferar mucho más rápido en el modelo de IAS a corto plazo-, unas entidades pueden desarrollar confianza en otras que actúen CAs a través de acuerdos privados.

Como ya explicamos en la Sección 7.6, existen al menos dos listas de confianza esenciales. La primera lista de confianza es la de CAs designadas por una autoridad confiable. La segunda lista de confianza es la lista de revocación de certificados que cada CAs ha emitido a otras entidades y su estado. De este modo, es posible crear raíces de confianza para verificar si un certificado digital emitido por una entidad que desconocemos o en la que no confiamos está certificado por una entidad en la que sí confiamos.

Los marcos de confianza también permiten definir los niveles de garantía de los diferentes certificados, dependiendo de quién y cómo se emitieron. Uno de los marcos de referencia para los niveles de aseguramiento de la identidad digital proviene de la Organización Internacional de Normalización (ISO, 2013) como puede verse a continuación:

En Europa, una de las principales referencias para los Niveles de Aseguramiento es STORK[60] (*Secure Identity Across Borders Linked*), un proyecto dentro del Programa de Apoyo a la Política de TICs bajo el Programa Marco de Innovación y Competitividad (CIP). Los niveles de garantía de STORK se definen en el marco de garantía de calidad de autenticación (QAA). La imagen 19 muestra el nivel de garantía requerido dependiendo de la probabilidad de los riesgos y el impacto de los daños.

A corto plazo prevemos una combinación de listas de confianza tradicionales *off-chain*, certificados X.509 y niveles de garantía en la identificación con nuevas redes blockchain, identificadores descentralizados y credenciales digitales verificables. A medio plazo, prevemos una migración de listas de confianza centralizadas hacia contratos inteligentes descentralizados desplegados en redes públicas de blockchain, un reemplazo de X.509 por credenciales digitales verificables y una adaptación de los niveles de seguridad teniendo en cuenta las ligeras variaciones introducidas por estos nuevos elementos.

60. https://ec.europa.eu/digital-single-market/en/content/stork-take-your-e-identity-you-everywhere-eu

Imagen 18. Niveles de aseguramiento ISO/IEC DIS 29115.

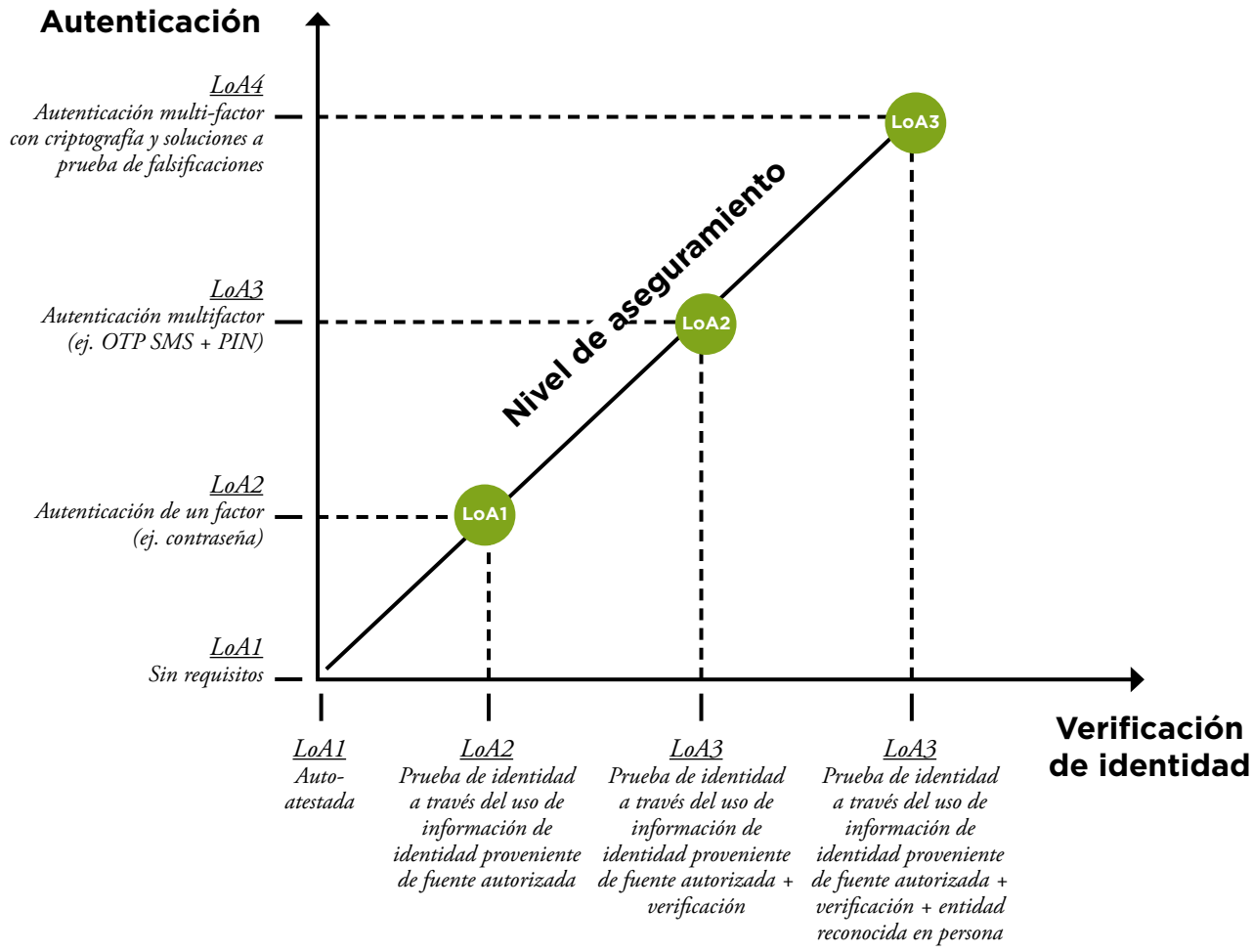


Imagen 19. Impacto de daños definido por STORK (Alamillo, 2020).

