BANCO DE DESARROLLO DE AMÉRICA LATINA Y EL CARIBE

Dirección de Transformación Digital

Identidad Digital Autosoberana (IDA)

Hacia la construcción de una infraestructura pública digital en América Latina y Caribe

Temas asociados: Autenticación, Criptografía, Datos Abiertos, Blockchain, Gobierno Digital, Gobernanza de Datos, Identidad Descentralizada, Infraestructura de Datos, Infraestructuras Digitales, Inteligencia Artificial, Interoperabilidad, Portabilidad.

Tiempo estimado de lectura: 22 minutos

Nota de CAF -Banco de Desarrollo de América Latina & el Caribe.

Elaboración de la nota:
Soledad Cánepa, Tamara Bagdassarian y Sabrina Díaz Rato

Coordinador & Editor de la publicación: Camilo Cetina – Ejecutivo Principal (Dirección de Transformación Digital)

Revisión y comentarios: Mauricio Agudelo, Eduardo Chomali, Camilo Cetina, Diego Gutiérrez Zaldivar, Alejandro Narancio, Romina Salveraglio y Gustavo Quevedo

Director de Transformación Digital (E) Mauricio Agudelo

Tabla de contenido

Prólogo

En un mundo cada vez más conectado, donde la digitalización permea todos los aspectos de nuestra vida cotidiana, surge un concepto revolucionario que redefine la manera en que interactuamos en línea: la identidad digital descentralizada o identidad digital autosoberana (IDA).

Desde CAF – Banco de Desarrollo de América Latina & el Caribe estamos apoyando a los gobiernos de la región en la adopción de nuevas tecnologías digitales para mejorar la entrega de bienes y servicios públicos, bajo principios de innovación, transparencia, eficiencia. En la construcción de este portafolio, la IDA surge como una innovación tecnológica que promete empoderar a los individuos al proporcionarles el control total sobre su identidad en línea, mientras garantiza la seguridad, la privacidad y la interoperabilidad.

Desde las primeras incursiones en la web, hemos sido testigos de la creciente centralización de nuestros datos personales, lo que ha generado preocupaciones sobre la privacidad y la seguridad de nuestros perfiles digitales. La IDA surge como respuesta a esta problemática, ofreciendo un enfoque radicalmente diferente: una identidad que es propiedad y está bajo el control exclusivo de su titular, en lugar de estar alojada en servidores centralizados susceptibles a violaciones de seguridad y abusos de privacidad.

En este contexto, desde CAF ponemos al servicio de los diferentes actores del ecosistema de la innovación digital esta publicación que se erige como una guía esencial para comprender qué es la identidad digital descentralizada y cómo se implementa en la práctica. Desde los fundamentos teóricos hasta los casos de uso concretos, exploramos el potencial transformador de la IDA.

A través de entrevistas con expertos líderes en el campo, estudios de caso y análisis detallados, CAF contribuye con insumos acerca de los desafíos y oportunidades que presenta la IDA en la región. Asimismo, aspira a fomentar un diálogo informado y constructivo sobre cómo podemos aprovechar esta tecnología para construir un futuro digital más inclusivo, seguro y resiliente.

Es nuestro sincero deseo que esta publicación inspire a lectores de todas las disciplinas a contribuir al campo de la identidad digital autosoberana y gobierno digital en el que CAF brinda asistencia técnica para podamos forjar un camino hacia un ecosistema digital, más humano y equitativo.

¡Bienvenidos a la era de la identidad digital descentralizada!

CHRISTIAN ASINELLI
Vicepresidente Corporativo de Programación Estratégica de CAF-Banco de Desarrollo de América Latina & el Caribe

Resumen

Este documento aborda aspectos necesarios para el desarrollo de Infraestructura Pública Digital para construir sistemas de Identidad Digital Autosoberana (IDA) en América Latina y Caribe. Se exploran algunas experiencias piloto que entidades gubernamentales desarrollaron en un esfuerzo por modernizar y adoptar nuevos paradigmas de identidad digital. La IDA es una alternativa que le permite a los usuarios tener control sobre los datos que alimentan su propia identidad en línea y llevar consigo su identidad de una plataforma o servicio a otro, sin depender de intermediarios o proveedores de servicios de identidad centralizados. Esta descentralización trae mejoras en la privacidad, la seguridad, la eficiencia y la transparencia frente la prestación de servicios gubernamentales por medios digitales. Este documento busca ser un recurso para líderes de política pública e interesados en tecnologías descentralizadas, Blockchain y Web 3 en general, para que cuenten con una guía práctica de implementación en sus casos de uso de la identidad digital autosoberana centrada en el usuario.

Introducción

Los sistemas de confianza o trust frameworks basados en Identidad Digital Autosoberana (IDA), constituyen una oportunidad de mejora para el ecosistema de economía digital y de servicios de gobierno en América Latina y el Caribe. En la perspectiva de **infraestructura pública,** estos sistemas tienen el potencial de catalizar la innovación en cada territorio, empoderar a la ciudadanía y contribuir a la transformación digital en el sector público. Asimismo, estos **ecosistemas de confianza** pueden resultar muy atractivos para emprendedores y startups que buscan nuevos modelos de negocios digitales basados en tecnologías descentralizadas y web 3. De hecho, el Foro Económico Mundial sostiene que -diseñadas correctamente- las identidades digitales pueden proporcionar a los países un valor económico equivalente al 13% de su PIB, ahorrar millones de horas de trabajo gubernamental y reducir costos para las empresas. En contextos gubernamentales, la implementación de la Identidad Digital Autosoberana (IDA) comprende además a los planes locales de gobierno digital, especialmente en términos jurídicos, sociales y tecnológicos, (Weidenslaufer, C. y Roberts, R., 2022) En este documento, resultado de una colaboración técnica entre CAF y Fundación IOV, abordaremos los aspectos conceptuales y técnicos de la implementación de la IDA en gobiernos, desde una perspectiva de infraestructura pública digital que promueve las Naciones Unidas.

El documento desarrolla en la primera parte las características fundamentales que componen la IDA e igualmente explica las ventajas que su adopción tendría tanto en el sector público como en el privado. Posteriormente se brinda una guía detallada en un lenguaje asequible para iniciar una estrategia de implementación en entornos gubernamentales, las consideraciones básicas que deben tenerse en cuenta en cada etapa de la planificación, así como la convivencia e interacción de los modelos de datos (centralizados y descentralizados).

El capítulo 6 aborda y describe dos modelos de implementación según los contextos organizaciones, sus recursos y sus necesidades para la emisión de credenciales de identidad según experiencias piloto y proyectos en desarrollo. Finalmente, se presentan las conclusiones y recomendaciones de políticas para tomadores de decisión (policy makers), comunidades de desarrollo y equipos técnicos de gobierno, especialmente funcionarios de áreas de innovación y transformación digital.

1.¿Qué es la Identidad Digital Autosoberana (IDA)?

La identidad digital, en los modelos descentralizados, suele presentarse como "Identidad Digital Autosoberana", "Identidad Digital Autogestionada" o "Identidad Digital Descentralizada"[1]. La **autosoberanía** es la cualidad que expresa el derecho de las personas a decidir sobre sus credenciales de identidad y la **autogestión,** esto es, la capacidad activa del usuario para gestionar su identidad no solo al compartirla, sino también decidir cómo configurarla. El término **descentralización** varía según contextos y modelos de aplicación, pero en la línea conceptual del modelo que abordamos en este informe, la cualidad descentralizada hace referencia directa a los **identificadores descentralizados o DIDs[2],** por sus siglas en inglés. Los DIDs, que alcanzaron en 2022 el rango de "recomendación" por el Consorcio World Wide Web (W3C), son la pieza clave de la Identidad Digital Autosoberana.

La identidad digital es un conjunto de datos e información en línea de un individuo, organización o cosa. Incluye datos personales, nombres, usuarios y contraseñas y trazas de actividades en línea para identificarse e interactuar en la red. En el modelo tradicional centralizado, las identidades pertenecen a organizaciones proveedoras de servicios (gobiernos, empresas) y son administradas en bases de datos privadas. Un aspecto fundamental que distingue la Identidad Digital Autosoberana de los sistemas centralizados[3] es su base en **tecnologías avanzadas de criptografía,** específicamente, en el uso de firmas digitales y la generación criptográfica de datos. Esto significa que cada pieza de información, o credencial, asociada a una identidad digital, es firmada digitalmente por el emisor (ya sea un individuo, una institución educativa, un banco, o incluso un ente gubernamental) usando una llave privada[4] única.

Esta firma garantiza que la información no solo proviene de manera auténtica del emisor, sino que también permanece inviolable: una vez que los datos están firmados, cualquier intento de alteración hará que la firma sea inválida. **Esta característica se basa en funciones matemáticas que toman un conjunto de datos y producen una salida (hash) de longitud fija, de manera que cualquier cambio en los datos originales producirá un hash completamente diferente. Esto asegura la integridad e interoperabilidad de los datos a nivel global sin importar el país o la jurisdicción.** La verificación de estas credenciales se realiza mediante el acceso a la llave pública correspondiente del emisor, permitiendo a cualquier parte interesada confirmar la autenticidad y la integridad de la información sin necesidad de interactuar directamente con el emisor.

Este proceso criptográfico asegura que los datos de identidad sean seguros y confiables, superando significativamente las limitaciones de los modelos tradicionales (centralizados) al descentralizar la gestión de identidad y empoderar a los usuarios con la gestión sobre sus propios datos, alineándose perfectamente con la visión de promover la autonomía, la privacidad y la seguridad en el entorno digital. Para entender la comparación entre ambos paradigmas basta pensar en los sistemas de identidad digital centralizados, los cuales comparten documentos completos

1 Para una profundización conceptual sobre la evolución de la identidad en línea sugerimos la lectura de este artículo del blog de Christopher Allen, copresidente del CG de Credenciales W3C que trabaja en normas para la identidad descentralizada: https://www.lifewithalacrity.com/article/the-path-to-self-soverereign-identity/

2 El DID es un identificador portable basado en asociar una URL a una entidad, entendiendo por esta cualquier cosa con existencia propia e independiente, como una persona, una organización o un dispositivo que juegue algún papel en el ecosistema. Los DIDs son identificadores que los propios usuarios crean y gestionan de forma autónoma, habitualmente con el soporte de un sistema basado en tecnologías DLT/Blockchain.

