Julio, 2020

Good ID en América Latina

Fortaleciendo los usos apropiados de la Identificación Digital en la región

Autores
Alexandre Barbosa
Celina Carvalho
Cláudio Machado
Janaina Costa

Sumário

Agradecimientos

Le agradecemos a Omidyar Network por el apoyo brindado a este proyecto de investigación, no solo desde el punto de vista financiero, sino también por colaborar en red con colegas que trabajan con identidad digital provenientes del sur global. Asimismo, deseamos agradecerles a nuestros colegas del Center for Internet and Society (CIS), de India, y del Center for Intellectual Property and Information Technology Law (CIPIT) por los intercambios esclarecedores y por la cooperación. Nos encauzamos hacia el fortalecimiento del Movimiento Good ID.

Colaboradores expertos

Este informe se basa en la experiencia y los aportes de los siguientes colaboradores expertos:

Fabro Steibel • Director Ejecutivo, ITS Rio

Alejandro Barros • Consultor internacional sobre políticas públicas de desarrollo digital

Edgar Vásquez Cruz • Proveedor de soluciones de TI

Evelyn Téllez Carvajal • Investigadora, INFOTEC México

Fernanda da Escóssia • Periodista y profesora universitaria,IBMEC Rio

José Villalba • CEO, Electronic-ID

Juan Carlos Lara • Director de Investigación y Políticas Públicas, Derechos Digitales

Miguel Arce • Gerente comercial, Pagos Digitales Peruanos

Miguel Morachimo • Director Ejecutivo, Hiperderecho

Raquel Chrispino • Juez de derecho, Tribunal de Justicia del Estado de Río de Janeiro

Ricardo Saavedra • Gerente de Registro y Certificación Digital, RENIEC

Edición

Celina Bottino • Directora de proyecto, ITS Rio

Clara Langevin • Consultora Titulada, Columbia University

Proyecto de diseño

Ana Luisa Figueiredo • ITS Rio

Fotos

Tales Duarte • ITS Rio

Agência Brasil

Traducción

Sara Iriarte • IECH, CONICET-UNR

Financiado por

OMIDYAR NETWORK

ITS Instituto de Tecnologia & Sociedade do Rio

Abreviaturas y acrónimos

CadÚnico	Registro Único para Programas Sociales
CEDN	Coordinación de Estrategia Digital Nacional
CEN	Certificado Electrónico de Nacimiento
CEV	Cartilla Electrónica de Vacunación
CURP	Clave Única de Registro de Población
DDC	Diligencia Debida respecto del cliente
DNI	Documento Nacional de Identidad
DUDH	Declaración Universal de los Derechos Humanos
ID4D	Identificación para el Desarrollo
INFOTEC	Centro de Investigación e Innovación en TIC, de México
KYC	Conozca su cliente
NHDID	Identificador Nacional Digital de Salud
OCDE	Identificador Nacional Digital de Salud
ODS	Objetivos de Desarrollo Sostenible
OEA	Organización de los Estados Americano
OMS	rganización Mundial de la Salud
ONU DAES	División de Estadística de las Naciones Unidas
ONU	Organización de las Naciones Unidas
ONUSIDA	Programa conjunto de las Naciones Unidas sobre el VIH/SIDA
OPS	Organización Panamericana de la Salud
PBF	Programa Bolsa Familia
PPS	Programas de Protección Social
RCEV	Registro Civil y Estadísticas Vitales
RENIEC	Registro Nacional de Identificación y Estado Civil
RG	Registro civil
SAID	Sistema Automático de Identificación Dactilar
SID	Sistema de Identidad Digital
SIG	Sistema de Información Gerencial
TIC	Tecnologías de la Información y la Comunicación
UNESCO	Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura

Sumario

Foto: Agência Brasil

Sumario

La transformación digital de la economía y de la sociedad es una realidad. Por esta razón, la identidad digital ha pasado a un primer plano en tanto elemento esencial del futuro. Bajo la misma lógica analógica, uno debe ser capaz de probar digitalmente con facilidad (o demostrar) quién es, o correr el riesgo de ser excluido del futuro.

A pesar de que la transformación digital ofrece muchas oportunidades, no debe considerarse la panacea para los problemas latinoamericanos. Las tecnologías disruptivas, los enfoques innovadores y, sobre todo, las expectativas de los nuevos usuarios entran en juego a un campo donde viejas problemáticas persisten. En lo que respecta a la identificación, las poblaciones carenciadas y vulnerables continúan deparándose con barreras para acceder a documentación personal básica, así como afrontan prácticas de protección de datos y privacidad endebles, sistemas de identificación con una arquitectura altamente centralizada y una baja utilización de la identificación para mejorar la prestación de servicios.

De manera concomitante, el desafío de cómo identificar a las personas a la vez que se preservan sus derechos, crece al mismo tiempo que las responsabilidades y el control sobre los datos. Asimismo, la identificación puede variar considerablemente en su conceptualización, configuraciones legales y organizativas, al igual que la infraestructura operativa y tecnológica adoptada. La identificación se está convirtiendo en una palabra de moda, empleada de forma diferente de acuerdo con las agendas políticas.

A su vez, no pueden pasarse por alto cuestiones clave como la exclusión, la discriminación y la vigilancia. Adaptadas a una perspectiva latinoamericana, las cuestiones mencionadas fueron empleadas como base para el presente informe. La inclusión constituye el principio rector de este estudio y servirá como lente para nuestro análisis.

Conforme se vigoriza la adopción y la promoción de los sistemas nacionales de identidad digital en todo el mundo, surgen inquietudes sobre cómo garantizar su uso adecuado. Se necesitan enfoques sectoriales y regionales para abordar verdaderamente los desafíos tradicionales y emergentes de la inclusión y la privacidad. En asociación con Omidyar Network, el equipo de ITS Innovation, a través de un proyecto de investigación de un año de duración, diseñó un análisis para identificar los marcos regionales de buena identificación –o Good ID, como se lo conoce en inglés– y fomentar

estratégicamente prácticas apropiadas en los usos sectoriales de la identificación digital. En vistas a dicha propuesta, el presente proyecto de investigación define como objetivos principales:

- Investigar los usos apropiados de la identidad digital en sectores específicos, tales como las prácticas de identificación contemporáneas y las circunstancias en las cuales la identificación digital puede resultar riesgosa para los derechos individuales.
- Mapear los principios y determinar las pautas para la concepción, el ajuste y la implementación de la identificación digital de modo que se asegure el desarrollo sostenible en América Latina, ubicando, por consiguiente, la inclusión, los sistemas seguros y la buena gobernanza en el centro de la agenda.
- Apoyar a los formuladores de políticas y profesionales de América Latina en la implementación de los principios de un sistema de identificación bueno y, por lo tanto, inclusivo, y de este modo fortalecer y consolidar el movimiento Good ID en el continente.

Para fundamentar nuestros objetivos, realizamos una vasta revisión bibliográfica que nos permitiera entender la identificación digital como un fenómeno, a la vez que a las partes involucradas. A continuación, evaluamos los diferentes impactos y relaciones de la identificación digital en casos de uso sectoriales específicos. Por último, realizamos entrevistas a una muestra de las partes interesadas provenientes de México, Chile, Perú y Brasil a fin de respaldar dichos estudios de casos específicos.

Nuestros resultados se estructuran en escenarios de uso para comprender cómo debe funcionar un sistema de identificación en estos contextos específicos y cómo puede interrelacionarse con los impactos de la identificación digital. Los sectores seleccionados fueron **los servicios gubernamentales digitales, la inclusión financiera, la atención sanitaria y la protección social**. Este enfoque era necesario debido a la complejidad del problema y dado que establecer una respuesta única para todos los casos de uso sectorial resultaría un enfoque frívolo. Como aportes fundamentales para los usos apropiados en los sectores, destacamos lo siguiente:

Servicios gubernamentales digitales

Varios países del mundo están desarrollando e implementando agendas de gobierno digital nacionales y regionales. La forma en que las personas se registrarán y accederán a estas plataformas y el valor que alcancen los mecanismos participativos son determinados por la identificación digital. Por lo tanto, la identificación digital puede disminuir o aumentar la distancia

entre el Estado y la sociedad, así como mejorar o disminuir la confianza hacia el sector público. Conclusiones fundamentales:

1. **Los servicios gubernamentales digitales deben abarcar, como primer paso, un sistema de identificación ampliamente accesible que aporte valor al usuario al simplificar los procedimientos, reducir los costos directos e indirectos y habilitar los servicios de transacción.**
2. **Las estructuras de autenticación integradas o federadas que usan datos compartidos de diferentes sistemas deben seguir e incorporar prácticas de transparencia sólidas e informar a los usuarios acerca del tratamiento de sus datos personales, en conformidad con la ley nacional de protección de datos o, en ausencia de dicha ley, siguiendo las mejores prácticas internacionales.**
3. **Los servicios gubernamentales digitales deben llegar a los grupos más vulnerables, por lo que debe existir una opción de identificación digital sin costo para dichos usuarios. Independientemente del nivel de garantía requerido por determinados servicios del gobierno digital, las credenciales digitales deben ser las mismas y, por lo tanto, resultar inclusivas para los usuarios, idealmente gracias a la implementación de credenciales digitales sin costo.**