		Impact of damages				
	Likelihood	Very High	High	Medium	Low	Negligible
Risk	Almost certain	(1)	(1)	Level 4	Level 3	Level 3
	Likely	(1)	Level 4	Level 3	Level 3	Level 2
	Moderate	Level 4	Level 3	Level 3	Level 2	Level 2
	Unlikely	Level 3	Level 3	Level 2	Level 2	Level 1
	Rare	Level 3	Level 2	Level 2	Level 1	Level 1

(1): Not applicable to remote authentication over open networks

8.3. Iniciativas de referencia

Existen algunas iniciativas relevantes destinadas a crear marcos de confianza para el funcionamiento de la identidad digital que sean aplicables a la identidad soberana. Tres de los más destacados son Open Identity Exchange (OIX), eIDAS y Sovrin.

8.3.1. Open Identity Exchange (OIX)

OIX es una organización no tecnológica y sin ánimo de lucro que colabora con el sector y cuyo objetivo es el de acelerar la adopción de servicios de identidad digital basados en estándares abiertos. OIX es una referencia internacional en materia de marcos de confianza para la identidad digital. Según OIX (OIX, 2017), para que un marco de confianza se convierta en un conjunto sistemático de reglas que permita la confianza entre los participantes, debe tener:

- **Aplicabilidad:** ser legalmente vinculante, generalmente mediante contratos entre partes interesadas, pero también a través de normativa.
- **Autoría y control:** los autores del contenido y el órgano de gobierno.
- **Contenido:** roles, funciones y asuntos técnicos, operativos y legales.
- **Forma:** generalmente, un conjunto de documentos.
- **Objetivo:** el sistema que gobierna.
- **Propósito:** la gobernanza de ese sistema.

Además, OIX destaca que el objetivo de un marco de confianza no es otro que establecer:

- **Confiabilidad:** al abordar y gestionar riesgos, derechos legales, responsabilidades y deberes; eliminando incertidumbres; y facilitando la accesibilidad y la comprensión de los marcos de confianza para todos los participantes.
- **Funcionalidad:** garantizando el funcionamiento adecuado y el cumplimiento de cualquier ley aplicable.

OIX identifica cinco funciones participantes en las que generalmente se enfoca un marco de confianza y que están totalmente alineadas con los requisitos técnicos presentados en este documento. Dichas funciones son: emisión de identidad, verificación

Tabla 14. Comparación entre las funciones de participación de OIX y los componentes técnicos de LACChain ID.

OIX	LACChain ID
Emisión de identidad	Identificadores descentralizados (Sección 7.1) Credenciales verificables (Sección 7.2)
Verificación de identidad	Presentaciones verificables (Sección 7.3) e Identificación (Sección 7.4.1)
Gestión de autenticación	Autenticación (Sección 7.4.2)
Gestión de autorización	Autorización (Sección 7.4.3) Repositorios digitales y billeteras (Sección 7.5)
Gestión de atributos, declaraciones o aserciones	Identificadores descentralizados (Sección 7.1) Presentaciones verificables (Sección 7.3) Repositorios digitales y billeteras (Sección 7.5)

Tabla 15. Los cinco tipos de marcos de confianza de acuerdo con los cinco tipos de entidades diseñando y gobernando esos marcos, de acuerdo con OIX (OIX, 2017).

Tipo	Definición	Ejemplo
Entidad de gobierno independiente	Una entidad designada para desarrollar, mantener y hacer cumplir el marco de confianza. Útil para la solución de identidad a gran escala con varios emisores de identidad y proveedores de servicios	Sistema de identidad SAFE-BioPharma gestionado por la Asociación SAFE-BioPharma[61]
Consorcio de entidades participantes	Un grupo de algunas o todas las entidades participantes. Útil para pequeñas soluciones de identidad	Foro CA/Navegador[62]
Entidad de un solo miembro	Una entidad central es responsable del marco de confianza. Es común cuando hay un único emisor de identidad o proveedor de servicios, que también se convierte en la entidad central	Emisor de identidad: Google, Facebook. Proveedor de servicios: gobiernos (Login.gov del gobierno de los EE. UU., Programa de verificación GOV. UK del gobierno del Reino Unido).
Normas no gubernamentales u organización de certificación.	Una entidad independiente establecida para desarrollar y actualizar el marco de confianza. También puede certificar emisores de identidad.	Iniciativa Kantara[63] Perfiles de aprobación de tScheme emitidos por tCheme[64]
Acuerdo mutuo entre los participantes.	Acuerdos mutuos entre entidades en soluciones de identidad a menor escala. Por lo general, a través de ARM.	Proyecto Cadena entre las Aduanas de Chile, Colombia, Costa Rica, México y Perú.

de identidad, gestión de autenticación, gestión de autorización y gestión de atributos, declaraciones o aserciones. Estas funciones se han explicado con detalle en el Bloque 7 de este documento y se comparan ahora en la Tabla 21.

OIX distingue cinco tipos de marcos de confianza de acuerdo con los tipos de entidades que escriben y controlan el marco de confianza que se presentan en la Tabla 22.

