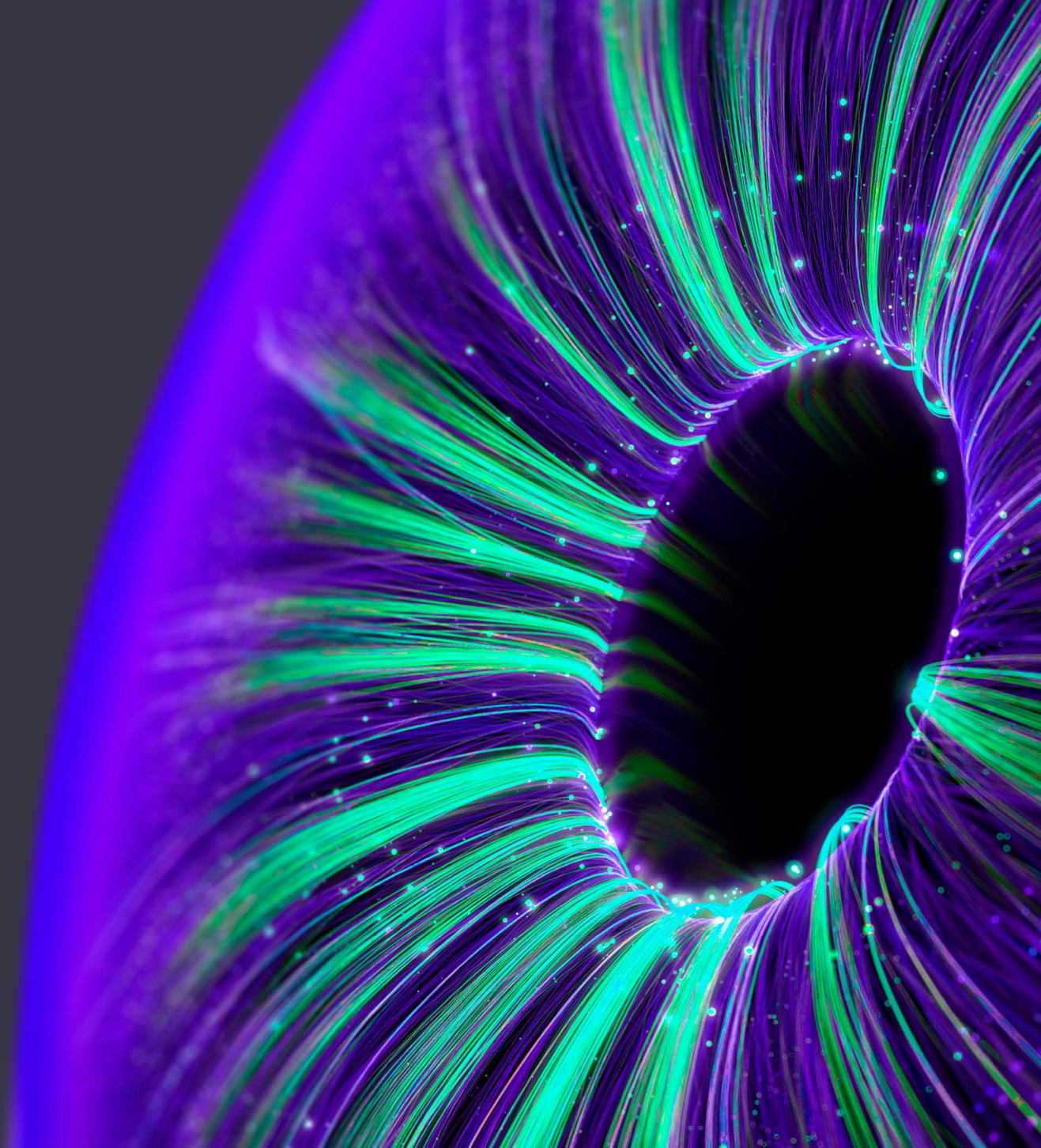
Softtek®

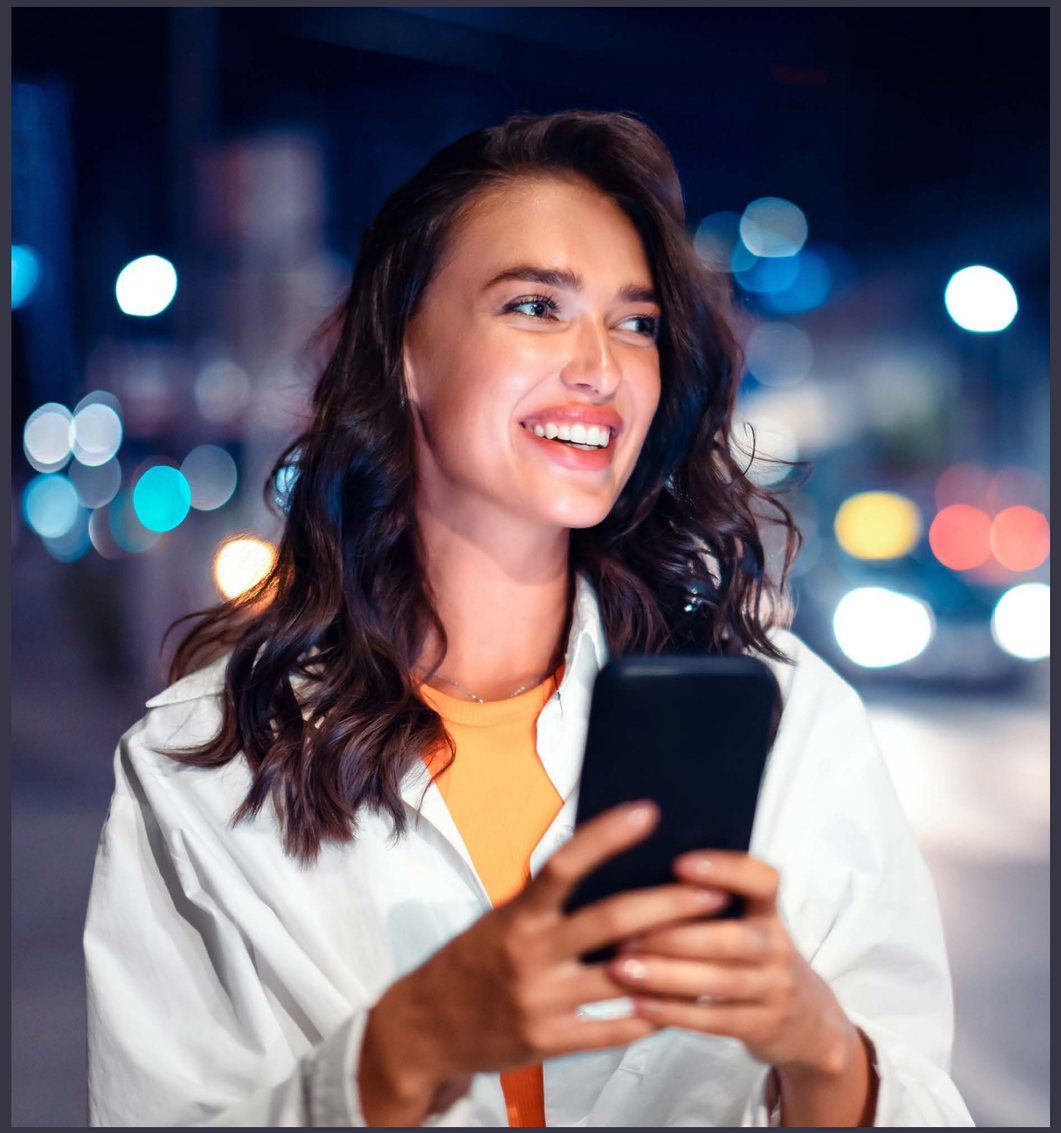
Self-Sovereign Identity: unlocking the future of trust



Índice

01

Security and trust: el fin de la identidad tal y como la conocemos



En los últimos años, la seguridad y privacidad en línea han evolucionado significativamente. Lo que antes era un entorno con poca regulación y control sobre el uso de los datos por parte de las empresas, hoy ha dado paso a **políticas más estrictas de seguridad de datos y a usuarios más conscientes**, que ya pueden decidir cómo y qué información compartir.

No obstante, el camino hacia una mejor privacidad acaba de empezar. Las empresas necesitan una orientación más clara para cumplir con la legislación actual, y las normativas de privacidad deben adaptarse al ritmo acelerado de la industria digital. **Aprovechar estas oportunidades de mejora será clave para ganar la confianza del cliente y mantener una ventaja competitiva.**

En este sentido, **la identidad digital autogobernada (*Self-Sovereign Identity*, SSI)** ha emergido como un modelo revolucionario que otorga a los individuos el control total sobre sus identidades digitales. Su enfoque aspira a reducir los riesgos de filtraciones de datos, al mismo tiempo que refuerza la privacidad y la autonomía. Además, promueve la interoperabilidad entre plataformas, permitiendo que los usuarios verifiquen su identidad de manera segura en diferentes contextos, sin necesidad de depender de terceros. Se trata, por tanto, de un modelo de gestión de identidades digitales en el que **individuos y empresas tienen la propiedad exclusiva sobre sus credenciales personales.**

Desde una perspectiva ética, la existencia de los sistemas SSI está impulsada por **el derecho de los individuos a representarse a sí mismos**, mientras que los sistemas de identidad tradicionales a menudo operan bajo la obligación de que las personas sean identificadas, reforzando un enfoque de gestión de identidad *top-down*.

En efecto, el SSI pone al **usuario en control de sus propios datos**, pudiendo almacenarlos en sus dispositivos y proporcionarlos para verificación y transacciones sin necesidad de depender de un repositorio central de datos. En esta línea, la identidad digital autogobernada otorga a los usuarios la capacidad de **decidir qué información compartir, con quién, en qué contexto y por cuánto tiempo.**

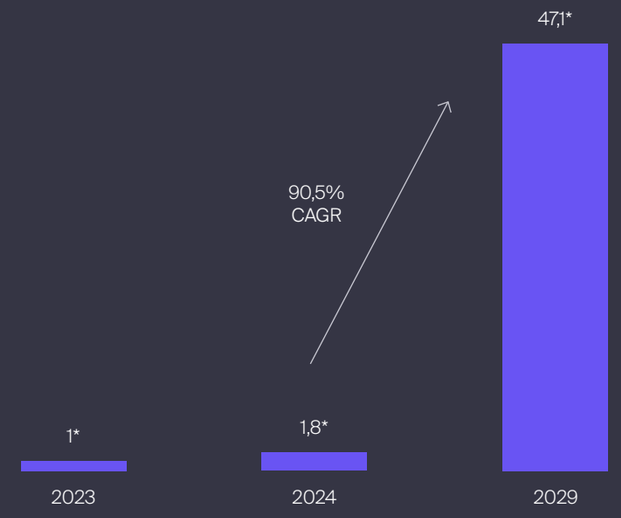
El mercado global de SSI

~$1.000M

Tamaño del mercado global de SSI en 2023

90,5%

CAGR del mercado global de SSI entre 2024 y 2029



*En miles de millones de dólares estadounidenses

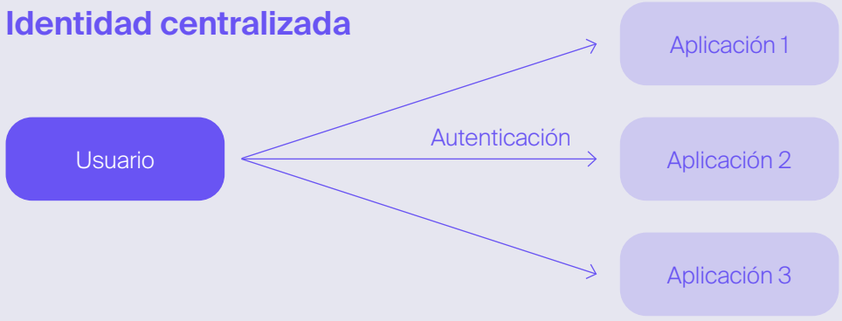
Modelos tradicionales: ¿Centralizada o Federada?

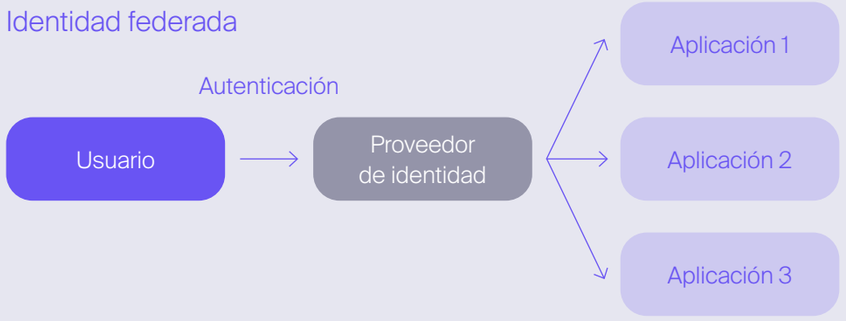
Los modelos tradicionales de gestión de identidad, tanto centralizados como federados, han dominado durante mucho tiempo la forma en que los usuarios acceden a servicios y aplicaciones. Por un lado, en el **modelo centralizado**, los datos de identidad personal se almacenan en bases de datos controladas por distintos proveedores de servicios, lo que aumenta los riesgos de seguridad y privacidad.