Inclusión financiera

La identificación es clave para determinar la confiabilidad del cliente y reducir el fraude. La identificación digital puede facilitar la aplicación de procedimientos para conocer al cliente (KYC, por sus siglas en inglés) de manera más eficiente y más simple, lo cual permitiría una mayor inclusión financiera. Asimismo, la identificación digital puede servir de apoyo para políticas y sistemas contra el lavado de dinero y contra el terrorismo. La identificación digital ha recibido creciente atención debido al aumento de la banca abierta (es decir, el intercambio de datos financieros y personales entre instituciones financieras) en todo el mundo. Conclusiones fundamentales:

1. **Los requisitos básicos para reconocer al cliente idealmente deben ser gratuitos para garantizar la inclusión financiera de la población a la que se destinan y deben ser fáciles de cumplir. Es importante separar claramente los datos básicos utilizados para identificar a alguien en base a la información complementaria que es requerida para acceder a servicios específicos y la diligencia debida respecto del cliente.**
2. **En tanto sector líder en identificación desde una perspectiva tecnológica, las compañías de tecnología financiera y los grandes**

bancos deberían apoyar y ser impulsores fundamentales de las tecnologías que garanticen la privacidad. Vale considerar a este respecto que la inexistencia de mecanismos de reparación y de reclamo para acceder al historial de los datos de uno mismo constituye un indicador importante de malas prácticas, si se tiene en cuenta el desarrollo tecnológico alcanzado por el sector.

3. **Los reguladores financieros deben trabajar en estrecha colaboración con las autoridades de identificación y protección de datos para garantizar la interoperabilidad con el sistema nacional de identificación.**

Assistencia sanitaria

La identificación involucra varias cuestiones importantes, desde el derecho universal a la atención sanitaria hasta la seguridad del paciente y la eficiencia en la prestación de servicios públicos. La correcta identificación contribuye a evitar que un paciente reciba un tratamiento inapropiado como, por ejemplo, que se administre a un paciente un medicamento al cual es alérgico. La identificación digital también puede facilitar la emisión de registros electrónicos agregados y generar datos para respaldar políticas de salud basadas en evidencias. Conclusiones fundamentales:

1. **Al establecerse una identificación nacional única para los servicios sanitarios, esta puede ser vinculada a una identificación fundacional. Sin embargo, este enlace no debe permitir el acceso a datos médicos confidenciales por parte de terceros. En caso de ser necesario acceder a ellos para satisfacer necesidades de información de interés para la salud pública, los datos deben ser anónimos, de forma que se evite que el paciente pueda ser reidentificado.**
2. **El acceso a servicios médicos urgentes, no solo emergencias, nunca debe estar condicionado a la identificación. Este principio se aplica, consecuentemente, a la identificación digital.**
3. **Es posible que resulte necesario desarrollar métodos de identificación alternativos para garantizar la integridad del proceso de solicitud de sistemas nacionales que requieren identificación (como los programas de vacunación). La identificación digital podría constituir en elemento que facilite dicho fin.**

Protección social

A menudo se requiere identificación para demostrar la calificación para acceder a programas sociales como transferencias de efectivo, pensiones, tarjetas de alimentación, seguridad social y otros afines. Esto constituye un problema dado que quienes más necesitan dicha asistencia son también quienes tienen menos probabilidades de contar con un documento de identidad, incluidas las personas carenciadas, oriundas de zonas rurales y marginadas. Por esta razón, la identificación digital se postula como una solución para los sistemas de identificación deficientes, en la medida en que constituye una forma de superar el problema, incluso al facilitar la inscripción de beneficiarios y las transacciones entre gobierno y las personas. Sin embargo, esto puede resultar problemático, especialmente en los países en desarrollo (lo cual implicaría una negligencia hacia el papel esencial que desempeña la documentación básica). Conclusiones fundamentales:

1. **Los gobiernos deberían crear un registro único para ofrecer protección social, adoptando una perspectiva inclusiva que permita mejorar su capacidad de llegar a la población vulnerable. Es crucial simplificar y hacer que los servicios de identificación sean más accesibles para la población indocumentada equilibrando los requisitos y las condiciones de los beneficiarios.**
2. **La integración de los sistemas de información gerencial y los sistemas de identificación digital deben tener en cuenta el riesgo de excluir a la población más vulnerable, al tiempo que no deben perder de vista la efectividad de las políticas.**
3. **La adopción de la tecnología biométrica con el objeto de proveer protección social debe ser precedida de una evaluación integral del sistema nacional de identificación, en la cual los marcos institucionales y legales sean evaluados a través de los lentes de promoción de la inclusión y los derechos, asegurando que los grupos de personas carenciadas y más vulnerables no resulten excluidos.**

Sección 1

América Latina y la identificación en la era digital

Foto: Agência Brasil

1. América Latina y la identificación en la era digital

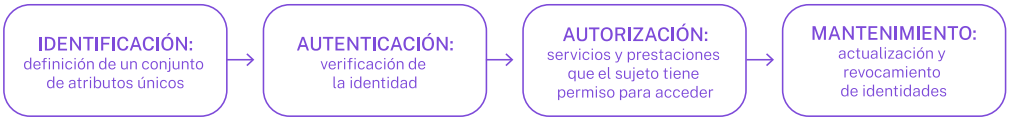
1.1. Un vistazo a la identidad digital

En las últimas décadas, dos perspectivas sobre la identificación de personas en la era digital se han destacado en la bibliografía referida a la identificación digital. Una percibe las identidades digitales, combinadas con tecnologías emergentes, como una herramienta para la vigilancia masiva y, por esta razón, las ve con desconfianza. La otra percibe la digitalización de los sistemas de identificación como un medio para fortalecer los derechos y mejorar el acceso a los servicios.

La identificación digital puede referir elementos diferentes: se puede definir como un conjunto de atributos capturados y almacenados electrónicamente (por ejemplo: nombre, género, fecha de nacimiento y datos biométricos –como un escáner de iris, huellas digitales y faciales, entre otros) y/o credenciales (por ejemplo: claves, tarjetas de identificación, aplicaciones móviles) que identifican a una persona de manera única. Por nuestra parte, propugnamos una visión más sistémica de la identificación digital, una que va más allá de la autenticación digital, o el inicio de sesión en un sitio web, una identidad legal basada en dispositivos móviles, certificados digitales o registros de nacimiento electrónicos de forma aislada.

Desde nuestro punto de vista, la identificación digital constituye un mecanismo técnico para la identificación digital y segura de personas, en el cual no resulta necesario el contacto cara a cara. En un sistema de identificación fundacional (Banco Mundial, 2018d)[1], la identidad digital debe cimentarse en una institución responsable, en una legislación coherente y en medios técnicos que permitan la interoperabilidad con diferentes sistemas de información. En otras palabras, se asume que la identidad digital hereda las mismas características deseables que la identificación civil; es decir, es inclusiva, accesible, portátil y persistente.

Figura 1: Ciclos de gestión de la identificación



Fuente: elaboración propia

Tradicionalmente, la gestión de la identificación suele dividirse en cuatro pasos: (i) registro o identificación, (ii) autenticación, (iii) autorización y (iv) mantenimiento. Cada paso comprende etapas específicas. Por ejemplo, el primero abarca la emisión, uso y gestión de identidades personales (incluyendo la recopilación de datos de identidad, la validación a través de la prueba, la deduplicación de identidad y la emisión de credenciales). La identificación se relaciona con el proceso por el cual una persona declara o reivindica quien dice ser. En lo que respecta a la autenticación y la autorización, vale la pena destacar las distinciones que existen entre los dos. La autenticación es la validación de la identidad. Debe garantizar que una persona sea real (humana) y singular (única). Sin embargo, mientras la identificación puede ser considerada información pública, la autenticación debe ser privada. Esta suele estar asociada con algo que la persona posee (por ejemplo, un identificador físico, también conocido como *token*), algo que la persona sabe (por ejemplo, una contraseña) y algo que la persona "es" (por ejemplo, la identificación a través de sus huellas digitales). Este último componente, "algo que la persona es", está ganando cada vez más relevancia gracias al desarrollo de la tecnología biométrica, como ocurre con la identificación facial.

Cuando una persona es verificada y autenticada en una transacción, es importante determinar a qué servicios o instalaciones específicos puede acceder. El proceso para determinar esta elegibilidad se denomina autorización. Se puede argumentar que cada una de estas etapas se vuelve más desafiante en sistemas totalmente digitales o, incluso, híbridos. Po último, el mantenimiento es el paso que se asocia a la posibilidad de actualizar o revocar identidades y credenciales.