3 Con el término centralización nos referimos a las funciones administrativas, jurídicas y presupuestarias concentradas en un sólo actor social, ya sea un Estado, empresa o institución.

4 Ver Anexo II más sobre qué son las llaves criptográficas.

(como PDF, por ejemplo) con firmas digitales incrustadas, sin mecanismos eficientes para validar si el documento ha sido alterado después de su firma y antes de su entrega. Este vacío en la seguridad puede ser explotado para alterar la información contenida en el documento sin que el receptor tenga forma de verificar la autenticidad de los cambios. Por contraste, la Identidad Digital Autosoberana, mediante su enfoque en firmas digitales y verificación criptográfica, ofrece una solución robusta a este problema, garantizando que cualquier alteración del documento sea fácilmente detectable, fortaleciendo así la seguridad y la confianza en el intercambio de información digital.

Los atributos de la IDA sobresalen frente al surgimiento de la Inteligencia Artificial (IA) como herramienta dominante para el análisis y procesamiento de datos personales. Al garantizar que cada usuario mantenga el control soberano sobre su identidad digital y los datos asociados, la IDA establece un marco fundamental para la interacción ética y segura con sistemas de IA, asegurando que los individuos puedan beneficiarse de la innovación tecnológica sin comprometer su privacidad o autonomía. Este enfoque proactivo hacia la gestión de identidades en la era de la IA no solo refuerza la protección contra el uso indebido de datos personales, sino que también habilita nuevas formas de interacción digital que respetan y empoderan al usuario final.

Otras importantes ventajas que ofrece la IDA son:

Para el sector público y privado:

- Elimina la necesidad de mantener y asegurar bases de datos masivas y centralizadas, simplificando las operaciones y mejorando la seguridad.

- Reduce incentivos frente a los ciberataques y ransomware al reducir la centralización de datos, haciendo que sea menos atractivo (y significativamente más costoso) para los perpetradores realizar ataques para robar o alterar datos personales.

- Disminuye la necesidad de desarrollar aplicaciones propias para la validación y gestión de identidad de los beneficiarios de los servicios entregados, reduciendo costos y complejidades asociadas.

- Agiliza los tiempos de validación de identidad de los ciudadanos al interior de las organizaciones gubernamentales. Es decir, optimiza las dinámicas actuales por las que distintos organismos trabajando en “silos” diferentes deben pedirle al ciudadano su identificación cada una de las veces que éste se vincula con el Estado.

- Optimiza recursos y dinero en los procesos de emisión y validación de documentos, licencias y permisos a ciudadanos y empresas.

Para los ciudadanos

- Libera a las personas de la carga de destinar espacio limitado en sus dispositivos móviles a múltiples aplicaciones gubernamentales, bancarias, universitarias o sociales, evitando así el perjuicio en el rendimiento de los dispositivos móviles y eliminando la necesidad de invertir en la compra de dispositivos más potentes.

- Habilita una nueva forma de acceder a servicios digitales al utilizar las credenciales del individuo para verificar su identidad. Esto unifica el proceso de autenticación en diversas plataformas, ya sean públicas o privadas. En particular, elimina el costo para los ciudadanos de crear múltiples cuentas o proporcionar la misma información repetidamente para cada plataforma que usan.

- No requiere una conexión permanente a internet, brindando flexibilidad y libertad a los usuarios para gestionar su identidad sin necesidad de estar siempre conectados.

- En ámbitos rurales y sectores vulnerables, los representantes que actúan como notarios oficiales de nacimiento podrían viajar a áreas rurales no desarrolladas para emitir certificados de identidad digital que serían administrados por las personas con un mínimo grado de uso de billeteras digitales. Esto permitiría identificar a individuos de población vulnerable y rural con un grado aceptable de precisión y brindarles todo tipo de servicios, como educación y atención médica.

RECUADRO 1: ¿Qué relevancia tiene para los gobiernos la adopción de la IDA y de qué manera impacta en la gestión pública y la entrega de servicios ciudadanos?

Iván Durán, Ex-Consejero Distrital de TIC, Alcaldía Mayor de Bogotá (Colombia):
"La promesa de valor de las políticas de Gobierno Digital no se ha cumplido del todo, en parte debido a la experiencia del ciudadano al interactuar digitalmente con el Estado. Los trámites digitales, por ejemplo, pueden tener fricciones que hacen difícil la interacción, y hace que los ciudadanos puedan preferir la interacción análoga. Un factor clave en esa fricción se relaciona con la identidad digital, debido a la fragmentación de nuestra identidad, propio de la Web 2. La identidad digital autosoberana, propia de la Web 3, ofrece una solución para que cada ciudadano tenga una única identidad, que facilite la interacción con el Estado. Además, la tecnología blockchain, que se encuentra en la base de la identidad digital autosoberana, brinda mejores estándares de seguridad y privacidad de la información, lo cual es clave en la sociedad digital actual y del futuro."

Cintia Smith, Secretaría de Innovación y Gobierno Abierto de Monterrey (México):
"Los gobiernos deberían considerar y liderar el tema de la identidad digital debido a su papel central en la protección de los derechos individuales, la seguridad pública y la eficiencia administrativa. La gestión descentralizada de identidades digitales empodera a los ciudadanos al otorgarles un mayor control sobre sus datos personales, fortaleciendo así la privacidad y la seguridad en línea. Al liderar este cambio hacia identidades, los gobiernos pueden promover la innovación, la interoperabilidad y la adopción generalizada de estándares abiertos, lo que beneficia tanto a los ciudadanos como a las entidades gubernamentales y privadas."

Diego Fernández, Secretario de Innovación y Transformación Digital de la Ciudad Autónoma de Buenos Aires (Argentina)
Desde el Gobierno de la Ciudad de Buenos Aires desarrollamos Quark ID para crear un nuevo sistema de identidad digital autosoberana con el objetivo de otorgarles a las personas el control sobre su información, con un anclaje de seguridad en blockchain. El paso que estamos dando con este desarrollo es enorme y convierte a Buenos Aires en la primera ciudad de América Latina, y una de las primeras en el mundo, en integrar y promover esta nueva tecnología. Quark ID sigue estándares internacionales utilizados en frameworks de seguridad pública de todo el mundo (W3C, Trust Over IP, Sovrin Foundation) por lo que es capaz de interoperar con otros protocolos similares. De esta manera, se genera un ecosistema internacional de intercambio de credenciales sin intermediarios que beneficia a millones de personas, simplificando la manera en que el Estado, el sector privado y la sociedad se relacionan, a través de interacciones más ágiles y seguras.

2. El uso de *"blockchain"* en la Identidad Digital Autosoberana

La tecnología *blockchain*, o 'cadena de bloques', funciona esencialmente como un libro de contabilidad digital descentralizado e inmutable. Es una base de datos distribuida y compartida en la que se registran y almacenan transacciones de forma segura y transparente. Cada transacción se agrupa en un 'bloque' y se enlaza de forma secuencial con los bloques anteriores mediante funciones criptográficas, formando así una cadena continúa de información. La descentralización significa que esta base de datos no está controlada por una sola entidad o autoridad central, sino que está distribuida entre muchos nodos o participantes en la red. La inmutabilidad se refiere a que una vez que se registra una transacción en la *blockchain*, no se puede modificar ni borrar, lo que garantiza la integridad y la confianza en la información almacenada.

Estas tecnologías de registro distribuido pueden configurarse de diversas maneras, basadas en su infraestructura, participación y transaccionalidad, y visualización. Estas configuraciones determinan cómo se estructura la red, quién la gestiona y mantiene, y cómo se accede a la información contenida en ella. A continuación, se presenta una exploración tridimensional que profundiza en la definición de los tipos de *blockchain:*

TABLA 1: Tipos de *blockchain* según sus características

Dimensión	Característica	Descripción
Infraestructura	**Pública o Privada**	La infraestructura de una *blockchain* puede ser pública o privada, estableciendo cómo se estructura la red, quién la gestiona y mantiene. Los ejemplos emblemáticos de una *blockchain* de infraestructura y gestión pública son Bitcoin y Ethereum. Mientras que el ejemplo de una *blockchain* de infraestructura privada es Hyperledger Fabric, diseñada para uso empresarial.
Participación	**Permisionada o No Permisionada**	En el caso de una *blockchain* permisionada, los participantes deben solicitar algún tipo de autorización o cumplir con condiciones específicas para poder participar y realizar transacciones en la red *blockchain.* Por otro lado, en una *blockchain* no permisionada, no se requiere ningún tipo de autorización previa para participar y realizar transacciones en la red. Bitcoin y Ethereum son cadenas de bloques no permisionadas. Ripple o Polkadot son, por contraste, permisionadas.
Visualización	**Abierta o Cerrada**	Se relaciona con la accesibilidad y la visibilidad de las transacciones y datos almacenados en la *blockchain,* que pueden ser abiertas o cerradas. No es algo común el uso de una visualización cerrada en general, pero se utilizan en casos de uso muy concretos donde la privacidad de la información guardada en la blockchain es un factor crítico y, también, quien pueda validarla. Un ejemplo de esto es la *blockchain* "Quorum", basada en Ethereum y creada en el 2016 por JPMorgan, luego adquirida por Consensys, restringen la visibilidad para mantener en privado las transacciones de sus clientes.

Fuente: Elaboración propia.

Podemos establecer una comparación conceptual entre Internet, Intranet y Extranet y los diferentes tipos de *blockchain.* Internet refleja las características de una *blockchain* con una infraestructura pública, una participación sin necesidad de autorización y una visualización abierta. Por otro lado, una Intranet se asemeja a una *blockchain* privada, permisionada y cerrada, ya que solo pueden acceder las personas con permisos y es gestionada por la empresa que la creó. En contraste, una Extranet permite la participación y visualización de externos, por lo que sería similar a una *blockchain* privada, permisionada pero abierta en ciertos aspectos específicos.