Cada servicio tiene su propio sistema de autenticación, lo que obliga a los usuarios a gestionar múltiples credenciales y exponerse a vulnerabilidades, como el robo de contraseñas o fugas de información a través de almacenamiento centralizado.

Por otro lado, **la gestión federada de identidad** surgió como una solución para simplificar la experiencia del usuario mediante el inicio de sesión único (SSO), permitiendo acceder a múltiples servicios con una sola credencial gestionada por un proveedor de identidad, como Google o Facebook. Sin embargo, aunque mejora la comodidad y ofrece autenticación robusta, este modelo sigue planteando problemas, ya que **transfiere el control de la identidad a terceros.**

A pesar de las ventajas que ofrecieron en su momento, tanto los modelos centralizados como los federados han demostrado numerosas vulnerabilidades. En este contexto, estos métodos han quedado atrás frente a **nuevas alternativas más seguras, interoperables y centradas en el usuario**, que buscan devolver a las personas el control total sobre su identidad digital.





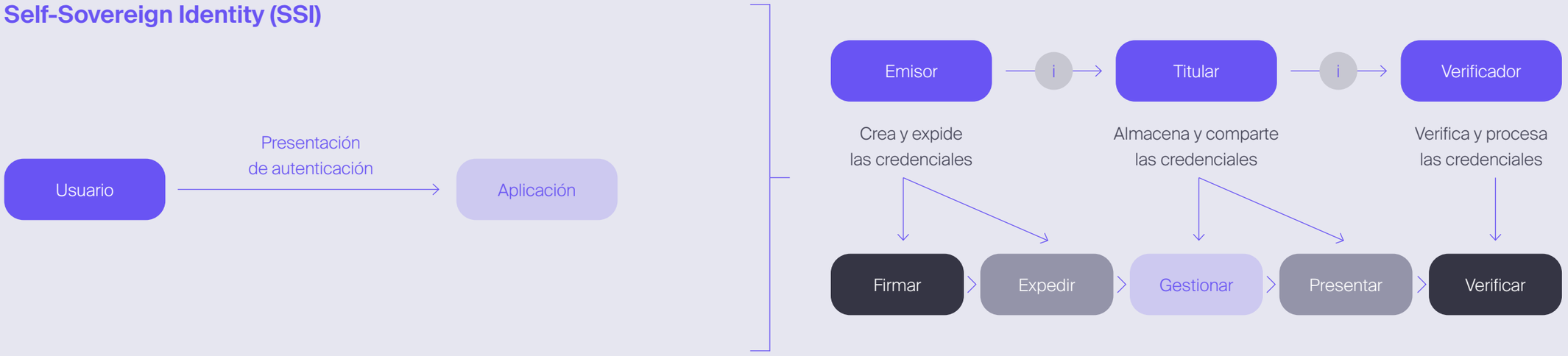
A diferencia de los sistemas tradicionales donde los datos son almacenados y gestionados por terceros, **los individuos pasan a tener plena autoridad y control sobre su identidad con la SSI**. En este sentido, los sistemas de identidad autogobernada son típicamente descentralizados, basados en tecnología Blockchain y, por tanto, eliminando cualquier autoridad centralizada.

La **SSI simplifica la experiencia del usuario al permitir compartir datos de manera sencilla,** reemplazando los métodos tradicionales como formularios o cargas por interacciones de un solo clic. Gracias a su arquitectura centrada en el usuario, ofrece un **control total sobre el almacenamiento, acceso y portabilidad de los datos**, brindando independencia al no estar limitados por plataformas específicas. Además, fomenta interacciones de confianza, ya que **permite la verificación de datos para prevenir fraudes e identidad falsa.** SSI también mejora la seguridad al mitigar riesgos de filtración de datos eliminando contraseñas y almacenamiento centralizado, y garantiza la privacidad mediante técnicas de minimización de datos como la divulgación selectiva.

SSI también supone un paso adelante para las empresas, ya que **pueden ofrecer a sus *stakeholders* un acceso más fluido a servicios o productos**, lo que se traduce en mayores tasas de conversión, menos solicitudes al servicio de atención y una mayor satisfacción general.

SSI permite a las organizaciones **recibir datos confiables y verificados por terceros de confianza**, mejorando la calidad de los datos. Además, ayuda a prevenir comportamientos maliciosos como el spam, el robo de identidad y la falsificación de documentos. SSI también **refuerza la seguridad al eliminar factores de riesgo como contraseñas y almacenamiento de datos centralizado**, y garantiza el cumplimiento de normativas de privacidad y protección de datos gracias a su gestión centrada en el usuario y el consentimiento.

Self-Sovereign Identity (SSI)



El gran reto: seguridad, privacidad y confianza

A fecha de julio de 2024, el porcentaje de población mundial que tiene acceso a Internet alcanzó el 67,1%, y el 63,7% tenía perfiles en redes sociales. Este crecimiento de la exposición de las personas en espacios en línea es paralelo a un aumento de su riesgo. De hecho, **casi 7 de cada 10 adultos** (68%) **en todo el mundo se sentían más vulnerables al robo de identidad** en 2022 en comparación con años anteriores. Por su parte, **el 57% de los usuarios de internet** a nivel global consideraban en enero de 2023 que era **imposible proteger su privacidad online.**

En esta línea, **el 30,7% de los internautas globales afirmaban estar preocupados por el uso indebido de sus datos personales** en el primer trimestre de 2024. A fecha de enero de 2023, el 83% afirmó que les gustaría hacer más para proteger su privacidad y el 70% decidió tomar al menos una medida para remediar esa inseguridad.

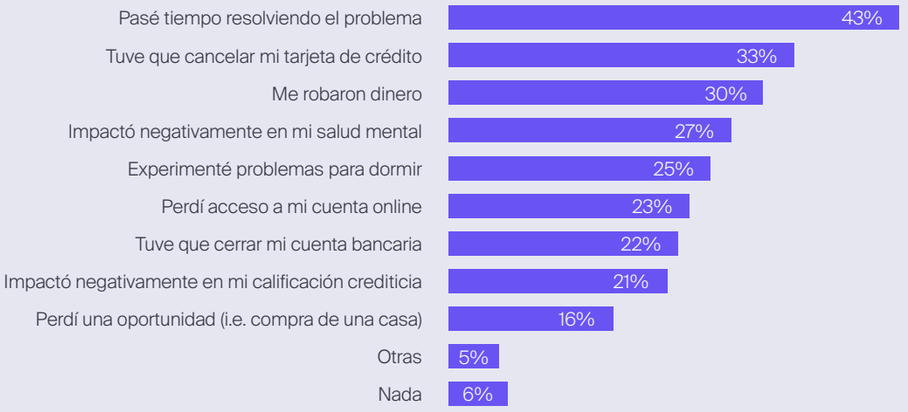
63%

Internautas **dispuestos a aceptar riesgos** para su privacidad en línea por **comodidad**, a fecha de enero de 2023

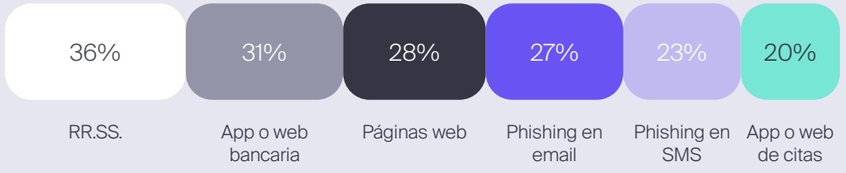
3.500M

Horas empleadas por **víctimas de delitos informáticos** en 2022 para resolver problemas relativos a los delitos

El 94% de los usuarios que experimentaron un robo de identidad online en 2022 sufrieron alguno de los siguientes impactos



La mayoría de los delitos informáticos se gestaron en apps o páginas web



A pesar del desconocimiento, los internautas toman cada vez más medidas para proteger su identidad online

Si bien abunda el **desconocimiento sobre la privacidad de los datos online**, los ciudadanos están tomando conciencia progresivamente sobre la necesidad de educarse en este asunto para garantizar el control y resiliencia de su información personal. En este sentido, frente al aumento de los delitos cibernéticos y filtraciones de datos, los internautas están implementando medidas para proteger su identidad. En 2023, el 36% de los usuarios utilizaba controles parentales, 20% había activado la autenticación multifactor, 28% había cambiado la configuración de privacidad por defecto de sus dispositivos, y **hasta el 27% había utilizado ya un servicio de protección contra el robo de identidad.**

La mayoría de los adultos no tienen conocimientos sobre los robos de identidad online, y carecen de las herramientas para hacer frente a potenciales robos

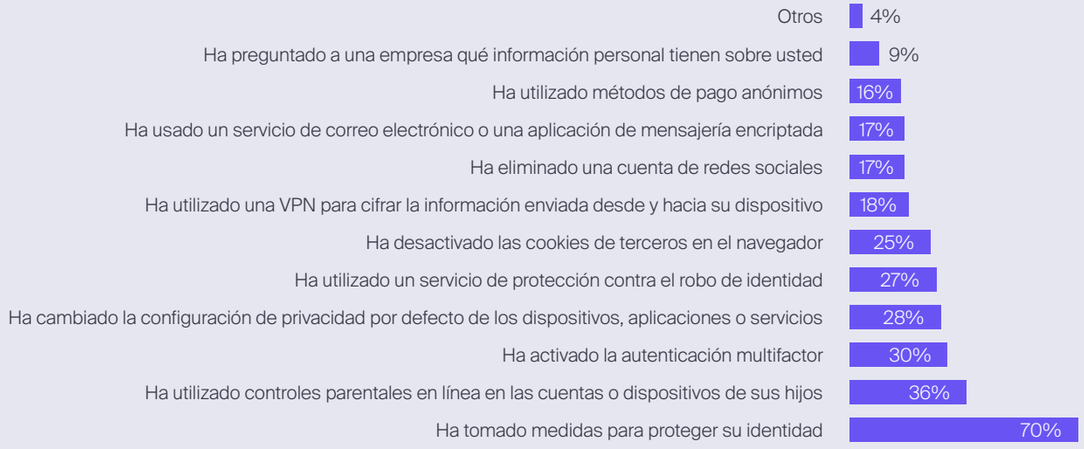
Internautas desconocen cómo comprobar si han robado su identidad

Internautas no sabrían qué hacer si robaran su identidad

Internautas no han considerado que podrían haber sido víctimas de robos de su identidad

Internautas no saben qué es un robo de identidad online

Siete de cada diez internautas han tomado alguna medida para proteger su identidad online



02

The user in control: Self-Sovereign Identity (SSI) redefine las reglas

La SSI tiene el potencial de remodelar la identidad digital y poner al usuario en el centro del sistema. Con ese foco, hay diversos factores que impulsan su desarrollo y adopción:

Privacidad y protección de datos

Los ciudadanos están cada vez más preocupados por la privacidad y la seguridad de sus datos personales. La SSI ofrece una forma de mantener el control sobre la propia información de identidad, reduciendo el riesgo de filtraciones de datos y accesos no autorizados al minimizar la dependencia de bases de datos centralizadas. En esta línea, debe protegerse el derecho a la intimidad de las personas.

Seguridad y confianza

Los sistemas de identidad centralizados son vulnerables a delitos informáticos y usurpación de identidad. SSI utiliza técnicas criptográficas y redes descentralizadas, como Blockchain, para mejorar la seguridad y generar confianza garantizando que los datos de identidad sean a prueba de manipulaciones y verificables.

Enfoque centrado en el usuario

SSI sitúa al individuo en el centro del proceso de gestión de identidades, permitiéndole decidir qué aspectos de su identidad compartir y con quién. Permite a los individuos crear identidades portátiles que pueden utilizarse en diversos contextos y plataformas, fomentando la comodidad y la autonomía del usuario.

Cumplimiento de la normativa

Diversas normativas, como el Reglamento General de Protección de Datos (RGPD) de la UE, hacen hincapié en los derechos de los datos individuales y el consentimiento. SSI se alinea con estas regulaciones al proporcionar a los individuos un mayor control sobre sus datos personales, facilitando el cumplimiento de los requisitos de privacidad y consentimiento.

Beneficios empresariales y económicos

SSI puede ofrecer un ahorro de costes para las organizaciones al reducir la necesidad de procesos de verificación de identidad, almacenamiento de datos y cumplimiento de complejas normativas de identidad. También puede permitir nuevos modelos de negocio, como los servicios basados en la identidad y las aplicaciones descentralizadas.

Autonomía, control y portabilidad

La privacidad de los datos y la seguridad constituyen el núcleo central de la identidad digital autogobernada, si bien también orbitan en torno a esta otra serie de principios como la transparencia, el consentimiento, la persistencia, o la minimización. Prevalecen especialmente los conceptos de **autonomía, control y portabilidad,** fundamentados en el empoderamiento del individuo para gestionar su propia identidad sin depender de intermediarios centralizados.

En primer lugar, **la autonomía hace referencia al hecho de que el individuo, propietario de sus datos, tiene libertad para elegir los datos que comparte.** Este principio permite a los usuarios tener propiedad completa sobre sus credenciales digitales, almacenándolas de manera segura en sus dispositivos personales. Este enfoque descentralizado elimina la necesidad de que terceros controlen o almacenen la información personal de los usuarios, minimizando riesgos de fugas y filtraciones de datos y ataques cibernéticos.

