Secretaría General Iberoamericana
Secretaria-Geral Ibero-Americana

CLAD
CENTRO LATINOAMERICANO DE ADMINISTRACIÓN PARA EL DESARROLLO

Estudio

Prácticas de identificación digital para el acceso a servicios de gobierno en Iberoamérica

Octubre, 2024

Con el apoyo de:

Cooperación Española

Estudio Prácticas de Identificación digital para el acceso a servicios de gobierno en Iberoamérica[1]

Iris Palma y Alexis Rojas

[1] Las opiniones expresadas son responsabilidad exclusiva de los autores, sin que comprometa ni refleje necesariamente los puntos de vista de la SEGIB o sus países miembros.

INDICES

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

SIGLAS

BID	Banco Interamericano de Desarrollo
CIPDED	Carta Iberoamericana de Principios y Derechos en los Entornos Digitales
GPRD	Reglamento General de Protección de Datos
ID	Identidad Digital
SID	Sistema de Identificación Digital
OCDE	Organización para la Cooperación y el Desarrollo Económico
ODS	Objetivos de Desarrollo Sostenible
OSC	Organizaciones de la Sociedad Civil
UIT	Unión Internacional de Telecomunicaciones

RESUMEN EJECUTIVO

Iberoamérica se caracteriza por su rica diversidad cultural, lingüística y geográfica, abarcando países de América Latina y la península ibérica. La región, compuesta por 22 países, presenta una amplia variedad de tradiciones, costumbres y patrimonios, resultado de la mezcla cultural que da identidad a sus habitantes. Sin embargo, millones de personas en Iberoamérica, especialmente en comunidades rurales, áreas marginales y entre grupos vulnerables, no cuentan con una forma de ser identificadas en sus derechos y deberes, tanto en lo presencial como en entornos digitales.

Ante esta situación, los países han impulsado diferentes iniciativas con el uso de tecnologías digitales para cerrar la brecha de identificación. La identidad digital y los sistemas de identificación digital en Iberoamérica están en proceso de evolución y consolidación, impulsados por la creciente digitalización de servicios públicos y privados. A medida que los gobiernos y las empresas adoptan tecnologías digitales, la gestión de la identidad se convierte en un aspecto determinante para garantizar la seguridad, la privacidad y el acceso a servicios esenciales. Sin embargo, la región enfrenta desafíos significativos, como la fragmentación de sistemas, la falta de infraestructura adecuada y la necesidad de educar a la población sobre el uso seguro de sus datos. A pesar de estas dificultades, iniciativas en varios países han comenzado a implementar sistemas de identificación digital que permiten a los ciudadanos acceder a trámites, servicios de salud, educación, entre otros, de manera más eficiente. Este avance no solo busca facilitar la vida cotidiana, sino también fomentar la inclusión social y económica, promoviendo una mayor participación de los ciudadanos en la era digital.

Este estudio se desarrolla desde la óptica de las reflexiones y compromisos de la Carta Iberoamericana de Principios y Derechos en los Entornos Digitales, promulgada en noviembre de 2023, para analizar la identidad digital, los servicios públicos digitales y la interoperabilidad como un todo que cataliza los derechos digitales de las personas frente a sus relaciones con las administraciones públicas.

A lo largo del documento se describen las fronteras entre la identidad digital, los sistemas de identificación digital, la interoperabilidad y la firma electrónica; además, se presentan hallazgos sobre las regulaciones y el funcionamiento de los sistemas de identificación digital, y se exponen seis casos que muestran el panorama de la identidad digital en Iberoamérica.

Los hallazgos de este estudio se reflejan en las reflexiones descritas en los últimos capítulos, y en especial, en el emparejamiento entre las acciones recomendables y los compromisos de la Carta Iberoamericana de Principios y Derechos en los Entornos Digitales, para orientar a los países en la construcción y/o fortalecimiento de las competencias de sus servidores públicos y el desarrollo de sus sistemas de identificación digital centrados en las personas.

Figura 1

Infografía de hallazgos del estudio

Fuente: elaboración propia con base a datos de SEGIB (2023).

INTRODUCCION

El ser humano es un ser social por naturaleza[2], en cuya agrupación se establecen vínculos y relaciones recíprocos, e interacciones estables, a las que se llama sociedad[3]. Para que estos vínculos se propicien efectivamente, es clave la definición de los atributos y rasgos que simbolizan la identidad de cada persona, y es igualmente importante establecer los mecanismos a través de los cuales se reconoce esta identidad, es decir, los sistemas de identificación.

Sin embargo, más de 850 millones de personas en el mundo en desarrollo carecen de cualquier forma de identificación oficialmente reconocida, ya sea en papel o por medios electrónicos[4]; un número preocupante de cara a lograr la meta del Objetivo de Desarrollo Sostenible 16.9 «Proporcionar acceso a una identidad jurídica para todos, en particular mediante el registro de nacimientos». Sin una identidad y forma de identificación clara, las personas pueden verse y sentirse excluidas de todos los procesos sociales, tales como el derecho al voto, el acceso al empleo, la educación o los servicios básicos a los que tienen derecho como habitantes en su país. Una persona sin identidad o, empeorando el caso, una persona que no puede ser identificada, está en inminente riesgo de ser excluida de todo beneficio social.

A partir de la evolución digital, los sistemas de identificación han incrementado el uso de herramientas de tecnología digital durante todo el ciclo de vida de la identidad, incluyendo, por ejemplo: la captura, validación, almacenamiento y transferencia; gestión de credenciales; y verificación y autenticación de identidad[5]. Como podrá verse en este estudio, los Sistemas de Identificación Digital (SID) pueden impactar ampliamente en la eficiencia, transparencia, control y economía de los recursos, tanto para los gobiernos como para las personas; aunque esto no necesariamente implica que su implementación sea sencilla.

La Carta Iberoamericana de Principios y Derechos en los Entornos Digitales (CIPDED), tomada como punto de referencia en este estudio, llama a la reflexión y acción de los países iberoamericanos a servirse de estos avances tecnológicos para reducir las brechas que limitan los derechos y beneficios sociales de la población, orientando a los gobiernos a garantizar condiciones para que la identidad y los SID sean lo más robustos, seguros, confiables y viables que se puedan.

Este estudio, impulsado por la Secretaría General Iberoamericana, y el Centro Latinoamericano de Administración para el Desarrollo, analiza y presenta hallazgos relevantes del entorno de los SID en Iberoamérica, con referencia a seis países: España, Argentina, Brasil, Chile, Uruguay y Colombia; destaca, además, buenas prácticas realizadas en Costa Rica y República Dominicana. Se pretende que esta mirada al estado del arte de los marcos normativos, tecnologías y funcionamiento de los SID respalde una serie de recomendaciones para acelerar el paso a la madurez de dichos sistemas,

[2] Aristóteles (1988).
[3] Encyclopaedia Herder (2017).
[4] Clark *et al.* (2023).
[5] World Bank (2018).

tomando como referencia a los principios y compromisos establecidos en la Carta Iberoamericana de Principios y Derechos en los Entornos Digitales (CIPDED).

1. COMPRENDIENDO LOS SISTEMAS DE IDENTIFICACIÓN DIGITAL

En este apartado se describen las perspectivas de la CIPDED sobre el valor de la Identidad Digital (ID) y los Sistemas de Identificación Digital (SID) para asegurar los derechos de las personas en los entornos digitales. Se señalan también los elementos que la CIPDED considera deben ser incorporados en todo proceso de diseño de SID en la región iberoamericana. Además, se ofrece una aproximación conceptual de la ID y los SID, con el fin de identificar los aspectos que caracterizan y motivan la implementación de estrategias de identificación digital.

1.1 Perspectiva de la CIPDED

La Carta Iberoamericana de Principios y Derechos en los Entornos Digitales (CIPDED) es una guía orientadora para la reflexión sobre los retos y oportunidades que ofrecen los entornos digitales a los países de la región iberoamericana. De acuerdo con la CIPDED[6], «las personas deben verse protegidas en los entornos digitales como sujetos de derechos y deberes» (p. 6), que implica un reconocimiento a que dicha protección pasa indudablemente porque cada persona sea consciente de su identidad, y pueda ser identificada.

A nivel mundial, 3.4 mil millones de personas tienen alguna forma de identificación, pero no rastro digital; 3.2 mil millones tienen alguna forma de identificación y rastro digital, y se estima que 1 mil millones se estima las personas que carecen legalmente de forma reconocida de identificación que habilita sus derechos y derechos[7]. Este contexto expone la importancia y urgencia de promover de forma segura y confiable la utilización intensa de tecnologías digitales, a fin de activar la identidad digital (ID) de cara a resguardar la dignidad y derechos de los ciudadanos.

Conceptualizar a la ID, los SID y la interoperabilidad para la prestación de servicios públicos permite comprender, que como bien indica la CIPDED, que para que «la prestación de servicios digitales por parte del Estado y los trámites administrativos digitales sean personalizados, sencillos, inclusivos, accesibles, interoperables y seguros» (p. 23)[8], debe existir esta triada de elementos que ofrezcan confianza y seguridad a los ciudadanos para actuar en las relaciones con sus gobiernos, y ser objeto de sus servicios y beneficios. Estos deben actuar de forma coordinada en igualdad de fortalezas para lograr que su uso sea permanente y ético a lo largo del tiempo. En la Figura 2 se exponen los elementos que la CIPDED anhela en el diseño de SID.

[6] SEGIB (2023).
[7] Banco Mundial (2019).
[8] SEGIB (2023).

Se considera que no todos los países de la región iberoamericana cuentan con un SID. De acuerdo con el Índice de Gobierno Digital de la OECD, solo el 58% de los países miembros de la organización tenían al menos la mitad de los servicios accesibles a través de estos sistemas[9]. En Iberoamérica, un poco más de la mitad de los países ofrecen un mecanismo de servicios públicos digitales que utiliza, al menos, uno de los elementos de identificación. Con este panorama es fácil comprender la relevancia que tiene implementar tecnologías digitales con propósito, con el ciudadano al centro de todo sistema, y políticas para acelerar la prestación de servicios públicos digitales; esto incrementa los lazos de confianza para que los ciudadanos puedan ser identificados no solo en el sector público, sino en el deseado escenario de una identificación plena aún en procesos privados. Después de todo, es la confianza ciudadana en su entorno y en los servicios y relaciones que tiene con su gobierno lo que sostiene el funcionamiento de la democracia[10].

Figura 2

Elementos claves de la CIPDED que promueven la identificación digital

Fuente: CIPDED.

Si bien a nivel mundial los SID se pueden encontrar de diferentes formas y niveles de sofisticación (pudiendo incluir un dispositivo móvil, una tarjeta electrónica, una contraseña y usuario, un dato biométrico, etc.) y pueden ser denominados de acuerdo con las condiciones de cada país, todos tienen en común que son sistemas que obligatoriamente utilizan tecnologías para identificar y verificar personas[11]. En un escenario ideal, estos SID tienen como fin último la prestación de servicios públicos, la ayuda social y el ejercicio de derechos; sin embargo, sin un buen diseño e implementación no pueden garantizar ser mecanismos de inclusión digital[12]. Esto se convierte es

[9] Weidenslaufer y Roberts (2022).
[10] Asociación por los Derechos Civiles (2019).
[11] Onuoha y Nucera (2022).
[12] Banco Mundial (2019).

un aspecto primordial en los compromisos de la CIPDED para propiciar condiciones que hagan posible que «la transformación digital incorpore a las mujeres, niñas, adultos mayores, personas con discapacidad y otros grupos en situación de vulnerabilidad» (p. 9)[13]; para lo cual el mundo en general aún enfrenta datos preocupantes, como el hecho que solo una de cada dos mujeres en el mundo en una economía de ingreso bajo posee un carnet nacional de identidad o un tipo de identificación de similar magnitud[14], y los adultos con solo educación primaria tienen alrededor de 9 puntos porcentuales menos de probabilidades de poseer una identificación que aquellos con secundaria o superior educación, controlando por otras características demográficas[15].

Por otra parte, los débiles registros civiles pueden dejar en la exclusión a menores. Solo en América Latina se estima que alrededor de 3 millones de niños menores de cinco años no tienen una partida de nacimiento[16]. Un registro civil fuerte y seguro es la piedra angular de un buen SID; si estos registros no son lo suficientemente sólidos pueden habilitar serios problemas en la automatización de los sistemas de identificación, abriendo puertas a la duplicidad de identidad, registros incompletos o poca trazabilidad en el ciclo de la identificación de los ciudadanos. En Iberoamérica, solo Chile, Panamá, Guatemala, España y Portugal contaban con registro civil soportado por documentos electrónicos[17].

La CIPDED pone de manifiesto, a lo largo de su contenido, que la identificación de las personas es indispensable en el futuro digital de Iberoamérica. Las tecnologías, en especial el Internet, son habilitantes para mejorar las condiciones económicas, sociales, culturales y políticas de las personas, pero no pueden garantizar por si solas la inclusión si no existe un total reconocimiento que la gobernanza de los servicios públicos y de la ID no es un tema digital, sino de derechos.

1.2 Los sistemas de identificación digital: aproximaciones a sus elementos característicos

La **identidad** puede definirse como el conjunto de rasgos que hace a una persona ser quien es y la distingue de los demás, permitiéndole interactuar con su entorno. El Estado es el único responsable de identificar a cada persona y otorgarle una identidad legal, vinculada a documentos físicos como el documento de identidad o cédulas de identidad, los cuales son inequívocos y verificables.

La identidad de una persona, tradicionalmente, está vinculada a la recopilación de una serie de rasgos que, unidos, conforman características de esa persona, como pueden ser las huellas dactilares, el aspecto físico, la edad, el lugar de nacimiento, etc.

[13] SEGIB (2023).
[14] Banco Mundial (2019).
[15] Clark *et al*. (2022).
[16] Muente (2018).
[17] Barbosa *et al.* (2020).

Para la UIT, la identidad digital (ID) es «una representación digital de información conocida sobre una persona específica, un grupo u organización» (p. 13)[18]. Para el Banco Mundial, un sistema de identificación digital (SID) es «el proceso de verificar la identidad digital de una persona utilizando uno o más factores o credenciales para establecer que son quienes dicen ser» (p. 13)[19]. Como fundamentos a estos conceptos y, tal como se mencionó antes, los sistemas de registro civil son la piedra angular de un buen sistema de identidad que puede ser verificable, autenticado y validado por los SID. La seguridad y confiabilidad de un SID depende en gran medida del sistema de identidad o registro civil de un país sobre el cual se construye.

La **ID** es un concepto en constante evolución, en donde distintos autores pueden diferir, por lo que es importante establecer sus dos dimensiones:

- La oficial, o legal, que está vinculada a registros de identidad legal, estando a cargo del Estado.
- La simple, que no requiere estar vinculada a identidades legales de personal, es decir, aquella que depende de las empresas, organizaciones o medios digitales.

Además, cuenta con atributos de: verificación y autenticación; privacidad y seguridad de los datos; estandarización e interoperabilidad; identidad única; consentimiento y captura mínima de datos.

En su concepto más amplio, todo un SID debe estar sustentado por un sólido registro civil, con definición de claros procesos de tratamiento de datos, tecnología, credenciales y marcos legales asociados con la captura, gestión y uso de datos personales para una finalidad general o específica[20]. Una ID comprende dos componentes fundamentales: un sistema de identificación y la autenticidad; es decir, que una persona pueda demostrar que es quien dice ser por medios electrónicos, sin necesidad de presentarse físicamente o de ser verificada por otra persona. Aquí se encuentra el reto más grande en la madurez de SID en la región; un SID debe de ser capaz de identificar a una persona sin equivocarse, distinguiéndola de entre los demás por medios electrónicos.

Un SID debería proporcionar un estándar de identificación entre distintos sistemas, es decir, un servicio único de identificación reconocido para todas las entidades de un país, donde todos los trámites y servicios que una persona requiera pueda identificarse de la misma forma (por ejemplo, los *single sign-on* o las firmas electrónicas), para evitar duplicidades, confusiones y costos elevados. Un SID con un servicio único transversal asegura que las administraciones públicas se centren en el desarrollo de herramientas que protejan dicho proceso, y faciliten canales seguros de autenticación y verificación de la identidad. Mientras, las entidades prestadoras de servicios, podrán concentrarse en la provisión de su servicio sin tener que preocuparse en la autenticación de las personas.

[18] Guerrero (2020).
[19] World Bank (2016).
[20] World Bank (2018a).

El Banco Mundial establece que la ID es la colección de datos y atributos que son capturados electrónicamente[21]. Requiere de un proceso nato digital y no implica obligatoriamente la virtualización de un proceso de identidad en papel. Por ello, los registros civiles son tan relevantes para la construcción de una ID, ya que podrían, en un momento dado, dar paso a la definición de una ID de las personas desde la «cuna a la tumba»[22]. Mientras se superan los retos de fortalecer estos registros civiles, la ID puede concretarse con la colección de datos y atributos por lo general durante la adultez. Resaltan casos como en Chile que ha habilitado que la obtención de mecanismos de ID sean a partir de los 14 años, con el otorgamiento de datos a través de tecnologías digitales como biometría; mientras que en Portugal, la Tarjeta de Ciudadano es de carácter obligatorio a partir de los 20 días de edad, y brinda la oportunidad de utilizar el certificado de autenticación digital, en este país, la activación remota de la ID es posible a partir de los 16 años por medios de biometría.

El mismo Banco Mundial hace referencia a que la ID tiene una característica específica, y es que son datos y atributos que, colectados y almacenados digitalmente, describen a una persona en un contexto y son empleados para realizar transacciones electrónicas. En algunos casos, como en Colombia, coexisten modelos de cédula de identificación digital y física, que son válidos para todos los trámites de gobierno y son generados por solicitud de las personas y no por obligación de los gobiernos.

En la mayoría de los países iberoamericanos existe una cédula o carné de identidad que sirve como la principal forma de identificación de las personas. Estos documentos, en su mayoría físicos, establecen la identidad legal de una persona. Con base en estos documentos se pueden generar los documentos de identidad funcionales (pasaporte, licencia de conducir, seguro social, etc.), y estos registros fundamentan las bases para disponer de identidades digitales legales. También tienen una versión electrónica; ejemplos incluyen el Documento Nacional de Identidad (DNI) en España y el Registro Federal de Electores (RFE) en México. Para emitir estos documentos de identidad, suelen utilizarse los registros civiles y las bases de datos nacionales que almacenan información básica sobre las personas, como nombre, fecha de nacimiento, dirección y número de identificación. Es decir, para que exista una ID legal, segura y confiable, debe estar sustentada en una identidad legal generada por el Estado por medio de los registros civiles.

Los SID son parte de la ID y facilitan las tecnologías por medio de las cuales se identificará a las personas por medios digitales. Además, ofrecen servicios de identificación centralizados o estandarizados, que sean reconocidos por distintas entidades y métodos de validación de las credenciales, con un soporte tanto legal como de procesos y tecnológico.

Para que puedan brindarse servicios de identificación centralizados, es necesario que los sistemas compartan credenciales de forma transparente a través de estándares y tecnologías; así, las identificaciones de las personas serán reconocidas en otros sistemas y podrán ser transversales a

[21] World Bank (2018a).
[22] Peiro y Pomeda (2019).

distintas instituciones; es decir, es necesaria la interoperabilidad. Según la Comisión Europea, se define como «la habilidad de los sistemas TIC, y de los procesos de negocios que ellas soportan, de intercambiar datos y posibilitar compartir información y conocimiento» (p. 13)[23], lo cual es un elemento determinante para mejorar la eficiencia y la calidad de los servicios públicos. Se enfoca en cómo los sistemas pueden integrarse para facilitar el flujo de información y servicios entre diferentes entidades.

Para efectos de la puesta en marcha de los SID, la interoperabilidad tiene sentido cuando las personas son capaces de identificarse ante un tercero (ya sea el gobierno o un privado) y operar entre diferentes sistemas con su misma identificación, logrando una trazabilidad efectiva de todas las relaciones entre los ciudadanos y sus gobiernos.

Una implementación efectiva de estrategias de interoperabilidad requiere un sólido proceso de identificación e ID, ambos conceptos que, en términos digitales, requieren de sistemas tecnológicos que otorguen el mismo nivel de seguridad *online* que en el mundo físico. Mientras la identidad física incluye atributos inherentes a la persona (nombre, edad, huella digital, fecha de nacimiento), la ID se construye con más datos, como los acumulados (datos médicos, gustos, datos de comportamiento) y los atribuidos (número de teléfono, correo electrónico o número de identificación nacional)[24].