Blockchain es la tecnología subyacente que se utiliza para implementar sistemas de identidad descentralizada de manera segura y confiable. Dicha tecnología proporciona un método seguro y descentralizado para almacenar datos de identidad. En lugar de almacenar información de identidad en un servidor centralizado, donde es vulnerable a ataques cibernéticos, la información de identidad se distribuye y se almacena en múltiples nodos de la red *blockchain.* Esto hace que sea extremadamente difícil para los atacantes comprometer o manipular la información de identidad.

Una vez que se registra la información de identidad en la *blockchain,* se vuelve inmutable, lo que significa que no se puede modificar ni eliminar sin el consenso de la red. Esto garantiza la integridad de los datos de identidad y previene la falsificación o alteración no autorizada de la información.

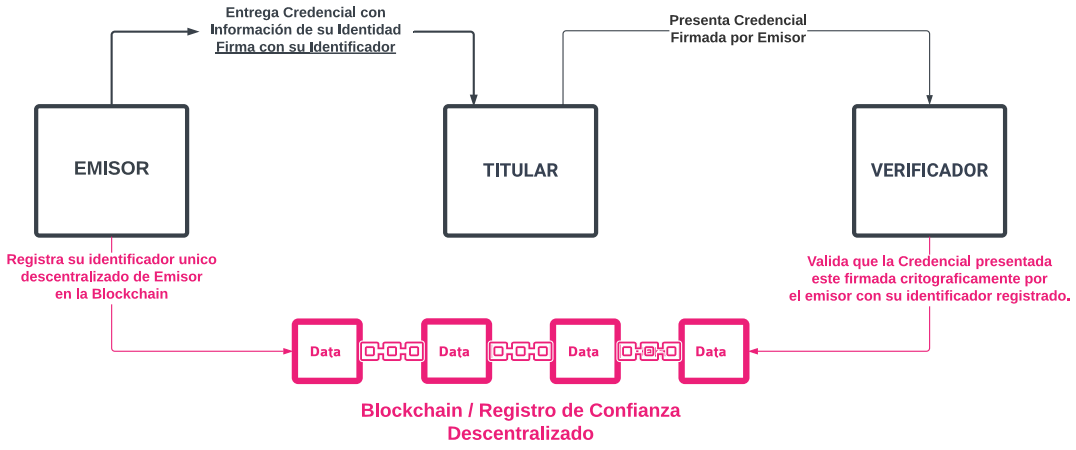
Dentro de este enfoque más amplio hay dos soluciones que permiten escalar la funcionalidad de la *blockchain* que registra datos en una base inmutable.

- Soluciones de Segunda Capa: Son redes dependientes de la *blockchain* principal. Sus transacciones están directamente conectadas con esa *blockchain* principal. Algunos ejemplos son zkSync o Optimism Rollup para la red principal Ethereum o Lightning Network para la red principal Bitcoin.

- Cadenas Laterales (“Sidechains” en inglés): Son cadenas de bloques independientes con una vinculación concreta con la *blockchain* principal pero operan de forma separada y pueden tener sus propias reglas y características. Algunos ejemplos son Rootstock (RSK) con la *blockchain* de Bitcoin o Polygon con la red Ethereum, entre muchas otras.

El análisis sobre los beneficios y costos de cada enfoque dependerá de los casos de usos definidos y los objetivos o problemas a resolver.

GRAFICO 1.- Ilustración de *Blockchain* interactuando con el sistema de Identidad Digital Autosoberana



Fuente: Elaboración propia.

La IDA se apoya en "ecosistemas de identidad", estructuras que fomentan la confianza entre individuos y organizaciones en el entorno digital, garantizando la fiabilidad y la veracidad de los datos e información intercambiados. Un componente clave en estos ecosistemas son los "registros de confianza", que actúan como fuente única y verificable de información. Las *blockchains* son la elección preferida para implementar estos registros debido a su descentralización y otras cualidades como mejoras de privacidad, Interoperabilidad, Transparencia y seguridad.

Aunque no son imprescindibles en todos los casos, las *blockchains* resultan valiosas en los ecosistemas de identidad. El nivel de integración deberá requerir un análisis específico que permita definir cuáles son los problemas a resolver y cuáles los costos que esto conlleva. Por lo tanto, hay que tener en cuenta:

- Usabilidad
- Costos de transacciones (sostenibilidad)[5]
- Eficiencia de la Infraestructura y rendimiento en las interacciones
- Interoperabilidad

Los usuarios pueden poseer y gestionar sus claves privadas, lo que les permite acceder y compartir su información de identidad según sus propias preferencias y necesidades. La tecnología *blockchain* puede facilitar la interoperabilidad entre diferentes sistemas de identidad descentralizada, permitiendo que los usuarios utilicen una sola identidad digital en múltiples plataformas y servicios sin tener que crear múltiples cuentas o proporcionar información de identidad redundante.

Otro elemento del stack tecnológico que conforma a la IDA es el **protocolo: un conjunto de reglas, estándares y especificaciones técnicas que definen cómo se debe establecer, gestionar y verificar la identidad digital** de manera descentralizada y autosoberana. Según los principios de Trust over IP[6] (ToIP), que busca potenciar a los individuos dentro de un ecosistema digital abierto, confiable, seguro y transparente, cada usuario debe tener el control sobre su identidad digital y los datos asociados. Se aspira a que las relaciones se basen en la confianza mutua, respaldadas por una red tecnológica segura y validada por los propios usuarios.

5 Los costos de transacción dependen de la tecnología de blockchain y el valor de mercado de las redes. Aunque puedan resultar, en muchos casos, menores para gobiernos, son cruciales en el análisis de escalabilidad y de sostenibilidad.

6 https://trustoverip.org/

Entre las características a destacar de los protocolos IDA bajo estos principios, podemos enumerar:

- **Descentralización:** Las identidades se crean y verifican sin depender de intermediarios centralizados. Esto significa que no se necesita confiar en una sola entidad o empresa para gestionar la identidad digital.

- **DIDs (Identificadores Descentralizados):** Los DIDs son identificadores únicos y descentralizados para cada sujeto (individuo, organización, dispositivo, etc.), permitiendo la creación de identidades digitales sin depender de un registro central[7].

- **Verifiable Credentials (Credenciales Verificables):** Los protocolos denominados Self Sovereign Identity (SSI) por su sigla en inglés, utilizan Verifiable Credentials (VCs o bien CVs) para permitir que las partes emisoras emitan credenciales digitales verificables (por ejemplo, certificados, diplomas, etc.) que luego pueden ser verificadas por otras partes sin revelar información adicional más allá de lo necesario para la verificación y sin depender de una comunicación directa con el ente emisor.

- **Billetera de IDA (Wallet)[8]:** es una aplicación que permite a los titulares de la identidad controlar y compartir de forma segura su información personal (Credenciales Verificables). Funciona con llaves criptográficas, una privada que guarda el usuario y una pública que comparte junto con su DID, para verificar su identidad sin depender de terceros.

- **Consentimiento informado:** Los usuarios tienen control sobre su información y dan su consentimiento informado antes de compartir datos, mediante el uso de mecanismos criptográficos y la gestión descentralizada de claves.

- **Interoperabilidad:** Para que IDA funcione correctamente, es clave que los protocolos que soportan a IDA sean interoperables, permitiendo que diferentes implementaciones y sistemas interactúen y verifiquen identidades de manera coherente y consistente.

- **Privacidad por diseño:** Los usuarios tienen la capacidad de compartir sólo la información necesaria y relevante en un contexto específico, minimizando la exposición de datos personales.

3. Estrategia de implementación de la IDA.

La IDA puede forjar la piedra angular de una nueva manera de relacionarnos en el entorno web, moldeando un futuro donde la tecnología respalda la autonomía, la seguridad, la confianza y el respeto a la individualidad[9]. Ahora bien, para aterrizar estos conceptos en entornos reales de aplicación, deberán abordarse de forma simultánea o secuencial las siguientes 4 etapas:

7 Ver explicación detallada en Workshop ¿Qué es un DID? Workshop a cargo de Soledad Cánepa.

- **Etapa de exploración**
  - Identificación de un problema a ser resuelto
  - Análisis del problema
  - Definición de Caso de Uso:
    - Análisis de Actores
    - Reglas
    - Roles
    - Requisitos
    - Dinámica de interacciones
    - Flujos
  - Análisis de Viabilidad:
    - Viabilidad técnica
    - Viabilidad económica
    - Marco normativo juridico
    - Relevamiento técnico

- **Etapa de diseño**
  - Selección de tecnologías
  - Diseño de la solución
  - Análisis de actores
  - Planificación del proyecto:
    - Definición de objetivos
    - Alcance
    - Capacidad técnica
    - Recursos
    - Cronograma de actividades y tareas

- **Etapa de implementación**
  - Tecnología:
    - Desarrollo y despliegue de las infraestructuras tecnológicas necesarias
    - Integración de protocolos de SSI
    - Integración con servicios propios
    - Establecimiento de procesos operativos
    - Pruebas técnicas y pruebas de usuario
    - Sensibilización y capacitación de equipos de gobierno

- **Etapa de post implementación**
  - Despliegue en territorio (estrategia territorial, incluyendo capacitaciones)
  - Monitoreo y mejora continua
  - Mantenimiento técnico
  - Capacitación / Formación continua

El proceso inicia con la **exploración e identificación de un problema** que requiere ser resuelto con la IDA como una herramienta de valor social para definir lo más detalladamente posible **el caso de uso.** Esto significa establecer el encuadre específico del caso de uso, considerando los actores críticos y sus roles en cuanto a la emisión, verificación y validación de los datos de identidad.

Una vez identificado el caso de uso, se realiza un a**nálisis de viabilidad tanto técnica como económica,** al menos en una primera estimación. Al referirnos a la viabilidad técnica, nos referimos no sólo al aspecto tecnológico (es decir, si existe la tecnología necesaria para su utilización en este contexto, si se puede aplicar, etc.) sino también a los aspectos vinculados a la **institucionalidad** en cuanto a las voluntades de los actores involucrados y sus capacidades operativas, así como el análisis de la población objetivo y las posibilidades de llegada.