En segundo lugar, **el control se refiere a la capacidad del individuo para decidir qué datos compartir, con quién y en qué contexto.** Este principio se encuentra estrechamente vinculado a otro, **el acceso**, ya que el individuo debe poder acceder a todos sus propios datos. Gracias a la arquitectura SSI, los usuarios pueden seleccionar de manera granular qué información revelan en cada interacción, evitando la divulgación excesiva de datos. Además, este control se extiende al poder revocar el acceso a terceros en cualquier momento, lo que refuerza la seguridad y privacidad de la identidad digital.

Finalmente, **la portabilidad es otro aspecto clave**, ya que el individuo debe poder transportar su información y credenciales en su wallet digital, sin estar restringidas a plataformas concretas y **sin necesidad de duplicar datos o crear nuevas cuentas** para cada servicio. Junto a la portabilidad surge precisamente la **interoperabilidad**, ya que la **SSI** promueve normas y protocolos abiertos, reduciendo la redundancia y simplificando los procesos de verificación de la identidad. En definitiva, las credenciales deben poder ser utilizadas lo más ampliamente posible por las distintas partes interesadas. Las organizaciones, las bases de datos y los registros deben poder comunicarse entre sí de forma rápida y eficaz a escala mundial a través de un sistema de identidad digital.

Existen otros principios que informan la SSI y garantizan que el usuario tenga el control sobre sus datos:

- **Transparencia**
  La forma en que se gestionan y actualizan los sistemas de identidad debe estar a disposición del público y ser razonablemente comprensible.

- **Consentimiento**
  En un proceso interactivo e informado, el usuario otorga el consentimiento explícito para el uso de sus datos en cada caso.

- **Minimización**
  Las personas deben poder compartir la menor cantidad posible de datos necesaria, evitando el intercambio de información excesiva.

- **Persistencia**
  Los datos de identidad deben ser duraderos, afincados en infraestructuras resilientes y modelos sostenibles.

La regulación, un driver clave: eSSIF, eIDAS 2 y GDPR

Europa es una de las regiones más avanzadas en la regulación de temas relacionados con la identidad digital y la privacidad, y varias normativas concretas impactan el desarrollo de la SSI: **el reglamento GDPR, el reglamento eIDAS o la iniciativa ESSIF**, respaldada por la European Blockchain Service Infrastructure (EBSI).

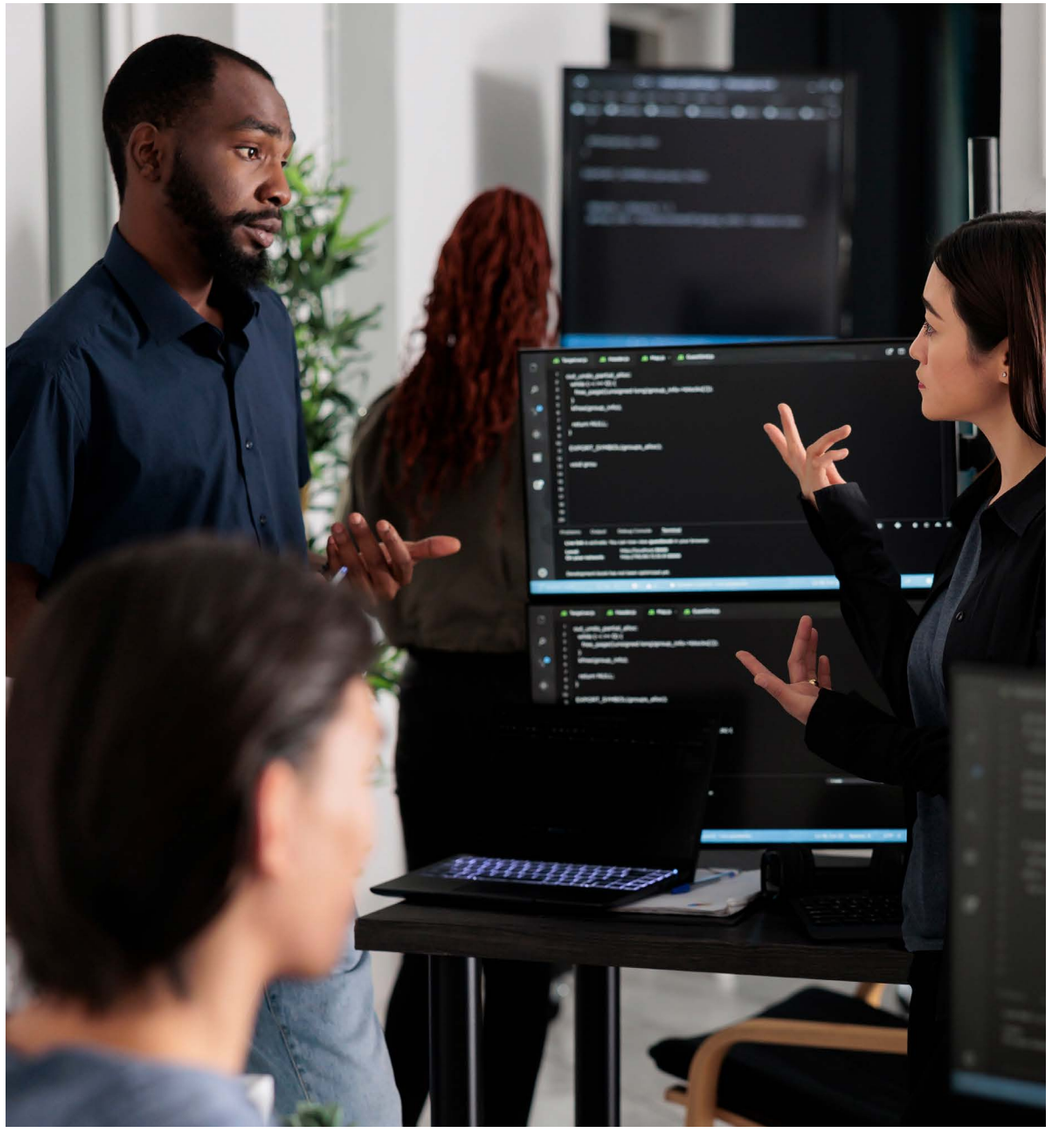
Reglamento General de Protección de Datos (GDPR)

Determina que **el control sobre los datos personales recae en el individuo**, lo que refuerza la idea de que cada persona debe tener el poder de gestionar, controlar y decidir quién puede acceder a su información.

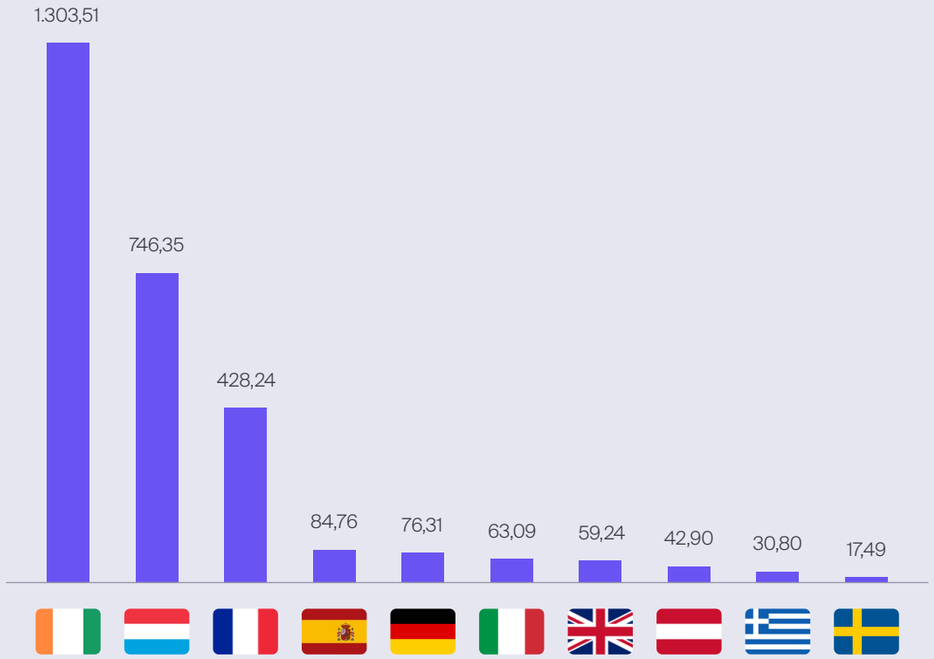
Establece **principios de privacidad**, como el derecho al olvido y la portabilidad de los datos, que son clave para el desarrollo de SSI.

Exige un **consentimiento claro y explícito** para el procesamiento de datos, alineándose con el principio de la SSI de que los individuos deben dar su consentimiento antes de compartir sus datos.

El **principio de minimización de datos** asegura que solo se recojan los datos necesarios, una idea que la SSI respalda, ya que permite a los usuarios compartir únicamente la información estrictamente necesaria.



Valor agregado de las multas GDPR impuestas en Europa entre mayo de 2018 y enero de 2023 (expresado en millones de euros)



€4.884M

Volumen total de las multas GDPR en toda la UE en septiembre 2024

Multas impuestas por infracciones GDPR entre mayo de 2018 y mayo de 2023 (expresado en millones de euros)

El eIDAS 2, actualización del eIDAS, establece un marco jurídico para la identificación, autenticación y firma electrónica. La normativa está destinada a **mejorar la seguridad de las transacciones digitales y los servicios de identificación** en todos los Estados miembros de la UE. Introduce un monedero europeo de identidad digital que permite a los ciudadanos controlar sus datos de identidad y utilizarlos para servicios públicos y privados. A diferencia del eIDAS, que cubría principalmente la firma electrónica y los servicios de confianza, el eIDAS 2 se centra en aplicaciones más amplias, como el reconocimiento transfronterizo de credenciales digitales y características de seguridad más sólidas, con el objetivo de lograr una mayor adopción en toda la UE.

Electronic Identification and Trust Services (eIDAS)

Reglamento establecido para la **creación de una identidad digital reconocida legalmente** en todos los estados miembros de la UE, reforzando la interoperabilidad.

Fomenta el desarrollo de un **marco tecnológicamente neutro** que no favorezca ninguna solución técnica concreta para la implantación de la identificación electrónica.

Establece un marco jurídico claro para que **las personas, las empresas y las administraciones públicas** puedan acceder a los servicios y realizar transacciones en línea de forma segura.

eIDAS **regula los servicios de confianza** (servicios de entrega electrónica registrada, ERDS), como firmas digitales y sellos electrónicos, lo que garantiza que los datos e identidades verificadas bajo un sistema SSI cumplan con los requisitos legales y de seguridad.

Cronología de la implementación del eIDAS 2 en la Unión Europea

2024

Adopción de eIDAS 2

Adopción en febrero de 2024 por el Parlamento Europeo.

Adopción de actos de ejecución en octubre de 2024.

2025

Pruebas piloto

Empresas y gobiernos de la UE deben llevar a cabo pruebas piloto de e-wallets de identidad para anticipar la implementación obligatoria. (Abril 2024 – Diciembre 2025)

2026

Propuesta de EUDI Wallet

Los Estados deben proponer al menos un EUDI Wallet para todos los ciudadanos 24 meses después de los actos de ejecución.

2027

Aceptación de EUDI Wallet

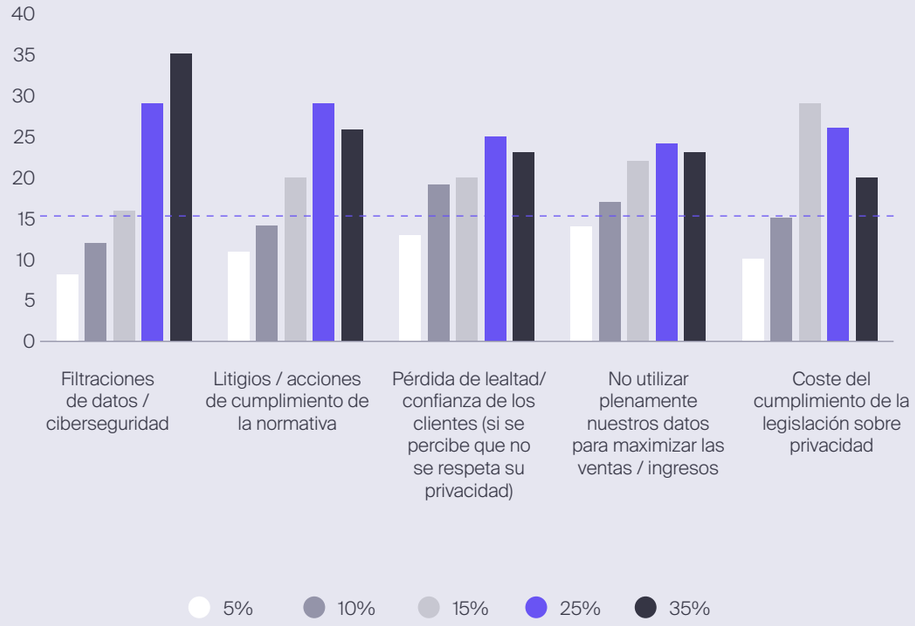
Los servicios privados y públicos deben aceptar el EUDI Wallet 36 meses después de los actos de ejecución.