Los SID complementan a la firma electrónica, a la interoperabilidad y son piedras angulares del gobierno digital; también son indispensables para vincular a las personas con servicios privados[25] como los financieros, bancarios, educativos, de empleo, vivienda, etc. Además, y no menos importante, son la puerta para el ejercicio de su derecho y deber al voto: alrededor de un tercio de los adultos en el mundo que no poseen una identificación, enfrentan barreras para participar en procesos electorales[26]. En términos digitales, los mecanismos que se implementan para la identificación a una persona son tan importantes como la ID misma.

La ID busca proveer seguridad a distancia de que la persona es quien dice ser, y los SID son el mecanismo garante que permite esta identificación. Para los gobiernos, la identificación de las personas ofrece una oportunidad única para diseñar nuevos servicios públicos o rediseñar, con un enfoque de eficiencia, los existentes. Por ejemplo, un par de años antes de la pandemia por COVID-19, solo nueve países iberoamericanos disponían de un SID implementado. Luego, el número de servicios públicos digitales para implementar programas sociales de apoyo durante la pandemia incrementó sustancialmente. El Programa Vale Digital del Plan Panamá Solidario es una iniciativa creada por el Gobierno Nacional de Panamá desde marzo de 2020, al inicio de la pandemia por COVID-19, que permitió que más de 1.4 millones de panameños y panameñas que perdieron su trabajo durante la crisis sanitaria recibieran una transferencia monetaria para adquirir alimentos y productos de primera necesidad, a través de un SID implementado en

[23] CEPAL (2007).
[24] Weidenslaufer y Roberts (2022).
[25] Onuoha y Nucera (2022).
[26] Clark *et al*. (2022).

www.panamasolidario.gob.pa al cual los ciudadanos accedían con su número de identificación y un PIN generado a partir de su registro.

Para que la ID sea empoderadora en ciertos contextos, los aspectos tecnológicos, legales y políticos deben estar articulados, a fin de reconocer la elección del usuario, el consentimiento informado, el reconocimiento de múltiples formas de identidad, el espacio para el anonimato y el respeto a la privacidad[27]. En un SID, todos sus formularios de identificación están directamente relacionados entre sí y utilizan tecnología digital para identificar y verificar a las personas bajo un mismo número, entrada o identificador. Al hacerlo, eliminan la necesidad de diferentes formas de identificación o garantizan que están estrechamente vinculadas entre sí de una manera que es imposible con sistemas analógicos.

Para los objetivos de la prestación de servicios públicos digitales la ID es indispensable; pero no debería serlo para para la obtención de servicios públicos en sí mismo[28]. La ausencia de una ID no implica la invisibilidad de las personas, más bien, es la obtención de una ID la que permite a las personas valer sus derechos en los entornos digitales, tal como se hace en el mundo físico. Por lo tanto, es una responsabilidad de los gobiernos diseñar estrategias que trasciendan entre lo digital y presencial, con miras a lograr la inclusión social como el fin último de la inclusión digital, en especial considerando el alto grado de penetración de propiedad de teléfonos móviles en el mundo, que alcanzan los 6.5 millones de usuarios, que pueden ser un catalizador para impulsar estrategias innovadoras de implementación de SID[29].

La motivación de las personas para registrarse en los SID está fuertemente relacionada con sentimientos de confianza, percepciones sobre si el propósito y los objetivos del sistema son legítimos, y expectativas sobre cómo el sistema podría usarse (o potencialmente usarse indebidamente)[30]. El éxito de los SID depende de su usabilidad y accesibilidad por parte del público objetivo, incluidos aquellos que tal vez no tengan acceso a la tecnología o soluciones digitales, para garantizar que los servicios esenciales estén disponibles para todos.

Desafortunadamente, demasiados SID y registros civiles se han desarrollado previamente desconectados de las necesidades de las personas y de los avances digitales que podrían impactar positivamente en ellos. Estos proyectos, a menudo, se han desarrollado bajo un modelo de comunicación unidireccional, dejando poco espacio para la retroalimentación y la colaboración con las personas usuarias. Cuando las autoridades de identificación no incluyen una participación pública fuerte y activa dentro del marco del proyecto de ID, desde la planificación y el diseño hasta la implementación, se limitan las posibilidades de éxito[31]. Un caso interesante es la creación de la primera fase del modelo de ID de la República Dominicana, que evidencia la interacción con las

[27] Access Now (2018).
[28] Access Now (2018).
[29] Ho (2022).
[30] World Bank (2022).
[31] World Bank (2022).

personas para identificar elementos de la experiencia de usuario necesarios para la creación de la Carpeta Ciudadana SoyYoRD.

En los servicios públicos digitales, el primer paso es identificar a las personas o entidades a las cuales se les está brindando un servicio o trámite, debido a que estos se realizan generalmente por medio de portales, aplicaciones, quioscos u otros, de forma no presencial y, en algunos casos, sin intervención humana.

Para que un servicio público digital esté disponible para las personas, son necesarias tres condiciones: primero, que el servicio público tenga la misma validez tanto en su dimensión digital como en la presencial; segundo, que el servicio público esté sustentado en un proceso diseñado o rediseñado para estar disponible en línea; y tercero, que el servicio público esté disponible por los medios propicios para que las personas se identifiquen, se aprovisionen de los beneficios de este servicio y puedan realizar todas las fases del mismo. Así, la gobernanza digital, que implica los pagos electrónicos, la identificación digital y el acceso a los servicios públicos digitales, funciona y habilita nuevos espacios de innovación al servicio del ciudadano.

Figura 3

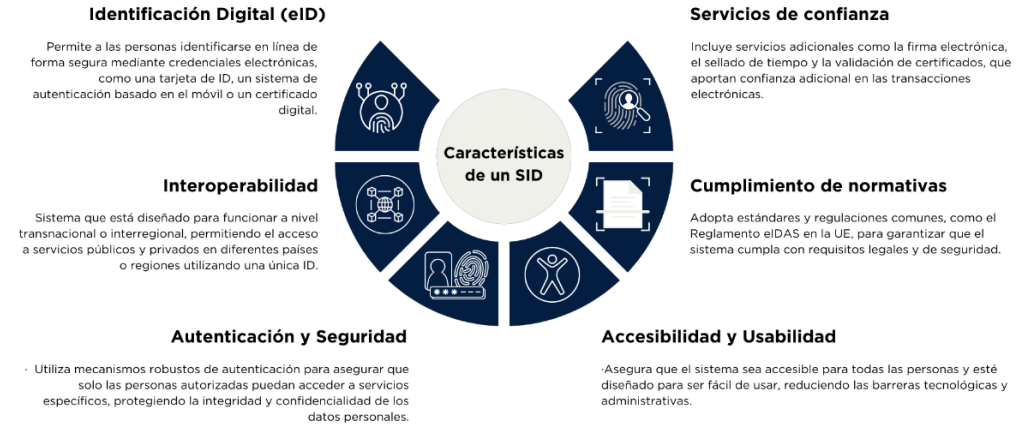
Relaciones entre los conceptos de identidad digital, sistemas de identidad digital, interoperabilidad y registros civiles

Fuente: elaboración propia.

Los SID utilizan marcos legales, políticas, tecnologías y personas para verificar una ID y autenticarla con un alto grado de seguridad a través de canales digitales únicos preestablecidos. La Guía de Sistemas de Identificación del Banco Mundial describe que los SID son aquellos que utilizan tecnología digital durante todo el ciclo de vida de la identidad, incluyendo la captura, validación, almacenamiento y transferencia de datos; gestión de credenciales; y verificación y autenticación de identidad[32]. Para la Unión Europea, los SID se refieren a una infraestructura digital que permite a las personas acceder a servicios de manera segura y eficiente utilizando una forma estandarizada de identificación digital, a partir de un abanico de características, que se detallan en la Figura 4.

Figura 4

Características de los SID



Fuente: elaboración propia.

[32] CFATF GAFIC (2021).

En general, la definición de normativas y su cumplimiento permiten que los SID sean escalables y se adapten a las necesidades de los ciudadanos, así como a la incorporación de nuevas tecnologías. Por otro lado, la definición de servicios de confianza, como la firma electrónica, y la implementación de estándares de accesibilidad y usabilidad, brindan mayor seguridad a las personas para utilizar su ID en transacciones con el gobierno y el sector privado.

Los SID en su funcionamiento consideran un rol básico que responde a una tríada de condiciones de autenticación:

- ¿Quién soy?: edad, género, dirección, huellas dactilares, datos biométricos, voz, etc.
- ¿Qué sé?: contraseñas, preguntas secretas, PIN, patrones, etc.
- ¿Qué tengo?: tarjeta o carné de identidad, token de seguridad, teléfono móvil, etc.[33]

En cada SID se utilizan tres etapas en el proceso de identificación. La primera es la identificación, que surge de la interacción entre las personas y la entidad que otorga la identidad; dado que es el primer paso, su diseño debe ser clave para generar confianza en el ciudadano respecto al uso de sus datos. En la segunda etapa, la autenticación, una persona ya identificada es reconocida en su identidad digital, y en la tercera, la validación, se le permite acceder al servicio público requerido.

Figura 5
Identificación, autenticación y validación

Fuente: elaboración propia.

[33] United Nations Economic Commission for Africa (2024).

Los SID reconocen a la autenticación como el elemento que habilita la validez de las transacciones electrónicas que hacen las personas con su ID. La autenticación digital relaciona a las personas con uno o más factores o autenticadores para demostrar que es la misma persona a la que la identidad o credencial fue emitida originalmente[34]. La autenticación es, por lo tanto, un proceso para establecer confianza en la ID de una persona. Los datos biométricos se utilizan, a menudo, como autenticadores para verificar la identidad de las personas[35], pero pueden ser utilizados otros medios como:

- Autenticación digital por contraseña
- Autenticación digital por huella dactilar
- Autenticación digital por reconocimiento facial
- Autenticación digital por token físico
- Autenticación digital por certificado digital

Los datos biométricos, en el contexto de los SID, son características que son atributos personales únicos que pueden ser utilizados para verificar la identidad de una persona que está físicamente presente en el punto de verificación. Estas características pueden ser físicas o de comportamiento e incluyen rasgos faciales, huellas dactilares, patrones de iris, huellas de voz, y muchas otras características.

En Iberoamérica, aproximadamente la mitad de los países cuentan con un SID que cumple con las condiciones de permitir la identificación digital, la autenticación única con un mecanismo multidispositivo y la validación en tiempo real. En la mayoría de los casos, el proceso de identificación requiere una acción presencial por parte de las personas, en la que deben acudir a una oficina pública para darse de alta con sus datos y atributos, usualmente a través de datos biométricos. Aunque esto sucede solo una vez, puede ser una limitación para masificar el SID y representar un obstáculo para personas que no pueden trasladarse, como aquellas con capacidades especiales, adultos mayores o quienes viven fuera de las zonas urbanas.

En algunos países, los SID cuentan con un marco legal, estrategia de ciberseguridad y protección de los datos personales y una entidad responsable con las competencias necesarias para velar por la confianza de todo el proceso de identificación digital para los ciudadanos. Luego, en otros, los SID no evidencian al público que cuenten con mecanismos de base legal sobre su seguridad o privacidad, y en pocas ocasiones se evidencia que existan mecanismos de vinculación con organizaciones de sociedad civil para garantizar que los usuarios participen continuamente desde el inicio del SID y esto genere la confianza y valor en las personas. Por ejemplo, en Bolivia, el proceso de registro de votantes en 2019 se desarrolló a través de asociaciones locales y organismos no gubernamentales para difundir el mensaje, utilizando lemas como como «Tus huellas, tu voto»; fue ideado para incentivar a las personas a registrarse y vincular el trámite con una sensación de empoderamiento cívico[36].

[34] World Bank (2018b).
[35] Access Now (2018).
[36] World Bank (2019).

2. LOS SISTEMAS DE IDENTIFICACIÓN DIGITAL EN IBEROAMERICA

Algunos países han comenzado a implementar SID que permiten a las personas acceder a servicios públicos digitales de manera segura. Estos sistemas suelen incluir una tarjeta de identidad electrónica (comúnmente llamada e-ID) o una aplicación móvil con credenciales digitales. Por ejemplo, en Costa Rica, el SID para la prestación de servicios de salud se concretar en el Expediente Digital Único de Salud que ocupa la cédula como número de identificación único, en cumplimiento al inciso I del artículo 5 de la Ley orgánico del expediente, y promueve el desarrollo de servicios de valor como aplicación móvil para el uso de las personas en el proceso de identidad e identificación digital[37].

Figura 6

SID en Iberoamérica

Fuente: elaboración propia.

Las diferencias entre los SID para el acceso a servicios públicos digitales en Iberoamérica están dadas por al menos cuatro factores, según puede verse en la Figura 7.

[37] Ochoa Chaves (2023).

Figura 7

Factores diferenciadores entre los SID en Iberoamérica

Fuente: elaboración propia.

Al respecto, se describen a continuación cada una de ellas:

- **Las piezas faltantes en los marcos legales que propicien la ID y los SID y que son necesarios para impulsar iniciativas regionales.** En Iberoamérica, aún existen retos para que los países cuenten con un abanico de condiciones mínimas en su marco legal para el buen funcionamiento de un SID para el acceso a servicios públicos digitales, tales como: protección de datos personales, servicios y trámites en línea, firma electrónica, ciberseguridad, interoperabilidad, promoción de reducción de brecha digital, entre otros.

- **La automatización de servicios públicos para poder prestarlos en una dimensión digital estable, constante y segura para los ciudadanos**. En una muestra de 15 países de Iberoamérica, sin incluir a España y Portugal, el 27.5% de los trámites públicos están disponibles en línea; y 15% de esos trámites pueden ser completados en línea[38]. Como caso excepcional, España se registra como el país de la región que desde el 2020 ofrece el 100% de los trámites administrativos en formato digital.

- **La vinculación de la ID y de los SID para la prestación de servicios públicos y privados digitales.** En Costa Rica, el Expediente Digital Único de Salud permite acceder a servicios de salud privados, y en Ecuador entidades privadas pueden hacer consultas de ID que incluyen información demográfica o biométrica con un costo asociado por tres medios: a) Un servicio

[38] Banco Interamericano de Desarrollo (2018).

basado en una página web; b) Una solución basada en un servicio web; y c) Un servicio basado en CD o DVD llamado «validación de registros»[39]. En el 2014, el Registro Civil Nacional de Panamá firmó un acuerdo con la Superintendencia de Bancos de Panamá para brindar servicios de verificación gratuitos a los bancos para facilitar un mayor acceso financiero y prevenir el fraude de identidad y suplantación de identidad, mientras que las instituciones públicas pueden conectarse a la base de datos del Registro Civil Nacional a través de un servicio web o a través de la página web mediante usuario y contraseña. Dependiendo de la información requerida y autorizaciones otorgadas, terceros pueden acceder a nombres, lugar y fecha de nacimiento, expedición y vencimiento fecha del documento de identidad, fotografía, firma y huellas dactilares; solo en 2018, el Registro Civil Nacional de Panamá respondió a 6,111,221 consultas de 51 públicos instituciones y 88,081 consultas de entidades privadas[40].

- **Los procesos de construcción de los registros civiles.** En Iberoamérica, entre el 60 a 70% de los países registran contar con medios digitales para la construcción de sus registros civiles, y para automatizar los mecanismos de actualización. En una mirada regional, se identifican casos relevantes como el de Ecuador, Panamá, España o Perú, que cuenta con un registro civil que utiliza tecnologías intensamente; mientras que otros países aún tienen niveles emergentes de procesos digitales.

En general, los países han implementado algún mecanismo ya sea para la identificación o la autenticación de su ID, pero los grados de madurez son muy diversos a lo largo de la región iberoamericana. Luego, el grado de alcance de estos SID también varía no solo entre países, sino también entre las instituciones públicas. La ausencia de estrategias integrales de SID para el acceso a servicios públicos es una de las condiciones que caracteriza el entorno regional.

Un caso relevante es Bolivia, que, en el 2009, lanzó un sistema de identificación funcional y robusto para el propósito específico y limitado de crear un registro de votantes para apoyar el proceso electoral. Para lograr este objetivo, el gobierno dedicó dos años a preparar una campaña de registro de votantes de 75 días que se desarrolló de agosto a octubre de 2009, logrando identificar a 5.1 millones de personas a través de las huellas dactilares, una fotografía y la firma de los registrantes. Los registros utilizaron un Sistema Automatizado de Identificación de Huellas Dactilares (AFIS). La decisión de iniciar el registro en zonas rurales de baja densidad poblacional permitió la detección de problemas que deben abordarse en entornos de menor intensidad, antes de que el sistema se implemente en zonas urbanas y áreas más concurridas. La campaña de Bolivia también fue adaptativa con respecto a diferentes entornos y poblaciones, desarrollando enfoques personalizados para facilitar la inscripción rápida e inclusiva en zonas urbanas, rurales y periurbanas, regiones de ultramar, para zonas remotas inaccesibles por carretera y entre poblaciones indígenas[41].

[39] World Bank (2019b).
[40] World Bank (2019b).
[41] World Bank (2019a).

Aunque los SID pueden utilizarse para la identificación con fines electorales, o recepción de auxilio social, en la Tabla 1 se describen los SID de algunos países de Iberoamérica en función de su capacidad de ser la puerta de entrada para el acceso a servicios públicos digitales.

Tabla 1

Países de Iberoamérica con SID

País	Usos en la administración pública	Mecanismo de identificación digital	Ente rector	¿Existe un portal de servicios públicos digitales?	Acceso a servicios públicos digitales
Argentina	El proceso de verificación: verifica que la imagen del rostro del ciudadano coincide en rasgos con las tomadas al momento de la generación del DNI.	Mi Argentina	DNI Digital en la app móvil MiArgentina	Argentina.gob.ar	+/- 3,500 trámites digitales, incluyendo servicios de seguridad social, documentación, impuestos, salud, educación y registro de empresas.
Chile	Clave Única es un sistema de identificación digital personal e intransferible que permite a los y las ciudadanas acceder a diferentes servicios del Estado y realizar trámites en línea de manera segura.	Clave Única	Secretaría de Gobierno Digital	Chile Atiende	+/- 2,800 trámites en línea, que incluyen servicios de pensiones, educación, salud, trámites de vehículos, y subsidios gubernamentales.
Colombia	Además de identificar a los colombianos en trámites presenciales y no presenciales, es la llave de acceso que permite la identificación	Cédula Digital Colombia	Registraduría Nacional del Estado Civil	Gobierno Digital	+/- 1,500 trámites en línea que incluyen procesos de pagos y

País	Usos en la administración pública	Mecanismo de identificación digital	Ente rector	¿Existe un portal de servicios públicos digitales?	Acceso a servicios públicos digitales
	segura a través de servicios ciudadanos digitales.				notificaciones electrónicas.
Ecuador	Gob.ec permite verificar la autenticidad del documento de ID, a través del código QR.	Cédula Digital	Ministerio de Sociedad de la Información y Telecomunicaciones	Gob.ec	+/- 1,500 servicios disponibles en línea, desde servicios de educación, salud, hasta trámites relacionados con impuestos y registros.
El Salvador	La única forma de acceso a los servicios en línea disponibles es el sistema SIMPLE.SV El sistema no ocupa tecnologías biométricas, y el registro de las personas se valida a través de la interconexión con la base de datos del registro civil del país.	Login.gob.sv	Secretaría de Innovación y el Registro Nacional de las Personas Naturales	Simple.sv	+/- 200 trámites digitales, incluyendo educación, seguridad social, registro de empresas.
España	Cl@ve es un sistema orientado a unificar y simplificar el acceso electrónico de los ciudadanos a los servicios públicos. Su objetivo principal es que el ciudadano pueda	Cl@ve	Dirección de Tecnologías de la Información y las Comunicaciones	Administracion.gob.es	+/- 8,000 trámites disponibles, que incluyen gestiones de seguridad social,

País	Usos en la administración pública	Mecanismo de identificación digital	Ente rector	¿Existe un portal de servicios públicos digitales?	Acceso a servicios públicos digitales
	identificarse ante la administración mediante claves concertadas (usuario más contraseña), sin tener que recordar claves diferentes para acceder a los distintos servicios. Cl@ve complementa los actuales sistemas de acceso mediante DNI-e y certificado electrónico, y ofrece la posibilidad de realizar firma en la nube con certificados personales custodiados en servidores remotos. Con la app Cl@ve, también se habilita Cl@ve Móvil , que permite identificarse sin claves ni contraseñas, simplemente escaneando un QR o confirmando la petición que llega al móvil.		Ministerio de Presidencia		empleo, impuestos, educación y sanidad.
Portugal	Los recursos de atenticação.gov, como la Clave Móvil Digital, permiten realizar servicios y acceder a portales de diversas entidades públicas y privadas, de sectores empresariales como Banca,	Autenticación	Agencia de Modernización Administrativa	Gov.pt	+/- 1,000 servicios digitales, abarcando una amplia gama de trámites, que incluyen registro civil, impuestos, seguridad social, salud,

País	Usos en la administración pública	Mecanismo de identificación digital	Ente rector	¿Existe un portal de servicios públicos digitales?	Acceso a servicios públicos digitales
	Telecomunicaciones, Energía, Salud, Turismo, entre otros.				educación, vehículos y transporte.
Perú	La Plataforma Nacional de Identificación y Autenticación de la Identidad Digital (IDGob.pe) se enfoca en la verificación en línea de la identidad de las personas naturales, peruanas o extranjeras, cuando requieren acceder a trámites y servicios en cualquier entidad del Estado.	ID Gob.pe	Registro Nacional de Identificación y Estado Civil	Gob.pe	+/- 1,000 trámites disponibles, principalmente relacionados con salud, servicios de educación, y trámites tributarios.
República Dominicana	Soy Yo RD es una aplicación móvil que ofrece a los ciudadanos un espacio para reunir sus datos y documentos, y revisar el estado de estos. Con una cuenta única cada dominicano tiene la oportunidad de visualizar sus datos, obtener alertas de expiración y manejar toda su información en un solo lugar. Gracias a esta carpeta Soy Yo RD, el ciudadano también verifica el estado de sus datos, para cuando vaya a realizar trámites en la plataforma gob.do o los	SoyyoRD	Oficina Gubernamental de Tecnologías de Información y Comunicación (OGTIC)	Gob.do	+/- 1,400 trámites en línea, que incluyen servicios de seguridad social, trámites de vehículos, educación, empleo y salud.