Riesgos y equilibrio

Los sistemas de identidad digital están sometidos a riesgos de consecuencias adversas, así como son propensos a desviarse de su misión (Bhadra, 2019). En primer lugar, el sistema puede distorsionarse y excluir a parte de la población, así como puede violar derechos fundamentales, tales como el derecho a la privacidad y al acceso a servicios básicos. En otras palabras, existen riesgos de exclusión legal, cultural, económica y tecnológica (Banco Mundial, 2019b).

En segundo lugar, la brecha digital continúa siendo una barrera para muchas personas en los países en desarrollo, a la vez que la alfabetización digital genera riesgos aún mayores de exclusión de las poblaciones carenciadas y vulnerables. Muchos proyectos de identificación digital dependen de aplicaciones móviles y, por lo tanto, requieren niveles significativos de conectividad y acceso a dispositivos tecnológicos. En este sentido, si no son implementados y diseminados de forma cuidadosa, dichos programas tienden a aumentar la brecha digital y social (Ratcliffe, 2019).

Por último, la sensibilidad de los datos de identificación es digna de mención, y esto puede profundizarse cuando se trata de usos sectoriales, como la atención sanitaria. El riesgo del mal uso de la información aumenta como consecuencia de la digitalización. El acceso no autorizado o el uso indebido de la información personal puede reducir la confianza, socavar los derechos de privacidad, promover la discriminación y, en algunos casos, exponer a los grupos vulnerables a un grave riesgo de sufrir perjuicios (Banco Mundial, 2019b). Independientemente de un consenso sobre el tema, es necesario seguir un enfoque equilibrado, en el que se mitiguen los riesgos derivados de la adopción de sistemas de identificación digital.

Principios

El ODS 16.9 de la ONU establece que todos tienen derecho a la identidad legal, pero no existe ningún sistema de identificación completamente adecuado para incluir a todos. No resulta práctico abogar por un modelo único de sistema de identidad digital, pero es crucial informar a las partes interesadas sobre ciertos principios rectores, opciones técnicas y buenas prácticas, para que el sistema pueda adaptarse mejor a las necesidades, objetivos y contextos.[2]

Los gobiernos, los organismos multilaterales internacionales, el sector privado y las organizaciones de la sociedad civil han deliberado acerca de los sistemas de identificación digital y sus posibles riesgos y oportunidades. Como resultado, se han establecido algunos principios para mitigar los riesgos antes mencionados y mejorar los beneficios y oportunidades al implementar un sistema de identificación digital.

En este sentido, destacamos el trabajo realizado por un grupo de organizaciones internacionales facilitado por el Banco Mundial y el Centro para el Desarrollo Global, el cual contribuyó al debate estableciendo los Principios sobre la identificación para un desarrollo sostenible (Banco Mundial, 2016). Para lograr resultados de nivel superior, se reunieron los principios rectores en tres pilares: i) fomentar la inclusión, garantizando la cobertura de la identidad universal y la accesibilidad; ii) establecer un diseño preciso, seguro,

receptivo y sostenible, y iii) garantizar un buen gobierno y generar confianza mediante la protección de la privacidad y los derechos de los usuarios.

Por su parte, el movimiento Good ID, una coalición multisectorial, también contribuye a informar las políticas, el diseño tecnológico y la práctica sobre el tema en todas las regiones[3], abogando por sistemas que garanticen la privacidad, la inclusión, el valor del usuario, el control en manos del usuario y la seguridad.

El presente trabajo tiene como objetivo contribuir a la promoción y la comprensión de la aplicación de estos principios dentro de los usos sectoriales de la identidad digital analizados en el contexto latinoamericano.

Usos sectoriales de la identificación digital

Existe una distinción entre sistemas de identificación digital "funcionales" y "fundacionales". Los sistemas funcionales generan identificaciones con el objeto de cumplir una función específica en un sector determinado. Estos sistemas establecen la prestación o autorización de un servicio específico y pueden o no estar vinculados a sistemas de identificación que admitan otras funciones. Cualquier persona puede tener una variedad de identificaciones funcionales (por ejemplo: licencia de conducir, tarjeta de seguro médico, registro de votante). En cambio, los sistemas fundacionales tiene como objeto principal proporcionar identificación en tanto bien público, no a proporcionar un servicio específico.[4]

Los sistemas de identificación digital tienen diferentes características, funcionalidades y riesgos según su uso. En este trabajo, presentaremos algunos ejemplos, abordando sus usos con respecto al gobierno digital, los servicios financieros, la atención sanitaria y la protección social.

Existen varios otros casos de uso sectorial para la identificación digital que no se abordarán en este documento. Por ejemplo, muchos países asocian su identificación civil asociada a su agenda electoral. Un caso consolidado mencionado y recurrente es el sistema de votación electrónica de Estonia. Con respecto a los sistemas fiscales, la identificación digital tiene un gran potencial para facilitar el pago y la recaudación de impuestos a través de transacciones de personas al gobierno (P2G, por sus siglas en inglés), así como para evitar la evasión fiscal. Por lo tanto, puede impulsar la capacidad del Estado (Gelb, A. et. Al., 2020). Estos son solo algunos de los muchos usos prácticos para las identidades digitales.

1.2. Inclusión al centro

La identidad es un derecho que debe extenderse a todas las personas. Esto no significa que la identificación deba ser obligatoria; sino que cualquiera que desee ser identificado por el sistema debería poder hacerlo.

El derecho a la identidad no es solo un "pasaporte" a otros derechos, sino un derecho per se. La identidad personal está intrínsecamente vinculada a los derechos a una nacionalidad y al derecho al reconocimiento en todo lugar como persona ante la ley. La comunidad internacional reconoce estos como derechos humanos (Declaración Universal de Derechos Humanos, 1948) y deben estar protegidos por marcos institucionales y legales sólidos.

Registro Civil y Estadísticas Vitales

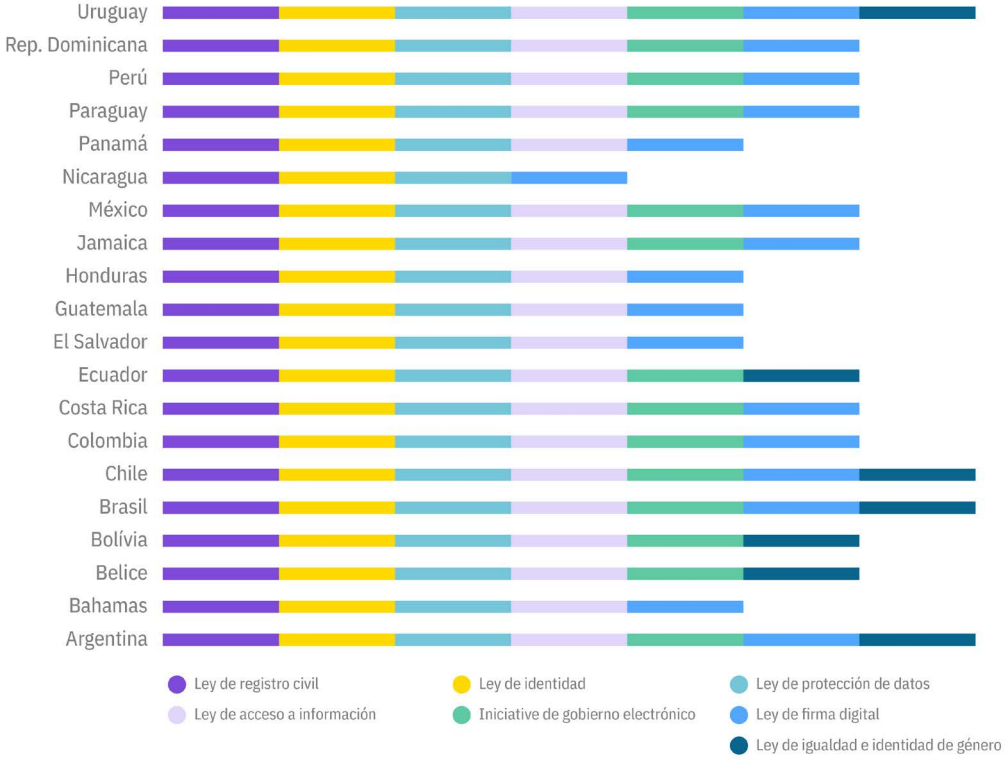
Según la División de Estadística de las Naciones Unidas (ONU DAES), el Registro Civil y Estadísticas Vitales (RCEV) es el registro continuo, permanente, obligatorio y universal de la ocurrencia y características de eventos vitales de la población de acuerdo con la ley.

El Grupo de Expertos en Identidad Legal de la ONU recomienda vincular el RCEV y la identificación porque el sistema RCEV desempeña un papel crucial en un marco legal como medio oficial para probar la información biográfica necesaria para certificar muchos derechos humanos, como el derecho a un nombre y a la paternidad. Además, al integrar RC e identificación digital, se puede contar con una visión integral (del nacimiento a la muerte) de las personas, lo cual muestra cómo un vínculo orgánico entre los sistemas podría mejorar los servicios de gestión de identidad y facilitar la prestación de servicios a los ciudadanos.