2030

80% de ciudadanos con e-wallet

El objetivo de la Comisión Europea es que el 80% de los ciudadanos europeos tengan una e-wallet de identidad para 2030.

Nivel de preocupación entre las organizaciones de Estados Unidos y el Reino Unido en relación con determinadas cuestiones de privacidad de datos en mayo de 2023



La falta de regulación extracomunitaria podría lastrar el avance de SSI

Más allá de la Unión Europea, escasean los marcos regulatorios integrales y facilitadores del desarrollo de los sistemas SSI. En **Reino Unido**, el heredado UK GDPR regula la privacidad de los datos, pero no existe un marco específico para SSI, más allá de marcos de confianza como el *UK Digital Identity and Attributes Trust Framework.*

En **Estados Unidos**, por ejemplo, tampoco existe una regulación específica a nivel federal, más allá de la propuesta de ley *Digital Identity Act*. Existen algunas iniciativas estatales en Wyoming, donde se han aprobado leyes que reconocen la identidad digital y los *smart contracts,* en Illinois, donde se ha lanzado un programa piloto para explorar el uso de la tecnología Blockchain en la gestión de identidades, o en California, con la Ley de Privacidad del Consumidor de California (CCPA), que otorga derechos a los consumidores sobre el acceso y control de sus datos personales, similares al GDPR en Europa.

En **Canadá**, donde tampoco hay una regulación específica, el *Pan-Canadian Trust Framework,* liderado por el *Digital ID and Authentication Council of Canada (DIACC)*, es una guía para la adopción de tecnologías de identidad digital, incluidas soluciones basadas en SSI. Además, Canadá cuenta con leyes de protección de datos como la *Personal Information Protection and Electronic Documents Act (PIPEDA)*, que establece principios para la recolección y uso de información personal por parte de organizaciones privadas. Por su parte, el **parlamento australiano** adoptaba la Digital ID Bill en mayo de 2024, prevista para ser implementada en noviembre. La ley introduce un sistema nacional de Identificación Digital, con medidas estrictas de privacidad y seguridad, participación voluntaria y almacenamiento local de datos, para agilizar las transacciones en línea y garantizar la protección de la información personal.

Fuera de la UE, hay escasez regulatoria. En EE.UU. o Reino Unido las principales empresas se preocupan especialmente por las posibles filtraciones de datos y los litigios en materia de privacidad

Key actors: emisores, verificadores y titulares

En el contexto de SSI existen tres actores que interactúan en el sistema:

1. Titulares (*Holders*)

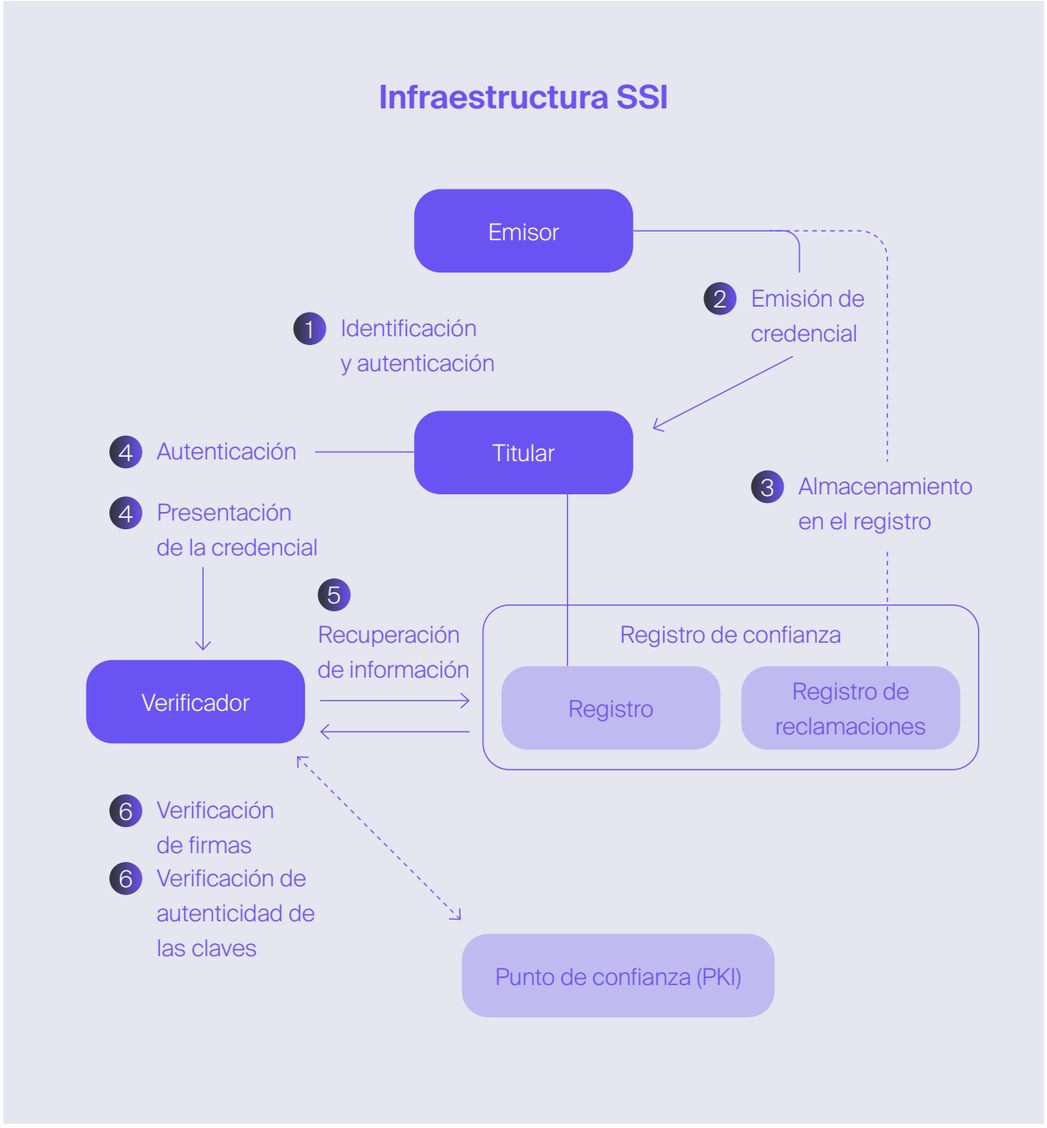
Los individuos u organizaciones que poseen y controlan su propia identidad digital. Estos titulares tienen la capacidad de **almacenar y gestionar sus credenciales** en dispositivos seguros, y decidir cuándo y con quién compartir su información. Ellos son dueños de sus datos, y pueden ofrecer pruebas de su identidad de manera descentralizada, sin depender de intermediarios.

2. Emisores (*Issuers*)

Las entidades que crean y emiten credenciales verificables a los titulares. Estas credenciales pueden ser cualquier tipo de documento o certificación digital. Los emisores son **responsables de garantizar la autenticidad y veracidad** de las credenciales que emiten.

3. Verificadores (*Verifiers*)

Las entidades que reciben, revisan y validan las credenciales que los titulares comparten. Utilizan mecanismos criptográficos para **verificar la autenticidad de las credenciales** sin necesidad de comunicarse directamente con el emisor y manteniendo la privacidad del titular.



Blockchain, DID, VC y criptografía: el *toolkit* tecnológico de SSI

La tecnología detrás de SSI se apoya en **tecnología Blockchain y DLT** (*distributed ledgers*), lo que permite a los usuarios crear identidades digitales seguras y verificables, protegidas criptográficamente. Mediante el uso de pares de claves públicas y privadas, los datos pueden ser firmados y cifrados, permitiendo compartir información de manera selectiva y segura.

En resumen, en la SSI interactúan varios conceptos tecnológicos esenciales que garantizan la seguridad, el control y la privacidad de la identidad digital:

- **Registros de confianza** (*trust registries*)
  Actúan como una "capa de confianza" compartida, donde se registra información confiable, como referencias a credenciales o emisores autorizados. Aunque no almacenan datos personales, estos registros aseguran que las interacciones y verificaciones se realicen con entidades confiables, sin depender de un tercero centralizado.

- **Claves criptográficas**
  Las claves criptográficas, tanto públicas como privadas, son fundamentales para el control de identidades en SSI. Permiten autenticar al usuario y cifrar la información que se comparte. La clave privada, en manos del usuario, asegura que solo él tenga control sobre su identidad, mientras que la clave pública permite a terceros verificar su autenticidad.

- **Identificadores descentralizados (DID)**
  Los DID son identificadores únicos y descentralizados que no dependen de ninguna autoridad central. Están vinculados a claves criptográficas y permiten que distintas partes interactúen entre sí de forma segura. Estos identificadores son la base de la infraestructura de clave pública en SSI, ya que conectan las identidades digitales con las claves criptográficas de forma descentralizada.

Blockchain, DID, VC y criptografía: el toolkit tecnológico de SSI

- **Credenciales verificables (VC)**
  Las credenciales verificables son documentos digitales que pueden ser compartidos y verificados fácilmente por cualquier entidad. Permiten comprobar su validez, integridad y autenticidad sin comprometer la privacidad del usuario. Es importante destacar que estas credenciales no se almacenan en una cadena de bloques, lo que protege la privacidad y asegura el cumplimiento normativo.

- **Wallets o carteras digitales**
  Las carteras digitales o wallets son aplicaciones que almacenan las claves criptográficas y las credenciales verificables. Estas wallets permiten al usuario gestionar su identidad digital y compartir credenciales de forma segura y controlada, manteniendo siempre el control sobre qué datos compartir y con quién.

En definitiva, estos elementos tecnológicos trabajan en conjunto para proporcionar **un sistema de identidad digital seguro, descentralizado y centrado en el usuario.** El uso de registros de confianza, claves criptográficas, DID, credenciales verificables y wallets asegura la privacidad y autonomía del usuario en cada interacción.

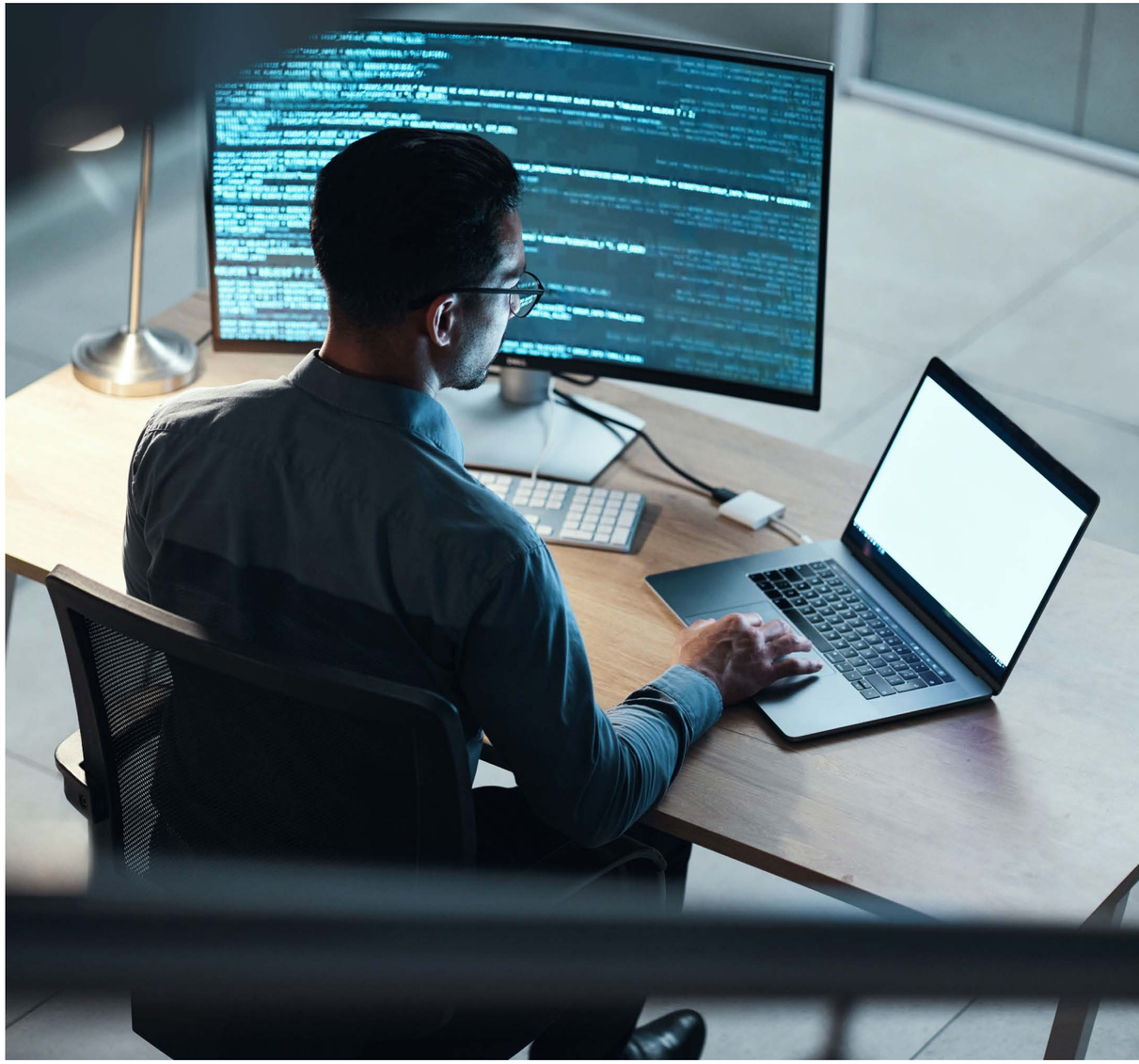
En 2025 se estima que **el 20% del total** de la identificación digital se realizará con **tecnología DLT/ Blockchain**, frente al 5% de 2020.