País	Usos en la administración pública	Mecanismo de identificación digital	Ente rector	¿Existe un portal de servicios públicos digitales?	Acceso a servicios públicos digitales
	puntos gob.				
Uruguay	Usuario gub.uy es un método de identificación digital que pone a disposición el Estado uruguayo. Tiene dos niveles de garantía: básico (autorregistrado) e intermedio (verificado). Utiliza diferentes mecanismos de ID: Cédula de Identidad con Chip, ID Digital Abitab, TuID Antel	Usuario gub.uy	Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento	Gub.uy	+/- 1,200 trámites disponibles, principalmente relacionados con identificación, salud, licencias, servicios de educación, y servicios municipales.

Fuente: elaboración propia, con base a sitios consultados.

2.1 Políticas y normas

Para la CIPDED, «deben hacerse esfuerzos relevantes para garantizar que la privacidad de las personas y el procesamiento de sus datos personales estén protegidos en entornos digitales, respetando las legislaciones nacionales en la materia» (p. 12)[42], propiciando la cooperación efectiva entre los países para mejorar y ampliar la protección de datos y privacidad en los procesos de ID, que permita una mayor inclusión social, el reconocimiento efectivo de los derechos y, en especial, la prevención del robo o fraude de identidad. Al menos dos países de la región (Argentina y Uruguay) han sido declarados países adecuados por la Comisión Europea, por tanto, sus sistemas de protección de datos personales ya se encuentran alineados con los estándares europeos previstos inicialmente por la anterior Directiva 95/46/CE[43].

El marco legal de los países de Iberoamérica en materia de seguridad, validez y confianza en el proceso de identificación digital es diverso. En algunos casos, como Argentina, Uruguay, Colombia, Chile y España, se identifica terminología relacionada con ID, SID o autenticación como parte de la normativa, lo cual incluye la protección de datos personales en ámbitos digitales. Las experiencias de estos países son determinantes para caracterizar a la región, ya que evidencian el grado de madurez de los marcos legales, indispensables para un SID saludable. En la mayoría de los casos, los países cuentan con algún tipo de regulación sobre la protección de datos personales, aunque aún hay casos, como el de El Salvador, donde no se ha logrado establecer un marco legal para tal fin. No obstante, el desarrollo de marcos legales para respaldar y fomentar las ID y los SID ha avanzado a diferentes ritmos entre los países. En general, de una muestra de 22 países en estudio, se identificaron 12 con una ley de protección de datos personales y 11 con un marco legal relacionado con la ID y/o el establecimiento de SID.

En relación con el concepto de datos personales, Argentina, Chile y México comparten definiciones similares, en tanto se refieren a los datos de personas físicas identificadas o identificables[44]. Dado que los sistemas de identificación implican la recopilación, el almacenamiento y el uso de datos personales, es esperado que los países también definan mecanismos de protección y respeto a la privacidad, como un factor fundamental para la confianza del ciudadano con las interacciones con el gobierno.

A pesar de estos positivos números, muchas de las leyes de protección de datos personales necesitan de una importante y urgente modernización, que responda a los vertiginosos avances tecnológicos que generan desafíos que trascienden límites geográficos[45], en especial, frente a los retos de tecnologías emergentes como la inteligencia artificial. Estas renovaciones deberían, además, considerar el desarrollo de las capacidades de las personas y aporten «al desarrollo inclusivo a nivel económico, social y cultural al servicio de toda la sociedad» (p. 12)[46], según lo anhela la CIPDED.

[42] SEGIB (2023).
[43] Asociación por los Derechos Civiles (2016).
[44] Asociación por los Derechos Civiles (2016).
[45] Red Española del Pacto Mundial (2018).
[46] SEGIB (2023).

A inicios del 2024 entró en vigor el Reglamento (UE) 2024/1183, del 11 de abril, conocido como Reglamento eIDAS2, que modifica el Reglamento 910/2014. En esta nueva versión se establece la «identidad digital europea unificada»; se espera que se convierta en un estándar sobre el tratamiento de la ID, no solo para efectos país, sino también para fortalecer los procesos transfronterizos. En el marco de ello, países iberoamericanos también han participado en diálogos políticos de gobernanza digital con miras a profundizar su aprendizaje sobre las experiencias de países en Europa desarrollando tecnologías, apropiación y cultura digital, para que los ciudadanos adopten y usen su ID con la misma confianza que si fuera un dispositivo físico.

De acuerdo con el Banco Mundial, las leyes, regulaciones y políticas relacionadas con la identificación deberían permitir a las personas con identidad genuina controlar el uso de sus datos, incluida la capacidad de revelar selectivamente los atributos que desean compartir. Algunos países, como Brasil, definen que las personas puedan tener control sobre sus datos, no solo en el proceso de compartirlos con una autoridad sino como estos se distribuyen para acceder a servicios públicos a través de la plataforma de servicios en línea Gov.br. Para los SID, el reto está en convertirse en entidades transparentes en cuanto a gestión de la identidad[47], otorgando oportunidades a los usuarios para gestionar sus condiciones de privacidad, es decir, que puedan a través de mecanismos administrativos corregir o mejorar sus datos, sin implicar acciones judiciales que generen costos tanto para las personas como para el Estado.

En el 2017, La Red Iberoamericana de Protección de Datos (RIPD) lanzó *los Estándares de Protección de Datos de los Estados Iberoamericanos*[48], que son directrices orientadoras que contribuyan a la emisión de iniciativas regulatorias de protección de datos en aquellos países de la región iberoamericana que no cuentan con estos ordenamientos, o que sean referentes para la modernización y actualización de las legislaciones existentes. Para la elaboración de los Estándares Iberoamericanos se tomaron como referencia algunos instrumentos internacionales, tales como: las directrices relativas a la protección de la intimidad y de la circulación transfronteriza de datos personales de la Organización para la Cooperación y Desarrollo Económicos (OCDE); el Convenio número 108 del Consejo de Europa y su Protocolo; el Marco de Privacidad del Foro de Cooperación Económica Asia Pacífico; y el Reglamento del Parlamento Europeo y del Consejo, relativo a la protección de las personas en lo relacionado con el tratamiento de datos personales y la libre circulación de estos datos, entre otros[49]. La existencia de marcos orientadores para desarrollar legislación precisa y coherente con el resguardo de los derechos y deberes de las personas en los entornos digitales, es una ventaja para acelerar el fortalecimiento de marcos legales en la región. En especial, sobre la protección de datos personales, que es una de las piezas claves del marco legal que sustenta la identificación digital y la ID en sí misma.

Los marcos legales de ciberseguridad, ciberdelito y manejo de tecnologías emergentes se vuelven, igualmente, importantes en la definición del ecosistema legal que promueve la ID. En Iberoamérica,

[47] World Bank (2019c).
[48] Red Iberoamericana de Protección de Datos (2017).
[49] Red Española del Pacto Mundial (2018).

más de 15 de los 22 países cuentan con un marco legal de ciberseguridad, y son, a su vez, adherentes con el Convenio de Budapest[50].

Figura 8

Muestra de países de Iberoamérica y sus marcos legales de ID, protección de datos personales y firma electrónica

Fuente: elaboración propia.

Las leyes que rigen la identificación digital deben prever sistemas de rendición de cuentas para los organismos que implementan y operan el SID, reguladores, actores públicos y privados que utilicen la ID de cualquier forma, y otros actores facilitadores o de apoyo[51]. En la mayoría de los países de Iberoamérica un solo ente rector hace las veces de implementador de las leyes de protección de datos personales, y a la vez de generador de procesos de autenticación y validación (Tabla 2).

[50] Budapest Convention on Cybercrime of the Council of Europe (2023).
[51] The Centre for Internet & Society (2020).

Tabla 2

Marcos legales de países de Iberoamérica relacionados con la ID y los SID

País	Marco legal	Descripción de sus marcos legales
Andorra	**Datos personales**	La Ley de Protección de Datos Ley 29/2021, es una adaptación a las directrices del Reglamento General de Protección de Datos (GDPR) de la Unión Europea. Esta ley es determinante para la gestión segura de la ID, asegurando que los datos personales se manejan con los más altos estándares de seguridad y privacidad.
	Firma electrónica	Ley de Firma Electrónica Ley 21/2007, de 18 de octubre, regula el uso de la firma electrónica en Andorra, otorgando validez jurídica a los documentos firmados electrónicamente, siempre que cumplan con los requisitos establecidos. Establece la base legal para la ID en términos de autenticación y verificación de firmas.
Argentina	**Identidad presencial e ID**	• Decreto Nº 1265/2016 que lleva el nombre «Plataforma de Autenticación Electrónica Central». El mismo atribuye a la Secretaría de Innovación Pública, ex Ministerio de Modernización, la responsabilidad de creación de una plataforma (Autenticar) de autenticación electrónica que brinde un servicio centralizado para resolver la necesidad de instrumentar la autenticación digital del mercado digital actual. Mientras que el Decreto N° 894/2017 - Implementación del DNI Digital, establece la implementación del DNI en formato digital, permitiendo a los ciudadanos llevar su documento de identidad en sus dispositivos móviles y utilizarlo para trámites y gestiones electrónicas. • Ley N° 27.078 de Argentina Digital, declara de interés público el desarrollo de las Tecnologías de la Información y las Comunicaciones (TIC) y establece un marco para el acceso a estas tecnologías, lo que incluye aspectos relacionados con la ID.
	Datos personales	• Ley de Protección de Datos Personales (Ley N° 25.326) protege a los datos de identidad, de salud o de crédito si son usado sin consentimiento. Si bien no se refiere directamente a la ID, establece el marco legal para la recolección, tratamiento y protección de datos, que es fundamental para cualquier SID. • Ley 27.699 del 2022 Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter

País	Marco legal	Descripción de sus marcos legales
		Personal, establece un marco legal para el tratamiento de datos personales, que incluye la recolección, almacenamiento, procesamiento, y uso de dichos datos.
	Firma electrónica	Ley de Firma Digital (Ley N° 25.506), reconoce y establece las condiciones para el empleo de la firma electrónica y de la firma digital y su eficacia jurídica, y crea la Infraestructura de Firma Digital de la República Argentina.
Bolivia	**Identidad presencial e ID**	La Ley N° 1080 de Ciudadanía Digital de Bolivia establece las condiciones y responsabilidades para que los ciudadanos bolivianos puedan ejercer su ciudadanía digital. La ciudadanía digital es la identidad digital de los ciudadanos bolivianos, que les permite interactuar con el Estado a través de servicios digitales.
	Firma electrónica	La Ley Nº 164 de 8 de agosto de 2011, también conocida como Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación, regula la firma electrónica en Bolivia. Esta ley le otorga validez jurídica a la firma digital.
Brasil	**Identidad presencial e ID**	• Ley Nº 14.063/2020, no define directamente «ID». La regulación de firmas electrónicas y documentos electrónicos bajo esta ley implica un enfoque en la verificación y autenticación de identidades en entornos digitales. • El Decreto Nº 10.543 del 2020, establece el Reglamento del Documento Nacional de Identidad (DNI) en Brasil. Este decreto es una medida importante para la implementación y regulación del DNI, que busca unificar y simplificar la identificación de los ciudadanos brasileños. • El Decreto Nº 9.319, trata sobre la Regulación del Registro Nacional de Identificación Civil (RNIC), un sistema que busca unificar la identificación de los ciudadanos brasileños.
	Datos personales	• En la Ley Nº 13.709/2018, la Ley General de Protección de Datos (LGPD), la ID se relaciona con los datos personales que permiten identificar a una persona en entornos digitales. La ley define datos personales como «información relacionada con una persona natural identificada o identificable». Esto incluye datos que pueden formar parte de la ID, como nombre, número de identificación, dirección IP, datos biométricos, y cualquier otra información que pueda ser utilizada para identificar a una persona en el ámbito digital.

País	Marco legal	Descripción de sus marcos legales
		• Ley Nº 12.965/2014 «Marco Civil de Internet», es un marco legal que regula, entre otras cosas, la protección de datos personales y la privacidad en línea, que son componentes esenciales de la ID.
	Firma electrónica	La Ley 14.620 establece los parámetros de la Infraestructura de Clave Pública (ICP-Brasil), que es la base para la seguridad de las firmas electrónicas. Esta infraestructura, regulada por la Autoridad Nacional de Protección de Datos (ANPD), es responsable de garantizar la autenticidad e integridad de documentos firmados electrónicamente.
Chile	**Identidad presencial e ID**	• En términos legales, la Clave Única no está contenida en una ley, por lo que Chile en rigor no cuenta con una legislación que homologue los sistemas físicos de identidad (como el carné de identidad o el pasaporte) a sistemas digitales[52]. En el 2024 se inició una propuesta de proyecto del Gobierno que busca implementar una cédula de ID que permita a los ciudadanos realizar trámites en línea de manera segura y eficiente. • En proceso está la Norma Técnica de Autenticación que establecería la Clave Única como el mecanismo oficial de autenticación para acceder a servicios digitales del Estado, según lo dispuesto en la Ley N° 21.180 de Transformación Digital del Estado. El SID referente en Chile es el de registros personales digitalizado que administra el Servicio de Registro Civil e Identificación, que a su vez es obligatorio y recolecta datos biométricos. • La Ley Ley N.º 21.180 (Ley de Transformación Digital del Estado) no define explícitamente «ID», pero establece un marco normativo que facilita su implementación y uso en la administración pública.
	Datos personales	• La Ley N.º 21.459 (Ley de Protección de Datos Personales) introduce un marco regulatorio más robusto para la protección de datos personales, alineado con estándares internacionales como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea. No define directamente a la ID, pero sus principios y regulaciones sobre la protección de datos personales son fundamentales para la seguridad y gestión adecuada de la ID en Chile. • La actualización a la Ley de Protección de la Vida Privada (Ley N.º 19.628) regula el tratamiento de datos personales y establece principios sobre la protección de la privacidad de los ciudadanos en Chile.

[52] Weidenslaufer y Roberts (2022).

País	Marco legal	Descripción de sus marcos legales
	Firma electrónica	La Ley de Firma Electrónica (Ley N.º 19.799) del 2022, regula el uso de firmas electrónicas y documentos electrónicos en Chile. Facilita la autenticación y la integridad de las transacciones digitales, contribuyendo a la confianza en la ID.
Colombia	**Identidad presencial e ID**	• Actualmente, tanto la cédula digital como la cédula amarilla con hologramas (física) están vigentes y ambos documentos contienen la misma información. De conformidad con la Constitución Política de Colombia, el decreto 1413 de 2017, Ley 1955 de 2019, el Decreto Ley 2106 de 2019, entre otros, los documentos de identidad expedidos por la Registraduría Nacional del Estado Civil son los únicos que acreditan la identidad de los colombianos y, por ende, deben ser reconocidos y avalados por las diversas autoridades; la versión digital de la cédula recolecta datos biométricos. El Decreto 620 del 2020, reglamenta la autenticación de los ciudadanos mediante la ID para el acceso a trámites y servicios electrónicos ofrecidos por el Estado. Ley Estatutaria 1266 de 2008, Ley de Habeas Data, regula el manejo, protección y administración de la información personal en bases de datos, y establece normas para la protección de datos personales y el derecho a la información. • Aunque la Ley 1342 del 2009 no trata específicamente la ID, establece el marco general para el desarrollo y regulación de las TIC, lo que incluye aspectos relacionados con la seguridad, la privacidad y la infraestructura digital. En la misma línea, el Decreto 2106 de 2019 no trata directamente la ID. Su regulación sobre la gestión de la información pública contribuye a la creación de un entorno más transparente y accesible para la ciudadanía; esto puede influir indirectamente en el desarrollo y la implementación de soluciones de ID.
	Datos personales	La Ley de Protección de Datos Personales o Ley 1581 de 2012, reconoce y protege el derecho que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos, o archivos que sean susceptibles de tratamiento por entidades de naturaleza pública o privada.
	Firma electrónica	El Decreto 2364 de 2012, reglamenta la interoperabilidad y uso de las firmas digitales, documentos electrónicos y certificados digitales en Colombia.
Costa Rica	**Datos personales**	• La Ley General de Protección de Datos Personales (Ley No. 8968), regula el tratamiento de los datos personales, tanto en medios físicos como digitales, y establece derechos y obligaciones para proteger la privacidad de los ciudadanos.

País	Marco legal	Descripción de sus marcos legales
		• Ley No. 8239 Derechos y deberes de las personas usuarias de los servicios de salud públicos y privados, contempla en el artículo 2, que los pacientes y usuarios de servicios de salud tienen derecho a hacer que se respete el carácter confidencial de su historia clínica y de toda la información relativa a su enfermedad, salvo cuando por ley especial, deba darse noticia a las autoridades sanitarias. • La Ley 9162 Expediente Digital Único de Salud, contempla, en el artículo 11, que toda la información contenida se considera información privada que contiene datos sensibles y se prohíbe el tratamiento de dichos datos.
	Firma electrónica	Ley de Certificados, Firmas Digitales y Documentos Electrónicos Nº 8454, regula el uso de firmas digitales y documentos electrónicos, otorgándoles validez legal equivalente a la de documentos en papel.
Ecuador	**Identidad presencial e ID**	La Ley Orgánica para la Transformación Digital y Audiovisual, publicada en el Registro Oficial Tercer Suplemento No. 245, del 07 de febrero de 2023, incorpora al ordenamiento jurídico de forma plena la noción de la ID. La Dirección General de Registro Civil, Identificación y Cedulación de Ecuador, implementa el SID que hace obligatorio el registro desde el nacimiento y recolecta datos biométricos de los ciudadanos ecuatorianos, incluyendo a extranjeros residentes en el país[53]. El Proyecto de Cedulación Electrónica (2016), permite una representación electrónica de la identidad física de un ciudadano, utilizando cédulas con chips que almacenan información biométrica, lo que permite una autenticación segura y efectiva en entornos digitales.
	Datos personales	La Ley Orgánica de Protección de Datos Personales, permite identificar a una persona en entornos digitales, garantizando la privacidad y el control de su información en dichos espacios.
	Firma electrónica	El Código Orgánico General de Procesos, habilita el uso de medios electrónicos y firmas electrónicas para la presentación de documentos y actos procesales, validando la autenticidad e integridad de las personas involucradas en los procedimientos judiciales digitales.
España	**Identidad presencial e**	• Según la Ley 11/2007, los ciudadanos pueden utilizar los siguientes sistemas para identificarse ante la administración: el DNI electrónico, el sistema de firma electrónica avanzada, incluyendo los que se basan

[53] Derechos Digitales América Latina (2023).