Sin embargo, en algunos contextos puede ser difícil integrar el RCEV y la identificación digital.

Los países latinoamericanos cuentan con legislaciones muy avanzadas e integrales sobre la identificación y la protección de datos. Para proporcionar una visión general del marco legislativo, el siguiente cuadro muestra qué países regulan i) el registro civil; ii) la emisión de un documento único de identidad; iii) la protección de datos personales; iv) el acceso a la información; v) el gobierno electrónico; vi) la firma digital, y vii) la igualdad e identidad de género. Los sistemas de identificación digital crean nuevas posibilidades, así como riesgos para las personas.

Figura 2: Marcos legales por país



Fuente: Adaptado de Registros civiles y oficinas de identificación: Análisis y fichas de país, Banco Interamericano de Desarrollo (BID), Estefania Calderón, 2019, <Registros civiles y oficinas de identificación: análisis y fichas de país>

A pesar de que el reconocimiento institucional de la identidad como derecho y la legislación de la protección de datos resultan esenciales, pueden ser necesarias salvaguardas complementarias para garantizar su cumplimiento y un sistema de identificación digital inclusivo. Por ejemplo, un enfoque centrado en el usuario, que coloca a las personas en el núcleo del concepto de identificación digital y el control de cuándo, cómo y si desean confirmar sus identidades en línea, es primordial (GSMA, 2016). Desde la perspectiva de la protección de los derechos y la inclusión socioeconómica, estas salvaguardas deben entenderse como enraizadas en un marco institucional y legal más amplio que las soluciones tecnológicas autónomas.

A su vez, cabe señalar que en determinados contextos y en muchos ejemplos históricos, la identificación podría poner a un individuo en peligro de violencia o exclusión. Intencionalmente o no, los sistemas de identificación pueden facilitar la persecución de grupos pertenecientes a determinada

religión, origen étnico, género o ideología política, y contribuir a la estigmatización de los individuos (por ejemplo, al exponer un estado de enfermedad o una situación de vulnerabilidad económica con el objeto de demostrar la calificación para recibir un beneficio social).

La digitalización no elimina los riesgos antes mencionados y podría acarrear otros. Los sistemas de identificación digital pueden incrementar notablemente los riesgos de exclusión de las poblaciones carenciadas y vulnerables. El acceso digital y la alfabetización resultan aspectos clave. La brecha digital continúa siendo un desafío en todo el mundo, especialmente en los países en desarrollo. Es por eso que es primordial contar con un diseño claro de identificación digital para promover la inclusión en todas sus dimensiones y fortalecer las salvaguardas para todos. Un sistema no puede clasificarse como Good ID sin ello.

Cobertura universal

Los Objetivos globales para el desarrollo sostenible de las Naciones Unidas exigen que todas las personas cuenten con una prueba oficial de su identidad en 2030 (Objetivo 16.9). Al establecer esta meta, las Naciones Unidas no determinaron que los sistemas de identidad fueran obligatorios para todos, sino que se reconoció que todos tienen derecho a la identidad. La diferencia entre la cobertura universal y la identidad obligatoria no es un juego de palabras. La implementación de políticas de Good ID implica un sistema de identificación digital que permita la inclusión de todas las personas, para que participen plenamente en la sociedad y la economía en la que viven. Sin embargo, es notorio que el proceso enfrenta muchos desafíos clave para ser efectivamente inclusivo en lugar de exclusivo.

Asimismo, las tecnologías de la información y la comunicación (TIC) y las infraestructuras de datos del país constituyen elementos críticos. Un nivel mínimo de infraestructura de TIC para proporcionar identidad digital debe ser considerado, de tal manera que sea posible incluir a todos los residentes de un país. Las políticas también deben tomar en cuenta las poblaciones remotas que poseen bajas tasas de acceso a la infraestructura y que sufren con la brecha digital.

Enfoque multicanal y prioridades

Las identidades digitales y los mecanismos de identificación tradicionales pueden coexistir. Es posible que en muchos países no resulte factible reemplazar completamente los documentos personales físicos por un sistema digital. A la vez, las personas también deben contar con acceso a medios alternativos de identificación y opciones de cómo se identifican.

Por lo tanto, se debe considerar un enfoque multicanal en países donde no se puede garantizar un nivel mínimo de infraestructura de TIC a lo largo y ancho del territorio.

Este sistema híbrido requiere especial atención en el siguiente punto: es pasible de iniciar un proceso de diferenciación entre aquellos que cuentan con acceso a servicios habilitados para la identificación digital y aquellos que continúan en el sistema físico. Por ejemplo, si los servicios digitales fueran más eficientes que los servicios presenciales, esto podría incrementar la desigualdad resultante de la brecha digital.

Equidad de género

La prueba de edad e identidad puede ser crucial para garantizar la independencia y la inclusión financiera de las mujeres, además de ser una herramienta para proteger a las niñas del matrimonio infantil[5] y la trata. Sin embargo, la desigualdad de género está muy presente en las estadísticas de inclusión, registro civil y registros vitales. Según el Centro de Excelencia para Sistemas RCEV, las mujeres se ven afectadas de forma más negativa por los registros de defunción y están sujetas a mayores dificultades para registrar a sus hijos que los hombres (Centro de Excelencia para Sistemas RCEV, 2020).

Esto significa que enfrentan mayores barreras y están infrarrepresentadas en estadísticas vitales, como las utilizadas en las políticas públicas para reducir la mortalidad femenina, por ejemplo. Cabe considerar, asimismo, que los registros de matrimonio, divorcio y defunción son imprescindibles para que las mujeres puedan obtener beneficios de pensión y reclamar derechos de herencia. La digitalización de la identidad debe abordar estas preocupaciones.

Accesibilidad

Un buen sistema de identificación está diseñado para su contexto y garantiza un acceso adecuado para los usuarios y el funcionamiento satisfactorio del sistema. Cuando estos aspectos fallan, una gran parte de la sociedad puede quedar excluida del acceso a servicios vitales. Por ello, es importante considerar cuál debería ser el estándar mínimo para la infraestructura necesaria y cómo abordará el sistema, en particular, a las minorías y a las personas vulnerables. Es decir, debe evitar excluir, por defecto, a aquellas personas que gozan de un nivel más bajo de alfabetización digital[6] o a aquellas con dificultades socioeconómicas para acceder a los medios digitales, como las comunidades rurales, ribereñas, indígenas y cimarronas.

1.3. Identificación digital en América Latina

América Latina ha jugado un papel importante en el desarrollo de tecnologías modernas de identificación, especialmente en la mejora de la tecnología de dactiloscopia (huella digital) (Ferrari, 2015). Juan Vucetich y sus colaboradores en La Plata, Argentina, mejoraron el método y diseñaron una nueva perspectiva sobre el uso de huellas digitales en un contexto no criminal.[7] La dactiloscopia fue más simple de usar y más efectiva que el sistema Bertillonage, creado por Alphonse Bertillon, en Francia, y adoptado, en el siglo XX, como el método oficial para la identificación criminal y civil en casi todos los países latinoamericanos. El enfoque de Vucetich fue el punto de referencia hegemónico antes de que la identificación comenzara a automatizarse utilizando el Sistema Automatizado de Identificación de Huellas Digitales (AFIS, por su sigla en inglés) durante la década de 1970. Esto demuestra que América Latina siempre ha estado abierta a las innovaciones en tecnología de identificación, por lo que, lógicamente, las partes interesadas de la región se encuentran en búsqueda de identificaciones digitales para aplicarlas en muchos sectores.

Dicho esto, el éxito de cualquier programa nacional, digital o no, depende más del proceso y el contexto que de la tecnología. No se puede pasar por alto la situación política del país y la capacidad del gobierno para implementar un sistema dado. Adicionalmente, otros factores a considerar son el medio ambiente, la cultura, la historia de los conflictos y los niveles de pobreza. Por esta razón, en la presente sección proporcionamos una visión general de la interrelación entre dichos factores y la identidad en la región.

Aspectos regionales y culturales de identificación

La identificación de una persona puede ser percibida como un derecho *per se* o, por el contrario, como un apuntalamiento del derecho a la privacidad. Los países latinoamericanos, en sus propios contextos históricos, también atravesaron esta dicotomía en el desarrollo de sus sistemas de identificación. A diferencia de otros países del sur global, América Latina tiene una herencia cultural, religiosa y colonial notablemente similar. Este terreno común se refleja en la forma como se percibe la identificación en la región.