Esta clasificación es independiente y compatible con las capas de gobernanza propuestas en la Sección 8.1.

8.3.2. El marco europeo de confianza para la identidad digital: Reglamento eIDAS

Para que los gobiernos sigan siendo la pieza central de la identidad digital en la próxima era de IAS, deben:

61. https://www.safe-biopharma.org
62. CA/Browser Forum, https://cabforum.org/. Este marco de confianza rige la emisión de certificados de servidor EV-SSL.
63. Kantara Initiative, https://kantarainitiative.org
64. tScheme, www.tscheme.org

- Definir órganos de gobierno a nivel nacional.
- Certificar y mantener listas de confianza.
- Establecer formas estándar y seguras de comunicar información, como autoridades de certificación, emisores de identidad y listas de revocación de certificados.
- Requerir la aceptación de credenciales entre diferentes partes cuando las credenciales se hayan emitido cumpliendo los requisitos de garantía.

Un claro ejemplo de esto es el Reglamento eIDAS (EU-eIDAS, 2014). Esta regulación europea, vista en la Sección 6.1.2, no solo proporciona una base regional para la estandarización de los servicios electrónicos y el reconocimiento entre todos los Estados miembros europeos, sino que también cumple los cuatro requisitos anteriores (o al menos lo pretende). Como se indica en su Artículo 17.1, "los Estados Miembros designarán un organismo de supervisión establecido en su territorio o, previo acuerdo mutuo con otro Estado Miembro, un organismo de supervisión establecido en otro Estado Miembro. Dicho organismo será responsable de las funciones de supervisión en el Estado Miembro que efectúa la designación". Además, cada Estado miembro opera un nodo eIDAS que es un software estandarizado para comunicarse con los demás. Por último, como se establece en su Artículo 6, "cuando sea necesaria una identificación electrónica utilizando un medio de identificación electrónica y una autenticación en virtud de la normativa o la práctica administrativa nacionales para acceder a un servicio prestado en línea por un organismo del sector público en un Estado Miembro, se reconocerá en dicho Estado Miembro, a efectos de la autenticación transfronteriza en dicho servicio en línea, el medio de identificación electrónica expedido en otro Estado Miembro", siempre que se cumplan unas condiciones mínimas. De lo anterior se puede inferir que "el efecto legal del reconocimiento transfronterizo de la identificación electrónica está garantizado solo en las relaciones entre individuos y organismos del sector público" (Alamillo, 2020), excluyendo al privado.

La introducción de nuevos elementos tecnológicos también proporciona nuevas herramientas para el intercambio de información entre los Estados miembros. En este sentido, hay al menos dos elementos que podrían ser mejorarse en esquemas de IAS, que están relacionados con el uso de redes blockchain.

- **Comunicación:** en el eIDAS, los Estados miembros de la UE son responsables del desarrollo de marcos nacionales. La comunicación entre nodos se realiza actualmente a través de nodos eIDAS (no nodos de blockchain sino software centralizado). SEC demosntró en octubre de 2019 que estos nodos son vulnerables (SEC, octubre 2019). Los libros mayores descentralizados se pueden usar para una comunicación más segura, ya que cada país puede ejecutar un nodo blockchain conocido y cuentas blockchain conocidas que se pueden usar para comunicar información pública y privada sobre proveedores de fideicomisos y entidades certificadas. Además, ser parte del libro mayor que se aprovechará como registro para IAS hace que los procesos sean más eficientes y seguros.[65]
- **Listas de confianza:** en relación con el punto anterior, las redes blockchain pueden ser un registro ideal para listas de confianza y listas de revocación de certificados. Actualmente, las listas de confianza se mantienen en registros centralizados e independientes por países. También las haría más eficientes y seguras.

8.3.3. Sovrin

Uno de los modelos de gobernanza más relevantes y reconocidos para la identidad auto-soberana es el Marco de Gobernanza de Sovrin que "sirve como constitución de la Red Sovrin, así como base para marcos de gobierno de dominio específicos (DSGF) más especializados" (SOVRIN, 2019). La Red Sovrin es una red permisionada pública que incorpora IAS de forma genuina, lo que permite una forma descentralizada de intercambiar y verificar credenciales. Su modelo de gobernanza incluye cinco acuerdos legales:

65. https://sec-consult.com/en/blog/2019/10/vulnerability-in-eu-cross-border-authentication-software-eidas-node/

- El acuerdo sovrin-inspector: el acuerdo entre la Fundación Sovrin y los Inspectores que operan los nodos de la red de Sovrin.
- El acuerdo de autor de transacciones: el acuerdo entre la Fundación Sovrin y todos los propietarios de identidad que escriben transacciones en las redes Sovrin.
- El acuerdo de endorsante de transacciones: el acuerdo entre la Fundación Sovrin y las organizaciones que utilizan el acceso de escritura autorizado.
- El acuerdo de procesamiento de datos de inspector (DPA): El acuerdo bajo el cual los inspectores actúa como procesadores de datos desde el punto de vista regulatorio de protección de datos.
- El acuerdo de procesamiento de datos del endosante de la transacción: el DPA que se aplica a los endosantes de la transacción.

El marco de confianza de Sovrin está diseñado específicamente para sus redes de blockchain, aunque otras redes puedan replicarlo. Sovrin también ha desarrollado un marco de gobernanza compuesto por varios documentos que complementan el marco de confianza[66].