Este análisis de viabilidad tendrá dos objetivos: El primero y el más evidente es identificar si el proyecto es viable o no; el segundo, es el proceso creativo de iteración de la idea inicial, que ante posibles dificultades identificadas se irá reconfigurando en aquellos casos en los que se reconozca la necesidad de rediseñar la propuesta. Es importante tener en cuenta que, en el ámbito de las regulaciones, es necesario considerar las particularidades de cada organismo, ya que cada uno está regido por su propio marco normativo público.

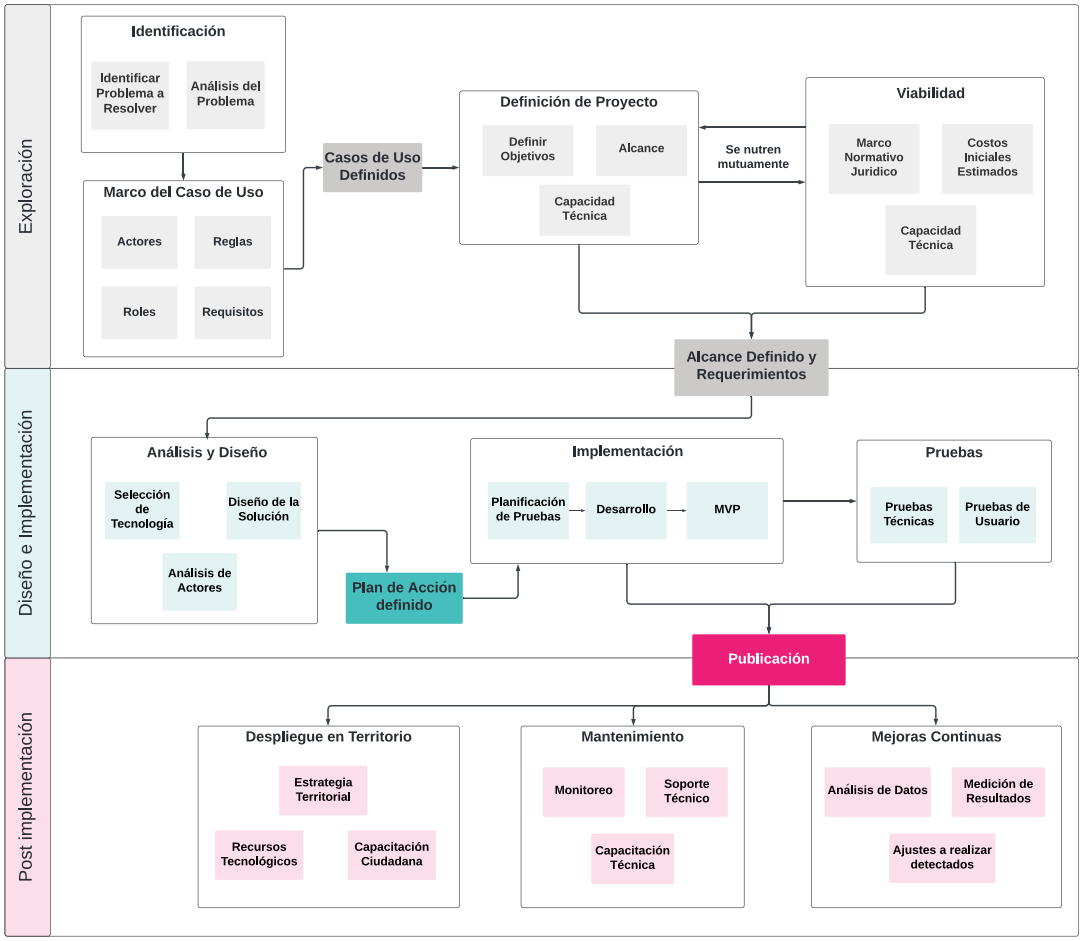
Sí estamos de frente a un proyecto viable, pasamos a la **etapa de diseño.** Aquí se procederá a realizar un análisis de actores más detallado, donde deberemos tener presente tanto los intereses de cada uno así como las interacciones entre estos, entre otros aspectos. En esta instancia se deberán definir las tecnologías con las que se trabajará y diseñar la solución a implementar. Con la información identificada en los pasos previos, se procede a crear un **plan de acción** mediante una planificación que defina claramente qué se propone hacer y cómo se llevarán adelante esas actividades. Esta instancia deberá contemplar tanto las actividades y tareas asociadas a fin de lograr el objetivo propuesto, así como la determinación de los recursos

necesarios para llevarlo a cabo (incluyendo la definición de equipos según las tareas a realizar y el organigrama) y el presupuesto requerido.

Posteriormente, se procede con la **etapa de implementación.** Es en esta instancia que se llevará adelante el desarrollo y despliegue tecnológico, que incluye las infraestructuras necesarias, la integración de protocolos, la integración con los servicios de la(s) institución(es) donde se está implementando, así como el establecimiento de los procesos operativos que introduce esta solución. Todo deberá ser acompañado por pruebas tanto técnicas como por pruebas de usuario. Al mismo tiempo, los equipos deberán formarse y adquirir los conocimientos relevantes para tener las herramientas necesarias.

En una **etapa post implementación,** se deberá realizar el despliegue con los usuarios finales, según la estrategia territorial definida. Esta instancia se deberá acompañar de capacitaciones y políticas de accesibilidad para garantizar una llegada efectiva. Es también en esta etapa que deberá diseñarse una propuesta de evaluación que sirva como guía a lo largo de la implementación. En líneas generales, podemos afirmar que en la mayoría de los casos nos encontraremos frente a destinatarios heterogéneos y que, para poder garantizar mejoras en cuanto a la eficiencia, la efectividad, la eficacia y la sostenibilidad del proyecto, el monitoreo y la mejora continua de la implementación se consideran factores claves. Finalmente, deberán contemplarse las tareas de mantenimiento técnico (gestión de servidores, resolución de conflictos, etc.) así como la formación y capacitación continua de los equipos que llevan adelante el proyecto. A continuación, se presenta un diagrama ilustrativo de las etapas mencionadas:

GRÁFICO 2.- Etapas de estrategia de implementación de la IDA



Fuente: Elaboración propia.

A modo de ejemplo y síntesis:

Escenario de aplicación: Las Manzanas del Cuidado es un programa de la Alcaldía de Bogotá que ofrece servicios gratuitos para mujeres vulnerables, desarrollo de capacidades y autonomía de las personas. Las Manzanas son áreas de la ciudad con infraestructura y servicios para atender de manera próxima y simultánea a las cuidadoras y a sus familias.

Actores del proyecto: Gobierno de Bogotá, Secretaría de Integración Social y mujeres bogotanas de bajos recursos económicos. Esta política pública alcanza a 400.000 mujeres en situación de vulnerabilidad.

Problema a resolver: Las beneficiarias de esta política, luego de pasar por una encuesta socioeconómica, obtienen un carnet físico (QR) de uso exclusivo para este programa. Existe una alta tasa de olvido o pérdida de esta tarjeta, teniendo, como consecuencia, que volver a pasar por el proceso de encuesta cada vez que se acercan a los espacios donde se otorgan los beneficios incurriendo en un reproceso que implica insumo de tiempo, tanto para las beneficiarias como para quienes trabajan en el programa. A su vez, al generarse un QR exclusivo para el programa, no cuentan con una credencial que las identifique cómo tales de cara a otras entidades, con información de valor que podría ser de utilidad para acceder a beneficios de otros programas externos (por ejemplo, a Transferencias Monetarias - IMG).

Solución: El Gobierno de Bogotá, a través de su portal de servicios podrá ofrecer el nuevo mecanismo de validación de identidad como Credencial Verificable (o CV) tanto para el ingreso a los espacios del programa como para brindar más y mejores servicios a las beneficiarias del programa de forma eficiente. Se generarán de esta forma credenciales con información de valor para nutrir la identidad digital del individuo, bajo el objetivo de fortalecer el derecho a la identidad de las personas, al mismo tiempo que se reducen los tiempos de verificación de la identidad de las mujeres.

4. Definición del Desarrollo tecnológico requerido para la IDA

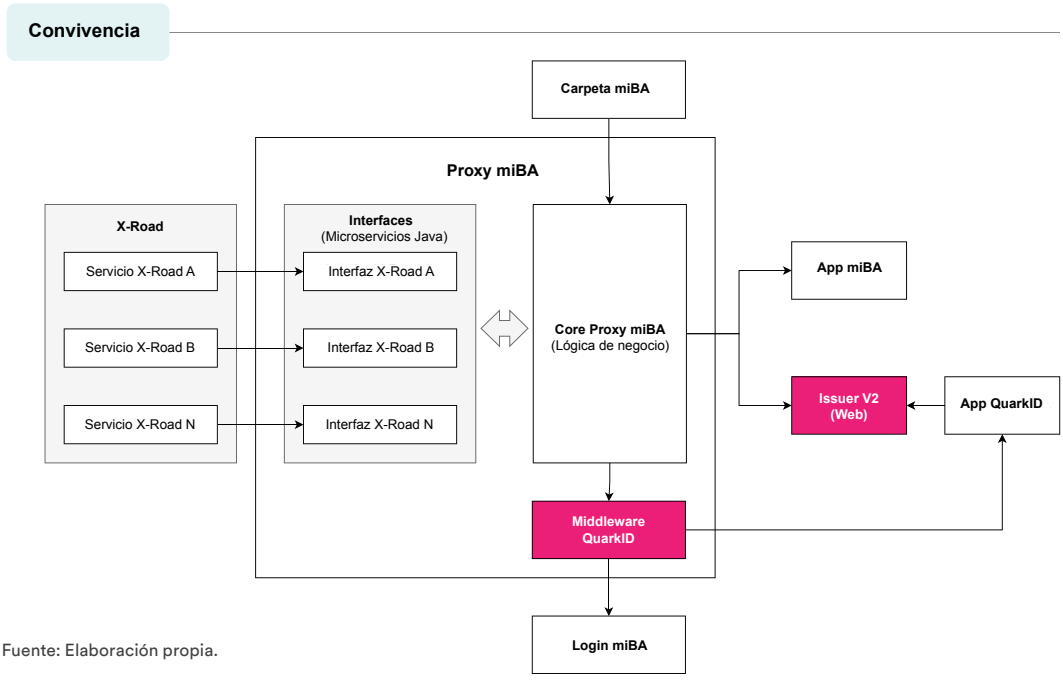
El primer paso para definir los desarrollos tecnológicos requeridos para la IDA es identificar cómo es el tipo de organización que desea implementar la tecnología, conocer los recursos con los que cuenta, conocer los sistemas de información que utiliza así como el alcance que se espera tener con el proyecto. De aquí que se deberá definir un modelo de implementación. Para mayor detalle de estos, ver los apartados Emisión de credenciales - Modelo de implementación gubernamental (emisión directa) y Emisión de credenciales - Modelo de implementación cooperativas (emisor web).