Cuarenta años antes de la Declaración Universal de Derechos Humanos de las Naciones Unidas, Vucetich (1916) menciona “el derecho a un nombre”. Ya sea que se trate de un anacronismo histórico o no, e independientemente de una definición precisa de un “derecho a la identidad”, es innegable que la argumentación de Vucetich fue muy innovadora en comparación con las de otros pioneros en identificaciones. Argumentó durante la redacción de la

Ley de Registro de Identidad de las Personas, de Argentina, que la identificación de todos los habitantes, sin distinción, sería un paso importante para garantizar el cumplimiento del derecho al nombre, así como para el correcto funcionamiento de las instituciones del Estado y, en consecuencia, para el bien de la sociedad. Esto puede considerarse como el reconocimiento del derecho a la identidad de referencia en la región.[8]

Por su parte, la antropóloga Mariza Peirano cuestionó los significados sociales y culturales de los documentos personales en Brasil (Peirano, 2009). Su investigación adoptó un enfoque innovador y destacó que los documentos no se limitaban a su uso formal y burocrático, sino que tenían un gran significado simbólico para las personas. La libreta de trabajo en Brasil es mucho más que una libreta de registro de empleo y de seguridad social, divide a la población en personas honestas y "vagabundos". La antropóloga concluye que "los documentos crean al ciudadano" de acuerdo con la percepción subjetiva de la población.

En este sentido, el trabajo de Fernanda da Escóssia es muy relevante para abordar la materia en América Latina (Escóssia, 2019a). Su tesis doctoral estudia la vida de personas no registradas en la ciudad de Río de Janeiro. Allí investiga la percepción de un individuo que carece de pruebas legales de identidad y demuestra que en dicha situación los sujetos no se ven a sí mismos como seres humanos.
"(...) Descubrí que esos sujetos se sentían muy privadas de la noción de 'Soy una persona', 'Tengo derechos'. Muchos de ellos solían decirme que se sentían como un perro... 'No soy nadie'.". La antropóloga enfatizó que el registro civil es una condición previa para un "sentido de mejor existencia" (Escóssia, 2019b).

La prueba de identidad, en lo que a esto respecta, no implica tan solo poseer un documento en papel o una aplicación móvil. Conlleva, en cambio, la posibilidad real de que la existencia del individuo sea oficialmente reconocida por el estado. Como lo demuestra la investigación de Escóssia, para muchos de los que carecen de registro civil, asegurarlo constituye un paso en el camino hacia la dignidad.

Empero, es importante destacar que la gestión de identidad en la región es llevada a cabo generalmente por una autoridad central de identificación, autorizada para la inscripción y la emisión de credenciales. Desafortunadamente, como la mayoría de los países latinoamericanos fueron gobernados por dictaduras en la segunda mitad del siglo pasado, los sistemas de identificación a menudo fueron apropiados con vistas a la vigilancia y la persecución (por ejemplo, la identificación biométrica facilitó la persecución de los opositores al régimen). De este modo, la historia

paradójica de la identificación en los países latinoamericanos muestra cómo la identificación se puede utilizar para fines buenos y malos.

La identificación se vuelve digital en la región

Como se indicó anteriormente, el primer paso de un sistema de identificación es el registro civil del individuo para emitir una identidad legal. En este sentido, los datos de UNICEF muestran que América Latina aún enfrenta un gran desafío para alcanzar el registro universal de nacimientos (UNICEF, 2016). (fig. 3)

En América Latina, hay un número significativo de grupos étnicos minoritarios. Un estudio realizado por la Organización de los Estados Americanos (OEA) concluyó que el factor clave que incidió en el subregistro fue la existencia de barreras legales para llevar a cabo el registro utilizando nombres étnicos (OEA, 2008). Asimismo, un informe de UNICEF también destaca cómo ciertos grupos pueden enfrentar barreras adicionales para ser incluidos en el registro civil (UNICEF, 2016). Vale la pena señalar que los niños rurales de la región amazónica representaron aproximadamente el 10 por ciento de aquellos sin identificación en 2015 (Center for Global Development, 2017b). Esto muestra cómo el proceso de registro en sí mismo a menudo carece de sensibilidad para permitir la inclusión de poblaciones indígenas y ribereñas. Las diferencias urbano-rurales también ocultan disparidades subyacentes más profundas, principalmente relacionadas con la pobreza. Asimismo, las poblaciones excluidas, como los inmigrantes indocumentados, a menudo desconocen sus derechos con respecto al registro de nacimientos o pueden ser reacias a registrar a sus hijos por temor a ser deportados a su país de origen (UNICEF, 2016). Estas barreras de acceso a menudo permanecen o aumentan con la identificación digital, la cual ha ganado importancia como clave para obtener acceso a los derechos y servicios en el mundo digital.

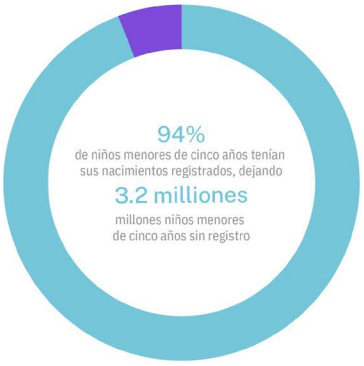
A su vez, la necesidad de mejorar la gestión pública y responder a las necesidades de los ciudadanos también está impulsando la promoción de la identidad digital como una herramienta esencial para la inclusión y la reducción de los costos de transacción en toda la economía, contribuyendo así a mejorar la calidad de los servicios, tanto en el sector público y privado (BID, 2019; BID, 2017). (fig. 4 y 5)

Dicho esto, la transformación digital se está operando en todo lugar, incluyendo los países latinoamericanos. A pesar de las similitudes regionales, el ritmo de digitalización y el impacto en la sociedad y en el sector público es proporcional a los índices de desarrollo humano de cada país. Por ejemplo, el índice de desarrollo del gobierno electrónico desarrollado por las Naciones Unidas[9] demuestra que mientras países como Uruguay (que

Figura 3: Estadísticas de registro de nacimientos en América Latina

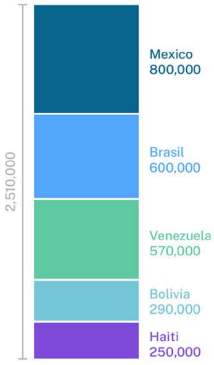
Los nacimientos de aproximadamente 3 millones de niños menores de cinco años en América Latina y el Caribe nunca ha sido registrado.

Porcentaje de niños menores de cinco años cuyos nacimientos están registrados y número de niños menores de cinco años cuyos nacimientos no están registrados.



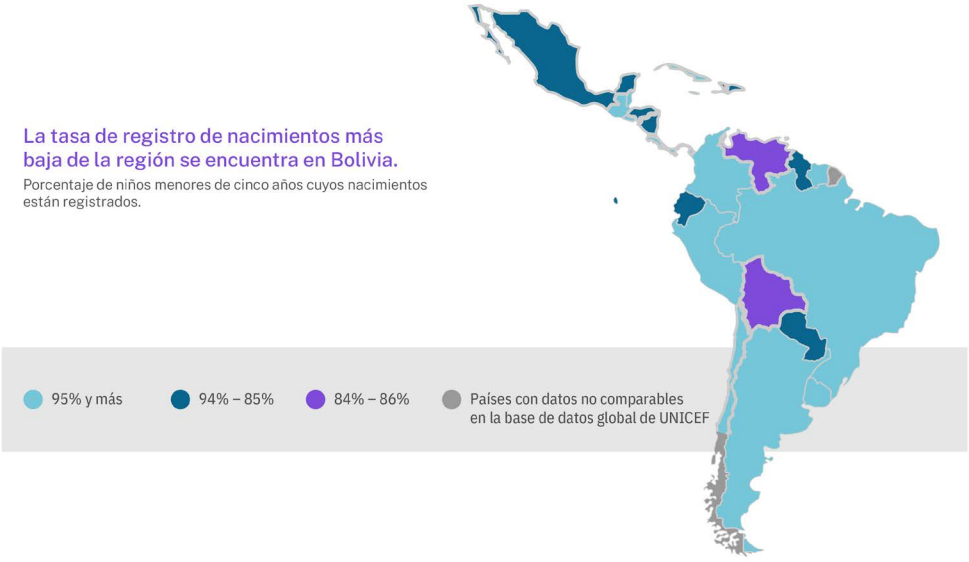
1 de cada 4 niños sin registro de nacimiento en la región vive en México

Número de niños menores de cinco años cuyos nacimientos no están registrados, en los cinco países con el mayor número de niños no registrados en la región.



La tasa de registro de nacimientos más baja de la región se encuentra en Bolivia.

Porcentaje de niños menores de cinco años cuyos nacimientos están registrados.



Fuente: Reimpreso del Registro de Nacimientos en América Latina y el Caribe: Cerrando las Brechas, UNICEF, 2016, <Birth Registration in Latin America and the Caribbean: Closing The Gaps>

Figura 4: En países con niveles generales más bajos, el registro de nacimientos es más común en áreas urbanas que rurales; donde los niveles son más altos, las disparidades debidas al lugar de residencia disminuyen

Porcentaje de niños menores de cinco años cuyos nacimientos están registrados, por lugar de residencia.