País	Marco legal	Descripción de sus marcos legales
	ID	en certificado electrónico reconocido, y otros sistemas como claves concertadas en un registro previo, o la aportación de información conocida por ambas partes u otros sistemas no criptográficos. • Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, permite identificar de manera única a un ciudadano o entidad en el entorno digital, asegurando la autenticidad de su identidad y la validez de sus actuaciones electrónicas • Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, ofrece mecanismos y herramientas que permiten a los ciudadanos y a las empresas identificarse de manera segura ante las administraciones públicas en entornos digitales, certificando la autenticidad de la identidad y la integridad de las transacciones electrónicas. • La identificación digital en España está respaldada por el Reglamento (UE) n.º 910/2014 (eIDAS) y por leyes nacionales como la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza. Este marco legal avala la validez y el reconocimiento de la identificación y la firma electrónica en todo el territorio de la Unión Europea.
	Datos personales	Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales: asegura que la gestión de la ID respete la privacidad de los ciudadanos y que el tratamiento de los datos personales se realice de manera segura y conforme a la ley.
	Firma electrónica	La firma electrónica se regula mediante la aplicación de la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza y el Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 (eIDAS), relativo a la identificación electrónica y los servicios de confianza en las transacciones electrónicas en el mercado interior.
Portugal	**Identidad presencial e ID**	• Ley 7/2007, de 5 de febrero (en su redacción actual), por la que se crea la tarjeta ciudadana y se regula su expedición y utilización;

País	Marco legal	Descripción de sus marcos legales
		• Ley 37/2014, de 26 de junio, en su redacción actual, por la que se establece un sistema alternativo y voluntario de autenticación de ciudadanos en los portales y sitios web de las Administraciones Públicas denominado Clave Móvil Digital; • Decreto-Ley N° 12/2021, de 9 de febrero, por el que se garantiza la ejecución en el ordenamiento jurídico interno del Reglamento (UE) 910/2014, relativo a la identificación electrónica y a los servicios de confianza para las transacciones electrónicas en el mercado interior.
	Datos personales	El Reglamento General de Protección de Datos (GDPR), permite identificar a una persona en el entorno digital. Esto puede incluir datos como nombres de usuario, contraseñas, y cualquier información asociada a la identificación en línea.
	Firma electrónica	Decreto-Ley N° 12/2021, de 9 de febrero, por el que se garantiza la ejecución en el ordenamiento jurídico interno del Reglamento (UE) 910/2014, relativo a la identificación electrónica y a los servicios de confianza para las transacciones electrónicas en el mercado interno.
Panamá	**Identidad presencial e ID**	• Ley N° 126 de 13 de diciembre de 2019 - Ley de Gobierno Digital, establece el marco para la transformación digital del gobierno panameño, promoviendo la digitalización de los servicios públicos y la implementación de la ID para mejorar la eficiencia y transparencia en la administración pública. • Decreto Ejecutivo N° 767, de 26 de octubre de 2021, reglamenta la implementación de la ID en Panamá, estableciendo los lineamientos para la creación, gestión y uso de la ID de los ciudadanos y residentes. • La Ley 44 del 2020, modifica y adiciona artículos a la Ley 83 de 2012, sobre el uso de medios electrónicos para trámites gubernamentales, y se adiciona el establecimiento de un portal único, donde el ciudadano podrá acceder de forma rápida y segura a todos los trámites que requiera realizar con el Estado, así como la incorporación de una ID, una billetera digital estatal, actualización del mecanismo de pagos en línea para los trámites gubernamentales y un sistema de gestión documental.

País	Marco legal	Descripción de sus marcos legales
	Datos personales	Ley N° 81- Ley de Protección de Datos Personales, que regula el tratamiento de datos personales en Panamá, estableciendo normas para la protección de la privacidad de los individuos en entornos digitales, un aspecto importante para la implementación de la ID.
	Firma electrónica	Ley N° 51 de 22 de julio de 2008 - Ley de Firma Electrónica, que establece la regulación del uso de la firma electrónica en Panamá, reconociéndola como un equivalente legal a la firma manuscrita en documentos físicos. Es un pilar fundamental para la ID en el país.
Perú	**Identidad presencial e ID**	• Del 2016, el Decreto Legislativo N° 1310, promueve la simplificación administrativa y la digitalización de trámites en el Estado peruano, facilitando el uso de la ID para interactuar con entidades públicas. • En el 2018, el Decreto Legislativo N° 1412 - Ley de Gobierno Digital, introduce la ID como un componente clave del Gobierno Digital en Perú, promoviendo el uso de tecnologías para la autenticación segura de los ciudadanos en trámites y servicios en línea. Para el 2021, la Resolución Ministerial N° 119-2021-PCM, aprueba la Estrategia Nacional de Transformación Digital, que incluye la promoción de la ID como un elemento determinante para la digitalización de servicios públicos y privados.
	Datos personales	La Ley N° 29733 - Ley de Protección de Datos Personales, la cual protege los datos personales que forman parte de la ID, regulando su tratamiento y garantizando los derechos de los ciudadanos sobre sus datos. El Decreto Supremo N° 003-2013-JUS - Reglamento de la Ley de Protección de Datos Personales, desarrolla las disposiciones de la Ley N° 29733, detallando las obligaciones de los responsables del tratamiento de datos y los derechos de los titulares. Refuerza la protección de la ID en el contexto del uso de tecnologías de la información y comunicación.
	Firma electrónica	Ley N° 27269 - Ley de Firmas y Certificados Digitales, establece el marco legal para el uso de firmas digitales y certificados digitales en Perú, facilitando la autenticación de la identidad de las personas en el entorno digital.

País	Marco legal	Descripción de sus marcos legales
República Dominicana	**Identidad presencial e ID**	La Ley 339-22 de 2022, habilita y regula el uso de medios digitales para los procesos judiciales y procedimientos administrativos del Poder Judicial, reconociendo que la autenticación de la ID en distintas plataformas del Poder Judicial[54].
	Datos personales	• Según la Ley 172-13, cuyo objetivo es proteger los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a informar, sean públicos o privados. Los datos personales se verificarán para validar la identidad e información del usuario, así como con fines operativos y estadísticos, como insumo para desarrollar políticas públicas o para cualquier uso destino que la OGTIC considere apropiado según su objeto institucional. • La Ley General de Protección de Datos Personales está actualmente en proceso de aprobación. Esta ley establecerá un marco legal completo para la protección de los datos personales de los ciudadanos, lo que tendrá un impacto directo en la gestión de la ID; la ley se centra en la protección de datos personales y establece que la «ID» puede ser comprendida en términos de protección de la información que permite identificar a una persona en el entorno digital.
	Firma electrónica	La norma dominicana que regula la firma digital es la Ley 126-02 sobre Comercio Electrónico, Documentos y Firmas Digitales, del 14 de agosto de 2002, y su Reglamento de Aplicación (Decreto No. 335-03).
Uruguay	**Identidad presencial e ID**	• Con las modificaciones introducidas en el año 2017, la Ley N° 18.600 establece la equivalencia entre la identificación presencial y aquella realizada por medios electrónicos seguros, según los criterios establecidos por la Unidad de Certificación Electrónica. Da paso a la implementación de la Política de Identificación Digital. • Ley N° 19.355 (Presupuesto Nacional 2015-2019): la ID se entiende como la capacidad de una persona para identificarse y autenticarse en servicios electrónicos mediante el uso de certificados digitales y otras tecnologías relacionadas.

[54] Congreso Nacional (2022).

País	Marco legal	Descripción de sus marcos legales
	Datos personales	Ley N° 18.331 de Protección de Datos Personales: establece que los datos personales deben ser tratados con estricta confidencialidad, garantizando que la información identificativa de los ciudadanos sea protegida de manera adecuada en los entornos digitales.
	Firma electrónica	Ley N° 18.600 de Firma Electrónica, que regula el uso de la firma electrónica y su validez jurídica en documentos digitales, un componente esencial de la ID en la interacción con entidades públicas y privadas.

Fuente: elaboración propia con base a fuentes legales consultadas de cada país.

2.2 Funcionamiento

La CIPDED reconoce que la «transformación digital debe incorporar a las mujeres, niñas, adultos mayores, personas con discapacidad y otros grupos en situación de vulnerabilidad» (p. 9)[55], es decir que, para que se reconozcan los derechos de las personas en entornos digitales, deben asegurarse amplias condiciones para que los grupos vulnerables no queden fuera de estos beneficios, y que todo proceso de transformación digital no genere (en la medida de lo posible) nuevas brechas para alcanzar óptimos de inclusión digital y social.

En un anhelo compartido por Iberoamérica, la CIPDED establece que «toda persona debería poder confiar en que los sistemas digitales que utilice, ya sea en su relación con el Estado o en el ejercicio de su actividad profesional, económica, social o recreativa, serán seguros y respetuosos de sus derechos a la integridad, a la protección de datos personales y a la privacidad, en el marco legal vigente en su país» (p. 12)[56]. Esto subraya que el diseño de los SID y de la ID no es solo una cuestión técnica. La seguridad que las personas perciben al ser identificadas a través de carnés físicos debe ser comparable a la experiencia digital, especialmente cuando los sistemas de autenticación de ID y las firmas electrónicas se utilicen para garantizar la integridad de documentos digitales.

En general, se evidencia un compromiso por desarrollar y mejorar los SID en los países de Iberoamérica. Cabe destacar que, en el apartado sobre *Casos iberoamericanos de SID para el acceso a servicios públicos digitales*, de este documento, se presenta una exposición detallada de los casos de algunos de estos países.

Figura 9

[55] SEGIB (2023).
[56] SEGIB (2023).

Ejemplos de iniciativas de ID

Fuente: elaboración propia.

2.2.1 SID centralizados

En un SID centralizado, existe una autoridad única (generalmente el Estado) que gestiona la ID de las personas. Este enfoque es común en muchos países, donde una sola entidad controla todos los aspectos del sistema, es decir, almacena y gestiona los datos de las personas, emite las credenciales y verifica la identidad. Todos los datos se almacenan en una única base de datos o servidor, lo que facilita la administración, pero incrementa el riesgo en caso de brechas de seguridad. La entidad central puede tener acceso a los datos de las personas, lo que genera preocupaciones sobre la privacidad. Si el sistema centralizado se ve comprometido (por fallos técnicos o ataques cibernéticos), podría afectar a todos los usuarios.

Uno de los beneficios de un SID es su capacidad para establecer la identidad en múltiples ámbitos, como transacciones financieras, atención médica o uso de transporte público. Sin embargo, esto también puede generar un riesgo de «punto único de falla». En algunos SID, cada vez que un individuo utiliza una credencial de identificación, se pueden generar datos de uso y transacciones, los cuales pueden ser recopilados y almacenados[57]. La OCDE recomienda a los gobiernos que la ID debe ser interoperable, única, accesible y fácil de utilizar por todos los ciudadanos[58], además de garantizarles el control sobre sus propias identidades digitales y que puedan acceder y administrar sus datos personales.

En Iberoamérica, algunos países con un diseño de SID centralizado son México (Registro Nacional de Población), Argentina (Registro Nacional de Personas), Chile (Registro Civil) y Colombia

[57] World Bank (2018a).
[58] Durango (2023).

(Registraduría Nacional del Estado Civil), los cuales comparten, en general, las siguientes características:

- Existe una única entidad de la administración pública responsable de recopilar, almacenar y gestionar los datos personales de los ciudadanos. Estas bases de datos suelen estar controladas por el gobierno, a través de organismos nacionales de registro civil o ministerios del interior o seguridad.
- Los ciudadanos deben registrarse en el sistema para obtener una identificación oficial, la cual es gestionada y verificada por la administración pública.
- Se almacena una amplia gama de datos personales, que incluyen nombres, fechas de nacimiento, huellas dactilares, direcciones y, en algunos casos, información biométrica.
- Los procesos de verificación de identidad dependen de la administración pública. Si un ciudadano necesita validar su identidad para acceder a un servicio, la verificación se realiza a través del mecanismo, estándar o tecnología que establezca la entidad.
- La escalabilidad de un sistema centralizado hacia nuevos servicios o tecnologías suele ser lenta y puede generar cuellos de botella, ya que requiere grandes inversiones en infraestructura tecnológica, capacitación y actualización de los sistemas.
- Los sistemas centralizados, al estar gestionados por una única administración pública, pueden no estar diseñados para interactuar con otros sistemas o bases de datos a nivel regional o global. Esto limita la capacidad de los ciudadanos para utilizar su identidad de manera fluida en diferentes países o servicios.

2.2.2 SID descentralizados

En los SID descentralizados, no existe una autoridad central que controle la identificación de las personas. En su lugar, las identificaciones son gestionadas por las propias personas mediante tecnologías que garantizan la confianza sin necesidad de intermediarios, como *blockchain* o las Tecnologías de Registros Distribuidos (DLT).

Las personas deciden qué información compartir y con quién; no hay una entidad única que controle los datos. La confianza se establece a través de redes descentralizadas: en sistemas basados en *blockchain*, las transacciones relacionadas con la identidad se registran de manera inmutable, lo que garantiza transparencia y seguridad. La Unión Europea, en su propuesta eIDAS2, ha adoptado algunos principios de la identidad soberana basada en *blockchain*, estableciendo su modelo en la billetera digital (*Wallet* o *App*). En esta billetera, las personas podrán vincular su identidad legal, además de almacenar y gestionar credenciales de sus atributos emitidos por fuentes auténticas (entidades públicas o privadas de confianza), como el pasaporte, la licencia de conducir, el carné profesional, los títulos académicos o la certificación que vincula a la persona con su empleador. En España, las normas ISO/IEC y la norma española UNE 71307-1 desarrollan el *Modelo de Gestión de Identidades Descentralizadas sobre Blockchain y otras Tecnologías de Registros Distribuidos*.

La W3C ha creado estándares de identificadores descentralizados, en donde se establece una arquitectura, modelo de datos y representación (Decentralized Identifiers [DIDs] v1.0 Core) que

garantizan la interoperabilidad, la seguridad y la eficiencia en el intercambio de información entre instituciones públicas y privadas[59].

Países como Chile, Colombia, Argentina y Brasil presentan un diseño de SID descentralizado, que tiene en general las siguientes características:

- No existe una entidad central que emita las credenciales; en su lugar, se trata de un ecosistema de confianza basado en estándares que fomentan alianzas entre entidades públicas y privadas.
- Los usuarios tienen completo control sobre sus datos, decidiendo a quién compartirlos y qué información proporcionar. Además, los sistemas de identidad son autogestionados.
- Se minimiza la cantidad de información compartida con otras entidades, utilizando técnicas como la verificación de prueba de conocimiento cero. Esto permite a los usuarios demostrar que cumplen ciertos criterios sin revelar todos sus datos personales.
- Se evita la dependencia de registros únicos nacionales que no fueron diseñados para entornos digitales y que podrían ser vulnerables a ataques o corrupción.
- En el caso de los registros almacenados en una red descentralizada, como una *blockchain*, estos son inmutables. Una vez almacenados, no pueden modificarse sin la aprobación de todas las partes involucradas.
- Se interactúa por múltiples credenciales de múltiples entidades, en donde existe confianza en las credenciales emitidas a una persona.

[59] W3C (2022).

2.2.3 SID híbridos

Los sistemas híbridos combinan elementos de los enfoques centralizados y descentralizados, buscando aprovechar las ventajas de ambos. En estos sistemas, una parte de la información es gestionada por una autoridad central, mientras que otros aspectos de la identidad son controlados de manera descentralizada o directamente por las personas.

Puede haber cooperación entre diferentes entidades (gubernamentales, privadas, redes descentralizadas) para gestionar la identidad de manera conjunta. Un ejemplo de esto son los identificadores que pueden ser gestionados de manera descentralizada, pero que interactúan con sistemas centralizados para autenticar la identidad, creando así un modelo híbrido.

En Brasil, se está trabajando en un SID conocido como Identidade Digital Nacional, que busca unificar múltiples registros de identidad en una sola plataforma digital. Aunque el enfoque inicial es centralizado, se están explorando mecanismos para que los ciudadanos tengan mayor control sobre el uso de sus identidades digitales en plataformas tanto privadas como públicas[60].

En México, su sistema actual de identificación dgitial es mayormente centralizado; sin embargo, existe un creciente interés en explorar soluciones descentralizadas, especialmente para otorgar a los ciudadanos mayor control sobre sus datos. Se han realizado pruebas con tecnología *blockchain* en áreas como la autenticación y certificación de documentos digitales, lo que podría sentar las bases para un sistema híbrido[61].

Los países con mecanismos robustos de ID y SID, como Chile y Colombia, presentan un diseño de SID híbrido que tiene, en general, las siguientes características:

- Los sistemas de identificación híbridos combinan elementos de los enfoques centralizados y descentralizados, aprovechando las ventajas de ambos tipos de sistemas.
- En los sistemas de identificación híbridos, la identificación y verificación se realizan de forma centralizada, mientras que otros aspectos de la información son administrados por las personas o por otras entidades. Además, existen colaboraciones que fortalecen el sistema híbrido.

2.2.4 Beneficios de los SID para el acceso a servicios públicos digitales

Brasil podría aprovechar la identificación digital para facilitar la creación de servicios de gobierno electrónico que podrían ahorrar a los brasileños hasta 2.800 millones de horas al año[62]. La implementación de mecanismos de ID y SID es parte indispensable de una estrategia para la prestación de servicios públicos digitales, adquiriendo mayor relevancia en el contexto de servicios relacionados con programas sociales que atienden las necesidades básicas de la población.

[60] Imamovic (2023).
[61] Cotait (2023).
[62] McKinsey Global Institute (2019).

Los programas sociales suelen ser iniciativas de gran alcance, caracterizadas por una definición específica de la población objetivo y una oferta de servicios públicos. El uso de la ID y los SID es propicio para la supervisión del uso de los recursos públicos y para asegurar que los beneficios de cada programa social se entreguen efectivamente a las personas. En la región iberoamericana, se han registrado diversas iniciativas que demuestran el uso de la ID y los SID en las fases de identificación digital de los ciudadanos. A continuación, se presentan algunos ejemplos:

Tabla 3

Ejemplos de programas sociales que utilizan SID en Iberoamérica

País	Programa social	Descripción
Argentina	Asignación Universal por Hijo	Emplea la identificación digital para gestionar el registro de beneficiarios y facilitar los pagos.
Brasil	Bolsa Familia	Utiliza un sistema de registro digital para identificar a beneficiarios y monitorear su situación socioeconómica.
Ecuador	Bono de Desarrollo Humano	Implementa un sistema de identificación digital para verificar la elegibilidad de las familias en situación de pobreza.
Panamá	Vale Digital	Este programa utiliza el registro digital de la cédula e identifica a los beneficiarios del subsidio para realizar las transferencias correspondientes. Habilita que, con el uso de las cédulas físicas, las personas puedan realizar transacciones.
Perú	Programa Juntos	Emplea un sistema de identificación digital para asegurar que los beneficiarios cumplan con los requisitos del programa.
Uruguay	Tarjeta Social	Utiliza la identificación digital para gestionar el acceso a diferentes programas sociales y beneficios.

Fuente: elaboración propia.

2.3 Tecnologías

De acuerdo con la CIPDED, «los sistemas digitales de información utilizados con fines personales, profesionales o sociales deben poseer, desde su diseño y por defecto, las medidas de seguridad adecuadas que permitan garantizar la integridad, confidencialidad, disponibilidad, resiliencia y autenticidad de la información procesada, así como la disponibilidad de los servicios prestados» (p. 12)[63]. Esto implica procurar especial atención a las condiciones que deben tomarse en cuenta en la selección de tecnologías y en las competencias digitales de los servidores públicos o privados que desarrollan los SID en la administración pública.

[63] SEGIB (2023).

En un SID, deben considerarse una serie de elementos tecnológicos prioritarios para garantizar que su funcionamiento sea efectivo, seguro, ágil y accesible tanto para las personas como para la administración pública. En esta línea, la adopción de tecnologías y métodos de autenticación biométrica puede alinearse con una serie de estándares digitales que propicien la implementación y faciliten procesos de interoperabilidad.

El tema central en la definición de la arquitectura tecnológica de los SID es que contribuyan a la protección de datos personales, desde el proceso de identificación, pasando por el almacenamiento y utilización de estos datos en los mecanismos de validación y autenticación. Un cifrado robusto, como la autenticación multifactor (MFA) y la gestión de identidades y accesos (IAM), permite la trazabilidad del acceso a la información y otorga un grado de confianza relevante para su uso.

Por otro lado, el uso de biometría (huella dactilar, reconocimiento facial, iris, etc.) es común en los SID para verificar la identidad de los usuarios de manera segura[64]. Otros elementos pueden ser combinados para fortalecer la seguridad en el uso de SID para el acceso a servicios públicos, como el uso de contraseñas o tokens de seguridad.