La digitalización de documentos/datos que originalmente, fueron creados en papel, convive con datos o documentos que nacieron de forma digital. **Esas bases de datos o documentación con las que cuentan los organismos públicos son los cimientos desde los cuales se deberán integrar los protocolos de Identidad Digital Autosoberana.** Esto presupone un correcto orden y funcionamiento de las bases de datos centralizadas con las que las instituciones vienen trabajando hace años. Es decir, es importante entender que este modelo es posible en un contexto de información ordenada y bien organizada dentro de las instituciones. De aquí que deberá llevarse adelante un relevamiento exhaustivo de los servicios y evaluar si existe la necesidad de mejoras en los servicios actuales y, luego de un mapeo e identificación de casos de uso posibles, se deberá diseñar la forma **de integración** con el modelo descentralizado.

Un posible modelo de aplicación es mediante el desarrollo de un middleware que tome los datos de las bases centralizadas y los transforme con el objetivo de emitir credenciales verificables descentralizadas. Con el mapeo completo, se procederá a diseñar un plan de desarrollo con el objetivo de integrar los servicios y datos disponibles al modelo de

Identidad Digital Autosoberana, generando las Credenciales Verificables que serán emitidas a los ciudadanos. A continuación, se presenta un **diagrama de arquitectura del caso de uso en la Ciudad de Buenos Aires,** donde se visualiza la interacción de los diversos componentes de la solución y la convivencia de los modelos de datos centralizados y los descentralizados.

GRÁFICO 3: Diagrama de implementación de la Ciudad de Buenos Aires.



Fuente: Elaboración propia.

5. Modelos de datos

Las aplicaciones, plataformas o sistemas de gobierno descansan fuertemente em la digitalización de documentos para operar sus servicios. Sin embargo, la IDA propone un nuevo paradigma que inicialmente incluye al mundo centralizado para poder generar un entorno de transición amigable y flexible.

La Tabla 2 compara dos enfoques distintos en aplicaciones digitales: por un lado, un modelo centralizado de digitalización de documentación y gestión de trámites; y por otro, aplicaciones basadas en la Identidad Digital Autosoberana, que representan un enfoque innovador en la gestión y control de la identidad digital. Esta comparación busca destacar las diferencias funcionales y estratégicas entre un modelo centralizado y otro descentralizado. Es importante subrayar que, **aunque diferentes en su estructura y enfoque, estos modelos no son necesariamente excluyentes y pueden ser complementarios**. Una integración efectiva de ambos enfoques puede enriquecer la experiencia del usuario, combinando la eficiencia y familiaridad de las soluciones centralizadas con la seguridad y autonomía de las opciones descentralizadas, creando así un ecosistema digital más robusto y versátil para los ciudadanos y el gobierno.

TABLA 2: Modelos centralizados para la digitalización de documentación y gestión de trámites vs. Modelos descentralizados con aplicación de IDA.

	Modelo Centralizado Actual	Identidad Digital Autosoberana	Detalles
Código	Cerrado	Abierto[10]	Los sistemas gubernamentales orientados a brindar servicios de identidad y gestión de trámites generalmente, operan con código cerrado, limitando la posibilidad de auditar su funcionamiento interno. Los ecosistemas de Identidad Digital Autosoberana se basan en el uso de código y estándares abiertos. Esta práctica fomenta la transparencia y fortalece la confianza en los sistemas públicos responsables de manejar información sensible. Los sistemas abiertos permiten verificar y asegurar que no existan vulnerabilidades o flujos de información no seguros.
Manejo de la información personal	Cerrado Retiene información privada del ciudadano (Nombre, Direccion Fisica del Ciudadano, Email)	No retiene información	Mientras que las plataformas centralizadas y cerradas retienen información personal del usuario, como nombre, dirección y correo electrónico, las aplicaciones con IDA están diseñadas para no retener datos personales. Incluso si el gobierno ya tiene esa información en sus bases de datos, la aplicación no la almacena adicionalmente. Este enfoque preserva la privacidad del usuario.
Infra-estructura	Centralizada	Descentralizada	La infraestructura de la Identidad Centralizada a menudo requiere que los usuarios instalen múltiples aplicaciones para acceder a diferentes servicios, limitando su capacidad de gestionar la privacidad y compartir digitalmente sus credenciales de forma segura. En contraste, la IDA permite a los usuarios recibir y almacenar credenciales en una única billetera digital, simplificando el acceso y mejorando el control sobre la privacidad y la compartición segura de la información.
Alcance	Nacional	Internacional	En cuanto a la estandarización para el alcance internacional, los servicios centralizados pueden adaptarse para trabajar con sistemas de otros países, pero esto requiere esfuerzos específicos para alinear modelos de datos y estructuras, lo que implica desarrollos adicionales y acuerdos entre estados soberanos. Por otro lado, la IDA, al basarse en estándares abiertos e internacionales, ya proporciona un marco común que facilita la verificación de credenciales a nivel global sin necesidad de desarrollos extra o esfuerzos significativos para unificar criterios. Esto promueve una mayor eficiencia y accesibilidad en la gestión de la identidad digital a nivel internacional.
Fuentes de información	La fuente de la información es únicamente gubernamental	La fuente de la información puede ser de cualquier emisor registrado (Gobiernos, Privados, Organizaciones)	Este es un beneficio relacionado con la comparativa de Sistemas de Identidad Centralizados vs. Descentralizados. La identidad de las personas no es sólo proporcionada por los Estados, sino también se nutren de sus interacciones sociales, financieras, educativas o comunitarias.
Experiencia de usuario / ciudadanía	El ciudadano solo puede mostrar su identidad a través del celular o capturas de pantalla.	El ciudadano puede compartir su identidad de forma total o parcial según desee	La IDA mejora la usabilidad y privacidad permitiendo a los usuarios compartir selectivamente información específica. A diferencia de los sistemas actuales que requieren mostrar un documento completo, en la IDA se puede compartir solo el dato necesario, como por ejemplo el "NOMBRE", verificado por su emisor, protegiendo así el resto de los datos y por ende la privacidad.

Fuente: Elaboración propia.

10 Vale destacar que el uso de código abierto no es una característica propia de la IDA. En esta publicación recomendamos el uso de código abierto a los fines de promover mayor transparencia e interoperabilidad. En ambos modelos, tanto el centralizado como el descentralizado (IDA), se puede optar por tecnologías de código cerrado o de código abierto según se considere conveniente.

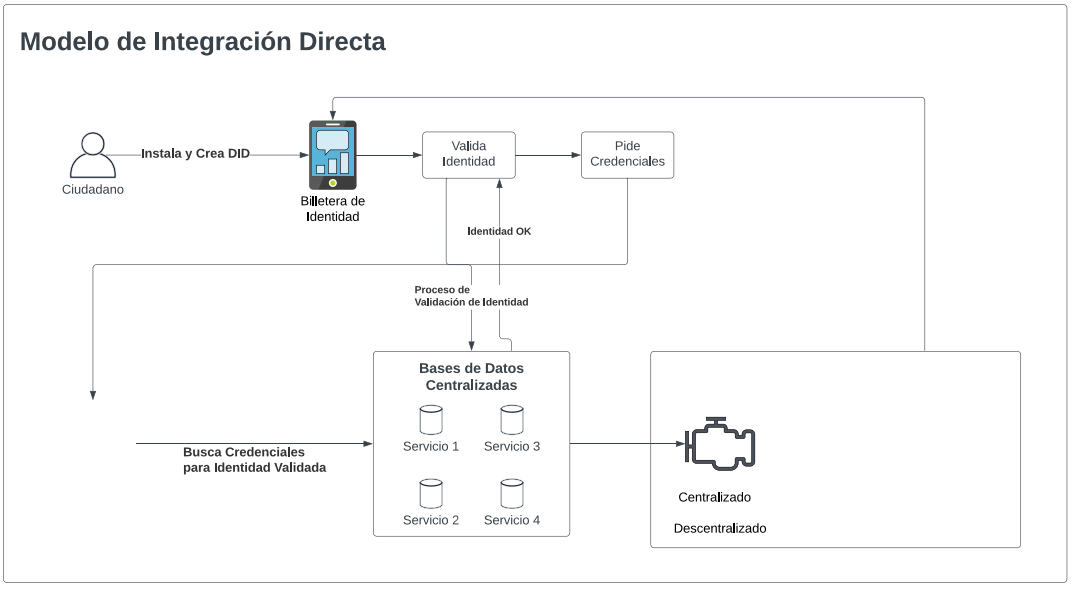
6. Modelos de Implementación

La implementación y diseño de la infraestructura y la arquitectura de la IDA es amplia y se puede aplicar con base en las necesidades de diversos casos de uso. A continuación proporcionamos dos modelos que hemos detectado a partir de experiencias en pilotos y proyectos en desarrollo.

6.1. Modelo de integración directa

Este modelo de implementación propone una solución de Identidad Digital Autosoberana integrada de modo directo sobre el sistema centralizado gubernamental. Esto quiere decir que las emisiones se realizan de modo automático cuando el ciudadano solicita su credencial. Hay diversos modos de organizar esta emisión y eso va a depender de las regulaciones y de las estrategia de implementación de la entidad. La emisión puede estar centralizada en una sola entidad, por ejemplo, Gobierno de la Ciudad o puede estar más descentralizada siendo la institución específica dentro del Gobierno que sea el emisor, por ejemplo: Registro Civil.