66. https://sovrin.org/library/sovrin-governance-framework/

IDENTIDAD DIGITAL AUTO-SOBERANA

Conclusiones

La identidad digital auto-soberana pone sobre la mesa una propuesta revolucionaria e innovadora para ofrecer a los individuos control sobre su persona digital y tiene potencial para resolver problemas, inconvenientes y desafíos que presentan hoy los sistemas de identificación, autenticación y autorización de personas, tanto presenciales como electrónicos, relacionados con regulación y estándares, tecnología y seguridad. Para ello, este modelo combina dos tecnologías innovadoras: las billeteras digitales y los registros descentralizados de información. Las billeteras digitales, repositorios privados bajo el control de los individuos como por ejemplo un aplicativo móvil, permitirán a las personas manejar todos sus activos digitales con completa autonomía y privacidad. Podremos tener acceso rápido y seguro a versiones digitales de nuestros documentos de identidad, de nuestros diplomas universitarios, de nuestros títulos de propiedad, etc. Podremos también manejar diferentes divisas digitales tokenizadas como dólares, euros, libras, pesos, yuanes, o incluso criptomonedas. Los registros descentralizados de información, redes en las que cada participante tiene una copia sincronizada de la misma como por ejemplo las blockchain, permitirán almacenar las pruebas criptográficas de la existencia y la propiedad de credenciales y activos digitales, aumentando la confianza, la interoperabilidad, la seguridad y la eficiencia, y respetando celosamente la privacidad de los datos de los individuos.

Esto permitirá y también requerirá evolución y adaptación por parte de gobiernos y entidades financieras para emitir esos activos en un formato digital compatible con los esquemas de identidad digital auto-soberana. Este esfuerzo ya se está llevando acabo hoy en día. En cuanto a la adopción de certificados o credenciales digitales verificables, destaca la Unión Europea con iniciativas como el eIDAS Bridge y el EBSI ESSIF para el desarrollo de marcos tecnológicos y legales de confianza de identidad digital auto-soberana entre los Países Miembros, que ya está comenzando a testear la emisión de documentos de identidad, licencias de conducir, o títulos académicos digitales cuyas pruebas criptográficas se registran en una red blockchain. En cuanto a las divisas digitales, son ya varios los bancos centrales que desde 2016 han estado piloteando la emisión de divisas digitales utilizando tecnología blockchain en proyectos como Jasper (Canadá), Ubin (Singapur), Khokha (Sudáfrica), RTGS RP (Inglaterra), Stella (Japón y Europa), LBChain (Lituania), an initiative by the Central Bank of Brazil (Brazil), Inthanon (Tailandia) o E-Krona (Suecia), entre otros.

Algunos de los beneficios de la identidad digital auto-soberana son la facilidad para tener soluciones interoperables, el control real sobre sus activos digitales por parte de los titulares de los mismos, la posibilidad de que los individuos tengan un mayor control sobre el consentimiento, la portabilidad de los datos gracias a las billeteras digitales, la protección de datos por diseño y por defecto, la posibilidad de tener a la vez confianza y seudónimo en la identificación y autenticación electrónica, la facilidad para registrar actividades de procesamiento, el derecho al olvido, la escalabilidad, la seguridad, o la utilidad, entre otros. Adicionalmente, el poder contar con estos esquemas de identidad habilita y contribuye también a una larga lista de casos de uso con alto impacto tanto económico como social, como por ejemplo acceso a una primera identidad, la recuperación de información tras catástrofes naturales, la emisión de diplomas digitales verificables, la inclusión financiera de individuos no bancarizados, la garantía de documentación confiable para de migrantes y refugiados, la mejora en el respeto de privacidad en el tratamiento de información electrónica, la reducción de costes y tiempos en envíos de remesas, la reducción de hackeos de datos médicos, la facilitación de ofrecimiento de servicios públicos digitales, transferencias condicionadas más eficientes y trazables o notarización de violencia doméstica con garantías de firma y sello electrónicos, entre otros.

La situación actual es aún de inmadurez, aunque también ilusionante y prometedora. Tal y como hemos presentado y discutido, es necesaria la combinación de tres capas: regulación, tecnología y marcos de confianza. Los avances en estas tres capas permitirán el desarrollo de soluciones completas de identidad digital auto-soberana tanto públicas como privadas en el transcurso de los

próximos años, sentando como base protocolos y estándares nacionales, regionales, internacionales y también sectoriales. En este proceso será necesario afrontar diferentes retos como la adaptación de la infraestructura y los modelos de datos actuales, la comprensión y el entendimiento de la tecnología por parte de juristas, notarios y reguladores, la maduración de las billeteras digitales, el desarrollo de campañas de captación de usuarios, la posibilidad de tener copias de seguridad confiables, la garantía del derecho al olvido, el establecimiento de marcos de confianza, la participación activa de las entidades de gobierno, la actualización de las políticas regulatorias, la garantía completa de la privacidad y la protección de datos, la posibilidad de pruebas de conocimiento cero, la recuperación de claves, la maduración de los registros descentralizados, la garantía del derecho al seudónimo o el uso de biometría para la identificación y autorización. Si bien los gobiernos seguirán teniendo la soberanía sobre la identificación de sus ciudadanos, se prevé que también se desarrollarán marcos de identidad auto-soberana soportados por acuerdos privados entre entidades del sector privado donde entidades financieras, aseguradoras, entidades médicas o universidades, entre otras, emitan credenciales digitales a sus usuarios e intercambien información de identidad con sus contrapartes.