Es importante que un SID utilice estándares abiertos para asegurar la interoperabilidad con otros sistemas y servicios. Así, los servicios pueden ofrecer interfaces de programación de aplicaciones (APIs) bien documentadas y basadas en estándares para permitir la integración con otros sistemas, ya sean públicos o privados.

Un SID debe estar diseñado para ofrecer alta disponibilidad, con mecanismos de *failover*, balanceo de carga y replicación de datos en tiempo real. Es fundamental contar con estrategias de respaldo y recuperación de datos en caso de fallos o ciberataques. Algunas consideraciones de tecnología digital en un SID son las siguientes:

Tabla 4
Tecnologías aplicables en un SID

Tecnología	Aplicación en SID
Biometría	• Reconocimiento de huellas dactilares: utiliza las impresiones digitales para verificar la identidad. Es ampliamente utilizado en dispositivos móviles y sistemas de control de acceso. • Reconocimiento facial: analiza características faciales para autenticar la identidad. Se usa en sistemas de seguridad y en aplicaciones móviles. • Reconocimiento de iris: utiliza patrones en el iris del ojo para la identificación, proporcionando un alto nivel de seguridad. • Reconocimiento de voz: analiza las características vocales para autenticar a una persona, a menudo utilizado en sistemas telefónicos y de asistencia. • Reconocimiento de la firma dinámica: analiza la forma y el ritmo de la firma manuscrita para verificar la identidad.

[64] 52. Asociación por los Derechos Civiles (2017)

Tecnología	Aplicación en SID
Certificados digitales y firmas electrónicas	Documentos electrónicos emitidos por una autoridad certificadora que verifican la identidad de una persona o entidad en línea. Se utilizan para cifrar datos y firmar documentos digitalmente.
Autenticación Multifactor (MFA)	Utiliza múltiples métodos de autenticación para verificar la identidad del usuario, combinando algo que el usuario sabe (contraseña), algo que el usuario tiene (token o dispositivo móvil), y algo que el usuario es (biometría).
Identidad Soberana (*Self-Sovereign Identity*, SSI)	Un enfoque emergente que permite a los individuos tener el control total sobre sus propios datos de identidad. Utiliza tecnología de cadenas de bloques (*blockchain*) para almacenar y gestionar credenciales de identidad de forma segura.
Tecnología de cadenas de bloques (*Blockchain*)	Utiliza un registro descentralizado para almacenar datos de identidad de manera segura y transparente. Ayuda a prevenir la falsificación y a asegurar la integridad de los datos. Aplicaciones: identidades digitales, gestión de credenciales y verificaciones de autenticidad.
Cifrado	Técnica para proteger datos mediante la transformación de información en un formato que solo puede ser leído por quienes tienen la clave de descifrado. Es esencial para la protección de datos en tránsito y en reposo; cifrado simétrico, cifrado asimétrico (como RSA), y cifrado de clave pública.
Tokenización	Sustituye datos sensibles con un token (un identificador no sensible) que puede ser utilizado en sistemas internos sin exponer la información original.
Redes Privadas Virtuales (VPNs) y Seguridad de Redes	Tecnologías para proteger la comunicación de datos a través de redes públicas. Las VPNs cifran la información transmitida, ayudando a mantener la privacidad y seguridad de las identidades digitales.
Autenticación basada en contexto	Utiliza información sobre el contexto del acceso, como la ubicación del usuario, el dispositivo utilizado, y el comportamiento del usuario, para tomar decisiones sobre la autenticación.
Identificación por Código QR y NFC	Utiliza códigos QR y tecnología de comunicación de campo cercano (NFC) para facilitar la identificación rápida y la autenticación en dispositivos móviles.
Gestión de Identidades y Accesos (IAM)	Sistemas y procesos para gestionar las identidades digitales y controlar el acceso a recursos y servicios. Incluye el almacenamiento seguro de credenciales, la gestión de permisos y la auditoría de accesos.

Fuente: elaboración propia.

2.4 Habilitantes

La CIPDED expresa que la «falta de medios, habilidades o competencias digitales no debe suponer una discriminación o exclusión para quienes no pueden o no están en disposición de integrarse en el proceso de transformación digital» (p. 6)[65]. Pocas estrategias de ID cuentan con un respaldo a

[65] SEGIB (2023).

propósito de una agenda propia de desarrollo de competencias digitales, reducción de la brecha digital y ampliación de las condiciones de conectividad.

Un buen SID cuenta con elementos tecnológicos, legales y de gobernanza propicios para su funcionamiento, pero para lograr su objetivo o alcanzar su real valor, deben abordarse las condiciones que inhiben que las personas puedan hacer uso de su ID y de los SID para acceder con seguridad a los servicios públicos. En línea con lo que indica la CIPDED, «la existencia de la brecha digital limita el acceso a las tecnologías de la información y comunicaciones, y plantea grandes desafíos para el logro de la plena inclusión digital en los países de Iberoamérica» (p. 9)[66]; sin una inclusión digital óptima, los ciudadanos no confiarán en los procesos de ID.
Con la implementación de SID, algunos grupos de personas podrían quedar excluidos de los beneficios de un SID por varias razones:

- **Brecha digital:** las identidades digitales y los mecanismos de identificación tradicionales pueden coexistir, y en algunos casos, es propicia su coexistencia para atender a poblaciones con bajos o nulos conocimientos digitales y/o que pueden estar en condiciones de no acceso a Internet. Al mismo tiempo, las personas también deberían tener acceso a medios alternativos de identificación y opciones sobre cómo identificarse. Por ejemplo, en Colombia, se establece la coexistencia de la ID y la identidad física a través de un carné de identificación, que, si bien cuenta con similares condiciones, ofrece a las personas la oportunidad de ser identificadas sin discriminación. En algunos casos, además, el uso de ID para el acceso a servicios públicos puede estar dado por el grado de eficiencia; es decir, si los servicios públicos digitales son más eficientes que los servicios presenciales, eso aumentaría la desigualdad generada por la brecha digital[67], que es uno de los hechos que la Carta Iberoamericana de Gobierno Electrónico establece como un riesgo, ya que los ciudadanos deben tener el mismo nivel de calidad, eficiencia y transparencia de los servicios públicos tanto en línea como de forma presencial.

- **Registros civiles previos**: algunas personas, especialmente en zonas rurales o marginadas, pueden carecer de documentos legales previos (acta de nacimiento, por ejemplo), lo que les imposibilita registrarse en el sistema de ID.

- **Desigualdad de acceso**: las personas en situaciones de vulnerabilidad (poblaciones indígenas, refugiados, personas sin hogar) pueden enfrentarse a obstáculos adicionales para acceder a estos sistemas.

- **Reutilización de datos personales**: las personas pueden temer que sus datos personales sean utilizados de manera indebida o compartidos con terceros sin su consentimiento, especialmente si no hay transparencia o regulación adecuada.

[66] SEGIB (2023).
[67] Barbosa *et al*. (2020).

- **Vigilancia masiva**: existe la preocupación de que los gobiernos utilicen la ID para monitorear a la población de manera intrusiva, limitando la privacidad y las libertades individuales. Las identificaciones digitales combinan tecnología y capacidades de procesamiento de *big data* con una gran cantidad de datos biográficos, lo que conlleva riesgos de elaboración de perfiles, vigilancia y efectos escalofriantes. Otros riesgos asociados con las ID incluyen errores humanos en la ejecución, uso no autorizado, exclusión de personas y vigilancia[68].

- **Preocupaciones sobre la ciberseguridad**: las personas pueden temer que los SID sean vulnerables a ciberataques, comprometiendo sus datos o que se produzcan errores que afecten su identidad legal. En septiembre de 2024, las bases de datos personales de más de un millón de salvadoreños fueron expuestas por hackers, quienes divulgaron información como nombre, teléfono, dirección, lugar de trabajo y sueldos de aquellas personas registradas en la entidad responsable de la seguridad social[69].
- **Inclusión de poblaciones extranjeras**: cualquier SID no debería limitarse solo a los ciudadanos, sino también registrar a todos los residentes, incluyendo ciudadanos en el extranjero. No obstante, esto puede ser problemático si el registro se basa en documentos disponibles solo para ciudadanos o si los no ciudadanos deben demostrar su estatus legal, lo que puede ser un desafío en países con fronteras porosas, migrantes irregulares, desplazamientos o poblaciones apátridas[70].

2.4.1 La interoperabilidad como habilitador de los sistemas de identificación digital

La interoperabilidad es un habilitador significativo para los SID en Iberoamérica. Permite que diversas plataformas, administraciones públicas y sistemas trabajen de manera conjunta, compartiendo y verificando información de identificación de forma fluida y segura. Esto tiene un impacto característico en áreas como la salud, la movilidad de personas, la eficiencia de los servicios públicos y privados, y la integración regional.

Dado que muchas personas se desplazan entre países por motivos de trabajo, migración o turismo, la interoperabilidad entre los SID puede facilitar el acceso a servicios en diferentes países de la región. Además, evita que las personas tengan que registrarse repetidamente en distintos sistemas o servicios de la administración pública, y reduce los costos asociados a la gestión de múltiples bases de datos y procesos de verificación.

En general, la interoperabilidad facilita el acceso a los servicios públicos digitales sin tener que lidiar con sistemas fragmentados. Esto es especialmente relevante en países donde la descentralización de los servicios puede generar ineficiencias si no hay una coordinación adecuada. En un sistema interoperable, la autenticación se basa en múltiples factores y se verifica a través de diferentes entidades, lo que mejora significativamente la seguridad de un SID.

[68] The Centre for Internet & Society (2020).
[69] IPANDETEC (2024).
[70] World Bank (2018).

A pesar de sus beneficios, la implementación de sistemas interoperables en Iberoamérica enfrenta varios desafíos. Entre ellos se incluyen la falta de infraestructura tecnológica adecuada, la necesidad de definir estándares y normativas, así como la coordinación de los procesos administrativos para proporcionar una experiencia valiosa a las personas usuarias de los SID.

2.4.2 La firma electrónica como habilitador de los sistemas de identificación digital

La firma electrónica actúa como un habilitador esencial para los SID, ya que facilita y asegura las transacciones digitales, reduce la necesidad de interacciones presenciales y simplifica el acceso a servicios públicos y privados de manera segura. A medida que la región avanza hacia la transición digital, la firma electrónica se convierte en un pilar para modernizar y digitalizar procesos, fomentando la confianza en el uso de sistemas digitales.

Este mecanismo valida la autenticidad de transacciones y documentos electrónicos, garantizando que la identidad del firmante sea verificable y que el contenido no haya sido alterado desde su firma. Respaldada por tecnologías de cifrado, como la criptografía de clave pública, la firma electrónica asegura la integridad y autenticidad de los documentos, lo cual es fundamental para fortalecer la confianza en los SID. Uno de sus principales aportes es la capacidad de realizar transacciones y firmar documentos sin necesidad de presencia física, un aspecto especialmente útil en áreas donde la infraestructura tecnológica es limitada.

En varios países de la región, como Chile, México y Uruguay, la firma electrónica se ha convertido en una herramienta importante para implementar plataformas de gobierno digital, mejorando la eficiencia de la administración pública y promoviendo la transparencia en los procesos. Al digitalizar procedimientos que anteriormente requerían la presencia física, se agiliza la burocracia, permitiendo que los documentos sean firmados y verificados en cuestión de minutos, en lugar de días o semanas.

Además, la firma electrónica es un componente determinante para la interoperabilidad entre los SID. Su integración con otros mecanismos de identificación, como certificados digitales y plataformas de verificación de identidad, promueve que los documentos y transacciones realizadas por ciudadanos de diferentes países o regiones sean reconocidos y validados en múltiples plataformas.

En Iberoamérica, la firma electrónica está regulada por diversas leyes y normativas que garantizan su validez y reconocimiento legal, lo que refuerza la confianza en los sistemas de identificación digital. Países como Argentina (Ley de Firma Digital), México (Ley de Firma Electrónica Avanzada) y Colombia (Ley de Comercio Electrónico) han adoptado marcos normativos que permiten el uso de la firma electrónica en trámites oficiales y privados. Estos marcos se alinean con estándares internacionales, facilitando la interoperabilidad y el reconocimiento legal de documentos firmados electrónicamente en otros países.

3. CASOS IBEROAMERICANOS DE SID PARA EL ACCESO A SERVICIOS PÚBLICOS DIGITALES

A continuación, se presentan las experiencias en la implementación de SID en seis países de Iberoamérica: Uruguay, Brasil, Argentina, Chile, Colombia y España. Estas son seguidas por la descripción de los casos emergentes de ID en Costa Rica y República Dominicana, los cuales contextualizan las acciones que los gobiernos están llevando a cabo para avanzar en materia de ID.

3.1 Uruguay

Uruguay ha sido un referente en Iberoamérica en cuanto a la implementación SID para servicios públicos. Su enfoque en la digitalización de trámites gubernamentales y la simplificación de la relación entre ciudadanos y el Estado ha generado un modelo innovador y eficaz.

Tabla 5
Identificación digital: caso Uruguay

Mecanismo de ID	Usuario.gub.uy o Clave Digital	**SID para acceso a servicios públicos**	Portal.gub.uy
Número de usuarios	Al 2028, más de 100,000 personas[71].		
Contexto	La Política de Identificación Digital (2018) está basada en el marco normativo vigente; las guías y recomendaciones para proteger la ID del NIST en su publicación SP 800-63; el marco eIDAS relativo a la identificación electrónica		

[71] Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (2018).

	y los servicios de confianza para las transacciones electrónicas en su Reglamento 910/2014 y las experiencias de proyectos como STORK (*Secure Identity Across Borders Linked*)[72]. La Cédula de Identidad Electrónica (CIE) en Uruguay es un documento de identificación que incluye un chip con información digital que permite a los ciudadanos uruguayos acceder a servicios públicos y privados en línea. El chip contiene un certificado digital que facilita la autenticación segura del usuario y permite la firma de documentos electrónicos con plena validez legal. Esta cédula es utilizada tanto para identificación presencial como para trámites electrónicos, y es un pilar del sistema de gobierno digital en el país. En el caso de Uruguay se utilizan múltiples niveles de seguridad, con los cuales se puede obtener un nivel de seguridad que implica el cumplimiento de requisitos para obtener servicios que requieren distintos niveles: • Nivel de seguridad Básico - Auto-registrado: es el nivel de confianza básico en el que se registra en un formulario en la web con confirmación a través de un correo electrónico y validación de teléfono. • Nivel de seguridad Intermedio – Verificado: se incrementa la seguridad de la identidad digital ya que verifica que la persona es quien dice ser de forma presencial. • Nivel de seguridad Avanzado - Equivalente a la presencialidad: cédula de identidad con chip; se obtiene la tarjeta inteligente desde la que se pueden generar firmas electrónicas de documentos. Además, se agregan los datos biométricos de huellas digitales y rostro. Existen proveedores de servicios registrados como: Abitab o TuID.
Interoperabilidad	Las instituciones gubernamentales en Uruguay están interconectadas mediante sistemas de interoperabilidad basados en una arquitectura orientada a servicios a nivel de Estado, que permiten compartir datos de manera segura entre distintas agencias. Esto significa que los ciudadanos pueden realizar múltiples trámites sin tener que proporcionar repetidamente la misma información, ya que la plataforma cuenta con un sistema de autenticación que emite un token de seguridad para la interacción segura entre los servicios.
Firma electrónica	La firma electrónica avanzada es generada mediante la cédula de identidad electrónica o dispositivos especializados, y está avalada por la Ley N° 18.600 de Documentos Electrónicos y Firma Electrónica.

[72] TuID (2018).

Servicios públicos accesibles a través del SID	92% de los trámites de la Administración Central en Uruguay se encuentran disponibles para ser realizados en línea de inicio a fin[73]	**Entidad rectora**	Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento
Identificación biométrica	• Se ha incorporado sistemas de identificación biométrica en ciertos procesos, como la verificación de identidad en el marco de programas de asistencia social y servicios públicos. • La biometría, como el reconocimiento facial y huellas digitales, se utiliza para verificar la identidad de las personas y mejorar la seguridad en el acceso a servicios públicos. • Los datos biométricos están protegidos por la Ley N° 18.331 sobre Protección de Datos Personales, que garantiza que la recolección, almacenamiento y uso de esta información se realice de manera segura y bajo estrictos protocolos de confidencialidad. • El uso de biometría debe realizarse con el consentimiento informado del usuario, y las entidades que manejan estos datos deben garantizar su correcta gestión y protección contra accesos no autorizados.		
Mecanismos de seguridad	El nivel de seguridad de una ID en Uruguay[74] es definido acorde a los aspectos de seguridad considerados en los siguientes elementos: • La etapa de registro de identificación digital: proceso de identificar a una persona, verificar sus datos, expedir o asociar uno o más medios de identificación digital a esta, y almacenar dicha asociación para su posterior utilización. • Los medios de identificación asociados: unidad material o inmaterial, procesable por un sistema informático, con una parte en control del sistema y otra en exclusivo control de la persona, ya sea mediante su conocimiento, un dispositivo físico o lógico, o algún rasgo físico o comportamental. • El proceso de autenticación de la ID: proceso de identificar a una persona a través de un sistema informático mediante uno o más medios de identificación digital. • La federación de la identidad: proceso que permite la transmisión de información de identidad y autenticación a través de un conjunto de sistemas en red.		
Vinculación con servicios de	Además de los servicios públicos, el certificado digital emitido por la cédula de identidad electrónica también se utiliza en transacciones privadas, como		

[73] Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (2020).
[74] TuID (2018).

privados	la firma de contratos electrónicos, gestión de cuentas bancarias y otras actividades comerciales.
Práctica relevante	• El chip de la Cédula de Identidad Electrónica (CIE) permite realizar autenticaciones y firmas electrónicas avanzadas con plena validez jurídica, lo que mejora la seguridad y facilita la realización de trámites sin necesidad de presencia física. • El uso de un sistema unificado para la prestación de servicios públicos digitales evita que las personas tengan que gestionar múltiples contraseñas y cuentas para diferentes instituciones, mejorando la accesibilidad y experiencia del usuario. • La autenticación de dos factores (2FA) reduce el riesgo de accesos no autorizados, mejorando la seguridad en los trámites en línea y protegiendo las cuentas de los ciudadanos. • La integración de servicios en una plataforma única mejora la experiencia del usuario, facilita la búsqueda de información y permite realizar múltiples trámites en un solo lugar, simplificando la interacción con el gobierno. • El registro civil, gestiona la recolección de datos biométricos, como las huellas dactilares, durante el proceso de emisión de la cédula de identidad electrónica, las cuales se utilizan para verificar la identidad de la persona de manera segura en oficinas públicas, servicios digitales y transacciones que requieren alta seguridad. • La recolección de datos sobre la experiencia del usuario y el rendimiento del sistema permite al gobierno ajustar y optimizar los servicios en tiempo real, asegurando que las soluciones digitales sigan siendo eficaces y relevantes.

Fuente: elaboración propia.

3.2 Chile

En Chile, la identificación digital es una parte fundamental de la estrategia de Gobierno Digital, facilitando el acceso a diversos servicios públicos y privados.

Tabla 6

Identificación digital: caso Chile

Mecanismo de ID	Clave Única	**SID para acceso a servicios públicos**	ChileAtiende.cl
Número de usuarios	A julio de 2023, 14.8 millones de chilenos la tienen y pueden acceder a más 1,792 trámites. La implementación de un carnet de identidad disponible en		

	formato digital iniciará en diciembre 2024
Contexto	Chile cuenta con un Servicio de Registro Civil que entrega un número de identificación único para cada ciudadano (RUT), que se materializa en la cédula de identidad. En virtud de eso, el Ministerio Secretaría General de la Presidencia, en conjunto con el Servicio de Registro Civil, desarrollaron el proyecto Clave Única, que permite a los ciudadanos contar con una clave de acceso única a los diferentes servicios del Estado. En primer lugar, las personas deben acudir presencialmente a una oficina del Registro Civil y solicitar su Clave Única. En el caso de renovaciones de cédula de identidad, se les consulta si quieren solicitar su clave. El oficial del Registro Civil verificará la identidad de la persona de forma biométrica con su huella dactilar y procederá a entregarle una clave de activación que la persona deberá utilizar para activar su clave en línea a través del sitio del Registro Civil. Registro Civil entrega a esta clave el carácter de identificación oficial, válida como la presentación de la cédula de identidad, permitiendo a las instituciones que tienen trámites que requieren la validación de identidad, poner a disposición estos trámites *online* sin problemas. Clave Única es un SID personal e intransferible que permite a los y las ciudadanas acceder a diferentes servicios del Estado y realizar trámites en línea de manera segura; provee a los ciudadanos de una Identidad Electrónica Única (RUN y contraseña) para la realización de trámites en línea del Estado; eliminando así la necesidad de realizar múltiples registros para cada servicio de manera fácil y segura.
Interoperabilidad	• La conectividad del proceso de registro y la integración con múltiples bases de datos ha mejorado dramáticamente. Se redujo el tiempo de inscripción a solo una hora. • Se utilizan portales con tecnología conocida como OpenID 2.0, que es una tecnología abierta, que permite su integración simple a cualquier plataforma tecnológica sin requerir complejas ni costosas adaptaciones. • Además, se provee de un conjunto de conectores adaptables para diferentes lenguajes de programación y plataformas que las instituciones puedan tener, con el fin de simplificar la integración del portal de autenticación.
Firma electrónica	Chile ahora está explorando la funcionalidad ampliada de la tarjeta inteligente, incluidas las firmas digitales para la autenticación.