GRÁFICO 4: Diagrama de flujo del modelo de integración directa



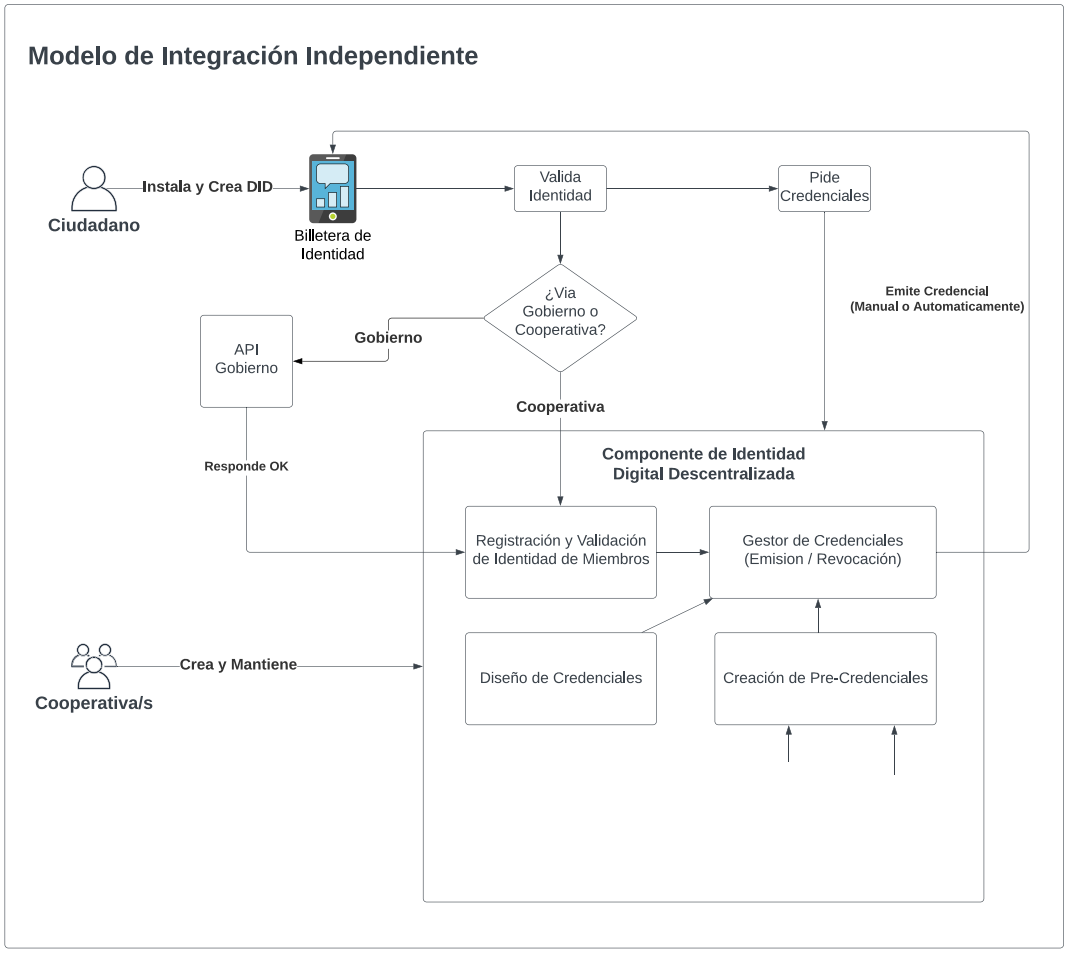
Fuente: Elaboración propia.

Este modelo requiere desarrollar módulos que se encarguen de comunicarse con los sistemas centralizados y traducirlos al formato necesario para generar la Credencial Verificable solicitada por el ciudadano. Este proceso se hace de modo directo sin pasar por procesos intermedios de alojamiento de información de los ciudadanos. De los sistemas centralizados pasa directamente a los servicios de IDA que no aloja información sino que la emite de modo descentralizado al ciudadano. Un ejemplo de esta implementación es la Ciudad de Buenos Aires que integró sus sistemas centralizados con el protocolo de Identidad Digital Autosoberana Quark ID.

6.2. Modelo de integración independiente

Este modelo está orientado a organizaciones o cooperativas que no poseen una sistematización previa de sus datos, que no tienen los recursos o la estructura para contar con un sistema complejo. El propósito de este modelo es facilitar la aplicación de esta tecnología aun cuando no se cuenta con una gran infraestructura previa.

GRÁFICO 5: Diagrama de flujo del modelo de integración independiente.



Fuente: Elaboración propia.

Se propone la generación de un sistema abierto que permita a las organizaciones diseñar y crear Credenciales Verificables según sus necesidades, así como emitirlas al titular de la información. Un ejemplo de esto fue la Cooperativa Coopsol en el Gran Chaco Argentino quienes implementaron un piloto para emitir credenciales a los productores apícolas. El caso consistió en la generación de credenciales verificables financieras, socioeconómicas, productivas y de resiliencia climática. La cooperativa, tras verificar el estado de la producción de cada uno de sus miembros productores, emitía credenciales con las características verificadas. Con estas credenciales en su poder, los productores podían acceder a servicios de seguros o créditos. Este piloto fue muy positivo y generó un modelo accesible en comunidades alejadas de las zonas urbanas.

7.Conclusiones y recomendaciones de política

Para escalar proyectos de Identidad Digital Autosoberana es recomendable que gobiernos y comunidades exploren sus casos de uso en la perspectiva de **infraestructura pública digital.** Esto significa desplegar **sistemas abiertos, interoperables y centrados en las personas** en materia de gestión de datos de cara a la ciudadanía y entrega de servicios públicos eficientes y transparentes. El enfoque de infraestructura pública también abarca a las **relaciones gobierno-gobierno y a los procesos de integración regional.** Como se sostiene desde Naciones Unidas, los sistemas que se desarrollan sobre infraestructura pública digital crean las condiciones de posibilidad para catalizar la innovación a escala y cerrar la brecha digital.

OCDE y CAF (2023) han identificado que una gobernanza regional de los datos es fundamental para avanzar en ámbitos como el diseño y la entrega de servicios públicos transfronterizos, los servicios compartidos entre gobiernos y la creación de infraestructuras de datos confiables que sirvan de base a las tecnologías de uso intensivo de datos, incluida la **inteligencia artificial (IA).**

En materia de intercambio comercial, la IDA también es relevante para **políticas de estandarización y aceleración del desarrollo económico en la región,** especialmente para ayudar a las empresas a ser más productivas y dinámicas. *"La ineficiencia en la logística, la interoperabilidad de las reglamentaciones digitales y los procedimientos aduaneros aún se encuentran entre los desafíos más difíciles para las empresas de América Latina y el Caribe que desean participar en las cadenas globales de valor, así como en el comercio transfronterizo, incluido el comercio electrónico" (Cepal, 2019).*

Un sistema de confianza digital interoperable entre naciones, que respete las soberanías locales pero que hable un mismo lenguaje tendrá impacto en el desarrollo regional. En palabras de Jorge Arbache, Vicepresidente de Sector Privado de CAF, en el sector comercial de servicios y exportaciones hay un enorme espacio de crecimiento para América Latina y Caribe: *"avanzar en la agenda del comercio de servicios requiere enfrentar desafíos y, entre los más importantes, se encuentran la armonización regulatoria y de estándares, la simplificación y la digitalización de trámites".*

En la misma línea, en los ámbitos locales las infraestructuras abiertas fortalecen los modelos de gestión documental tradicional (eGov) al empoderar a los gobiernos como **autoridades certificantes** y facilitar los servicios transaccionales que involucran a la ciudadanía, reduciendo costos y mejorando la resiliencia. Por ello **debe verse como complementaria a las identidades electrónicas emitidas por los Estados nacionales.** En efecto, a medida que más gobiernos locales, subnacionales, empresas y organizaciones adopten estas infraestructuras, **mayores posibilidades de construir sistemas de confianza digital con un marco seguro para las múltiples interacciones digitales de la sociedad actual.**

Para una adopción exitosa de IDA como infraestructura pública digital, recomendamos:

- Los estándares y la interoperabilidad son fundamentales para lograr una adopción exitosa y apropiación social masiva. **Los proyectos** deben iniciarse sobre **estándares internacionales abiertos** y las blockchains deben ser **públicas, no permisionadas e interoperables.** La documentación técnica debe ser asequible, de código abierto y de fácil acceso para los desarrolladores, tanto públicos como privados, a fin de evitar dependencias y complejidades que obstaculicen la innovación y desarrollo tecnológico para una nueva gestión de identidades.

- **La estandarización de los datos en el ámbito gubernamental juega un papel crítico**. Al momento de iniciar la planificación es importante contar con un sistema centralizado, previo, ordenado y seguro. El énfasis en una estructura bien organizada y en la seguridad de los datos es esencial para garantizar una **convivencia armoniosa entre los nuevos módulos descentralizados y el sistema centralizado existente.**

- **La correcta evaluación de los recursos tecnológicos presentes en las estructuras organizativas** es esencial para un diagnóstico previo a la planificación de implementación de IDA. Estos recursos refieren tanto a capacidades técnicas como a las personas que conforman los equipos de trabajo.

- Como ocurre con cualquier innovación digital en entornos gubernamentales, la adopción de IDA implica transformaciones en procesos y sistemas backend y frontend. La **transferencia de habilidades técnicas y la incorporación de nuevas formas de gestión de la identidad de los usuarios,** implica un proceso de aprendizaje tanto en los equipos internos como de los ciudadanos.

- Por ser un campo emergente, se recomienda contemplar la **capacitación continúa por medio de la participación proactiva en foros** regionales, talleres y workshops para el intercambio de conocimiento y experiencias. De esta forma se generan conocimientos compartidos y herramientas que potencian los modelos IDA en la región y una cooperación conjunta entre las áreas de innovación de las ciudades y países latinoamericanos.