En cuanto a regulación, será necesario trabajar en las áreas de transacciones y firma electrónica, y en la protección de datos personales para desarrollar políticas regulatorias en aquellos países que no disponen de ellas, y para actualizarlas en los que sí. En América Latina y el Caribe, 31 de los 42 países cuentan con regulación en materia de firma electrónica, lo que supone un 74%, pero solamente 17 de 42 tienen regulación en materia de protección de datos, lo que significa un 40%. Con respecto a la capa de tecnología, hemos presentado siete elementos complementarios que consideramos esenciales: identificadores descentralizados; credenciales verificables; presentaciones verificables; billeteras digitales; identificación, autenticación y autorización; autoridades de certificación y listas de confianza y tecnología de redes descentralizadas. Cada uno de estos elementos deberá ser analizado a conciencia a la hora de desarrollar soluciones, tomando en cuenta estándares y protocolos internacionales que garanticen escalabilidad e interoperabilidad. Al respecto de los marcos de confianza, será importante definir modelos de gobernanza y modelos económicos para el mantenimiento de las redes descentralizadas y las soluciones de identidad encima de ellas, así como establecer autoridades de certificación, proveedores de identidad y niveles de garantía de la identificación electrónica y los canales de comunicación.

Tal y como se deduce de las múltiples citas y referencias a documentos de ISO, ITU, NIST o la Unión Europea, entre otros, que se han presentado en este documento, en los próximos años veremos una actividad grande y creciente en torno a la identidad digital auto-soberana, y posiblemente en unos años y sin habernos dado cuenta estemos manejando todos nuestros activos digitales en una billetera móvil y utilizando tecnología blockchain para garantizar su veracidad. Sin duda, como ocurre ante todo cambio importante, se abre también la puerta de la oportunidad para aquellos gobiernos y empresas privadas que den el primer paso.

Referencias

[Alamillo, 2019] Alamillo, N. (2019). *Identificación, firma y otras pruebas electrónicas: la regulación jurídico-administrativa de la acreditación de las transacciones electrónicas.* Cizur Menor, Navarra: Aranzadi. Obtenido de https://almena.uva.es/discovery/fulldisplay/alma991008080150205774/34BUC_UVA:VU1.

[Alamillo, 2020] Alamillo, N. (2020). *SSI eIDAS Legal Report.* European Comission. Obtenido de https://joinup.ec.europa.eu/sites/default/files/document/2020-04/SSI_eIDAS_legal_report_final_0.pdf

[CAF, 2012] Corporación Andina de Fomento. (2012). *Fundamentos de la firma digital y su estado del arte en América Latina y el Caribe.* Obtenido de http://www2.congreso.gob.pe/sicr/cendocbib/con4_uibd.nsf/503ADEE40C4F859505257D1C00708FE4/$FILE/Di-7-12_Fundamentos_Firma_Digital_y_su_Estado_Arte_en_ALC-Final.pdf

[California, 2018] California State Legislature. (2018). *Bill AB/375 - California Consumer Privacy Act*. Obtenido de https://oag.ca.gov/privacy/ccpa

[Consensys et al., 2019] Consensys et al. (2019). Obtenido de https://drive.google.com/file/d/1gQrI02QjEiYHh6ViF-HbXxPKA6HWHgfMt/view

[EU, 2018] The European Union Blockchain Observatory and Forum. (2018). *Blockchain for government and public services.* Obtenido de https://www.eublockchainforum.eu/sites/default/files/reports/eu_observatory_blockchain_in_government_services_v1_2018-12-07.pdf

[EU, 2019] European Union. (2019). *EIDAS supported self-sovereing identity*. Obtenido de https://ec.europa.eu/futurium/en/system/files/ged/eidas_supported_ssi_may_2019_0.pdf

[EU-BDID, 2019] The European Union Blockchain Observatory and Forum. (2019). *Blockchain and digital identity.* Obtenido de https://www.eublockchainforum.eu/sites/default/files/report_identity_v0.9.4.pdf

[EU-GDPR, 2016] European Union. (2016). *Regulation No 2016/679 on general data protection. Directive 95/46/EC*. Obtenido de https://gdpr-info.eu/

[EU-eIDAS, 2014] European Union. (2014). *Regulation No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC*. Obtenido de https://www.eid.as/Regulation

[ETSI, 2015] European Telecommunications Standards Institute. *Quantum safe cryptography and security (White Paper No. 8. ISBN No. 979-10-92620-03-0). (2015)*. Obtenido de https://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf

[EWF, 2018] Energy Web Foundation. (2018). *The energy web chai*n. Obtenido de https://energyweb.org/wp-content/uploads/2019/05/EWF-Paper-TheEnergyWebChain-v1-201810-FINAL-1.pdf

[FATF, 2020] Financial Action Task Force. (2020). *Guidance on Digital ID.* Obtenido de https://www.fatf-gafi.org/publications/fatfrecommendations/documents/digital-identity-guidance.html

[FOMIN-I, 2014] Fondo Multilateral de Inversiones. (2014). Las remesas a América Latina y el Caribe en 2013: aún sin alcanzar niveles de pre-crisis. Obtenido de https://www.findevgateway.org/es/paper/2014/06/las-remesas-america-latina-y-el-caribe-en-2013-aun-sin-alcanzar-niveles-de-pre-crisis

[FOMIN-II, 2014] Fondo Multilateral de Inversiones. (2014). *Situación económica y envío de remesas.* Obtenido de https://www.microfinancegateway.org/sites/default/files/mfg-es-documento-situacion-economica-y-envio-de-remesas-de-migrantes-de-america-latina-y-el-caribe-en-el-periodo-post-recesion-4-2014.pdf

[FDIC, 2017] Federal Deposite Insurace Corporation. (2017). *FDIC National survey of unbanked and underbanked households*. Obtenido de https://www.fdic.gov/householdsurvey/

[FEMA, 2019] Federal Emergency Management Agency. (2019). *National Advisory Council DRAFT Report to the FEMA Administrator November 2019*. Obtenido de https://www.fema.gov/media-library-data/1572880188002-31454e3c26dff6922fde9d34cbe19e26/November_2019_NAC_Report_Draft_v5.pdf

[ForgeRock, 2019] ForgeRock. US Consumer Data Breach Report. (2019). *Personally Identifiable Information Targeted in Breaches that Impact Billions of Records.* Obtenido de https://www.forgerock.com/resources/view/92170441/industry-brief/us-consumer-data-breach-report.pdf.