Eficiencia operativa
vs. escalabilidad

Ventajas de SSI

Los sistemas de SSI ofrecen importantes **beneficios, impactando positivamente en la eficiencia operativa, la confianza del cliente y el cumplimiento normativo.** Al eliminar contraseñas y formularios, **SSI simplifica la autenticación**, lo que reduce la carga en el servicio de asistencia al cliente y mejora las tasas de conversión, eliminando fricciones en la experiencia del usuario. Además, los datos compartidos mediante SSI son verificados por entidades de confianza, como gobiernos, lo que reduce significativamente el riesgo de fraude y suplantación de identidad.

En cuanto al cumplimiento normativo, **SSI facilita la conformidad con regulaciones de protección de datos**, al ofrecer una gestión de identidades centrada en la privacidad del usuario. Esto refuerza la confianza entre empresas y usuarios, al asegurar que solo se compartan los datos necesarios. Otro beneficio clave es **la reducción del riesgo de violaciones de seguridad y filtraciones de datos, puesto que, al descentralizar la gestión de datos**, las organizaciones disminuyen su exposición a ciberataques y reducen los costos asociados a la protección de información, lo que convierte a SSI en una solución atractiva y segura para empresas y usuarios.



Desafíos de SSI

A pesar de los múltiples beneficios de los sistemas de SSI, estos presentan importantes desafíos, principalmente relacionados con la **interoperabilidad y la seguridad.** La falta de interoperabilidad entre las diferentes plataformas y aplicaciones de SSI puede fragmentar el ecosistema, obligando a usuarios y empresas a gestionar sus identidades digitales en múltiples sistemas. Esto dificulta la adopción masiva de SSI, ya que **requiere la creación de estándares compartidos y una confianza mutua entre diversas jurisdicciones y plataformas**. Además, los usuarios asumen una mayor responsabilidad sobre la seguridad de sus credenciales, lo que puede generar **riesgos en situaciones de pérdida o fallos en dispositivos como teléfonos móviles,** que son esenciales para verificar sus identidades. La pérdida de acceso, ya sea por un dispositivo dañado o extraviado, puede comprometer la capacidad del usuario para interactuar con los servicios.

El desafío de la escalabilidad va más allá de la interoperabilidad, involucrando también **la capacidad técnica para soportar un número creciente de usuarios y transacciones a gran escala.** Las organizaciones que implementen SSI necesitarán infraestructuras robustas y flexibles que puedan gestionar eficientemente este modelo de identidad sin comprometer la velocidad ni la seguridad del sistema. Para que SSI sea una solución viable a largo plazo, debe **adaptarse a múltiples sectores, desde la salud hasta las finanzas.** Este reto demanda la colaboración estrecha entre desarrolladores, reguladores y empresas para crear un marco común que permita superar los problemas técnicos y asegurar que el sistema pueda escalar de manera efectiva, cumpliendo con la promesa de ofrecer una identidad digital verdaderamente global y autogobernada.

Un futuro que ya está aquí: los casos de Singapur y Estonia

Este marco teórico sobre los sistemas SSI ya ha sido ampliamente testado por gobiernos del mundo. De hecho, este modelo transgresor se ha implementado de manera exitosa en países como **Singapur y Estonia**, donde las tasas de adopción de los sistemas Singpass y e-Residency respectivamente son muy prometedoras. A raíz de estos casos de éxito, numerosas organizaciones están lanzando productos y servicios basados en identidad soberana.

National Digital Identity (NDI) en Singapur

Iniciativa gubernamental que ofrece a ciudadanos y residentes un medio seguro de autenticación en servicios digitales públicos y privados.

- Firma electrónica de documentos públicos y privados con biometría.
- Verificación de identidad en línea para reducir fraude y robos de identidad.
- Acceso digital seguro a servicios gubernamentales, bancarios, de salud y educación.

4,2M Usuarios de la app Singpass

41M Transacciones cada mes

+2,7K Servicios a los que proporciona acceso

e-Residency en Estonia

Programa de identidad digital del gobierno de Estonia lanzado en 2014, legalmente vinculante para ciudadanos y residentes. Cuenta con una tarjeta física para almacenar claves criptográficas.

- Firma de documentos y pagos electrónicos de impuestos.
- Registro de empresas, gestión empresarial y acceso a servicios bancarios globales.
- Autentificación y protección de la identidad y los datos personales en servicios en línea.

96% de la población tiene una tarjeta de identidad válida

+339M Firmas digitales realizadas

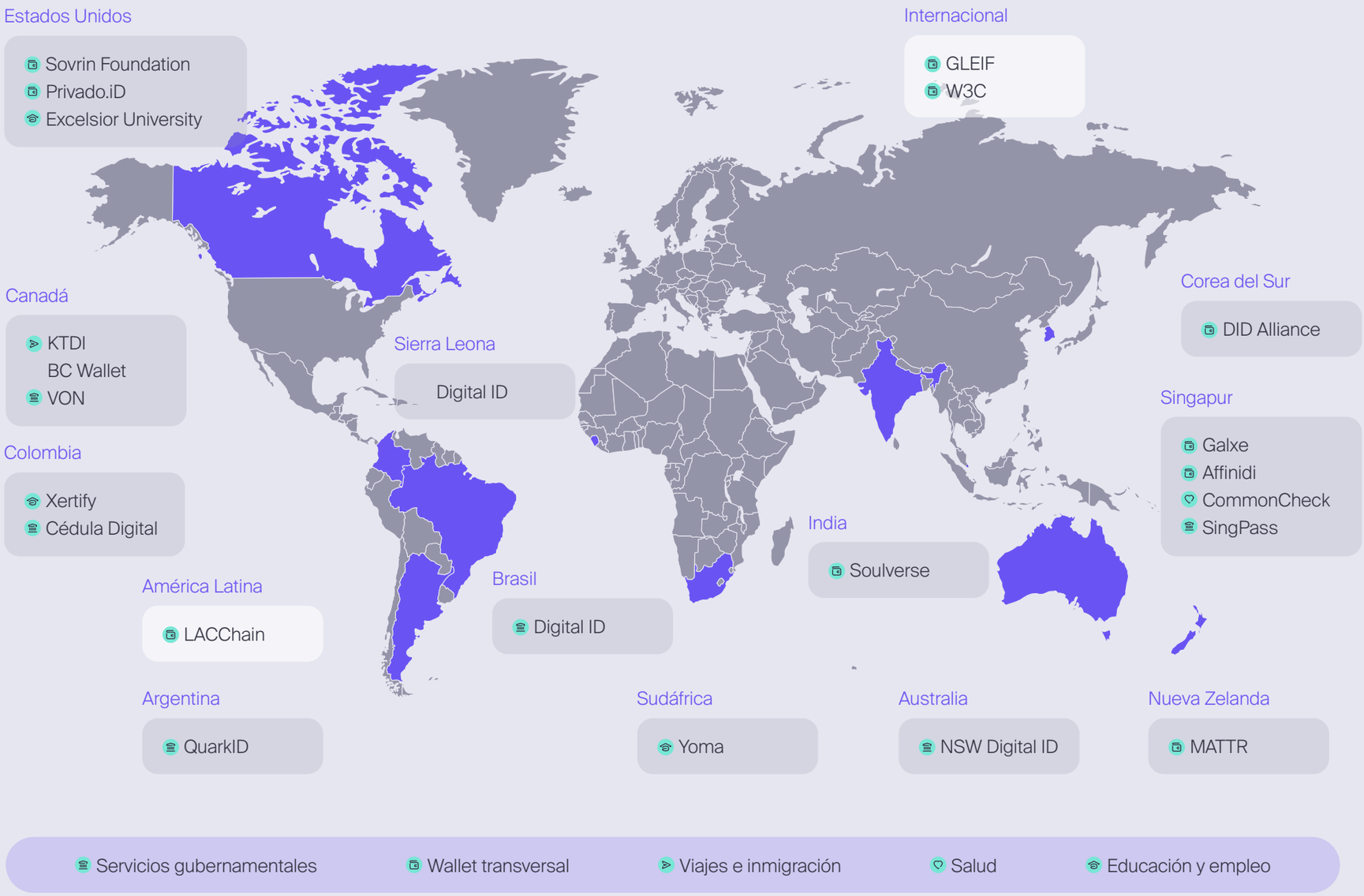
03

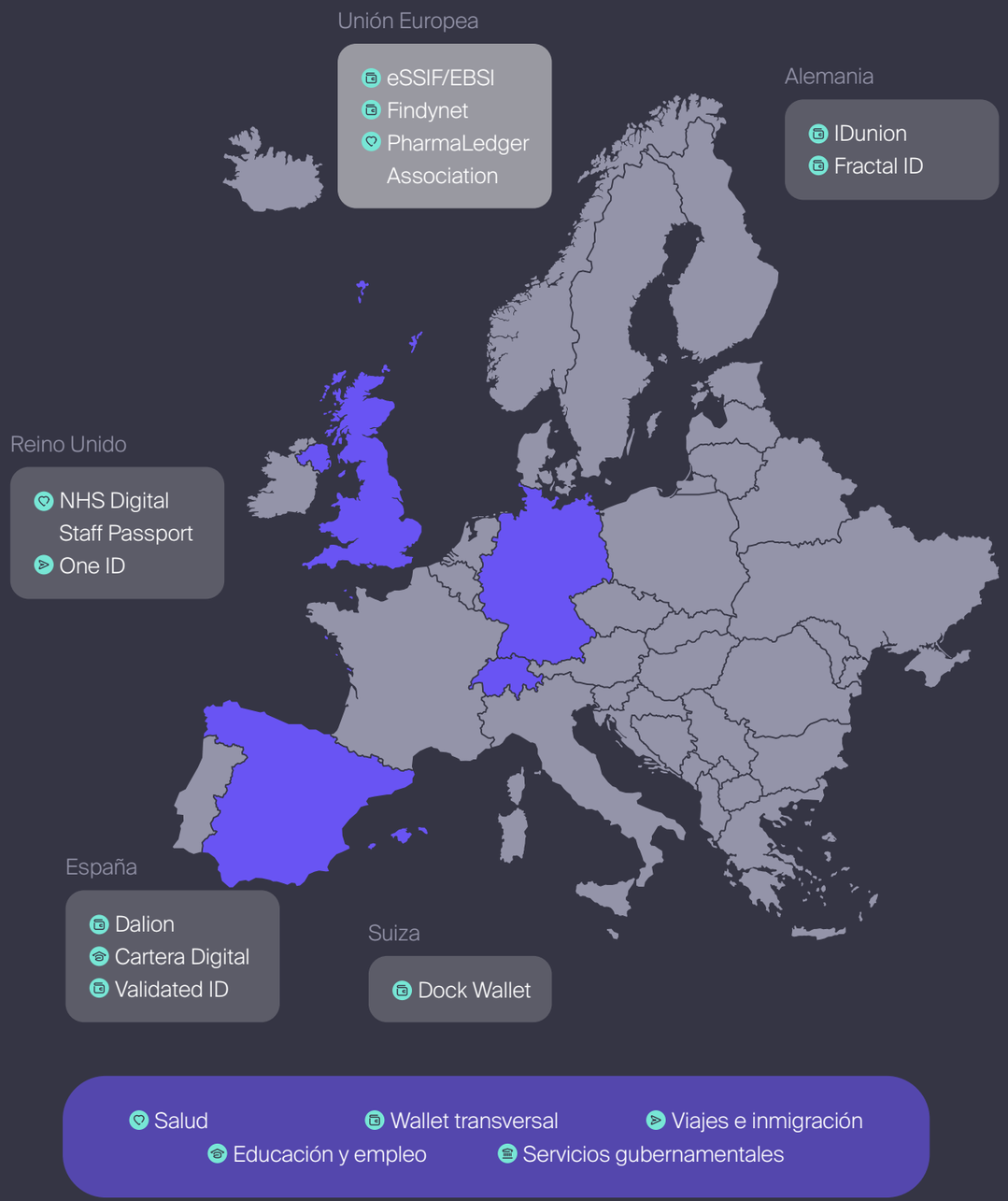
Beyond borders: SSI conquista todos los continentes

Entidades privadas a lo largo del todo el mundo han comenzado a idear e implementar modelos SSI. En Estados Unidos se originó una de las plataformas más reputadas: **Sovrin Foundation.** La fundación dispone de tres redes de SSI, basadas en Hyperledger Indy y cada una está formada por entre 4 y 25 nodos que son operados por los administradores de Sovrin. Además, actúa como Autoridad de Gobierno y opera la red en su conjunto, supervisando y mejorando su rendimiento.