Fuente: Reimpreso del Registro de Nacimientos en América Latina y el Caribe: Cerrando las Brechas, UNICEF, 2016, <Birth Registration in Latin America and the Caribbean: Closing The Gaps>

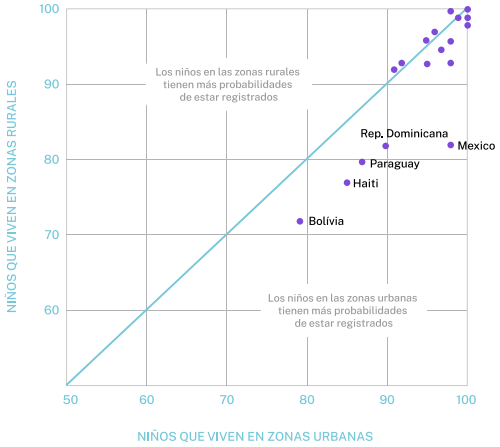
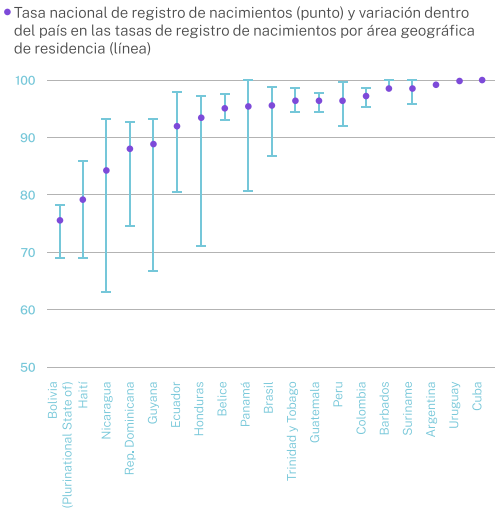


Figura 5: La prevalencia del registro nacional de nacimientos puede ocultar importantes disparidades geográficas

Porcentaje de niños menores de cinco años cuyos nacimientos están registrados y el área geográfica con los niveles más altos y más bajos de registro de nacimientos

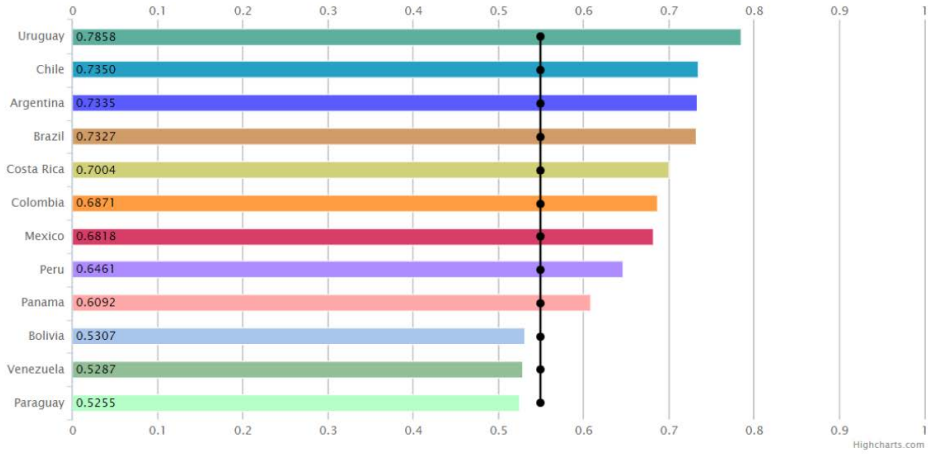
Fuente: Reimpreso del Registro de Nacimientos en América Latina y el Caribe: Cerrando las Brechas, UNICEF, 2016, <Birth Registration in Latin America and the Caribbean: Closing The Gaps>



tiene un índice muy alto), Chile, Argentina, Brasil y Costa Rica obtienen una puntuación superior a 0,7 de 1, otros cuentan con una tasa realmente baja, como Haití (0,34) y Nicaragua (0,42).[10] (fig. 6)

En lo que respecta al registro civil y la identificación, el desarrollo de nuevas soluciones y servicios que faciliten la verificación y autenticación de los datos de identificación no solo permitiría a los ciudadanos acceder sencillamente a los servicios, sino que también facilitaría la recopilación de información para mejorar la planificación gubernamental y gestión de programas y servicios mejor enfocados (BID, 2019).[11]

Figura 6: Índice de desarrollo del gobierno electrónico de las Naciones Unidas



Fuente: Reimpreso del América Latina en el Índice de Gobierno Electrónico de las Naciones Unidas, Naciones Unidas (ONU), 2018, <2018 UN E-Government Survey | Multimedia Library - United Nations Department of Economic and Social Affairs>

Muchos organismos de identificación y registro pueden trabajar en línea en muchos países latinoamericanos, pero el uso de libros de contabilidad impresos aún no se ha eliminado. En algunos países, los marcos legales actuales requieren registrar eventos vitales en libros físicos.[12] (fig. 7)

En Argentina, el documento nacional de identidad fue respaldado por el Sistema de Identidad Digital (SID). Uruguay ha mejorado considerablemente el desempeño del gobierno digital, convirtiéndose en uno de los países líderes en este campo en América Latina. Desde 2007, el país ha tenido un plan de digitalización del gobierno y, como resultado, ofrece identificación digital de forma gratuita para todos sus ciudadanos. Además, se espera que para 2020 el 100 por ciento de los uruguayos tenga una identificación digital. El gobierno peruano desarrolló recientemente un documento nacional de identidad electrónico (DNI-e), una tarjeta basada en tecnología con chip y con claves criptográficas de autenticación incrustadas.

A pesar del lado negativo del uso de identificación biométrica en regímenes autoritarios, la población latinoamericana tiende a preferir la autenticación biométrica debido a que percibe una mayor facilidad de uso (Mastercard, 2019b). Si bien el informe citado fue realizado por una empresa extranjera con fines comerciales, proporciona información útil acerca del desarrollo futuro de la identificación digital en la región.

Figura 7: Tipo de apoyo documental en registros civiles por país

Fuente: Adaptado de Registros civiles y oficinas de identificación: Análisis y fichas de país, Banco Interamericano de Desarrollo (BID), Estefania Calderón, 2019, <Registros civiles y oficinas de identificación: análisis y fichas de país>

De todas formas, una parte importante de la población de América Latina aún no cuenta con acceso a la infraestructura básica, una condición previa para la implementación adecuada de los sistemas de identificación digital.[13] Los bajos niveles de electricidad, telecomunicaciones e infraestructura de datos aumentan la brecha digital entre las áreas rurales y urbanas (Domínguez, 2018); a la vez que las altas tasas de analfabetismo (UNESCO, 2009) representan desafíos fundamentales. El informe de la UNESCO (2017)[14] indica que más de 200 millones de latinoamericanos no cuentan con conexión a Internet, aunque los países latinoamericanos han dado pasos significativos hacia la digitalización (OCDE, 2019a).

1.4. Abordaje

Desde el comienzo de nuestro proyecto de investigación, hemos buscado comprender las situaciones en las que se debe solicitar la identificación digital, de qué manera y por quién. Tras varias rondas de debates y talleres, quedó claro que era necesario profundizar en el sistema de identificación, las formas en que este diverge entre sectores específicos y cómo la identidad digital impacta y se ve afectada en cada sector. Asimismo, asumimos una perspectiva de derechos humanos y riesgos durante dicho proceso, centrándonos en elaborar recomendaciones para salvaguardar transformaciones digitales sostenibles en material de identificación.

Nuestros interrogantes generales fueron:

- ¿Cuáles son los usos apropiados de la identificación digital en el sector?
- ¿Cómo se puede usar la identificación digital para fomentar el desarrollo sostenible de América Latina?

Para responder estas preguntas, durante el proceso de análisis sectorial de distintos casos de uso, nos cuestionamos:

- ¿Qué papel juega la identificación en el sector?
- ¿Cómo se realiza la identificación en el sector y cómo se relaciona con la identidad legal?
- ¿Cuál es el diagnóstico del sector en América Latina?
- ¿Cuáles son los riesgos de la identificación digital en el sector y cómo se pueden mitigar?
- ¿Cuándo se debe solicitar la identificación digital en el sector?

Para responder estas preguntas, dividimos nuestro enfoque en tres etapas: (1) Una revisión bibliográfica profunda; (2) un análisis sectorial de casos de uso; (3) estudios de caso (ver Anexo I para más detalles). A modo de apunte, el análisis de cada estudio de caso identificará tanto los paradigmas de uso apropiados como los riesgos asociados con el caso, así como las formas de avanzar hacia un sistema de buena identificación.