[Garner, 2000] Gartner. (2020). *Guidance for decentralized identity and verifiable claims.* Obtenido de https://www.

gartner.com/en/documents/3979940/guidance-for-decentralized-identity-and-verifiable-claim

[IDB, 2013] Brito, S., Corbacho, A., Osorio, R., & Harbitz, E. Inter-American Development Bank. (2013). *El registro de nacimientos: La llave para la inclusión social en América Latina y el Caribe*. Obtenido de https://publications.iadb.org/publications/spanish/document/El-registro-de-nacimientos-La-llave-para-la-inclusi%C3%B3n-social-en-Am%C3%A9rica-Latina-y-el-Caribe.pdf

[IDB, 2015] Inter-American Development Bank. (2015). *Inclusión financiera en América Latina y el Caribe.* Obtenido de https://publications.iadb.org/es/publicacion/13894/inclusion-financiera-en-america-latina-y-el-caribe-coyuntura-actual-y-desafios

[IDB, 2016] Inter-American Development Bank. (2016). *Programas de transferencias monetarias condicionadas e incusión financiera.* Obtenido de https://publications.iadb.org/publications/spanish/document/Programas-de-transferencias-monetarias-condicionadas-e-inclusi%C3%B3n-financiera.pdf

[IDB, 2017] Inter-American Development Bank. (2017). *Así funcionan las transferencias condicionadas*. Obtenido de https://publications.iadb.org/es/publicacion/17226/asi-funcionan-las-transferencias-condicionadas

[IDB-REM, 2017] Inter-American Development Bank. (2017). *Un mayor dinamismo en 2017 del envío de remesas.* Obtenido de https://publications.iadb.org/publications/spanish/document/Un-mayor-dinamismo-en-2017-del-ingreso-por-remesas-de-Am%C3%A9rica-Latina-y-el-Caribe.pdf

[IETF, 2012] Internet Engineering Task Force. (2012). *The OAuth 2.0 Authorization Framework.* Obtenido de https://tools.ietf.org/html/rfc6749

[ISO, 2013] International Organization for Standardization. (2018). *Information technology - Security techniques - Entity authentication assurance framework (ISO/IEC 29115:2013).* Obtenido de https://www.iso.org/standard/45138.html

[ISO, 2018] International Organization for Standardization. (2018). *Governance of blockchain and distributed ledger technology systems (ISO/TC 307/SG/ 6)*. Obtenido de https://www.iso.org/committee/6266604.html

[ISO, 2019] International Organization for Standardization. (2019). *IT Security and Privacy — A framework for identity management - Part 1: Terminology and concepts*. (ISO/IEC Standard No. 24760-1) Obtenido de https://www.iso.org/standard/77582.html

[ISO, 2020] International Organization for Standardization. (2020). *Guidelines for governance (ISO TS WD5 23635)*. Obtenido de https://www.iso.org/standard/76480.html

[ITU, 2018] International Telecommunications Union. (2018). *Digital identity roadmap guide.* Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO). ISBN: 978-92-61-27821

[ITU, 2019] International Telecommunications Union. (2019). *Distributed ledger technology reference architecture.* Obtenido de https://www.itu.int/en/ITU-T/focusgroups/dlt/Pages/default.aspx

[Josan & Pope, 2005] Josang, A., & Pope, S. (2005). *User Centric Identity Management.* Obtenido de http://folk.uio.no/josang/papers/JP2005-AusCERT.pdf

[Lum et al., 1988] Lum, M., Feldman, P., & Micali, S. (1988). Non-Interactive Zero-Knowledge and Its Applications. *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*. pp. 103–112. doi:10.1145/62212.62222. ISBN 978-0897912648.

[McKenzie, 2018] McKenzie. (2018). *Global Privacy and Information Management Handbook*. Obtenido de https://tmt.bakermckenzie.com/-/media/minisites/tmt/files/global_privacy_handbook-_2018.pdf?la=en

[NIST-DSS, 2019] National Institute of Standards and Technology. (2019). *Digital Signature Standard (DSS)*. (Natl. Inst. Stand. Technol. Spec. Publ. 186-5 (Draft)). Retrieve from https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-5-draft.pdf

[NIST-ECDM, 2019] National Institute of Standards and Technology. (2019). *Recommendations for Discrete Logarithm-Based Cryptography: Elliptic Curve Domain Parameters*. (Natl. Inst. Stand. Technol. Spec. Publ. 800-186 (Draft)). Retrieve from https://csrc.nist.gov/publications/detail/sp/800-186/draft

[NIST-IDG, 2017] National Institute of Standards and Technology. (2017). *Digital identity guidelines*. (Natl. Inst. Stand. Technol. Spec. Publ. 800-63-3). DOI: https://doi.org/10.6028/NIST.SP.800-63-3