A lo largo de Norteamérica y Sudamérica se encuentran otras iniciativas como la colombiana **Xertify**, con fines educativos, o la argentina **QuarkID**, aplicación de SSI multichain de la ciudad de Buenos Aires cuyo protocolo se encuentra anclado en las redes de zkSync, Ethereum, Polygon y Rootstock. En África y Asia han surgido proyectos como la plataforma sudafricana educativa para jóvenes **Yoma** o el e-wallet indio **Soulverse**. Regionalmente predomina, sin embargo, Singapur, con numerosos proyectos en estado de ejecución.

En última instancia, Australia y Nueva Zelanda se han unido a la ola de SSI a través de proyectos gubernamentales regional (**NSW Digital ID**) o soluciones privadas (**MATTR**).





Europa lidera el cambio: de iniciativas regionales a nacionales

Europa es la región donde mayor número de iniciativas y proyectos sobre SSI han surgido en el mundo. De hecho, es hogar de numerosas colaboraciones público-privadas en los campos de la identificación digital gubernamental, de e-wallets transversales para diversos propósitos, e iniciativas en los ámbitos de la salud, los viajes, o la educación. A nivel regional, la Unión Europea no solo ha sido pionera en materia regulatoria, sino también en el lanzamiento de proyectos prácticos de SSI. **El European Self-Sovereign Identity Framework (eSSIF)** es una iniciativa alineada con el GDPR y el eIDAS 2 de carácter regional. Tiene como objetivo proporcionar a los ciudadanos de la UE un control más directo y seguro sobre su identidad digital, basándose en tecnologías Blockchain para asegurar que las identidades digitales sean verificables y confiables, sin que se necesite una entidad intermediaria. Permite que las identidades sean **interoperables** en toda la Unión Europea, mejorando la transparencia y r**educiendo la burocracia en los procesos administrativos**, como la emisión de documentos y la verificación de credenciales educativas. La implementación comenzará en el **2026** y se espera que para el 2030 el 80% de la población disponga ya de un sistema de identificación europeo. Finalmente, en Europa existen otras iniciativas privadas de ámbito regional como Findynet, que permite al usuario recopilar recibos, tickets, permisos, certificaciones y otras pruebas para facilitar y reforzar las interacciones, o **PharmaLedge**r, que busca crear un ecosistema digital seguro para el ámbito de la salud.

A nivel nacional, destacan proyectos pioneros como **Dalion**, sistema SSI español fruto de un consorcio de empresas privadas basado en el modelo de identidad digital de Alastria, o el alemán **IDunion**, cuyo objetivo es crear un ecosistema global y descentralizado para la gestión de identidades, basado en valores europeos. Por su parte, **One ID** es la iniciativa británica fundada por IATA para agilizar los viajes mediante el intercambio digital anticipado de información, y **Dock Wallet** es la plataforma originaria de Suiza que permite a las organizaciones emitir, gestionar y verificar credenciales de forma eficaz y segura.

04

Cross-sector opportunities: ¿Qué significa SSI para tu industria?

La identidad digital autogobernada ofrece oportunidades transversales que pueden transformar múltiples sectores. En líneas generales, afecta directamente a cinco aspectos:

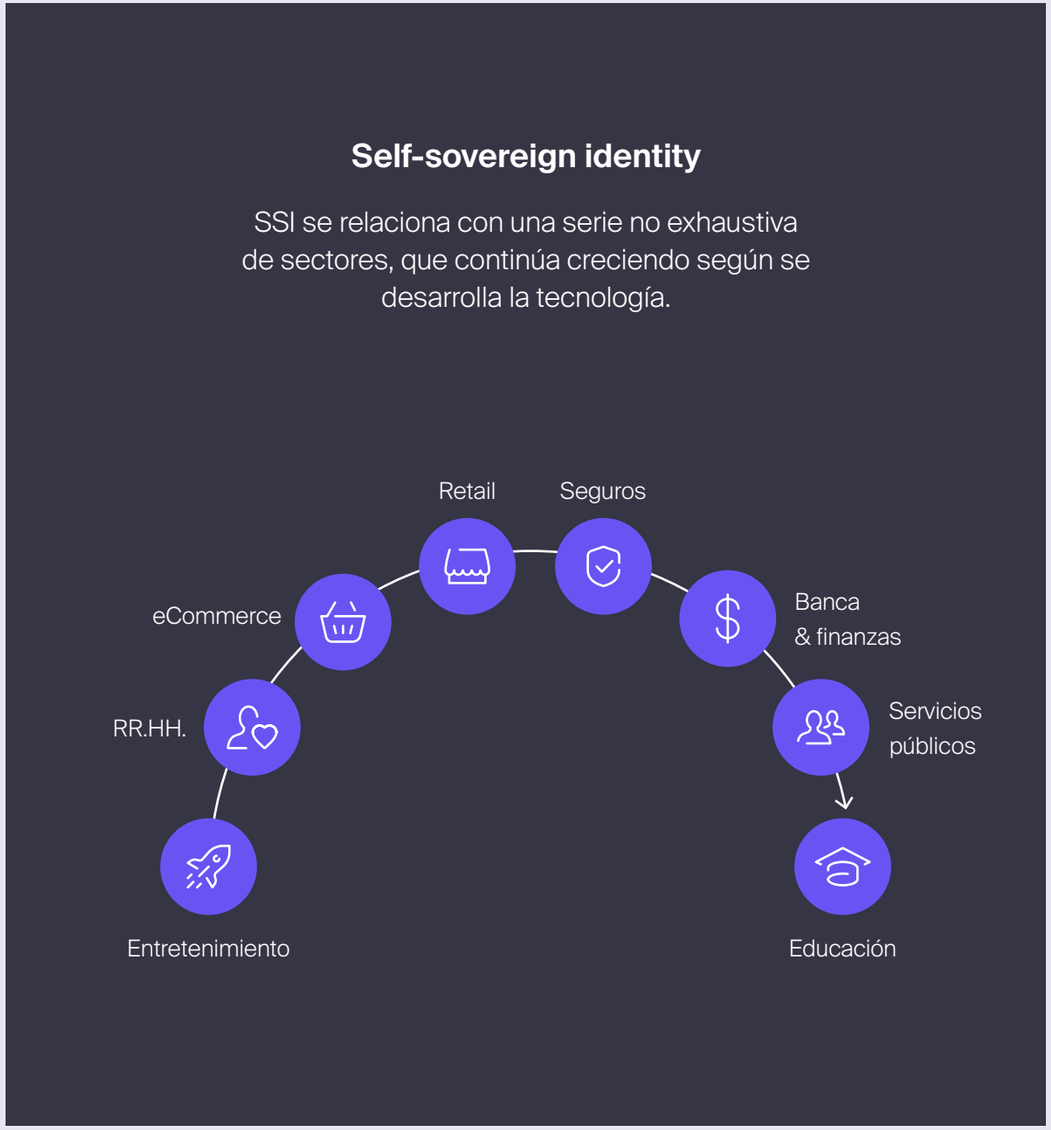
1. **Experiencia del usuario:** SSI puede simplificar los procesos de onboarding de clientes, reemplazando procedimientos complejos con procesos sencillos de un solo clic, mejorando significativamente la experiencia del usuario.

2. **Calidad de datos:** ante posibles problemas de precisión o coherencia de datos debido a errores tipográficos o información incorrecta proporcionada por los clientes, SSI asegura datos de alta calidad, basada en información verificada por terceros de confianza.

3. **Seguridad:** con SSI, las compañías pueden implementar métodos de autenticación más seguros y así minimizar los riesgos mediante el almacenamiento descentralizado y la reducción de datos sensibles.

4. **Privacidad y cumplimiento:** SSI facilita la gestión del consentimiento y automatiza el cumplimiento de las normativas sobre la protección de datos.

5 . **Automatización de procesos:** SSI permite acceder a datos confiables y estructurados, lo que potencia una mejor automatización de los procesos.



Banca y finanzas: la gestión del riesgo y compliance, transformados

En el sector bancario, la identidad digital autogobernada está **revolucionando la gestión del riesgo y el cumplimiento normativo.** Uno de los principales desafíos de la banca es la verificación de la identidad, necesaria tanto en las finanzas centralizadas (CeFi) como descentralizadas (DeFi), donde los procedimientos de verificación del cliente (KYC) suelen ser ineficientes y poco satisfactorios.

SSI proporciona una solución eficaz y respetuosa con la privacidad, creando una capa de identidad que actúa como puente entre los procesos tradicionales, que requieren gran cantidad de datos, y el enfoque anónimo de las finanzas descentralizadas. A diferencia del KYC tradicional, que se utiliza una vez por cada entidad, SSI permite que la información verificada se reutilice de manera segura y auditable, mejorando así la eficiencia y reduciendo el riesgo de fraude. En esta línea, SSI permite a los usuarios controlar completamente sus credenciales verificables.

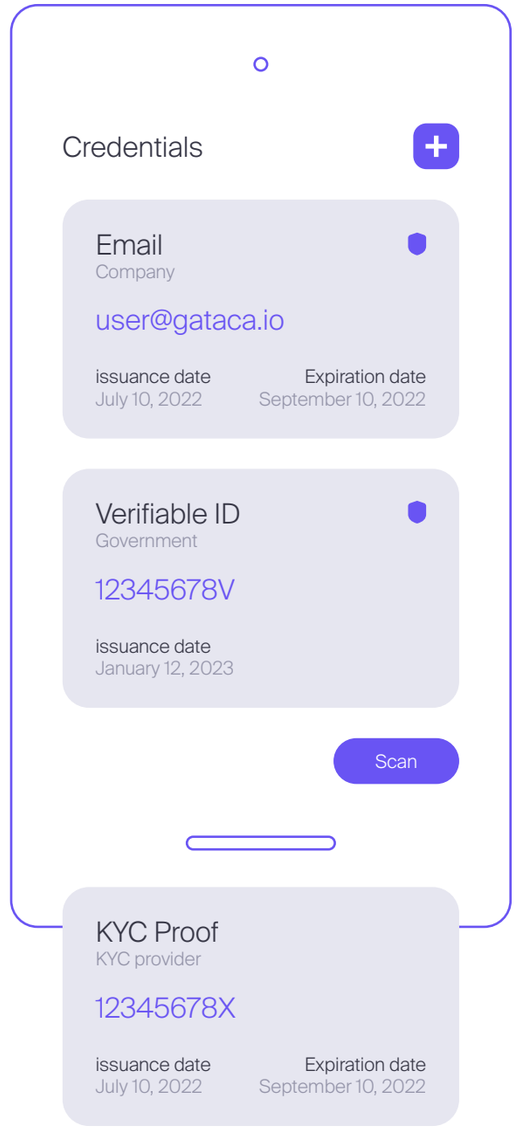
Esto significa que **el cliente solo comparte información estrictamente necesaria, garantizando mayor privacidad, pero sin comprometer la veracidad de los datos**.

Además, SSI introduce un **enfoque reutilizable para el KYC**, lo que evita que los usuarios tengan que repetir el proceso en cada institución o servicio financiero, optimizando así la experiencia de incorporación y fortaleciendo el cumplimiento normativo de manera más ágil y auditable.

En términos de cumplimiento normativo, SSI también facilita la adherencia a normativas como las leyes contra el lavado de dinero (AML) y los procesos de KYC, automatizando y simplificando la verificación de identidad a través de credenciales verificables emitidas por entidades de confianza. Esta tecnología no solo previene el fraude, sino que también permite a las instituciones bancarias reducir el riesgo crediticio mediante la validación instantánea de fondos y la evaluación precisa de riesgos.

Al proporcionar información personal rastreable y auditable, SSI garantiza que las instituciones puedan cumplir con los requisitos regulatorios sin comprometer la privacidad del cliente.

Asimismo, **SSI mejora la eficiencia operativa en la gestión de activos financieros**, facilitando la propiedad, el intercambio y la negociación de activos de manera más segura y transparente. La posibilidad de descentralizar la verificación de identidad y las transacciones financieras contribuye a reducir los costos operativos y los riesgos asociados al manejo de grandes volúmenes de datos personales. En conjunto, SSI puede transformar la forma en que los bancos gestionan el riesgo y el cumplimiento, **brindando mayor seguridad, privacidad y confianza tanto a las instituciones financieras como a sus clientes.**



Educación y HR: un nuevo ecosistema de credenciales y contratación

La utilidad transversal de SSI alcanza a sectores más allá de las finanzas o el *e-commerce.* De hecho, la **SSI también está transformando el ecosistema de la educación y los recursos humanos,** particularmente en la gestión de credenciales y procesos de contratación. En el ámbito educativo, SSI permite a los estudiantes tener control total sobre sus expedientes académicos. Esto significa que **los diplomas, certificados y logros educativos pueden ser almacenados de manera segura en un monedero digital y compartidos de forma rápida y eficiente** con cualquier institución o empleador. Esta gestión simplificada no solo mejora la experiencia del estudiante, sino que también garantiza la autenticidad y privacidad de los documentos, reduciendo el riesgo de falsificación o pérdida de información sensible. Al solicitar una plaza en una universidad o inscribirse en un examen, el ciudadano simplemente comparte las credenciales relevantes de su monedero con la institución educativa correspondiente. Esta universidad, utilizando tecnología SSI, puede verificar de inmediato la autenticidad de los diplomas, certificados y otros documentos, reduciendo así los procesos burocráticos.