Servicios públicos accesibles a través del SID	El 93% de los trámites que se realizan ante el Estado se realizan de forma digital[75]	**Entidad rectora**	Registro Civil e Identificación
Identificación biométrica	• Uno de los usos pioneros en Chile de la biometría ha sido en el sistema de identificación y migración. • El sistema biométrico de pasaporte electrónico ha permitido a Chile convertirse en el primer país latinoamericano en obtener acceso al programa *Visa Waiver* de EUA. • Desde septiembre de 2013, el Servicio de Registro Civil e Identificación cuenta con el SID Multibiométrico, que emite documentos de identidad y de viajes electrónicos. Con este sistema, se complementan las clásicas impresiones dactilares con el reconocimiento facial. Así, el chip del pasaporte electrónico permite su uso como documento de viaje electrónico con biometría facial y dactilar. El chip de la cédula de identidad tiene tres aplicaciones: servicios electrónicos (e-Services); verificación de identidad por biometría dactilar; y documento de viaje electrónico con biometría facial. Asimismo, el Registro Civil también impulsa la iniciativa «Civil Digital» que permite a los ciudadanos realizar trámites de manera digital y sin la necesidad de concurrir a una oficina de la institución. Se trata de un tótem que está en lugares públicos y comerciales que incorpora biometría (identidad validada con la huella digital)[76]. • La tecnología de identificadores biométricos es propicia para validar el rostro humano para acceder a la documentación. • El Servicio de Registro Civil e Identificación (Registro Civil) de Chile viene brindando identidad biométrica a servicios de verificación para instituciones públicas y entidades privadas desde 2005. Para instituciones públicas, el Registro Civil no cobra ninguna tarifa. En 2018 se verificaron más de 16 millones de consultas a petición de instituciones públicas, entre ellas el Servicio Nacional de Empleo, la Policía Nacional (Carabineros), el Ministerio de Salud y Ministerio Público. Para las entidades privadas, el Registro Civil ha establecido una escala de honorarios en función del tipo de datos consultados, donde cada consulta cuesta una cierta cantidad de «créditos» comprados previamente llamados unidades básicas de infraestructura (BUI)[77].		

[75] Mundaca (2023).
[76] Asociación por los Derechos Civiles (2017).
[77] Por ejemplo, una consulta de verificación con fotografía cuesta 2 BUI; una verificación con firma cuesta 1,5 BUI; a la verificación de identidad con una huella digital cuesta 1,5 BUI; una verificación con diez huellas dactilares cuesta 20 BUI; una verificación basada en la información indicada en la tarjeta de identificación consume 1,5 BUI; una verificación vía AFIS 1:1 usando. La imagen WSQ o NEC consume 5 BUI. Los terceros que verifiquen la información deben ingresar en el sistema el número de identificación único del usuario final (llamado Número de Lista Única Nacional – RUN), el dígito de control de RUN y la imagen de la huella dactilar para obtener una respuesta. El sistema devolverá un HIT o NO HIT dependiendo de si la probabilidad de una coincidencia está por encima o por debajo de un cierto umbral.

Mecanismos de seguridad	• En el gobierno de Chile se utiliza la tecnología de *Single Sign On* (SSO), donde una unidad centralizada se encarga de entregar las credenciales que se pueden usar a través de todos los servicios de gobierno, definiendo así una plataforma única de autenticación. • Para poder verificar información personal, instituciones públicas y empresas privadas deben firmar un acuerdo ante el Registro Civil que indique cómo se verificaría la información, las condiciones bajo las cuales se deberá presentar la información, así como los plazos de cumplimiento de la Ley de Protección de Datos[78].
Vinculación con servicios de privados	• Registro Civil e Identificación de Chile (SRCeI) otorgó una concesión a una empresa privada para modernizar su actual sistema de identificación civil mediante construir, instalar y mantener nuevo *hardware* y *software*, integración de bases de datos, capacitación personal de SRCeI y la personalización de tarjetas inteligentes de identificación electrónica y pasaportes. El gobierno opera el sistema y paga una tarifa por documento emitido[79]. • El socio del sector privado para la provisión de pasaportes y nuevas tarjetas de identificación es Morpho Sonda Chile.
Práctica relevante	• La implementación de un carnet de identidad disponible en formato digital iniciará en diciembre 2024. Las personas podrán acceder a su cédula y pasaporte en el teléfono celular a través de dos aplicaciones, que incluso permitirán el bloqueo de los documentos por robo o extravío. Se trata de las apps «Identificación Digital», que será para los usuarios comunes, y «Cédula Asistida» para personas con discapacidad visual. • La Superintendencia de Seguridad Social implementó la Licencia Médica Electrónica, que incorpora el sistema biométrico de verificación mediante la impresión dactilar. Con él se identifica al afiliado a través de su huella, lo que permite detectar delitos o mal uso de este beneficio. • El gobierno otorgó un plazo de 10 años de concesión a una empresa privada para actualizar su identidad nacional y emitir 25 millones de tarjetas de identificación electrónicas y 4 millones pasaportes electrónicos para 2020. • 900 estaciones de registro fueron implementadas en el país. Los ciudadanos se inscriben en una de las estaciones, y sus datos, incluidos los datos biométricos, se validan con la base de datos central. La empresa luego personaliza la tarjeta inteligente de identificación

[78] World Bank (2019b).
[79] World Bank (2016).

	electrónica, o el pasaporte electrónico, y lo envía de regreso a la estación de inscripción para que la persona lo recoja.

Fuente: elaboración propia.

3.3 Colombia

El SID en Colombia está centrado principalmente en el documento de identidad y servicios digitales asociados, de los cuales la mayoría se encuentran en una etapa transaccional en su madurez de servicios públicos en línea.

Tabla 7

Identificación digital: caso Colombia

Mecanismo de ID	Cédula Digital	**SID para acceso a servicios públicos**	Gov.co
Número de usuarios	El plan de masificación de la cédula digital ya tiene el 92% de cobertura de producción del país, con un total de 977 Estaciones Integradas de Servicio (EIS) a disposición de los colombianos. Al final del despliegue, se contará con 1407 EIS a nivel nacional. Se estiman que aproximadamente 640,219 ciudadanos están, además, registrados en la Plataforma del Servicio de Autenticación Digital, que permite consultas y ciertos trámites específicos en 9 instituciones públicas.		
Contexto	El gobierno ha emitido normativas para regular el uso de la cédula digital, asegurando su validez y la seguridad de la información almacenada en ella. A través de la iniciativa de Gobierno Digital, los ciudadanos pueden acceder a diferentes servicios públicos en línea utilizando su cédula digital. Además, los ciudadanos cuentan con una herramienta que permite a los ciudadanos almacenar y gestionar documentos personales y oficiales de manera digital.		
Interoperabilidad	• La Plataforma de Interoperabilidad del Estado Colombiano permite la comunicación y el intercambio de datos entre las diferentes entidades del Estado. A través de la plataforma, la información del SID puede ser utilizada por diversas instituciones para facilitar la prestación de servicios. • La interoperabilidad del SID permite que los ciudadanos se autentiquen de manera segura en estos servicios utilizando su cédula digital.		
Firma electrónica	• La cédula digital en Colombia incorpora la posibilidad de que los ciudadanos utilicen su firma digital para realizar trámites en línea. Al		

<table>
<tr><td></td><td colspan="3">integrar la firma digital con la cédula, los ciudadanos pueden firmar documentos de forma electrónica utilizando los datos biométricos almacenados en el chip de la cédula digital.
• En Colombia, la Ley 527 de 1999 y el Decreto 2364 de 2012 regulan el uso de la firma electrónica y digital. Estas leyes establecen que las firmas electrónicas tienen la misma validez y efectos jurídicos que las firmas manuscritas, siempre que cumplan con ciertos requisitos de autenticidad e integridad.</td></tr>
<tr><td>Servicios públicos accesibles a través del SID</td><td>En Colombia, existen actualmente 761 trámites y servicios disponibles en línea a través del portal único del Estado, GOV.CO</td><td>Entidad rectora</td><td>Registraduría Nacional del Estado Civil</td></tr>
<tr><td>Identificación biométrica</td><td colspan="3">• La Registraduría Nacional del Estado Civil mantiene una base de datos unificada que almacena la información biométrica de los ciudadanos, permitiendo que las instituciones autorizadas puedan acceder a ella para procesos de autenticación, siempre bajo estrictas normas de seguridad y protección de datos.
• La Registraduría Nacional del Estado Civil ha implementado una plataforma de autenticación digital para que los ciudadanos puedan acceder a servicios en línea de manera segura. Los ciudadanos pueden autenticarse utilizando sus datos biométricos registrados.
• Así, la recolección de las huellas dactilares no es requisito para realizar la mayoría de los trámites ante entidades públicas (Decreto 19 de 2012, artículo 17). Este requisito fue reemplazado por la consulta electrónica de la base de datos de la Registraduría Nacional, que cuenta ya con los sistemas de autenticación biométrica.</td></tr>
<tr><td>Mecanismos de seguridad</td><td colspan="3">• La cédula digital cumple las normas internacionales ICAO-Doc 9303, en cuanto al documento físico y a las fotografías de los ciudadanos.
• Los trámites y servicios que requieran la autenticación de la identidad del usuario, deben hacerlo a través del servicio de identificación digital en donde la Agencia Nacional Digital, en su rol de articulador, se encargará de redireccionar la solicitud al prestador del servicio del usuario, de modo que las credenciales obtenidas sean válidas para identificarse en los sistemas de información de cualquier entidad pública. Para ello se usarán los mecanismos de Servicio Web y OpenID Connect.
• La reglamentación de la Ley de Protección de datos (Decreto 1377 de 2013, artículo 6) especifica que ninguna actividad puede condicionarse al suministro de datos sensibles, dentro de los que se encuentran los</td></tr>
</table>

	datos biométricos[80]. En Colombia, la Ley 1581 de 2012 regula el tratamiento de datos personales, lo que implica que las instituciones deben proteger la información personal de los ciudadanos. • La cédula digital tendrá una vigencia de 10 años, dado que los mecanismos de seguridad que la habilitan están basados en la biometría y requieren actualización en el tiempo establecido para evitar que los cambios morfológicos afecten los procesos de autenticación[81]. • Los ciudadanos deben dar su consentimiento para que su información sea compartida entre entidades, y solo las entidades autorizadas pueden acceder a los datos de identificación digital.
Vinculación con servicios de privados	• Desde 2012, la Registraduría Nacional del Estado Civil permite a las instituciones públicas verificar la información en su base de datos sin costo alguno, facilitando la entrega eficiente de servicios en áreas como educación (Ministerio de Educación, universidades y liceos), justicia y seguridad (Ministerio de Defensa, Interior, Justicia y Poder Judicial), protección social (Ministerio de Salud y Protección Social, fondos de bienestar familiar, etc.), transporte (Ministerio de Transporte y Secretaría de Tránsito), y notarios. • Para entidades privadas, la Registraduría tiene diversas tarifas fijas dependiendo del número de consultas de verificación[82]. • Los bancos y otras instituciones financieras pueden integrar sus sistemas con la base de datos de la Registraduría para verificar la identidad de los clientes de manera rápida y segura, facilitando procesos como la apertura de cuentas o la solicitud de créditos. • Empresas de diferentes sectores (telecomunicaciones, comercio, etc.) pueden utilizar los datos de identificación digital para validar la identidad de los clientes y ofrecer servicios en línea, garantizando que las transacciones sean seguras y cumplan con la normativa de protección de datos.
Práctica relevante	• En Colombia, la cédula digital está dirigida a aquellos colombianos que voluntariamente la requieran mediante el trámite de duplicado, y a los jóvenes que cumplan la mayoría de edad y tramiten su cédula de ciudadanía por primera vez (sin costo alguno). Las recomendaciones de la ciudadanía son consideradas para la mejora del proceso de emisión de cédulas digitales, alineado, a su vez, con estándares internacionales.

[80] Asociación por los Derechos Civiles (2017a).
[81] Registraduría Nacional del Estado Civil (2023).
[82] Por ejemplo, de 1 a 100.000 consultas cobra COL $ 15.203.385 (~USD 4.751); por 100.001 a 200.000 cobra COL$ 30.406.770,80 (~USD 9.502); por 200.001 a 300.000 cobra COL $45.610.156 (~USD 14.253) y así sucesivamente, hasta el rango entre 11.000.001 y 12.000.000 consultas, donde cobra COL$ 519.742.188,00 (~USD 162.419).

	• El documento digital dispone de un chip en el que podrá incluirse la historia clínica, el registro civil y otros datos biográficos del ciudadano, además de poder descargarse en el celular. • La masificación del proceso de registro facilita a las poblaciones en zonas rurales, o con dificultades de movilización, tener acceso a este servicio para contar con mecanismos de servicios públicos digitales.

Fuente: elaboración propia.

3.4 Argentina

La ID en Argentina se orienta hacia una mayor inclusión, eficiencia y seguridad, alineándose con tendencias globales en la digitalización de servicios.

Tabla 8
Identificación digital: caso Argentina

Mecanismo de ID	DNI Digital	**SID para acceso a servicios públicos**	Argentina.gob.ar y la Plataforma de Trámites a Distancia
Número de usuarios	Hasta el 2023, se registran más de 20 millones de usuarios del DNI digital en Argentina. Existe experiencias de SID municipal como el caso del Gobierno de Buenos Aires y el de Santa Fe.		
Contexto	Argentina otorga un DNI Digital que es una versión virtual del DNI físico. El SID es un sistema que permite la validación o acreditación de identidad de un usuario de forma remota y en tiempo real. El mismo utiliza como base el Registro Nacional de las Personas y tiene integrados varias tecnologías como biometría y escáner de documentos para llevar a cabo la autenticación[83], y se materializa para la prestación de servicios públicos a través de la plataforma «Mi Argentina»: es un portal unificado que permite a los ciudadanos acceder a servicios digitales del Estado, incluyendo la gestión de su DNI Digital, la verificación de datos, y la realización de trámites en línea. Autenticar es el servicio brindado por la Plataforma de Autenticación Electrónica Central de la Nación, que oficia de intermediario entre una aplicación cliente (AC) y los proveedores de autenticación (IdP) elegidos para autenticar la identidad de los usuarios de sus sistemas.		

[83] Jamele (2023).

Interoperabilidad	El SID está diseñado para ser interoperable con diversas entidades, permitiendo la verificación de identidad en tiempo real durante la realización de trámites en organismos públicos y entidades privadas como bancos y empresas de servicios.		
Firma electrónica	El DNI Digital facilita la identificación en línea y puede ser parte del proceso de autenticación para acceder a servicios de firma electrónica, pero no contiene directamente la firma electrónica en sí. La firma electrónica requiere de un certificado digital específico para autenticar y validar documentos digitales.		
Servicios públicos accesibles a través del SID	Alrededor de 1,400 servicios están disponibles en línea a través de Argentina.gob.sv	**Entidad rectora**	Registro Nacional de las Personas (RENAPER)
Identificación biométrica	• El SID utiliza la biometría (huellas dactilares y reconocimiento facial) para validar la identidad del ciudadano al crear y acceder a su DNI Digital. • El RENAPER es el encargado de remitir la información biométrica y patronímica recolectada a través de la realización del DNI y del pasaporte nacional. En el año 2012 fueron lanzados tanto el DNI digital como el pasaporte electrónico, el cual almacena en un chip RFID56 los datos de su titular y su información biométrica, con el fin de poder identificar a su titular a través de su huella dactilar, su iris y/o su rostro[84]. • En el 2010, la Administración Federal de Ingresos Públicos (AFIP) emitió la Resolución General que crea el Registro Tributario, bajo el cual las personas que deseen solicitar la inscripción y obtener la Clave Única de Identificación Tributaria (CUIT), además de la Clave Fiscal con Nivel de Seguridad 3, deben proceder al registro digital de la fotografía de su rostro, su firma y su huella dactilar.		
Mecanismos de seguridad	• El Sistema Federal de Identificación Biométrica para la Seguridad (SIBIOS) fue introducido en el año 2011, a través del decreto 1766, el cual se basa en una lógica de seguridad y prevención del delito[85]; la autoridad de aplicación del Sistema es el Ministerio de Seguridad de la Nación, mientras que el responsable de la administración y mantenimiento de este es la Policía Federal Argentina, mediante la Superintendencia de Policía Científica[86].		
Vinculación con servicios de	• El RENAPER brinda cuatro tipos de servicios a entidades privadas para la verificación de ID, según el tipo de información a ser verificada:		

[84] Asociación por los Derechos Civiles (2017b).
[85] Asociación por los Derechos Civiles (2017b).
[86] Asociación por los Derechos Civiles (2017b).

privados	verificación mediante nombres, verificación mediante huellas dactilares, verificación mediante foto personal y verificación mediante combinación de la fotografía, y los códigos de barras en el anverso y reverso del documento de identidad.
Práctica relevante	• La cultura de innovación gubernamental digital en Argentina ha permitido que las instituciones públicas a nivel nacional y municipal puedan desarrollar mecanismos de ID para ofrecer servicios públicos digitales. • El uso de tecnologías emergentes como *blockchain*, es parte de la visión para fortalecer los mecanismos de ID. • La robustez de las estrategias y mecanismos de interoperabilidad han facilitado que los SID funcionen de forma articulada entre diferentes instituciones públicas.

Fuente: elaboración propia.

3.5 Brasil

En Brasil, la identificación digital es un sistema unificado y seguro que permite a las personas identificarse y realizar trámites en línea con validez legal.

Tabla 9
Identificación digital: caso Brasil

Mecanismo de ID	DNI Digital	**SID para acceso a servicios públicos**	Gov.br
Número de usuarios	Al 2023, se estima existen 152 millones de registros de ID en Brasil, es decir, un 74% de brasileños cuentan con un mecanismo para ser identificados digitalmente[87].		
Contexto	El DNI Digital, conocido en Brasil como Documento Nacional de Identidade (CIN, por sus siglas en portugués), es una identificación digital unificada que centraliza varios documentos en un solo código único (CPF - Cadastro de Pessoas Físicas). El portal de trámites públicos de Brasil Gov.br (creado por Decreto 9,756 en 2019) utiliza una única credencial para acceder a múltiples servicios, lo que simplifica el proceso de autenticación para los ciudadanos. En general, el SID combina varios elementos, como el Documento Nacional de Identidade		

[87] Governo Federal Brasil (2023).

	Digital (CNI), el portal Gov.br, y la Infraestructura de Claves Públicas Brasileña (ICP-Brasil). Se estima que, en 2024, Brasil presente en Río de Janeiro, Goiás y Paraná, experiencias relevantes en el uso de tecnología de *blockchain*[88] en un nuevo programa de ID a partir del uso de tecnologías que garanticen la inmutabilidad de los datos y mayor seguridad[89].		
Interoperabilidad	La Ley de Gobierno Digital 14.129/2021, define la adopción de soluciones digitales tanto para la gestión y tramitación de procesos administrativos internos, la prestación de servicios públicos al ciudadano, y el establecimiento de procesos de interoperabilidad entre plataformas para proteger los datos personales de los ciudadanos.		
Firma electrónica	En Brasil, la firma electrónica se realiza mediante certificados digitales emitidos por la Infraestructura de Claves Públicas Brasileña (ICP-Brasil). Estos certificados digitales, como el e-CPF para personas físicas y el e-CNPJ para empresas, están vinculados a la ID del usuario y permiten autenticar documentos y transacciones electrónicas con validez legal.		
Servicios públicos accesibles a través del SID	Brasil cuenta con más de 4,000 servicios públicos disponibles digitalmente[90]	**Entidad rectora**	Secretaría Especial de Desburocratización, Gestión y Gobierno Digital del Ministerio de Gestión e Innovación en Servicios Públicos
Identificación biométrica	En Brasil, los datos biométricos son recolectados por diferentes agencias gubernamentales y utilizados para diversos propósitos. Las huellas dactilares son recabadas por las fuerzas de seguridad (Secretarias de Segurança Pública), las direcciones Estatales de tráfico, el Departamento de la Policía Federal, y los Tribunales de Justicia Electoral, con el fin de expedir la tarjeta nacional de identidad (RG), el registro de conducir (CNH), pasaportes y tarjetas de registro de votantes, respectivamente.		
Mecanismos de seguridad	• La ID en Brasil se rige por la Ley General de Protección de Datos, que regula el tratamiento de datos personales y garantiza la privacidad y protección de la información de los ciudadanos.		