[NIST-IDGa, 2017] National Institute of Standards and Technology. (2017). *Digital identity guidelines.* (Natl. Inst. Stand. Technol. Spec. Publ. 800-63-3a). DOI: https://doi.org/10.6028/NIST.SP.800-63-3

[NIST-Q, 2016] National Institute of Standards and Technology. (2016). *Report on post-quantum cryptography*

(Internal Report NISTIR 8105). Obtenido de https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf

[NIST-TA, 2020] National Institute for Standards in Technology. (2020). *A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems*. Obtenido de https://csrc.nist.gov/publications/detail/white-paper/2020/01/14/a-taxonomic-approach-to-understanding-emerging-blockchain-idms/final

[NSA, 2016] National Security Agency. (2016). *CNSA suite and quantum computing FAQ (MFQ-U-OO-815099-15).* Obtenido de https://apps.nsa.gov/iaarchive/library/ia-guidance/ia-solutions-for-classified/algorithm-guidance/cnsa-suite-and-quantum-computing-faq.cfm

[OASIS, 2008] OASIS. (2008). *Security Assertion Markup Language (SAML).* Obtenido de http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html

[OIX, 2014] Open Identity Exchange. (2014). *The Vocabulary of Identity Systems Liability.* Obtenido de https://openidentityexchange.org/blog/2014/06/08/the-vocabulary-of-identity-systems-liability/

[OIX, 2017] Open Identity Exchange. (2017). *Trust frameworks for identity systems.* Obtenido de https://openidentityexchange.org/blog/2017/06/22/trust-frameworks-for-identity-systems/

[OIX-TF, 2010] Open Identity Exchange. (2010). *The open identity trust framework model*. Obtenido de https://www.openidentityexchange.org/wp-content/uploads/2017/03/open_identity_trust_framework_model_2010.pdf

[OIX-TOOLS, 2019] Open Identity Exchange. (2019). *Aligning the Rules and Tools of Digital Identity: Solving Today's Burning Business Problems*. Obtenido de https://openidentityexchange.org/blog/2019/11/12/aligning-the-rules-and-tools-of-digital-identity-solving-todays-burning-business-problems/

[OIX-UK, 2019] Open Identity Exchange. (2019). *Establishing a Trusted Interoperable Digital Identity Ecosystem in the UK*. Obtenido de https://openidentityexchange.org/blog/2019/10/04/establishing-a-trusted-interoperable-digital-identity-ecosystem-in-the-uk/

[SDG, 2016] Inter-Agency and Expert Group on SDG Indicators. (2016). *Final list of proposed Sustainable Development Goal indicators.* Obtenido de https://sustainabledevelopment.un.org/content/documents/11803Official-List-of-Proposed-SDG-Indicators.pdf

[SOVRIN, 2019] Sovrin Governance Framework. (2019). *Sovrin Trust Assurance Framework*. Obtenido de https://sovrin.org/wp-content/uploads/Sovrin-Trust-Assurance-Framework-V1.pdf

[UN, 1498] United Nations. (1948). *Universal declaration of human rights.* Obtenido de https://www.un.org/en/universal-declaration-human-rights/.

[W3C-DID, 2019] World Wide Web Consortium. (2019). *Verifiable Credentials Data Model 1.0.* Obtenido de https://www.w3.org/TR/vc-data-model/

[W3C-JSONLD, 2019] World Wide Web Consortium. (2019). *A JSON-based serialization for linked data.* Obtenido de https://json-ld.org/spec/latest/json-ld/

[W3C-VC, 2019] World Wide Web Consortium. (2019). *Decentralized Identifiers (DIDs).* Obtenido de https://www.w3.org/TR/did-core/

[WB-ID4D, 2018] World Bank. (2018). *ID4D Global Dataset.* Obtenido de https://id4d.worldbank.org/global-dataset

[WB-TS, 2018] World Bank. (2018). *Technical standards for digital identification systems*. Obtenido de http://documents.worldbank.org/curated/en/707151536126464867/pdf/129743-WP-PUBLIC-ID4D-Catalog-of-Technical-Standards.pdf

[Wu & Hang, 2014] Wu, H. & Wang, F. (2014). A Survey of Noninteractive Zero Knowledge Proof System and Its Applications. *The Scientific World Journal*, *560484*.

Regulación de firma electrónica

Antigua y Barbuda -http://legalaffairs.gov.ag/pdf/bills/Electronic_Transactions_Amendment_Act_2016.pdf

Argentina -https://www.argentina.gob.ar/firmadigital/normativa#:~:text=Ley%20N%C2%B0%2025.506%20de,Digital%20de%20la%20Rep%C3%BAblica%20Argentina.

Bahamas - http://laws.bahamas.gov.bs/cms/images/LEGISLATION/PRINCIPAL/2003/2003-0004/ElectronicCommunicationsandTransactionsAct_1.pdf

Barbados -https://www.barbadosparliament.com/uploads/bill_resolution/abebbcf80e26815632d4b130d9906644.pdf

Belice - https://www.global-regulation.com/law/belize/3268571/electronics-transaction-act.html

Bolivia - https://www.att.gob.bo/content/bolivia-ingresa-la-era-de-la-firma-digital#:~:text=BOLIVIA%20INGRESA%20A%20LA%20ERA%20DE%20LA%20FIRMA%20DIGITAL%20La,Telecomunicaciones%20y%20Transportes%2DATT%2C%20se

Brasil - http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70749/norma.htm