En este sentido, este ecosistema de credenciales verificables también tiene un impacto significativo en el mercado laboral y en los departamentos de recursos humanos. **Las empresas también pueden acceder a expedientes académicos y certificaciones de manera directa y segura a través de plataformas SSI**, eliminando la necesidad de verificaciones externas y reduciendo el tiempo necesario para confirmar la validez de los títulos y habilidades de los candidatos. Esto es especialmente valioso en industrias donde las certificaciones y la formación continua son cruciales, ya que los empleadores pueden obtener una visión más clara y precisa de las competencias de un candidato. En resumen, la combinación de SSI con los sectores de la educación y los recursos humanos está creando **un nuevo ecosistema de credenciales y contratación**. Los estudiantes y profesionales tienen más control sobre sus logros y experiencia, mientras que las instituciones educativas y los empleadores se benefician de procesos más eficientes y confiables para verificar estas credenciales.

eCommerce y la Experiencia del Cliente: más allá del UX tradicional

El comercio electrónico está experimentando una transformación radical gracias a la identidad digital autogobernada, avanzando las prácticas tradicionales de experiencia del usuario (UX). En este nuevo panorama, la tecnología SSI ofrece a los consumidores y empresas **una mayor transparencia y confianza en las transacciones, especialmente en la gestión de la cadena de suministro.**

En primer lugar, en cuanto al **UX, SSI otorga el control a los usuarios sobre su propia información personal y de pago.** Al utilizar SSI, los compradores pueden compartir de manera selectiva solo los datos estrictamente necesarios para completar una transacción, lo que mejora significativamente la privacidad y la seguridad. En el ámbito de las compras y la cadena de suministro, uno de los principales beneficios de SSI es la capacidad de **rastrear activos y productos desde su origen hasta el punto de venta, integrando redes de sensores e Internet de las Cosas (IoT).** Esto no solo mejora la trazabilidad, sino que también refuerza la confianza de los consumidores, quienes pueden estar seguros de la autenticidad de los productos que adquieren. En ese sentido, SSI juega un papel crucial al permitir que las empresas **verifiquen la autenticidad de los productos y la fiabilidad de sus proveedores.** Esta verificación es especialmente útil en sectores como el lujo, la alimentación o la tecnología, donde la autenticidad de los productos es un valor primordial. Este factor también garantiza que los proveedores cumplan cumplimiento con normativas, contratos y regulaciones, generando una mayor transparencia en todas las fases del proceso de suministro.

Ante la desconfianza de los consumidores sobre el tratamiento de sus datos, y paralelamente al auge de la normativa sobre privacidad, SSI se posiciona como una solución clave en el ámbito del comercio.

Opinión del consumidor global sobre cómo las empresas pueden generar confianza en materia de privacidad de datos en 2023

Perspectiva de las empresas globales sobre cómo generar confianza en el consumidor en materia de privacidad de datos en 2023

El impacto de SSI no se limita solo a la cadena de suministro. Las empresas pueden también utilizar esta tecnología para **verificar documentos relacionados con el envío, los detalles de la empresa o incluso las credenciales de los transportistas y operadores logísticos.** Este enfoque garantiza que todas las partes involucradas en el comercio, desde la producción hasta la entrega final, estén alineadas y cumplan con los más altos estándares de calidad y fiabilidad.

Al reducir las brechas de confianza entre las partes y aumentar la visibilidad en cada etapa del proceso, **SSI revoluciona la experiencia tanto del consumidor como del negocio**, mejorando la seguridad y eficiencia en las transacciones.

En definitiva, la transparencia, la autenticidad y la seguridad son elementos clave que transforman la relación entre las marcas y los consumidores. Este nuevo paradigma no solo garantiza **una experiencia de compra más fluida y confiable**, sino que también **fortalece el ecosistema comercial en su totalidad**, permitiendo a las empresas ofrecer productos auténticos y de calidad, respaldados por un sistema confiable de verificación digital.

SSI aporta mayor transparencia, trazabilidad, confianza en la autenticidad del producto, así como garantiza la protección de los datos a lo largo de la cadena de suministro

Onboarding digital sin fricción

El onboarding digital es uno de los procesos más impactados por SSI, **facilitando el proceso de incorporación de usuarios a plataformas y servicios de manera ágil y segura.** A diferencia de los métodos tradicionales que requieren el ingreso repetido de información personal, financiera o laboral en múltiples etapas, el uso de SSI permite a los usuarios compartir solo los datos estrictamente necesarios desde un monedero digital. Este enfoque elimina la necesidad de formularios, reduciendo el tiempo y el esfuerzo para completar el proceso de ingreso, mientras se asegura la autenticidad de la información. Esto mejora significativamente la experiencia del usuario al reducir la fricción y las barreras de entrada.

Desde una perspectiva estratégica, las empresas de múltiples sectores pueden utilizar SSI para **optimizar todos los aspectos del onboarding, ya sea para la incorporación de nuevos clientes, empleados o proveedores.** Por ejemplo, en lugar de requerir que los nuevos usuarios creen múltiples contraseñas y verifiquen su identidad con documentos en diferentes fases, SSI permite **una autenticación única y descentralizada.** Los usuarios simplemente comparten sus credenciales verificables, ya sea su identidad, datos de contacto o métodos de pago, de manera segura y eficiente. Esto minimiza los puntos de vulnerabilidad que suelen estar presentes en los tradicionales procesos de ingreso de datos.

Un aspecto clave del onboarding sin fricción es la capacidad de **mantener un equilibrio entre la simplicidad y la privacidad.** De nuevo, con SSI, los usuarios tienen el control total sobre qué información comparten y con quién, lo que genera mayor confianza y reduce el temor a posibles filtraciones de datos. Para las empresas, esto no solo mejora la satisfacción del cliente o del empleado, sino que también **minimiza el riesgo de errores humanos o fraudes, ya que las credenciales que se utilizan en el proceso de onboarding están verificadas y respaldadas por una infraestructura de seguridad robusta.**

En última instancia, SSI también puede simplificar procesos más complejos, como la configuración de pagos o la verificación de identidad para la contratación de empleados. Por ejemplo, al integrar SSI en un sistema de pagos, los usuarios pueden conectar de forma segura sus cuentas bancarias o tarjetas de crédito sin necesidad de ingresar sus datos una y otra vez. Esto acelera las transacciones y hace que el proceso sea más eficiente, ofreciendo **una experiencia de usuario fluida desde el primer momento.**

1. **El sector asegurador** también se podría beneficiar del SSI, gracias a una gestión más segura y eficiente de la información del cliente, así como el desarrollo de nuevos productos hiperpersonalizados y la creación de perfiles de riesgo precisos y dinámicos.

2. **En el ámbito de la salud**, los posibles usos incluyen la emisión de recetas, la reserva de citas, la gestión de historiales médicos, la presentación de reclamaciones a las compañías de seguros, el intercambio de registros médicos, facilitando la comunicación entre pacientes y profesionales sanitarios.

3. **En el sector inmobiliario**, la emisión de documentos clave de inquilinos, compradores y vendedores como VC podría reducir los procesos tediosos, disminuyendo las posibilidades de fraude de identidad.

05

Take action now: integrando SSI en tu estrategia digital

Colaboración público-privada: la clave para una adopción exitosa

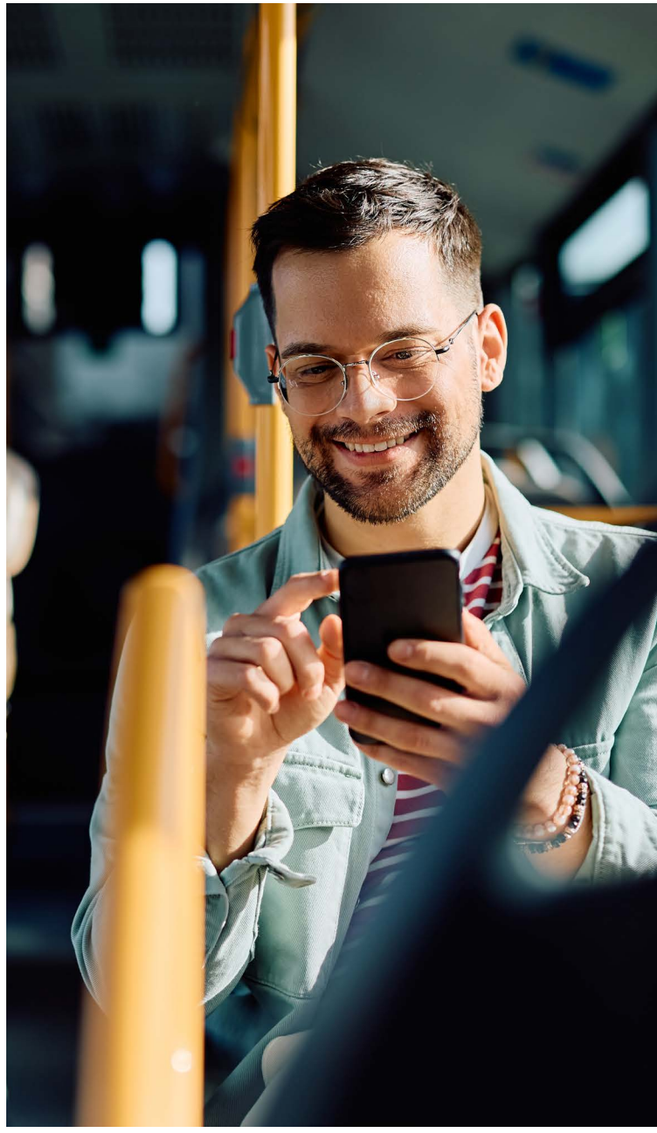
La colaboración público-privada es crucial para la adopción exitosa de la identidad digital autogobernada, y la legislación desempeña un papel clave como impulsor de esta adopción. En efecto, **los gobiernos**, al implementar normativas que regulan y respaldan el uso de SSI, **proporcionan una base jurídica y tecnológica sólida sobre la cual las empresas pueden desarrollar soluciones innovadoras y seguras**, creando el marco necesario para que el mundo corporativo pueda aprovechar esta infraestructura a favor de sus operaciones.

Por tanto, **la legislación no solo actúa como facilitador, sino que también crea incentivos para la adopción obligatoria de ciertos sistemas**, como las identidades digitales gubernamentales. Al estandarizar estos sistemas a nivel nacional o supranacional, como en el caso de la UE, las empresas tienen un marco de confianza sobre el cual construir, minimizando la fragmentación y maximizando la interoperabilidad.

Esto es fundamental, ya que uno de los mayores desafíos para la adopción de SSI es la falta de un ecosistema interoperable y regulado, donde tanto entidades públicas como privadas puedan interactuar bajo los mismos estándares tecnológicos y legales.

Un ejemplo de esta sinergia es el Reglamento eIDAS en Europa, que ha sentado las bases para un ecosistema de identidad digital más armonizado. Con la revisión del eIDAS 2.0, se propone una "**billetera de identidad digital europea**" que permitirá a los ciudadanos gestionar su identidad de manera soberana en múltiples contextos, **desde servicios gubernamentales hasta transacciones privadas**. Las empresas podrán utilizar esta infraestructura para reducir costos en procesos de verificación de identidad y mejorar la experiencia del usuario, apoyándose en las identidades verificadas por el Estado.

En el caso de **Singapur**, gracias a Singpass, una iniciativa originalmente gubernamental y ahora implementada de manera sólida, los ciudadanos ya tienen acceso a **más de 2.700 servicios de más de 800 organismos públicos y empresas**, lo que demuestra el potencial de las colaboraciones público-privadas. Los ciudadanos pueden tanto firmar documentación como verificar transacciones. Además, recientemente se ha integrado **SGFinDex**, una plataforma para facilitar la planificación financiera y que permite al usuario conectar sus cuentas con entidades financieras y organismos públicos y gestionar de forma segura todas sus finanzas en un solo lugar.



Invertir en infraestructuras SSI: construyendo las bases del cambio

Para implementar SSI de manera efectiva, las empresas deben invertir en **una infraestructura tecnológica que combine Blockchain/ DLT, criptografía avanzada, gestión de credenciales verificables y billeteras digitales seguras.** Este enfoque permite la creación de un ecosistema donde los usuarios controlan su identidad de forma segura, descentralizada y privada, minimizando la dependencia de intermediarios y mejorando la seguridad y privacidad de los datos.

1. **La tecnología Blockchain y DLT** proporcionan un mecanismo para asegurar la integridad, transparencia y descentralización en el almacenamiento de datos de identidad. Aunque la identidad misma no se almacena en la Blockchain, los registros verificables se pueden almacenar para garantizar la inmutabilidad de las transacciones relacionadas con la identidad.

- **Ethereum** puede usarse para contratos inteligentes y crear redes de confianza descentralizadas.
- **Hyperledger** Indy está específicamente diseñado para la gestión de identidades descentralizadas.
- **Corda, Quorum o Polkadot** se pueden utilizar para soluciones de identidad.

Inversión en **desarrollo o integración con una Blockchain pública o privada**, infraestructura de nodos y gestión de contratos inteligentes.