[88] Pereira (2023).
[89] G20 Brasil 2024 (2024).
[90] G20 Brasil 2024 (2024).

	• A través del e-CPF, Brasil ha adoptado una clave de firma criptográfica pública, lo que añade una capa de autenticación y garantiza la integridad de los datos en las transacciones electrónicas. • En Brasil, la ID contiene niveles escalable de seguridad: bronce (preguntas aleatorias y civiles), plata (servidor público, bancos acreditados y licencia de conducir), oro (biometría ICN y certificado digital)[91].
Vinculación con servicios de privados	De acuerdo con la investigación, en Brasil se está estableciendo como próximo paso la vinculación de la ID con servicios privados[92].
Práctica relevante	• Los ciudadanos tienen control sobre sus datos y pueden gestionar cómo se comparte y utiliza su información a través de la plataforma Gov.br. • La regulación, política digital y programas de desarrollo de ID trabajan de forma coordinada para resguardar los datos de las personas, y promover la confianza en el SID. • Brasil ha sido, junto a Uruguay, pionero en la implementación de un SID transfronterizo que permite a ciudadanos brasileños acceder y realizar trámites en línea con una institución del gobierno uruguayo.

Fuente: elaboración propia.

3.6 España

La identificación digital en España es un sistema que permite a los ciudadanos y las empresas realizar trámites y acceder a servicios públicos de manera segura y eficiente.

Tabla 10
Identificación digital: caso España

Mecanismo de ID	DNIe	**SID para acceso a servicios públicos**	Cl@ve
Número de usuarios	Al 2021, se estiman 85 millones de usuarios[93].		
Contexto	Cl@ve es un sistema orientado a unificar y simplificar el acceso electrónico de los ciudadanos a los servicios públicos. Su objetivo principal es que el ciudadano pueda identificarse ante la administración mediante claves concertadas (usuario más contraseña), sin tener que recordar claves		

[91] Governo Federal Brasil (2023).
[92] Governo Federal Brasil (2023).
[93] Ministerio del Interior (2021).

	diferentes para acceder a los distintos servicios. Cl@ve complementa los actuales sistemas de acceso mediante DNIe, que es una versión electrónica del documento nacional de identidad que incluye un chip con los datos personales del titular y certificados digitales que permiten la autenticación y la firma electrónica, y ofrece la posibilidad de realizar firma en la nube con certificados personales custodiados en servidores remotos. El Portal de Autenticación Electrónica (PAe) es un nodo español del Sistema Europeo de Reconocimiento de Identidades Electrónicas. Ofrece una aplicación web para ciudadanos y empresas que permite la validación *online* de firmas y certificados, así como un demostrador de los servicios web de firma electrónica. En noviembre de 2023, se alcanzó un acuerdo sobre el reglamento que establece la obligatoriedad de que, en dos años, todos los Estados miembros de la Unión Europea proporcionen una cartera de ID europea única, gratuita y voluntaria a ciudadanos y empresas. Esta cartera permitirá identificarse digitalmente con seguridad en todo el espacio europeo. Para el 2026, con la implementación de la Cartera de ID Europea, se espera que cada Estado Miembro emita una aplicación móvil que permitirá a los ciudadanos y residentes de la UE identificarse en línea con total seguridad para acceder a servicios en línea públicos y privados en toda Europa[94].
Interoperabilidad	• La identificación digital en España está diseñada para ser interoperable a nivel nacional y europeo. Esto permite a los ciudadanos utilizar su DNIe y certificados digitales para acceder a servicios de otros países de la UE que cumplan con el reglamento eIDAS. • El Esquema Nacional de Interoperabilidad, desarrollado por la Agencia Española de Protección de Datos (AEPD), establece los principios y requisitos para garantizar la interoperabilidad entre los sistemas y servicios electrónicos en España. Esto incluye la identificación digital, permitiendo la conexión y el intercambio de información entre diferentes entidades y sistemas.
Firma electrónica	La firma electrónica es una pieza clave en el SID de España y se utiliza para dar validez legal a documentos y transacciones electrónicas. A través de mecanismos como el Documento Nacional de Identidad Electrónico (DNIe), los certificados digitales, y la plataforma (email protegido), los ciudadanos y

[94] https://administracionelectronica.gob.es/pae_Home/pae_Actualidad/pae_Noticias/2024/Mayo/Noticia-2024-05-22-Entrada-en-vigor-del-Reglamento-de-Identidad-Digital.html

	entidades pueden firmar documentos de manera segura y con reconocimiento legal.		
Servicios públicos accesibles a través del SID	El 98% de los servicios de la administración pública se encuentra disponibles en línea; el 90% de estos utilizando la identificación digital como forma de inicio de sesión[95]	**Entidad rectora**	Dirección de Tecnologías de la Información y las Comunicaciones, Ministerio de Presidencia
Identificación biométrica	• El DNIe incorpora la biometría de la huella dactilar como parte de las características de seguridad del documento. Las huellas dactilares de los titulares se almacenan en el chip electrónico del DNIe y se utilizan como un método de verificación de identidad. • Aunque la huella dactilar en sí no se utiliza directamente en la autenticación en línea con el DNIe, sí es una característica de seguridad que fortalece la validez del documento. Para usos en línea, el DNIe se basa principalmente en certificados digitales y PINs. • El uso de datos biométricos en España está sujeto a la normativa de protección de datos, incluyendo el Reglamento General de Protección de Datos (RGPD) de la Unión Europea y la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD) en España. • Los datos biométricos son considerados datos personales sensibles, por lo que su recopilación y tratamiento requieren un alto nivel de protección. • Los sistemas biométricos en España emplean técnicas avanzadas de encriptación y almacenamiento seguro para proteger los datos biométricos de los ciudadanos. Por ejemplo, las huellas dactilares almacenadas en el DNIe están cifradas y solo pueden ser leídas por dispositivos autorizados y seguros.		
Mecanismos de seguridad	• Tanto el DNIe como los certificados digitales utilizan tecnologías criptográficas avanzadas para garantizar la seguridad de las transacciones. Esto incluye el uso de claves públicas y privadas, así como la encriptación de datos para proteger la información durante la transmisión. • El SID en España utiliza diferentes métodos de autenticación: – Contraseña permanente: un usuario y contraseña establecidos por el ciudadano.		

[95] Administración Pública Digital (2024).

	– Cl@ve PIN: un sistema de acceso rápido mediante un PIN temporal que se genera cada vez que se necesita acceder a un servicio. – Certificado Digital y DNIe: (email protegido) permite también el uso de certificados digitales y del DNIe para la autenticación.
Vinculación con servicios de privados	El DNI electrónico puede ser utilizado para acceder a servicios de la administración general del Estado, las Comunidades Autónomas, la Administración Local y el Sector Privado[96].
Práctica relevante	• Contar con un ecosistema legal propicio para la ID ha permitido a España avanzar a lo largo de los años en la protección de los datos personales y la generación de más servicios públicos digitales a la ciudadanía. • Las normas, regulaciones y experiencias de la Unión Europea han sido propicias para fortalecer la visión del país en la definición de un mecanismo efectivo de ID y SID. • La disposición de un alto porcentaje de servicios públicos digitales estimula el uso y confianza en los SID en la población.

Fuente: elaboración propia.

3.7 Casos emergentes de SID en Iberoamérica

Costa Rica y República Dominicana presentan experiencias de implementación de SID en áreas prioritarias para la sociedad. Las experiencias expuestas a continuación reflejan los avances de estos países en el fortalecimiento de la ID para el reconocimiento de los derechos humanos.

3.7.1 República Dominicana

En República Dominicana, la identificación digital es un proceso que busca modernizar y asegurar la forma en que se identifican y autentican los ciudadanos y residentes.

En agosto de 2024, la Oficina Gubernamental de Tecnologías de la Información y Comunicaciones (OGTIC) lanzó la primera fase de la carpeta ciudadana SoyYoRD, la cual permite a los ciudadanos dominicanos acceder a su información personal de la cédula de identidad, licencia de conducir, afiliación al seguro social y otros, como el expediente único educativo, a través de una app móvil disponible para iOS y Android. El principal objetivo de esta iniciativa es que los ciudadanos puedan tener acceso y control de sus datos, como una antesala al uso de estos en la gestión de servicios públicos digitales.

[96] Ministerio del Interior (2022).

Una de las características relevantes de SoyYoRD es que ha considerado diferentes pruebas de usabilidad[97], funcionalidad, diseño, accesibilidad y experiencia del usuario para su diseño final, a través de debates y retroalimentaciones con la sociedad. Por el momento, SoyYoRD permite la centralización de todos los datos de los ciudadanos, de ahí su denominación como una Carpeta Ciudadana. Se espera que, en una segunda fase, estos datos provean una ID que pueda homologarse a la presentación de carnés físicos para la identificación inequívoca de las personas, permitiendo así el acceso a servicios públicos como pasaportes, trámites tributarios, subsidios y seguridad social, entre otros. SoyYoRD es una iniciativa implementada por la OGTIC en el marco de la Estrategia Nacional de Interoperabilidad, que busca mejorar los servicios de derechos sociales. La Carpeta Ciudadana es uno de los proyectos estratégicos que facilitan la implementación de otras iniciativas, como el Expediente Único Educativo y el Expediente Único de Salud. La Agenda Digital 2030 de República Dominicana hace referencia a los SID y a la ID, con el objetivo de implementar una plataforma única de identificación y autenticación del ciudadano, que incluya la firma electrónica.

3.7.2 Costa Rica

La identificación digital en Costa Rica se centra en la integración de tecnologías avanzadas para mejorar la eficiencia y seguridad en la gestión de la identidad, permitiendo el acceso a servicios de salud tanto en el sector público como en el privado.

El Expediente Digital Único en Salud de Costa Rica es un modelo relevante en la región para la prestación de servicios a través de tecnologías digitales, abarcando tanto al sector público como al privado. Es uno de los expedientes electrónicos más integrales y masificados de la región, un proyecto que recibió el apoyo del Programa por Resultados para el Fortalecimiento del Seguro Universal de Salud del Banco Mundial. El Expediente Digital Único en Salud es administrado por la Caja Costarricense del Seguro Social, la cual presta la mayor parte de la atención médica en el país y cuenta con una cobertura casi universal. Destaca el impacto que tuvo la existencia de este expediente durante la pandemia por COVID-19, facilitando el seguimiento de la crisis y simplificando de forma efectiva los procedimientos administrativos en los centros de atención médica.

Junto al Expediente Digital Único en Salud, se ha desarrollado el Sistema Integrado de Ficha Familiar, que integra datos de vivienda y familias en áreas remotas o sin acceso a internet o energía eléctrica, lo que permite tomar decisiones más enfocadas en materia de salud.

La Ley 9162 del Expediente Digital Único en Salud establece que la cédula costarricense es el número identificativo único para el expediente, como un principio de interoperabilidad e identificación digital de los ciudadanos. Al abrir un nuevo expediente en el Sistema Integrado de Adscripción, Agendas y Citas, se requieren datos de carácter demográfico, como el lugar de vivienda, nombre y tipo de consulta médica, junto con el diagnóstico de atención.

[97] Oficina Gubernamental de Tecnologías de la Información y Comunicación de la República Dominicana (2024).

3.7.3 Casos: ID transfronteriza

En muchos aspectos, Brasil y Uruguay son países distintos, tanto en su extensión geográfica (Brasil 8,515,770 km^2; Uruguay 176,215 km^2), población (Brasil 216.42 millones; Uruguay 3.42)[98], e idioma (Brasil: portugués; Uruguay: español). Sin embargo, estas disparidades no han sido limitación para desarrollar en conjunto una de las primeras experiencias pioneras de identidad digital transfronteriza. En octubre del 2024, la Unidad Reguladora de Servicios de Energía y Agua[99] (Ursea) de Uruguay habilitó 36 trámites en línea para ciudadanos brasileños[100]. Como antesala a este proyecto, el Instituto Nacional de tecnologías de la Información (ITI) de Brasil, la Unidad de Certificación Electrónica (UCE) y la Agencia de Gobierno Electrónico y Sociedad de la Información de Uruguay (AGESIC) firmaron en 2023 un convenio que promueve que el código técnico sea compatible en ambos países, con el fin de lograr el reconocimiento y uso transfronterizo de los SID[101].

Las características de este proyecto incluyen un SID que no opera con una identificación uruguaya, sino con la ID de nivel oro de la plataforma Gov.br, permitiendo realizar trámites en línea para empresas y personas de forma segura, con la misma validez que un trámite presencial. Tanto Uruguay como Brasil han implementado protocolos y criterios robustos para definir niveles de seguridad: oro, plata y bronce (en Brasil) y básico, intermedio y avanzado (en Uruguay). Esta experiencia está liderada por el Ministerio de Gestión e Innovación en los Servicios Públicos de Brasil y la AGESIC, a través de ID Uruguay, abriendo la puerta para que otras vinculaciones regionales se desarrollen mediante el uso de ID en servicios públicos transfronterizos. Según lo reportado por autoridades de Brasil, se espera que personas con ID uruguaya (identificaciones avanzadas) también puedan acceder a servicios públicos digitales de forma remota mediante un proceso de interoperabilidad robusto y bidireccional.

Otros países, como Argentina y Paraguay, podrían sumarse a iniciativas transfronterizas para potenciar la ID en servicios públicos digitales. Se proyecta que las plataformas Autenticar e ID Uruguay podrían integrarse para implementar servicios públicos digitales accesibles para personas en ambos países, de forma remota y con la misma validez que si estuvieran de manera presencial.

3.8 Prácticas relevantes de los SID en Iberoamérica

- **Integración de firma electrónica e ID hace más robusto el SID**. En la región, la firma electrónica ha sido vista como un hito de la madurez digital de los países. Se ha avanzado mucho en el establecimiento de marcos legales e infraestructura nacional. Aunque la adopción de la firma electrónica en los servicios públicos y privados es aún emergente, la revisión de la región permite identificar que aquellos países que han integrado la firma electrónica, los certificados

[98] Banco Mundial (2024).
[99] Unidad Reguladora de Servicios de Energía y Agua (2024).
[100] La Mañana (2024).
[101] Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (2023).

digitales y sistemas de interoperabilidad mediante mecanismos de ID tienen mayores posibilidades de impactar en la confianza de las personas para apropiar y utilizar la ID.

- **Garantizar el control de los datos es clave para fortalecer la transparencia y confianza de las personas en los SID**. Las leyes de protección de datos personales de la región iberoamericana proporcionan un marco referencial óptimo para el desarrollo digital, contribuyendo a una agenda de derechos digitales. La evidencia muestra que la implementación de sistemas de ID y SID puede exponer a las personas a riesgos de filtración de datos o suplantación de identidad. Si bien las leyes pueden ser rigurosas en cuanto al control de datos personales, también es necesario desarrollar sistemas e infraestructuras confiables, con arquitecturas de ciberseguridad eficaces.

- **El proceso de captura e identificación a través de medios digitales reduce el riesgo de errores u omisiones en la información de las personas**. Los sistemas de registro civil en la región presentan asimetrías significativas: aproximadamente entre el 60 % y el 70 % de los países tienen al menos una fase del proceso automatizada mediante medios digitales. La implementación de mecanismos de captura de datos, tanto demográficos como biométricos, utilizando tecnologías digitales, reduce el riesgo de errores y facilita un primer acercamiento de las personas a la ID. Además, agiliza el proceso y garantiza la emisión de una ID actualizada.

- **El fortalecimiento de portales de trámites y servicios públicos en línea que permiten la autenticación y validación de ID incentiva el uso de la ID**. En Iberoamérica, existen países avanzados en la disposición de servicios públicos digitales, como España, Uruguay y Chile. Este estudio destaca la importancia de contar con portales de trámites automatizados, donde las personas puedan acceder, realizar y pagar trámites, y recibir resolución en línea. Estos portales proporcionan un marco propicio para que los SID ofrezcan experiencias de identificación útiles y satisfactorias para los usuarios.

- **Definir los estándares de ID y SID a través de normas técnicas respaldadas en marcos legales permite escalar la adopción de tecnologías digitales y procesos de ID más eficientes.** Este estudio identifica que una práctica relevante en las experiencias iberoamericanas es el trabajo simultáneo en varias dimensiones:
  - Actualización de marcos legales habilitantes que permitan a las administraciones públicas avanzar en la madurez de los SID, garantizando derechos digitales, privacidad y buena gestión pública.
  - Fortalecimiento de la institucionalidad que supervise el funcionamiento de los SID.
  - Definición de estándares tecnológicos y de procesos que faciliten la comunicación y apropiación por parte de la ciudadanía.

- **La interoperabilidad es un habilitador esencial de la ID de las personas.** La ID requiere un mecanismo de interoperabilidad que aborde cuatro dimensiones: legal, administrativa, semántica y técnica. La experiencia regional muestra que otorgar una ID reconocida digitalmente refuerza la confianza de las personas y mejora sus interacciones con la

administración pública, al tiempo que reduce costos y aumenta la eficiencia en la prestación de servicios. La interoperabilidad también es fundamental para el desarrollo de procesos transfronterizos.

- **Desarrollo de iniciativas de ID transfronteriza**. La cooperación entre países en el diseño e implementación de ID transfronteriza ha producido resultados tangibles y experiencias valiosas que merecen ser analizadas. La evidencia sugiere que, para avanzar en estos procesos, los países deben fortalecer sus sistemas, protocolos, estándares, procesos y marcos legales, asegurando que las relaciones transfronterizas mediante ID sean seguras y eficaces. Las iniciativas de diálogo y aprendizaje entre países señalan que los SID transfronterizos contribuirían significativamente a la competitividad, seguridad y modernización de las administraciones públicas.

4. REFLEXIONES SOBRE DESAFÍOS Y OPORTUNIDADES A FUTURO

Como un proceso de reflexión sobre el entorno analizado, se presentan a continuación una serie de reflexiones sobre los desafíos y las oportunidades previstas a futuro para impulsar estrategias de SID sólidas en la región.

Figura 10

Oportunidades para fortalecer los SID en Iberoamérica

Fuente: elaboración propia.

Figura 11

Desafíos para fortalecer los SID en Iberoamérica

Fuente: elaboración propia.

Los países iberoamericanos enfrentan desafíos importantes para reducir las brechas de identificación y potenciar los SID en beneficio de los derechos de las personas. La CIPDED hace un llamado a abordar estos desafíos para que los países puedan avanzar, aprovechando sus fortalezas, hacia SID confiables que propicien iniciativas transfronterizas.

5. RECOMENDACIONES PARA LA IMPLEMENTACIÓN DE LA CIPDED

En la tabla siguiente se presenta una serie de recomendaciones para fortalecer la implementación de SID desde la perspectiva de la CIPDED, propiciando la colaboración regional y la validación de los principios de los derechos de las personas en los entornos digitales.