- Al tratarse de una tecnología centrada en el usuario es fundamental tener presente la diversidad y especificidades de los distintos grupos poblacionales en lo que respecta a temas como inclusión y acceso a la tecnología. Es altamente recomendable acompañar las implementaciones de IDA con **políticas públicas de alfabetización digital y accesibilidad,** que aborden la problemática de la brecha digital.

- En términos de experiencia de usuario, es clave la interoperabilidad entre billeteras para garantizar la compatibilidad entre diferentes aplicaciones, plataformas y servicios. Al igual que los protocolos, recomendamos que sean desarrolladas bajo estándares abiertos y seguros, garantizando así la máxima transparencia y privacidad para los usuarios.

- Frente a la escasez de talento de IT en el sector público, la sostenibilidad de los proyectos están dados por comunidades distribuidas y con acceso a los códigos disponibles de los sistemas, lo que permite a cualquier parte interesada sugerir e intercambiar mejoras en las infraestructuras públicas y proponer nuevas soluciones digitales para problemas específicos.

- Por último, se recomienda articular las iniciativas con tomadores de decisión y **actores relevantes del campo de gov tech** de los países y ciudades, tanto públicos como privados, asociando la tecnología IDA con los problemas reales de la agenda pública, creando las condiciones para impulsar el ecosistema tech de innovación, nuevas soluciones y casos de uso escalables y de mayor impacto social.

ANEXO I - Experiencias internacionales

Unión Europea
La Comisión Europea propuso una actualización al marco de identidad digital paneuropeo, conocida como eIDAS 2.0, en junio de 2021. Esta actualización tiene como objetivo permitir a todos los europeos un conjunto de credenciales de identidad digital que sean reconocidas en toda la UE. Estas credenciales forman parte de las llamadas "Billeteras de Identidad Digital Europeas" o "European Digital Identity (EUDI) Wallets". Estas billeteras, que pueden ser aplicaciones móviles o servicios en la nube, recopilan y almacenan credenciales digitales y permiten su uso de manera segura y confidencial para una variedad de casos de uso tanto gubernamentales como no gubernamentales. El acuerdo final sobre la Billetera de Identidad Digital de la Unión Europa se alcanzó el 8 de noviembre de 2023, sujeto a la aprobación formal del Parlamento Europeo y del Consejo. Los Estados miembros de la UE tendrán que proporcionar las billeteras de Identidad Digital de la UE a sus ciudadanos 24 meses después de la adopción de los Actos de Implementación que establecen las especificaciones técnicas para la certificación. La Agencia de la Unión Europea para la Ciberseguridad (ENISA) ha desempeñado un papel importante en la investigación y análisis de tecnologías de Identidad Digital Autosoberana, evaluando su aplicabilidad y compatibilidad con los estándares y regulaciones existentes en la Unión Europea. Esto incluye el estudio de diferentes tecnologías y marcos de Identidad Digital Autosoberana de todo el mundo y su posible integración en el contexto europeo.

El proyecto IDunion ha entrado en la segunda fase de su proyecto para implementar una infraestructura de clave pública descentralizada, utilizando la cooperativa europea "Societas Cooperative Europaea S.C.E" como autoridad de gobierno. Este proyecto se integra con las billeteras digitales Lissi y Esatus. En España, se ha creado un estándar de Identidad Digital Autosoberana y se está promoviendo a nivel de la Unión Europea. La comunidad autónoma de España, Cataluña, también a legislado para una Identidad Digital Blockchain, que está esperando aprobación a nivel nacional.

Digital Identity Working Group (DIWG)
En 2020, ocho países (Australia, Canadá, Finlandia, Israel, Nueva Zelanda, Singapur, Países Bajos y Reino Unido), presidido por la Agencia de Transformación Digital de Australia y con el Banco Mundial como observador, formaron un grupo de trabajo (Digital Government Exchange (DGX) Digital Identity Working Group (DIWG)), en pos de la identificación digital. El grupo redactó un conjunto de principios para apoyar el desarrollo de sistemas e infraestructura de identificación digital interoperables y mutuamente reconocidos, y tiene como objetivo mejorar los acuerdos comerciales.

Bután
Es un proyecto para proveer a la población una identidad digital auto soberana que les permita gestionar la identidad de un modo autónomo, realizar trámites y mejorar acceso a servicios. Utilizan biometría. Es un proyecto de desarrollo cerrado y el Gobierno de Bután creó una compañía pública autónoma que tiene autoridad sobre el proyecto. En septiembre 2023 se lanzó la aplicación siendo el Príncipe de Bután el primer ciudadano en realizar el registro biométrico y creación de su Identidad. Tienen una aplicación móvil llamada "Bhutan NDI" publicada en Android y iOS. Utilizan una solución basada en Hyperledger Aries y anclada en la blockchain Polygon.

Corea del Sur[14]
Este proyecto fue iniciado en el 2018 para incorporar la tecnología de Identidad Digital Autosoberana en la sociedad surcoreana. Se está implementando progresivamente y de la mano con un trabajo de análisis y estandarización de datos nacionales. Se han desarrollado pilotos y pruebas de concepto.

11 https://www.tech.gov.sg/files/media/corporate-publications/FY2021/dgx_2021_digital_identity_in_response_to_covid-19.pdf
12 https://www.youtube.com/watch?v=I6idRDRu-5Y&ab_channel=BhutanNDI
13 https://www.biometricupdate.com/202310/bhutan-launches-wallet-pilot-unveils-website-for-national-ssi-digital-id
14 https://dgovkorea.go.kr/contents/blog/111

Ciudad de Buenos Aires, Argentina
Este proyecto lo lleva adelante la Secretaría de Innovación y Transformación Digital del gobierno de la Ciudad de Buenos Aires. Busca integrarse con los sistemas MiBA, la herramienta que utilizan los ciudadanos para realizar trámites, abonar impuestos o solicitar información. Se implementó de forma paralela al sistema centralizado actual brindando una nueva opción al ciudadano en el manejo de sus credenciales y permitiendo también un avance progresivo y flexible. El proyecto se denomina "Quark ID[15]" y opera en la blockchain de Ethereum con la integración de "ZK Sync", una solución de segunda capa. Este proyecto está en proceso de convertirse en código abierto, previsto para el primer semestre de 2024.

Proyecto DIDI / Argentina
Realizado entre 2017 y 2022, el proyecto piloto de la ONG Bitcoin Argentina y BIDLabs en Buenos Aires se enfocó en aplicar la Identidad Digital Autosoberana en sectores vulnerables de la Ciudad Autónoma de Buenos Aires y en áreas rurales del Gran Chaco Argentino. Su objetivo era evaluar la eficacia de esta tecnología en el terreno y estudiar su impacto en la mejora del acceso a servicios y recursos para estas comunidades. El proyecto buscó comprender cómo la Identidad Digital Autosoberana podría beneficiar a poblaciones en distintos contextos, tanto urbanos como rurales.
Algunos de los socios implementadores del proyecto fueron NEC, Accenture, IOV Labs, entre otros.

Se implementaron tres proyectos concretos:

- Integración de la Identidad Digital Descentralizada en un sistema de microcréditos productivos familiares otorgados por la Asociación Civil Ecomanía Conciencia Ambiental (Programa Semillas). Estos microcréditos otorgaban credenciales que acreditaban ser parte del programa al titular y su familia. Además, emite credenciales socioeconómicas, de vivienda y de salud. Se hicieron acuerdos con Mutuales de Salud que aceptaban estas credenciales verificables para brindar servicios a los beneficiarios del programa. Se puede ver más información sobre este caso de uso en el canal de YouTube de Proyecto DIDI[16].

- Integración con sistema de registración de productores apícolas de la Cooperativa Coopsol en el Gran Chaco Argentino junto con ACDI Argentina. La Cooperativa emitía credenciales socioeconómicas, financieras, de identidad y de resiliencia climática con el objetivo de brindarle a los productores un mejor acceso a servicios. En este piloto se trabajó junto con empresas aseguradoras y de microcréditos. Se puede ver su código, análisis, diseño e implementación en el repositorio público de ACDI[17].

- App RONDA[18]: Esta aplicación tenía como objetivo brindar una herramienta segura y fácil para los Ciudadanos que utilizan una metodología de ahorro llamado “Pasanaku” o “Ronda”. Es una forma tradicional de ahorro colectivo y crédito rotativo practicado en algunas regiones de América Latina. Esta aplicación móvil, a partir de la ejecución de esos sistemas de ahorro comunitario, emitía credenciales verificables financieras que acreditaban que el participante había cumplido con su compromiso de pago brindando prueba concreta de esto. Según se pudo relevar en territorio[19], este punto brindó gran valor a la comunidad que usa estos métodos de microahorro.

Este piloto fue desarrollado en Android, la totalidad del trabajo fue desarrollado bajo la metodología de código abierto y se encuentra en el repositorio de ONG Bitcoin Argentina. Utilizó la tecnología uPort y las blockchains integradas fueron RSK y LACCHAIN.

Finalizó en diciembre de 2022. Presentó informes detallados con recomendaciones y aprendizajes clave sobre la implementación y algunos casos de uso de la Identidad Digital Autosoberana en entornos específicos.

15 https://quarkid.org/
16 https://www.youtube.com/watch?v=3AWWsrQGGOk
17 https://github.com/ACDI-Argentina/identidad-digital/wiki
18 https://www.youtube.com/watch?v=JpyPxxpx99E
19 Video: Experiencias en primera persona:ronda.
20 https://github.com/ong-bitcoin-argentina/

ANEXO II - Glosario

Llaves criptográficas: La criptografía de llave pública asimétrica utiliza un par de llaves criptográficas: una llave pública, que se comparte abiertamente para cifrar mensajes o verificar firmas digitales, y una llave privada, que se mantiene en secreto por su propietario y se utiliza para descifrar mensajes cifrados con su llave pública correspondiente o para crear firmas digitales. Este sistema permite la comunicación segura y la verificación de identidad en el entorno digital, asegurando que solo el receptor pretendido pueda acceder al contenido cifrado y que la autenticidad de los mensajes firmados digitalmente pueda ser verificada por cualquier persona con acceso a la llave pública del emisor. La seguridad de este método depende de la protección de la llave privada y de la robustez de los algoritmos criptográficos utilizados.
La tecnología de Llave públicas asimétricas existe desde la década de 1970 y es algo que en la actualidad se usa en la mayoría de las Infraestructuras de Clave Pública (PKI) que utilizan esto para firmar documentos digitales o encriptar mensajes. Lo que propone la Identidad Digital Autosoberana es una mejora en el manejo de estas llaves al incorporarlas dentro del DID de cada usuario, generando una gestión más eficiente y segura.