Chile - http://www.oas.org/juridico/pdfs/mesicic4_chl_ley19799.pdf

Colombia - https://www.mintic.gov.co/portal/604/articles-3679_documento.pdf

Costa Rica - http://www.firmadigital.go.cr/Documentos/ley%208454.pdf

Ecuador - https://www.oas.org/juridico/spanish/cyb_ecu_ley_comelectronico.pdf, https://www.firmadigital.gob.ec/wp-content/uploads/2018/01/reglamento_ley_de_comercio_electronico.pdf

El Salvador - https://www.asamblea.gob.sv/decretos/details/166

Granada - https://www.yumpu.com/en/document/view/26268942/electronic-transactions-act-2008-government-of-grenada

Guatemala - https://www.minfin.gob.gt/images/archivos/leyes/tesoreria/Decretos/DECRETO%2047-2008.pdf

Haití - https://www.haitilibre.com/en/news-19982-haiti-politics-the-law-on-electronic-signature-finally-voted-in-the-senate.html

Islas Caimán - https://www.ofreg.ky/upimages/commonfiles/1506773099ElectronicsTransactionLaw2003Revision.pdf

Jamaica - https://moj.gov.jm/sites/default/files/laws/Electronic%20Transactions%20pgs.%201-34.pdf

México - https://eservicios.impi.gob.mx/seimpi/ayudaSEIMPI/LFEA.pdf

Nicaragua - http://legislacion.asamblea.gob.ni/Normaweb.nsf/9e314815a08d4a6206257265005d21f9/1ceea41dc1bdc53d06257951005bbc04?OpenDocument

Panamá - https://www.firmaelectronica.gob.pa/documentos/Ley_82-Que_modifica_la_Ley_51_de_2008.pdf

Paraguay - https://www.bacn.gov.py/archivos/3550/20150709092101.pdf

Perú - https://www.minjus.gob.pe/wp-content/uploads/2014/03/Ley27269.pdf

Puerto Rico -http://www.bvirtual.ogp.pr.gov/ogp/Bvirtual/leyesreferencia/PDF/Tecnolog%C3%ADas/148-2006/148-2006.pdf

República Dominicana- https://www.wipo.int/edocs/lexdocs/laws/es/do/do030es.pdf

San Cristóbal y Nieves - https://skncustoms.com/pdfs/GoSKN-ElectronicTransactionsAct2011.pdf

Santa Lucía -https://www.investstlucia.com/files/downloads/date_201102161647/Electronic%20transactions%20ACT.pdf

Surinam -https://www.loc.gov/law/foreign-news/jurisdiction/suriname/

Trinidad y Tobago - http://www.ttparliament.org/legislations/a2011-06.pdf

Uruguay - https://legislativo.parlamento.gub.uy/temporales/leytemp1979099.htm

Venezuela - http://www.conatel.gob.ve/wp-content/uploads/2014/10/PDF-Ley-sobre-Mensajes-de-Datos-y-Firmas-Electr%C3%B3nicas.pdf

Normativa de protección de datos

Antigua y Barbuda - http://www.ilo.org/dyn/natlex/docs/ELECTRONIC/102704/124275/F-167635569/ATG102704.pdf

Argentina - http://www.jus.gob.ar/media/3201023/personal_data_protection_act25326.pdf

Aruba - https://www.doingbusinessdutchcaribbean.com/aruba/intellectual-property/data-protection-privacy/#:~:text=There%20are%20no%20specific%20laws,data%20in%20general%20in%20Aruba.&text=Any%20such%20personal%20information%20may,concerned%20collection%20of%20personal%20data.

Bahamas - http://laws.bahamas.gov.bs/cms/images/LEGISLATION/PRINCIPAL/2003/2003-0003/DataProtectionPrivacyofPersonalInformationAct_1.pdf

Barbados - https://www.barbadosparliament.com/bills/details/396

Belice - https://www.right2info.org/laws/BelizeFreedomofInformationAct20002.pdf

Brasil - https://www.lgpdbrasil.com.br/wp-content/uploads/2019/06/LGPD-english-version.pdf

Chile - https://dfsobservatory.com/sites/default/files/LEY-20575_17-FEB-2012.pdf

Colombia - http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

Costa Rica - http://www.oas.org/es/sla/ddi/docs/CR4%20Ley%20de%20Protecci%C3%B3n%20de%20la%20Persona%20frente%20al%20Tratamiento%20de%20sus%20Datos%20Personales.pdf

República Dominicana - http://dominicanlaw.com/dominican-data-protection-law/

Ecuador - https://corporate.dataguidance.com/ecuador-bill-addresses-lack-of-data-protection-culture/#:~:text=The%20National%20Assembly%20announced%2C%20on,('the%20Bill').&text=Specifically%2C%20the%20Bill%20requires%20organisations,before%20collecting%20and%20using%20data.

Jamaica -https://www.japarliament.gov.jm/attachments/article/339/The%20Data%20Protection%20Act,%202017----.pdf

México - http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

Nicaragua - http://legislacion.asamblea.gob.ni/normaweb.nsf/b92aaea87dac762406257265005d21f7/7bf684022fc4a2b406257ab70059d10f?OpenDocument

Panamá - https://www.gacetaoficial.gob.pa/pdfTemp/28743_A/GacetaNo_28743a_20190329.pdf

Paraguay - https://www.pj.gov.py/ebook/monografias/nacional/informatico/Adriana-Marecos-Proteccion-de-datos-Py.pdf

Perú - http://www.leyes.congreso.gob.pe/Documentos/Leyes/29733.pdf

Uruguay - https://www.impo.com.uy/bases/leyes/18331-2008


BID

BID
LAB

LACCHAIN

BID BID | LAB LACCHAIN