Tabla 11

Recomendaciones a futuro para la implementación de la CIPDED en el fortalecimiento de los SID

Recomendación (Recc)	Observación	Alineación con la CIPDED
Recc 1: definir estándares/marcos/modelos de referencia sobre el abordaje de la identificación digital, tomando en consideración el análisis de las experiencias de los países de la región.	Los países de la región pueden verse altamente beneficiados al desarrollar, a partir de las experiencias y aprendizajes comunes, modelos de referencia en materia de ID para diseñar o mejorar los SID, con miras a eventualmente interoperar a nivel transfronterizo.	*Los sistemas digitales de información utilizados con fines personales, profesionales o sociales deben poseer, desde su diseño y por defecto, las medidas de seguridad adecuadas que permitan garantizar la integridad, confidencialidad, disponibilidad, resiliencia y autenticidad de la información procesada y la disponibilidad de los servicios prestados.*
Recc 2: definir modelos de referencia para la nueva generación de marcos legales de ciberseguridad, protección de datos personales, firma electrónica e ID.	Dado los avances tecnológicos y los impactos de tecnologías emergentes como *blockchain* e inteligencia artificial, los países pueden desarrollar modelos orientadores para la renovación o generación de marcos legales en áreas críticas para la identificación digital: protección de datos personales, firma electrónica, entre otros.	
Recc 3: fortalecer el espacio de interacción entre gobiernos y sociedad civil para diseñar estrategias de identificación digital que incorporen elementos de inclusión digital.	La identificación digital debe generar confianza para lograr su cometido de abrir más oportunidades para que las personas accedan a servicios públicos de forma más ágil y eficiente. Para los países, puede ser relevante diseñar o fortalecer espacios de intercambio e interacción con organizaciones de sociedad civil a fin	*Las personas deben verse protegidas en los entornos digitales como sujetos de derechos y deberes.*

Recomendación (Recc)	Observación	Alineación con la CIPDED
	de enriquecer los SID a partir de la experiencia de usuarios y sus expectativas.	
Recc 4: desarrollar guías de modernización de registros civiles para interoperar con los SID.	Los países pueden altamente beneficiarse al contar con guías técnicas, legales y de procesos para la modernización de sus registros civiles, a partir de estándares o experiencias regionales. Implementar mesas de trabajo para analizar la interoperabilidad entre registros civiles y los SID.	
Recc 5: fortalecer la cooperación regional de intercambio de experiencias y asistencia técnica para acelerar la construcción de estrategias de interoperabilidad, como un complemento a estrategias de identificación digital.	Uno de los retos de los países está en proporcionar a los SID de condiciones óptimas para que puedan identificar a las personas y permitirles el acceso a los servicios públicos. Dado que existen asimetrías entre los países sobre sus procesos de interoperabilidad, la cooperación regional puede ser propicia para aprender, experimentar y desarrollar estrategias de interoperabilidad.	*La prestación de servicios digitales por parte del Estado y los trámites administrativos digitales sean personalizados, sencillos, inclusivos, accesibles, interoperables y seguros.*
Recc 6: impulsar estudios de casos desde la experiencia de las personas utilizando sistemas de identificación digital para acceder a servicios públicos digitales.	La identificación digital implica el reconocimiento de los derechos de los ciudadanos, por lo que contar con experiencias sistematizadas de las vivencias de las personas en el uso de SID, puede proveer insumos importantes en el diseño de nuevas generaciones de SID y, además, señalar condiciones del entorno que deben atenderse para lograr los niveles óptimos de la identificación digital: competencias digitales, conectividad, etc.	
Recc 7: realizar hojas de ruta sobre servicios públicos prioritarios para los ciudadanos-empresas.	Los países pueden establecer una hoja de ruta sobre los servicios y/o trámites que son más vitales automatizar y que puedan incluir mecanismos de identificación digital, como una guía orientadora	

Recomendación (Recc)	Observación	Alineación con la CIPDED
	destinada a los gobiernos para fortalecer su provisión de servicios públicos.	
Recc 8: definir una caja de herramientas digitales implementadas por los países más avanzados en SID en la región.	Los países pueden beneficiarse al contar con una caja de herramientas digitales a disposición, bajo modelos como bienes públicos regionales o *software* público para fortalecer sus propios SID, propiciando así el intercambio entre los países y la reutilización de elementos digitales.	*Fomentar la transferencia de tecnología mediante la asistencia y cooperación técnica y financiera, así como la creación de capacidades científicas y tecnológicas para colmar la brecha digital y el desarrollo.*
Recc 9: realizar un mapeo intenso sobre las tecnologías del sector privado que propician la ID, definiendo los grados de riesgos y seguridad.	Los países pueden establecer espacios de acercamiento con el sector privado para conocer de las tecnologías innovadoras existentes en el mercado, con el objetivo de crear un canal transparente de exposición para las empresas en la región.	
Recc 10: crear o fortalecer iniciativas regionales para la formación de servidores públicos sobre el diseño de servicios públicos digitales con identificación digital.	Desarrollar mecanismos de formación de servidores públicos en tres dimensiones: tecnología, marcos legales y eficiencia de servicios públicos. Esto permitiría a los países formar o fortalecer las competencias de los equipos responsables del diseño de los SID. Además, puede incluirse en este proceso de formación la identificación de casos y el intercambio entre países en temas específicos.	*La falta de medios, habilidades o competencias digitales no suponga una discriminación o exclusión para quienes no pueden o no están en disposición de integrarse en el proceso de trasformación digital.*
Recc 11: diseñar proyectos tipo *sandboxes* para experimentar tecnologías que fortalezcan los SID.	Los países pueden diseñar proyectos para crear *sandboxes* o espacios controlados para experimentar con tecnologías y procesos de *software* público, a fin de identificar mejoras posibles a sus propios SID.	*Sean fomentados sistemas de autenticación y uso de firmas digitales que aseguren la integridad de los documentos digitales, dotándoles de mayor seguridad tanto técnica como jurídicamente si*
Recc 12: promover encuentros técnicos	Con la existencia de mesas de trabajo entre los países, puede	

Recomendación (Recc)	Observación	Alineación con la CIPDED
entre las oficinas rectoras de la identidad de los países de la región, para conocer experiencias en la implementación de tecnologías, normativas y servicios públicos digitales con el uso de diferentes modelos de identificación digital.	desarrollarse una serie de encuentros técnicos para conocer de primera mano las experiencias de los países más avanzados en la implementación de SID. Las experiencias compartidas también pueden integrarse en la caja de herramientas digitales y en la plataforma de formación.	*los suministraron previamente de manera electrónica.*

Fuente: elaboración propia.

El estudio de los SID en la región iberoamericana para la prestación de servicios públicos, muestra que existen asimetrías en la madurez de la ID y de los SID, así como en la definición de servicios públicos digitales para las personas. El uso de tecnologías como la biometría, el reconocimiento facial, *blockchain*, entre otras, pone de manifiesto que existe un gran potencial a nivel de herramientas e infraestructura para hacer los SID más accesibles, seguros y confiables; sin embargo, es necesario que las personas cuenten con mecanismos de protección y seguridad para evitar que sus datos sean filtrados o suplantados.

REFERENCIAS

Administración Pública Digital. (2024). *El 98% de los servicios públicos españoles están disponibles online*. https://www.administracionpublicadigital.es/actualidad/2024/07/el-98-de-los-servicios-publicos-espanoles-estan-disponibles-online

Access Now. (2018). *National Digital Identity Programmes: What's next?* https://www.accessnow.org/wp-content/uploads/2018/06/Digital-Identity-Paper-2018-05.pdf

Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento. (2018). *Casi cien mil personas usan su identidad digital.* https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/noticias/casi-cien-mil-personas-usan-su-identidad-digital

Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento. (2020). *Cómo vamos en el Programa Trámites en Línea.* https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/iniciativas/tramites-en-linea/vamos-programa-tramites-linea

Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento. (2023). *Uruguay y Brasil firman convenio de cooperación técnica en identificación digital.* https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/noticias/uruguay-brasil-firman-convenio-cooperacion-tecnica-identificacion-digital

Aristóteles. (1988). *Política* (Trad. y notas de García Valdés, M.). Biblioteca Básica Gredos.

Asociación por los Derechos Civiles. (2016). *El sistema de protección de datos personales en América Latina: oportunidades y desafíos para los derechos humanos – Vol. I.* https://adc.org.ar/wp-content/uploads/2019/06/023-A-El-sistema-de-protecci%C3%B3n-de-datos-personales-en-Am%C3%A9rica-Latina-Vol.-I-12-2016.pdf

Asociación por los Derechos Civiles. (2017a). *Cuantificando identidades en América Latina.* https://adc.org.ar/wp-content/uploads/2019/06/029-cuantificando-identidades-en-america-latina-05-2017.pdf

Asociación por los Derechos Civiles. (2017b). *La identidad que no podemos cambiar. Cómo la biometría afecta nuestros derechos humanos.* https://adc.org.ar/wp-content/uploads/2019/06/027-A-la-identidad-que-no-podemos-cambiar-04-2017.pdf

Asociación por los Derechos Civiles. (2019). *Mi huella por un voto. Acerca de la identificación biométrica en elecciones.* https://adc.org.ar/wp-content/uploads/2019/11/0049-Mi-huella-por-un-voto-04-2019-V2.pdf

Banco Mundial. (2019). *Sistemas de identificación digitales fiables e inclusivos pueden abrir oportunidades para las personas más vulnerables del mundo.* https://www.bancomundial.org/es/news/immersive-story/2019/08/14/inclusive-and-trusted-digital-id-can-unlock-opportunities-for-the-worlds-most-vulnerable

Banco Mundial. (2024). *Los datos relativos a Brasil, Argentina, Uruguay, Paraguay.* https://datos.bancomundial.org/?locations=BR-AR-UY-PY

Barbosa, A., Carvalho, C., Machado, C. y Costa, J. (2020). *Good ID in Latin America – Strengthening the appropriate uses of digital identity in the region.* Instituto de Tecnologia & Sociedade do Rio. https://itsrio.org/wp-content/uploads/2020/07/Report_Good_ID_ENG.pdf

Budapest Convention on Cybercrime of the Council of Europe. (2023). *Adhesión al Convenio sobre la Ciberdelincuencia: Beneficios.* https://rm.coe.int/cyber-buda-benefits-19april2023-es/1680aafa3f

CFATF GAFIC. (2021). *¿Qué es la Identidad Digital (ID)?* Mesa de Investigación de la Secretaría del GAFIC. https://www.cfatf-gafic.org/home-test/documentos-en-espanol/rinc%C3%B3n-de-investigaciones/17082-%C2%BFqu%C3%A9-es-la-identidad-digital-id-_nov_2021/file

Clark, J. M., Metz, A. y Casher, C. (2022). *ID4D Global Dataset 2021: Volume 1 - Global ID Coverage Estimates (English).* World Bank Group. http://documents.worldbank.org/curated/en/099705012232226786/P176341132c1ef0b21adf11abad304425ef

Clark, J., Metz, A. y Casher, C. (2023, 06 de febrero). En todo el mundo, 850 millones de personas no tienen un documento de identidad. ¿Por qué esto es importante y qué podemos hacer al respecto? *Voces. Banco Mundial Blogs*. https://blogs.worldbank.org/es/voices/en-todo-el-mundo-850-millones-de-personas-no-tienen-un-documento-de-identidad-por-que-esto

Comisión Económica para América Latina y el Caribe [CEPAL]. (2007). *Libro blanco de interoperabilidad de gobierno electrónico para América Latina y el Caribe.* https://repositorio.cepal.org/server/api/core/bitstreams/ec93d026-91b1-4d7e-9e9e-00d16b351fcb/content

Congreso Nacional. (2022). *Ley núm. 339-22 que habilita y regula el uso de medios digitales para los procesos judiciales y procedimientos administrativos del Poder Judicial. G. O. No. 11076.* https://poderjudicial.gob.do/wp-content/uploads/2023/08/Ley-339-22-que-habilita-y-regula-el-uso-de-medios-digitales-para-los-procesos-judiciales-y-procedimientos-administrativos-Gaceta.pdf

Cotait, C. (2023, 21 de febrero). How blockchain is influencing 2023 banking landscape in Mexico. *Mexico Business News.* https://mexicobusiness.news/tech/news/how-blockchain-influencing-2023-banking-landscape-mexico

Durango, J. E. (2023, 21 de mayo). El futuro de la identidad digital en Costa Rica. *Delfino CR.* https://delfino.cr/2023/05/el-futuro-de-la-identidad-digital-en-costa-rica#

Encyclopaedia Herder. (2017). *Sociedad.* Herder Editorial S.L. https://encyclopaedia.herdereditorial.com/wiki/Sociedad

G20 Brasil 2024. (2024). *El portal brasileño Gov.br se destaca a nivel global en el taller sobre Gobierno Digital e Inclusión.* https://www.g20.org/es/noticias/el-portal-brasileno-gov-br-se-destaca-a-nivel-global-en-el-taller-sobre-gobierno-digital-e-inclusion

Governo Federal Brasil. (2023). *El caso de Brasil.* https://www.redgealc.org/site/assets/files/16318/2023_09_19_mercosul_apresentacao_govbr_polly.pdf

Guerrero Argote, C. (2020). *Identidad Digital en Perú: Descifrando al Leviatán.* Asociación Civil Hiperderecho. https://hiperderecho.org/wp-content/uploads/2020/11/guerrero_identidad_digital.pdf

Guerrero, C. y Lara Castro, P. (2023). *Identidad digital en América Latina: Situación actual, tendencias y problemáticas. Derechos* Digitales América Latina. https://www.derechosdigitales.org/wp-content/uploads/DD_Reporte_Regional_GIF.pdf

Ho, A. (2022). Identidad digital*. Ratio Legis*, Año 2, No. 4. https://rinedtep.edu.pa/server/api/core/bitstreams/fa04fb08-fac2-4a11-b768-feef4be6fe4b/content

Imamovic, F. (2023, 01 de octubre). Brazil Embraces Blockchain Technology for National Identity. *Financial World.* https://www.financial-world.org/news/news/financial/22218/brazil-embraces-blockchain-technology-for-national-identity/

Instituto Panamericano de Derecho y Tecnología [IPANDETEC]. (2024). *Filtración masiva de datos en El Salvador y la necesidad de con contar medidas de ciberseguridad y regulación sobre protección de datos personales.* https://www.ipandetec.org/el-salvador/filtracion-masiva-de-datos-en-el-salvador-y-la-necesidad-de-contar-medidas-de-ciberseguridad-y-regulacion-sobre-proteccion-de-datos-personales/

Jamele, A. (2023, 05 de junio). Autenticación digital en Argentina: Qué es, tipos, normativas y cómo protegerte. *InnovaciónDigital360*. https://www.innovaciondigital360.com/cyber-security/autenticacion-digital-en-argentina-una-guia-completa-para-proteger-tu-identidad-en-internet/

La Mañana. (2024). *Ursea habilitó trámites digitales seguros con Brasil.* https://www.xn--lamaana-7za.uy/actualidad/ursea-habilito-tramites-digitales-seguros-con-brasil/

McKinsey Global Institute. (2019). *Digital identification. A key to inclusive growth.* https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/digital%20identification%20a%20key%20to%20inclusive%20growth/mgi-digital-identification-report.pdf

Ministerio del Interior. (2021). *Portal del DNI Electrónico.* https://www.dnielectronico.es/PortalDNIe/

Ministerio del Interior. (2022). *Servicios disponibles.* https://www.dnielectronico.es/PortalDNIe/PRF1_Cons02.action?pag=REF_500

Muente Kunigami, A. (2018, 23 de agosto). Identidad digital: Pasaportes virtuales para navegar la nueva burocracia. *Gobernarte. Ideas innovadoras para mejores gobiernos.* https://blogs.iadb.org/administracion-publica/es/identidad-digital-pasaportes-virtuales-para-navegar-la-nueva-burocracia/

Mundaca, R. (2023, 06 de julio). Clave Única: Especialistas destacan seguridad de esta herramienta de identificación digital. *Comunicaciones VTI. Universidad de Chile.*

https://uchile.cl/noticias/206842/clave-unica-destacan-seguridad-del-sistema-de-identificacion-digital

Ochoa Chaves, L., Jiménez Alvarado, O. y Martínez de Lemos, F. (2023). *Expediente digital único en salud (EDUS) de Costa Rica: buenas prácticas, historia e implementación.* Publicaciones BID. https://publications.iadb.org/es/expediente-digital-unico-en-salud-edus-de-costa-rica-buenas-practicas-historia-e-implementacion

Oficina Gubernamental de Tecnologías de la Información y Comunicación de la República Dominicana. (2024). *Encuentro Estratégico: Evaluación y Futuro de Mi Carpeta Ciudadana.* https://www.linkedin.com/posts/ogticrdo_soyyord-ogtic-carpetaciudadana-activity-7237839089947820033-N2rO/?originalSubdomain=es

Ọnụọha, M. y Nucera, D. (2022). *A Digital ID Handbook. Strategies for Navigating Electronic Identification Systems. A People's Guide to Tech*. https://www.theengineroom.org/wp-content/uploads/2024/02/A-digital-ID-handbook-APGT-The-Engine-Room-2022.pdf

Peiró, P. y Pomeda, Y. (2019, 18 de marzo). Una vida sin DNI. *El País.* https://elpais.com/elpais/2019/03/05/planeta_futuro/1551789785_453552.html

Pereira, A. P. (2023, 30 de septiembre). Brasil lanza identificación digital basada en blockchain. *Cointelegraph.* https://es.cointelegraph.com/news/brazil-rolls-out-blockchain-based-digital-id

Red Española del Pacto Mundial. (2018). *Empresas y derechos humanos: acciones y casos de éxito en el marco de la Agenda 2030.* https://www.pactomundial.org/wp-content/uploads/2019/11/Empresas-y-derechos-humanos.pdf

Red Iberoamericana de Protección de Datos. (2017). *Estándares de protección de datos personales para los Estados Iberoamericanos.* https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf

Registraduría Nacional del Estado Civil. (2023). *Preguntas frecuentes.* https://wapp.registraduria.gov.co/identificacion/cedula-digital/conoce-mas.html

Roseth, B., Reyes, A. y Santiso, C. (2018). *El fin del trámite eterno. Ciudadanos, burocracia y gobierno digital.* Banco Interamericano de Desarrollo. https://publications.iadb.org/es/publications/spanish/viewer/El-fin-del-tr%C3%A1mite-eterno-Ciudadanos-burocracia-y-gobierno-digital.pdf

Secretaría General Iberoamericana [SEGIB]. (2023). *Carta Iberoamericana de Principios y Derechos en los Entornos Digitales*. https://www.segib.org/wp-content/uploads/Carta_iberoamericana_derechos_digitales_ESP_web.pdf

The Centre for Internet & Society. (2020). *Governing ID. Principles for Evalution*. https://cis-india.org/internet-governance/governing-id-principles-for-evalution

TuID. (2018*). Política de Identificación Digital*. https://www.gub.uy/unidad-certificacion-electronica/sites/unidad-certificacion-electronica/files/documentos/publicaciones/Pol%C3%ADtica%2Bde%2BIdentificaci%C3%B3n%2BDigital_%2BVersi%C3%B3n%2B1.0.pdf

Unidad Reguladora de Servicios de Energía y Agua. (2024). *Trámites.* https://www.gub.uy/unidad-reguladora-servicios-energia-agua/tramites-y-servicios/tramites

United Nations Economic Commission for Africa [UNECA]. (2024). *Digital ID to unlock Africa's economic value if fully implemented, say experts. Communications Section, Economic Commission for Africa.* https://www.uneca.org/stories/digital-id-to-unlock-africa%E2%80%99s-economic-value-if-fully-implemented%2C-say-experts#:~:text=A%20digital%20ID%20is%20an,and%20established%20with%20individual%20consent

W3C. (2022). *Decentralized Identifiers (DIDs) v1.0. Core architecture, data model, and representations*. https://www.w3.org/TR/did-core/

Weidenslaufer, C. y Roberts, R. (2022*). Identidad digital: conceptos y legislación*. Biblioteca del Congreso Nacional de Chile. Asesoría Técnica Parlamentaria. https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/33658/2/Identidad_Digital_BCN_2022.pdf

World Bank. (2016). *Digital identity : towards shared principles for public and private sector cooperation (Inglês).* https://documents.worldbank.org/pt/publication/documents-reports/documentdetail/600821469220400272/digital-identity-towards-shared-principles-for-public-and-private-sector-cooperation

World Bank. (2018a). *G20 Digital Identity Onboarding.* https://www.gpfi.org/sites/gpfi/files/documents/G20_Digital_Identity_Onboarding.pdf

World Bank. (2018b). *ID Enabling Environment Assessment: Guidance Note (English).* http://documents.worldbank.org/curated/en/881991559312326936/ID-Enabling-Environment-Assessment-Guidance-Note

World Bank. (2019a). *ID Enrollment Strategies: Practical Lessons From Around The Globe.* https://documents1.worldbank.org/curated/ar/539361582557916734/pdf/ID-Enrollment-Strategies-Practical-Lessons-From-Around-The-Globe.pdf

World Bank. (2019b). *Identity Authentication And Verification Fees: Overview Of Current Practices. Identification for Development.* https://documents1.worldbank.org/curated/fr/945201555946417898/pdf/Identity-Authentication-and-Verification-Fees-Overview-of-Current-Practices.pdf

World Bank. (2019c). *ID4D Practitioner's Guide (English).* http://documents.worldbank.org/curated/en/248371559325561562/ID4D-Practitioner-s-Guide

World Bank. (2022). *Engaging Civil Society Organizations (CSOs) for Successful ID Systems: Guidance Note.* http://hdl.handle.net/10986/38106