2. **Criptografía asimétrica (PKI - *Public Key Infrastructure*)**, puesto que las identidades descentralizadas se basan en la posesión de pares de claves criptográficas (pública y privada) para firmar digitalmente las credenciales y verificar la autenticidad sin intermediarios.

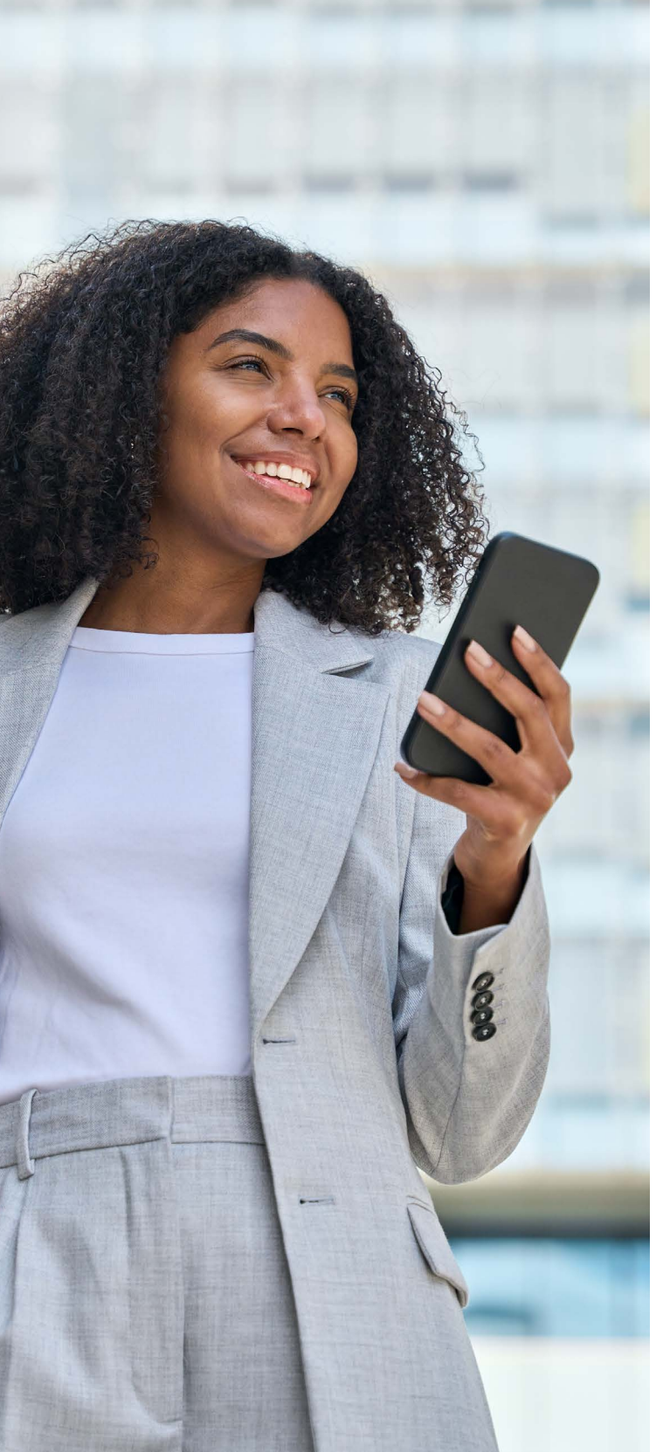
- **Sistemas de gestión de claves (*Key Management Systems, KMS*)** como AWS KMS o Google Cloud KMS para almacenar claves privadas.
- **Protocolos de firma digital:** herramientas como Elliptic Curve Digital Signature Algorithm (ECDSA) o RSA.

Inversión en **la integración de infraestructura para generación, almacenamiento y recuperación de claves** seguras para los usuarios.

3. **Identificadores descentralizados (DIDs)**, identificadores globales y únicos que permiten la creación de identidades sin necesidad de depender de una autoridad centralizada. Cada usuario tiene un DID asociado a su identidad.

- **W3C Decentralized Identifiers (DID) standard:** Estándares para la creación y administración de identificadores descentralizados.
- **Frameworks como Sovrin o uPort:** Estas plataformas implementan el estándar DID y ofrecen infraestructuras para la gestión de identidades SSI.

Inversión en **desarrollar la capacidad de gestionar y resolver DID**, así como la interoperabilidad con otras soluciones basadas en el estándar.



4. **Las credenciales verificables (VC)**, la base de la SSI, permiten a las empresas emitir, verificar y revocar credenciales de identidad que los individuos controlan y son compartidas de manera segura entre usuarios y verificadores.

- **El estándar W3C Verifiable Credentials standard**, que define cómo se emiten, almacenan y verifican las credenciales en un sistema SSI.

- Frameworks que implementan el estándar de credenciales verificables como **Hyperledger Aries y AnonCreds.**

Inversión en implementación de soluciones que permitan **emitir, verificar y gestionar credenciales** de manera segura.

5. **Digital wallets** para almacenar las claves criptográficas, DIDs y credenciales verificables de forma segura, permitiendo a los individuos gestionar su identidad de manera soberana.

- SSI Wallets como uPort, Sovrin Wallet, o Evernym.

- Desarrollo de **wallets white-label.**

Inversión en **desarrollo o integración de carteras digitales compatibles** con la infraestructura de SSI, y soporte para dispositivos móviles y escritorio.

6. **Almacenamiento Seguro y Off-Chain Data** para mantener los datos sensibles de identidad y credenciales fuera de la cadena (*off-chain*) para proteger la privacidad.

- Sistemas descentralizados para el almacenamiento seguro de datos off-chain como **IPFS (InterPlanetary File System) o Storj.**

- Bases de datos cifradas como **SQLCipher o MongoDB** con cifrado para gestionar datos de identidad.

Inversión en a**lmacenamiento descentralizado o soluciones de almacenamiento cifrado** para mantener los datos seguros y privados.

Educación del consumidor: un *must* en la era digital

Los sistemas tradicionales de gestión de identidad a menudo fijan la identidad en categorías rígidas, dificultando que las personas adapten su identidad a circunstancias cambiantes. Por el contrario, **SSI invita a una comprensión dinámica de la identidad que puede evolucionar con el tiempo**, permitiendo que los individuos actualicen los atributos de su identidad según sea necesario.

Esta flexibilidad, informada por los principios de autonomía, control y acceso, otorgan al usuario o consumidor una obligación de educación con respecto a su uso. Sin embargo, **el 46% de los internautas a nivel global desconocen la existencia o contenido de regulaciones protectoras de la privacidad de sus datos.** A pesar de su desconocimiento, en 2024 la proporción de la población mundial que estará cubierta por la normativa moderna sobre privacidad alcanzará el 79%, frente a un 10% en 2020.

Asimismo, el porcentaje de internautas que ya habían adoptado alguna medida para proteger la privacidad de sus datos en junio de 2023 se situaba en el 42% en los grupos de edad 18-24 y 25-34, mientras que la media de todos los grupos de edad equivalía al 33%. Se demuestra, por tanto, una necesidad de adaptar las estratégicas de educación según el grupo de edad.

Por su parte, están aumentando **el número de solicitudes de datos por parte de los usuarios a gigantes tecnológicos**, entre los que se encuentran Apple, Google, Meta y Microsoft. Los usuarios estadounidenses son los más activos en este sentido, y realizaron **más 1,2 millones de consultas entre 2013 y 2021**. Les siguieron los usuarios indios, con más de 460.000 solicitudes, los alemanes (~366.000 solicitudes), los británicos (~275.000) y los franceses (~271.000).

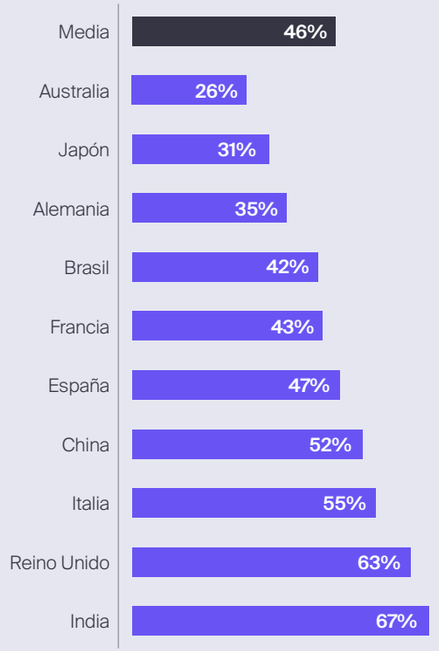
En esta línea, es vital para la implementación amplia de SSI que l**os consumidores o usuarios tomen cada vez más conciencia del marco de protección** que se le brinda desde las instituciones, a nivel regulatorio, y desde las compañías, para su uso diario. Su educación implicará una mayor confianza en los sistemas de identificación de SSI, y su toma de conciencia como propietarios de sus datos será esencial para el desarrollo y mejora de estos.

81% de los estadounidenses están **preocupados** por el uso de sus datos por parte de las **empresas.**

56% aseguran **no leer** nunca las **políticas de privacidad** antes de aceptarlas.

~35% de los europeos muestran **preocupación** por el uso de sus datos por las empresas.

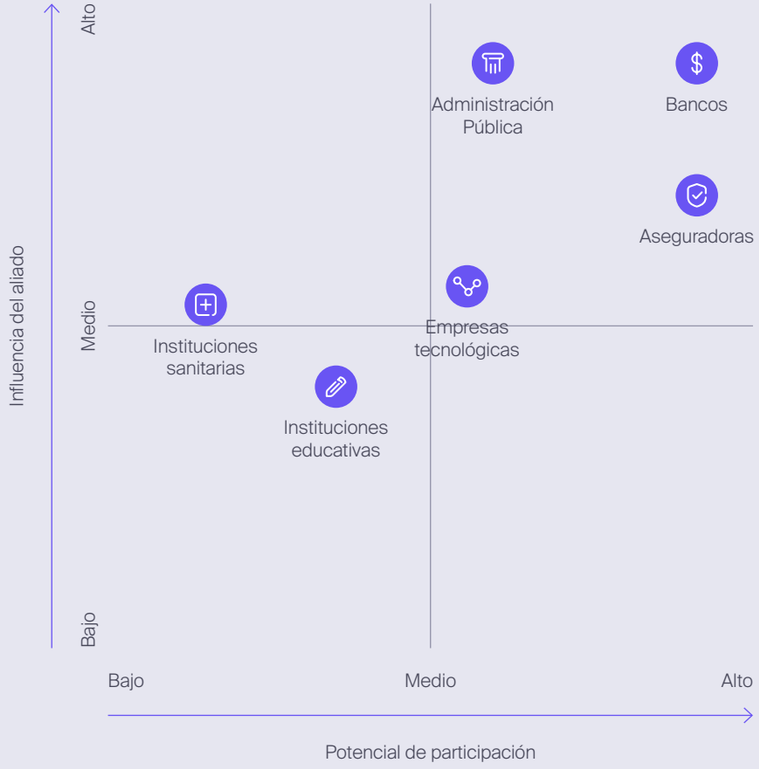
Conciencia de los internautas globales de la legislación sobre privacidad de su país en junio de 2023



Alianzas estratégicas: cocrear el futuro del ecosistema

Las alianzas estratégicas, junto con las cooperaciones intersectoriales entre diferentes industrias, refuerzan el ecosistema SSI, mejorando la experiencia de los usuarios y garantizando mayor control sobre sus identidades. De manera particular, l**as asociaciones estratégicas con bancos y aseguradoras** juegan un papel fundamental en la verificación de credenciales y el desarrollo del ecosistema SSI. Estas instituciones ya poseen grandes volúmenes de datos sobre sus usuarios, lo que las convierte en emisores y verificadores clave de identidades. Los **bancos**, por ejemplo, pueden emitir credenciales verificables (VC) basadas en la información que ya manejan de sus clientes, como datos financieros y personales. Esto no solo les otorga un rol central en el ecosistema de SSI, sino que también permite agilizar los procesos de verificación y aumentar la seguridad y privacidad, eliminando la necesidad de recurrir a terceros para autenticar la información. Asimismo, las **aseguradoras** pueden desempeñar un papel crucial al validar datos críticos relacionados con seguros y reclamaciones, mejorando la confianza y eficiencia en todo el ecosistema.

Otra alianza clave en este entorno es la colaboración con **empresas tecnológicas y plataformas Blockchain**, esencial para proporcionar la infraestructura técnica que permite a las identidades autogobernadas operar de manera segura y escalable. Estas alianzas incluyen el desarrollo de tecnologías de cifrado, Blockchain para garantizar la inmutabilidad de los datos, así como la creación de wallets digitales que permiten a los usuarios gestionar sus credenciales. Además de las alianzas con bancos y aseguradoras y empresas tecnológicas, existen otras alianzas estratégicas importantes que fortalecen este sistema. Entre estas, los **gobiernos** son actores clave en la emisión de credenciales oficiales, como identificaciones, permisos de conducir y títulos académicos. La colaboración con los gobiernos refuerza la legitimidad del sistema SSI y ayuda a establecer estándares globales para su implementación. Asimismo, las **universidades e instituciones educativas** también pueden emitir VC, como títulos y certificados, y las **instituciones sanitarias** emiten credenciales médicas, como historiales clínicos o certificados de vacunación.



softtek.com

Softtek®