DIDs: Un Identificador Descentralizado (“DID” por su sigla en inglés) es un tipo de identificador único que permite a un sujeto (una persona, organización, objeto o dispositivo) controlar su identidad digital de manera autónoma, sin necesidad de depender de una autoridad centralizada. Los DIDs se basan en tecnologías de registro distribuido, como por ejemplo blockchain, lo que asegura que la identidad digital sea verificable y resistente a la censura o al control por parte de terceros. Cada DID apunta a un documento DID que contiene la llave pública del sujeto y otros metadatos necesarios para la autenticación y la comunicación segura. Una especie de libro con instrucciones para entender cómo relacionarse con ese DID.
Se recomienda el Workshop “¿Que es un DID?” realizado por una de las autoras de este informe, Soledad Cánepa.

Credenciales Verificables: Las credenciales verificables son documentos digitales que contienen información certificada sobre una persona, entidad, objeto o dispositivo, emitidas de manera que puedan ser verificadas electrónicamente por terceros. Estas credenciales son emitidas por una autoridad o emisor confiable y pueden incluir datos como la identidad de una persona, calificaciones educativas, licencias profesionales, derechos de acceso o cualquier otro atributo o cualificación verificable. La tecnología detrás de las credenciales verificables utiliza criptografía avanzada para asegurar que la información sea inalterable y para proteger la privacidad del titular, permitiendo que el verificador confirme su autenticidad sin necesidad de acceder a información sensible o contactar directamente al emisor.

Actores participantes: Los actores en el ecosistema de Identidad Digital Autosoberana (IDA) juegan roles cruciales, interactuando a través de la emisión, gestión y verificación de credenciales digitales verificables. Estos actores son:

- **Titular:** La persona o entidad a quien se emiten las credenciales verificables. Estas credenciales pueden referirse directamente al titular o representar autoridad sobre otras personas, entidades o bienes. Un aspecto distintivo en la IDA es la capacidad de delegación, permitiendo que el titular pueda ser tanto el "Titular de la Identidad", que posee afirmaciones emitidas a su favor (como podría ser una organización), como el "Administrador de la Identidad", que gestiona la identidad en nombre de otro (por ejemplo, un padre administrando la identidad digital de su hijo menor de edad).

- **Emisor:** La entidad que crea y otorga credenciales verificables al titular, certificando la autenticidad de la información que contienen. Este rol puede ser desempeñado por organizaciones, instituciones educativas, empresas o autoridades gubernamentales que validan y respaldan la veracidad de los datos o identidades digitales. La IDA también contempla la posibilidad de que la función del emisor sea delegada a terceros confiables, lo que permite una emisión de credenciales más flexible y eficiente por parte de entidades autorizadas.

- **Verificador:** La entidad que solicita y verifica la autenticidad y validez de las credenciales presentadas por un titular. Este proceso asegura que la información no haya sido adulterada y que esté firmada por una entidad de confianza reconocida por el verificador.

En el contexto de la IDA, la flexibilidad de estos roles, especialmente con la capacidad de delegar tareas y responsabilidades, amplía significativamente las definiciones tradicionales y mejora la implementación en diversos escenarios de uso. Aunque generalmente se habla de Titulares y Emisores en términos simplificados, es crucial reconocer que estos roles pueden incorporar sub-roles que ofrecen mayor adaptabilidad y eficiencia en la gestión de identidades digitales.

Biometría: La biometría es una herramienta utilizada para la autenticación y verificación de identidad basándose en el uso de características físicas o comportamentales únicas de un individuo. Es decir, utiliza los rasgos distintivos inherentes a una persona para reconocer y verificar su identidad.
La biometría y la Identidad Digital Autosoberana no son mutuamente excluyentes e incluso, podrían combinarse en soluciones de identidad digital que incorporen y aprovechen la biometría para la autenticación bajo un marco de Identidad Digital Autosoberana. Por ejemplo, un individuo podría utilizar su biometría para confirmar su identidad generando así una credencial verificable que incluye un proceso biométrico de verificación previo a su emisión.

Billeteras de Identidad Digital (Wallets) Una billetera de Identidad Digital Autosoberana (IDA) es una aplicación que permite a los titulares de la identidad controlar y compartir de forma segura su información personal (Credenciales Verificables). Funciona con llaves criptográficas, una privada que guarda el usuario y una pública que comparte junto con su DID, para verificar su identidad sin depender de terceros. Es como una cartera digital para su identidad, dándoles el control total sobre quién ve sus datos.

Recomendamos que sean desarrolladas bajo estándares abiertos y seguros, garantizando así la máxima transparencia y privacidad para los usuarios. Es fundamental que los ciudadanos tengan la capacidad de auditar estas aplicaciones para asegurarse de que no contienen componentes ocultos capaces de desviar su información personal sin consentimiento. Este nivel de transparencia asegura que la información de identidad del ciudadano se maneje con la integridad que merece, protegiendo contra el uso indebido y fortaleciendo la confianza en las plataformas digitales.

Algunas de sus funciones principales son:

- **Generación y control de DID:** El usuario puede generar su DID con la aplicación y así comenzar a recibir credenciales y nutrir su identidad. Esta generación se realiza junto al proceso de generación de una llave privada y una llave pública.

- **Interacción con emisores y validadores:** Le permite al titular interactuar de forma segura con otros, dando la posibilidad de compartir de forma total o parcial su identidad con un verificador o recibir nuevas credenciales por parte de un emisor.

- **Gestión de la llave privada:** Este es un componente fundamental. La llave privada es la que permite al titular de la billetera firmar digitalmente transacciones y credenciales, asegurando así la autenticidad y la integridad de la comunicación. La billetera protege la llave privada para que solo el usuario tenga acceso a ella y pueda utilizarla para probar su identidad o autorizar operaciones de forma segura, sin revelar la llave misma. La seguridad y privacidad de la llave privada son críticas, ya que su compromiso podría permitir a un actor malicioso suplantar la identidad del usuario.
  Se pueden aplicar diversos modelos de protección de esta llave privada. Principalmente, hay dos categorías, las Billeteras con Servicio Custodio que promueven una mejor experiencia del usuario por sobre la autonomía y control del mismo sobre su identidad digital. O la Billetera sin Servicio Custodio que mantiene en el usuario el control total sobre su llave privada, lo cual también obliga al usuario a ser más responsable, ya que si la pierde no tendrá acceso a sus credenciales. En definitiva, lo recomendado es buscar diseños de gestión de llave privada que equilibren la necesidad del usuario de mantener autonomía pero beneficiando la experiencia de uso.

  Otros métodos de protección de esta llave privada incluye mejor encriptación, buenos procesos de recuperación de la llave y añadir una capa de Autenticación Multifactor (MFA). Esta decisión de diseño respecto al manejo de las llaves debe desprenderse de un análisis que considere temas como el equilibrio entre seguridad y comodidad-utilidad de la población usuaria, los mecanismos de acceso, respaldo y recuperación de las llaves, y qué es lo que se percibe como valor para el usuario.

- **Interoperabilidad y elección libre:** La interoperabilidad entre billeteras es esencial para garantizar que los usuarios puedan utilizar sus identidades digitales de manera consistente en diferentes aplicaciones, plataformas y servicios. La interoperabilidad permite a las billeteras interactuar y compartir información de identidad de manera eficiente y descentralizada, operando bajo estándares comunes. A su vez, el usuario tiene la libertad de elegir y operar con la billetera que considere más conveniente para la gestión de su propia identidad ya que implica que los DIDs y las credenciales puedan ser portables y, por ende, utilizados de forma coherente en diferentes billeteras, permitiéndole a los usuarios cambiar de billetera sin perder acceso a su identidad.

Esto refuerza cómo los estándares abiertos y la colaboración en la comunidad de IDA son clave para garantizar esta interoperabilidad.

Bibliografía

ARBACHE, J.(2022) Servicios e integración regional. Retrieved from:
https://www.caf.com/es/conocimiento/visiones/2022/09/servicios-e-integracion-regional/

ALLEN, C. (2016) El camino hacia la identidad soberana. Retrieved from:
https://www.lifewithalacrity.com/article/the-path-to-self-soverereign-identity/

BERTELSEN, B. PNUD (2023) Cómo la infraestructura pública digital puede catalizar el desarrollo.
https://apolitical.co/solution-articles/es/como-la-infrastrutura-publica-digital-puede-catalizar-el-desarrollo

CANEPA, S. (2023) ¿Qué es un DID? Una mirada técnica. Fundación IOV.
En: video.

OECD - CAF (2023) Revisión del Gobierno Digital en América Latina y el Caribe: Construyendo Servicios Públicos Inclusivos y Responsivos.

PROYECTO DIDI (2023) Banco Interamericano de Desarrollo (BID) Aprendizajes, resultados y desafíos de la identidad digital auto-gestionada para la inclusión.

SUOMINEN, K. (2019) "El comercio digital en América Latina: ¿qué desafíos enfrentan las empresas y cómo superarlos?", serie Comercio Internacional, N° 145. Santiago, Comisión Económica para América Latina y el Caribe (CEPAL)

WEF (2024) Digital Identity.
https://intelligence.weforum.org/topics/a1G0X000005JJGcUAO

Weidenslaufer, C y Roberts, R (2022) Identidad Digital. Conceptos y legislación.
Biblioteca del Congreso Nacional de Chile.

caf.com
@AgendaCAF