Sección 2

Usos sectoriales en el contexto latinoamericano

Foto: Tales Duarte

2. Usos sectoriales en el contexto latinoamericano

2.1. Servicios gubernamentales digitales

Los servicios del gobierno digital se refieren al uso de tecnologías digitales como una parte integrada de las estrategias de modernización del gobierno.[15] La digitalización de los servicios públicos (por ejemplo, la presentación de impuestos, la renovación de credenciales, la programación de citas, la actualización de información personal, la obtención de autorizaciones y certificaciones, entre otros) no es nada nuevo. Ha seguido el ritmo del desarrollo de Internet principalmente desde comienzos del milenio. Al principio, se lo denominó gobierno electrónico y, recientemente, se lo ha renombrado como gobierno digital (OCDE, 2019d).

Para promover la digitalización de los servicios públicos, los gobiernos han invertido durante mucho tiempo en métodos identificación digital y de autenticación que puedan garantizar un acceso fácil, seguro y legítimo a sus ciudadanos.

El rol de la identificación en los servicios gubernamentales digitales

Tradicionalmente, los servicios gubernamentales se han prestado en persona y han estado sujetos a la identificación para la realización de ciertos actos, como la presentación de impuestos, la renovación de la licencia de conducir y para programar vacunas, por ejemplo. Gracias a la transformación digital, la identificación digital se convierte en un facilitador clave de los servicios gubernamentales digitales. Un sistema de identificación digital bien implementado, que ofrece un alto nivel de seguridad y adopta características y protocolos de seguridad avanzados para proteger las identidades y los datos personales es primordial para desbloquear los beneficios potenciales en el sector. Estos comprenden no solo ahorrar dinero y tiempo en el desempeño de procedimientos burocráticos, sino también acercar a las personas a las decisiones públicas, aportando mayor seguridad y confianza en la búsqueda de un gran proceso participativo (OCDE, 2019c).

La identidad digital contribuye a facilitar el ejercicio de la ciudadanía y la participación política, por ejemplo, al habilitar canales de consulta digital. Un sistema de identificación digital confiable y seguro es esencial para

garantizar la legitimidad del proceso de consulta. Lo mismo puede aplicarse para facilitar los mecanismos de participación directa, como referéndums, plebiscitos o propuestas legislativas, como “Mudamos”.[16]

Métodos de identificación y posibilidades para los servicios gubernamentales digitales

La identificación de los servicios gubernamentales digitales puede variar de un país a otro. En determinado sistema, un procedimiento simple que envuelve un solo factor (es decir, el inicio de sesión con contraseña) permite a los usuarios iniciar sesión en una plataforma gubernamental. En otros sistemas, los usuarios deberán comprar o podrán recibir un *token* basado en operaciones PKI, gracias al cual pueden acceder a múltiples procedimientos, incluso a votar en línea.[17] A la inversa de estos sistemas centralizados, la identificación digital también se puede federar, y en algunos países hay disponibilidad de proveedores de autenticadores privados.[18]

Se podría utilizar una variedad de credenciales para lograr un alto nivel de garantía de autenticación y verificación, datos biométricos, contraseñas, certificados digitales, códigos QR y teléfonos móviles con información de identidad incorporada en los dispositivos. La identificación facial, en particular, se ha convertido en una tendencia para la autenticación gubernamental debido a su presunta mayor precisión. Pero también podría conllevar violaciones de la privacidad y discriminación.[19]

Contextualizando los servicios gubernamentales digitales en América Latina

La prestación de servicios en América Latina a menudo se diseña de manera no integrada, como una iniciativa aislada de la entidad gubernamental responsable de la prestación del servicio que se centra en sus propias prioridades internas.[20] En la interfaz digital, esta falta de integración se ve reflejada, en lugar de procurar eludirse. Esto tiene un impacto negativo en el ahorro potencial de tiempo y el valor de ofrecer facilidad para los usuarios; y, consecuentemente, en la adopción de los usuarios.

En 2015:

73%

DE LOS PAÍSES DE LA REGIÓN YA HABÍAN DESARROLLADO ESTRATEGIAS NACIONALES DE DESARROLLO DIGITAL

60%

TAMBIÉN HABÍA ESTABLECIDO PORTALES EN LÍNEA PARA ALGUNOS SERVICIOS GUBERNAMENTALES, ENTRE LOS QUE SE ENCUENTRAN COLOMBIA, MÉXICO, URUGUAY, BRASIL Y ARGENTINA.

- En parte gracias a estas iniciativas, se logró un rápido progreso en la conectividad de la región (OCDE, 2019b)
- Varios países han anunciado estrategias de gobierno digital alimentadas por organismos internacionales y empresas de consultoría, lo cual exhibe un gran potencial a la vez que plantea graves preocupaciones.

Riesgos de la identificación digital en el sector

La lógica del gobierno digital es que debe servir a los usuarios y no ser un fin en sí mismo.[21]

- Si cada entidad gubernamental implementa su propia identidad digital, surge un problema de interoperabilidad y se pierde gran parte de la eficiencia y el valor potencial para el usuario.
- Los servicios digitales pueden generar serios riesgos para la privacidad de una persona, debido a fugas y uso indebido de los datos de identificación y otros datos confidenciales vinculados al perfil del usuario (por ejemplo, sus ingresos en el caso de la presentación de impuestos).
- La identificación facial, en particular, se ha convertido en una tendencia en la autenticación del gobierno debido a su mayor precisión teórica. Pero también podría implicar violaciones de la privacidad y la discriminación.[22]
- Se supone que las regulaciones de protección de datos deben ser abordadas primero por el propio gobierno, a pesar de que no siempre ocurra de esta forma.
- Un enfoque "primero digital" para la prestación de servicios gubernamentales podría dar como resultado un conjunto de servicios públicos de dos niveles, que excluyan o empeoren la relación entre el gobierno y parte de la sociedad, específicamente aquellos que no pueden acceder o utilizar canales digitales con facilidad (OCDE, 2001).
- Dado que la identificación digital es la clave para acceder a estos servicios digitales, un sistema nacional de identificación digital mal diseñado puede dar lugar a que una gran parte de la población no logre acceder a los servicios.

- Para mitigar estos riesgos, resulta fundamental un enfoque multicanal para la prestación de servicios gubernamentales. Estos no deben restringirse al acceso digital. A su vez, las identidades digitales deben ser accesibles, idealmente de forma gratuita para el usuario. La persona debe poder acceder a toda la gama de servicios, independientemente de los niveles de garantía requeridos. Esto no significa que los certificados digitales PKI se deban utilizar para cada transacción, sino que los usuarios puedan elegir sus credenciales para servicios específicos, en consonancia.
- El sistema no debe implementarse por mera tendencia, sin tener en cuenta cuál sería la ganancia efectiva para el usuario.

Uso apropiado de la identificación digital en el sector

Los servicios del gobierno digital van más allá de ofrecer servicios digitalmente. También abarcan el establecimiento de una relación a través de un canal digital entre el gobierno y sus ciudadanos. Por un lado, el requisito de identificación para la prestación de servicios personalizados (digitalmente o no) es legítimo cuando es necesario un cierto nivel de autenticación para confirmar el estado del ciudadano, como para emitir certificados, obtener licencias, pagar impuestos, etc.[23]

Por otro lado, la identificación no debe depender de la prestación de servicios al ciudadano relacionados con el acceso a información útil, la transparencia de los actos gubernamentales y el fomento de la democracia y la participación ciudadana, ya que tal requisito no tiene sentido. Se debe evaluar críticamente, por lo tanto, la cantidad de datos necesarios para determinar la identidad del ciudadano, el método de autenticación[24] utilizado para los servicios del gobierno digital y si el proceso resulta inclusivo.

Conclusiones fundamentales para un uso adecuado de la identificación digital en el sector

- Los servicios gubernamentales digitales deben abarcar, como primer paso, un sistema de identificación ampliamente accesible que aporte valor al usuario al simplificar los procedimientos, reducir los costos directos e indirectos y habilitar los servicios de transacción.
- Las estructuras de autenticación integradas o federadas que usan datos compartidos de diferentes sistemas deben seguir e incorporar prácticas de transparencia sólidas e informar a los usuarios acerca del tratamiento de sus datos personales, en conformidad con la ley nacional de protección de datos o, en ausencia de dicha ley, siguiendo las mejores prácticas internacionales.
- Los servicios gubernamentales digitales deben llegar a los grupos más vulnerables, por lo que debe existir una opción de identificación digital sin costo para dichos usuarios. Independientemente del nivel de garantía requerido por determinados servicios del gobierno digital, las credenciales digitales deben ser las mismas y, por lo tanto, resultar inclusivas para los usuarios, idealmente gracias a la implementación de credenciales digitales sin costo.

Estudio de caso: **Gobierno digital de Chile e identificador único**

Desde 1943, el sistema de identificación chileno se enfoca en la identificación de todos los residentes, en lugar de identificar exclusivamente a los criminales (Laval, 2018). Posteriormente, en 1973, se creó el número único de identidad (Rol Único Nacional, RUN), el cual coincide con el RUT (Rol Único Tributario), que sirve como identificación civil y como identificador de contribuyente. Después de 1982, el RUT comenzó a emitirse en el momento del registro de nacimiento y ya ha sido informatizado.

La identificación es parte de la vida diaria de todos los chilenos, ya que es obligatoria para casi todas las interacciones formales. Como lo reportó Privacy International, **"si se no tiene el RUT (Rol Único Tributario), no se puede hacerlo"**. (Privacy International, 2018). En otras palabras, se requiere un RUT para acceder a casi todos los servicios gubernamentales.

Esto implica no solo que se proporciona una identificación para interactuar con el Estado, sino que también se condiciona dicha interacción a la presencia de un identificador. Ello puede conducir a la exclusión legal y a la violación de la privacidad. Por ejemplo, con los datos correspondientes al RUT de una persona, a través de esta información disponible públicamente, también se puede determinar su domicilio, estado civil, algunos datos electorales y verificar el nombre completo de la persona y de sus padres. Toda esta información puede ser recopilada legalmente.

En 2001, se habilitó el registro en línea de nacimientos y defunciones. Más tarde, en 2009, se lanzó una solución para realizar la autenticación digital, que se denominó "ClaveÚnica", y que se emite personalmente a través del sistema de Registro Civil. Se realiza un esfuerzo continuo para promover la ClaveÚnica como la única forma de autenticar los servicios digitales del gobierno.

El RUT es necesario para asegurar la ClaveÚnica[25]. Además, en la reciente Estrategia de Gobierno Digital de Chile, la identificación digital fue colocada entre los seis pilares principales (Gobierno Digital Chile, 2018). Los ejemplos de estas políticas de servicios gubernamentales digitales incluyen Cero Filas, lo cual evita la necesidad de pruebas de identidad fragmentadas en las instituciones públicas, y la Empresa en un día, programa que simplifica el proceso de creación de una empresa en el país. De todas formas, aproximadamente la mitad de los servicios públicos se pueden realizar en línea, entre los cuales menos del 15 por ciento requiere la ClaveÚnica (OCDE, 2019e).

Con base en eso, el presidente Sebastián Piñera declaró que *"... los servicios públicos, en sus plataformas digitales de procedimientos o servicios,*

solo deben usar la ClaveÚnica como un instrumento de identificación digital para las personas físicas, reemplazando cualquier otro sistema de autenticación de las instituciones administrativas."[26]

Chile cuenta con una ley de protección de datos personales (Ley 19.628/1999)[27]. Como principio general, estipula que los datos personales solo pueden procesarse sobre la base del consentimiento previo informado por escrito del interesado, con unas pocas excepciones (por ejemplo, en el caso de ciertos datos de acceso público o procesamiento de datos puramente interno para determinados propósitos). La ley también regula los derechos de los interesados para acceder, rectificar, eliminar o bloquear y objetar en ciertos casos.

Sin embargo, como lo señaló el Director de Derechos Digitales, el problema en Chile es allí donde la identificación digital y la protección de datos coinciden: existe *"una sensación de falta de protección como regla general"*. Dado que el RUT de una persona no constituye un dato privado, es posible obtener el número de identificación de una persona legalmente.

"Como es posible construir una base de datos con la información de alguien tan fácilmente, y considerando que también es simple transferir esta base de datos entre particulares, existe la percepción de que no es significativo almacenar esta información, que es muy fácil de conocer. Por lo tanto, casi no hay oposición a que otra persona la recoja". (Juan Carlos, Director de Investigación y Políticas Públicas en Derechos Digitales).

La integración del registro civil, la identificación civil y la identidad digital es un aspecto positivo del caso chileno. Sin embargo, debe haber estrategias claras para acceder a servicios digitales básicos para aquellos que no cuentan con ClaveÚnica. De lo contrario, se traducirá digitalmente en un aspecto de alta centralización del RUT. Asimismo, el modelo chileno ClaveÚnica puede y debe mejorarse para alcanzar estándares de privacidad y seguridad. Una posibilidad es hacer que el número de registro sea privado e implementar una plataforma para la supervisión de datos personales junto con la ClaveÚnica.

2.2. Servicios financieros (inclusión financiera)

Teniendo en cuenta nuestro enfoque de investigación orientado a comprender cómo la identidad digital puede contribuir para fomentar el desarrollo sostenible de América Latina, el análisis sectorial de casos de uso de servicios financieros se centra en la agenda de **inclusión financiera**.[28]

La inclusión financiera es más que tener una cuenta bancaria. En última instancia, implica tener acceso a productos y servicios financieros útiles y asequibles que satisfagan las necesidades de las personas y las empresas (transacciones, pagos, ahorros, crédito y seguros), lo cuales deben ser prestados de manera responsable y sustentable.[29]

Los servicios financieros digitales se han ampliado y juegan un papel destacado como herramienta para la inclusión financiera, principalmente a través de aplicaciones de dinero móvil implementadas en países en desarrollo como una forma de saltar los procedimientos bancarios convencionales y agilizar el acceso (Appaya y Varghese, 2019). Esto es importante para la agenda de desarrollo porque facilita la vida cotidiana y ayuda a las familias y las empresas a planificar todo, desde objetivos a largo plazo hasta emergencias inesperadas. También se posiciona prominentemente como un facilitador de otros objetivos de desarrollo en los Objetivos de desarrollo sostenible 2030.[30]

El rol de la identificación digital en la inclusión financiera

Para un tercio de los adultos en aproximadamente 50 países con los índices de desarrollo humano más bajos, la falta de documentación es la razón principal por la cual no tienen una cuenta bancaria (Banco Mundial, 2018b). Una de las principales razones argumentadas por las instituciones financieras para condicionar el acceso a sus servicios a través de la documentación es su obligación con respecto al cumplimiento de ciertos procedimientos estandarizados internacionalmente, además de otras regulaciones dentro de sus jurisdicciones que requieren la identificación del cliente. Por ejemplo, Conozca su cliente (KYC, por sus siglas en inglés) y Diligencia debida respecto del cliente (DDC)[31] son procedimientos obligatorios y fundamentales para garantizar que la institución cumpla las normas contra el lavado de dinero (AML, por sus siglas en inglés) así como aquellas que atacan la financiación del terrorismo (FT).

La identificación digital en el sector financiero puede catalizar los esfuerzos multidimensionales de los organismos reguladores financieros y las autoridades gubernamentales para simplificar los requisitos previos de DDC y KYC. Además, una identidad digital confiable podría aumentar la capacidad

de las instituciones financieras para cumplir con las pautas contra el lavado de dinero (AML) y abordar la financiación del terrorismo (FT) (GSMA, 2016).

El sector financiero ha sido el principal impulsor de la innovación en sistemas de identificación, autenticación y autorización en todo el mundo. Esto se debe probablemente a que la falta de identificación de alguien en una transacción dada puede conducir a una pérdida financiera directa. La gestión de identificación moderna en el sector va desde las arquitecturas de identificación de tarjetas de crédito federadas, a mediados del siglo, hasta la banca abierta en la actualidad, por ejemplo.

Desde otra perspectiva, muchas partes internacionales interesadas (Mastercard, 2019a y McKinsey Global Institute, 2019) han tratado de cuantificar predicciones muy optimistas sobre los impactos económicos que un sistema de identificación digital podría tener en el desarrollo del país que lo implementara (Center for Global Development, 2017a) y sobre la inclusión financiera y los beneficios globales para los más vulnerables en el globo (Banco Mundial, 2019a). Sin embargo, organizaciones de la sociedad civil como Access Now[32] y Privacy International han advertido que todavía no existen suficientes evidencias para respaldar los beneficios prometidos.

Métodos de identificación y posibilidades de inclusión financiera

Usando el registro de una cuenta bancaria dentro del contexto brasileño como ejemplo, observamos que los datos requeridos son: (i) el número del documento de identidad y su naturaleza; la entidad emisora y fecha de emisión del mismo; los nombres de la persona y de su madre; la fecha de nacimiento; la ciudadanía; la nacionalidad; el número de registro de pago de impuestos e información sobre si la persona está “expuesta políticamente”. Muchas entidades están realizando una transición hacia la verificación de la identidad legal a través de un Conozca su cliente electrónico. Varias compañías de tecnología financiera están utilizando una versión móvil de su sistema de prueba de identidad de forma exclusive.

La identificación del cliente se realiza cada vez más mediante la verificación de las identidades legales (por ejemplo, el documento de identidad civil, el pasaporte, la licencia de conducir) que son cargadas en una plataforma digital capaz de verificar, en bases de datos oficiales del gobierno, su validez a través de interfaces programables de aplicación (API, por su sigla en inglés). Las compañías de tecnología financiera también confían en los algoritmos de documentoscopia para prevenir el fraude. En el caso de la DDC, el procedimiento es similar: las técnicas automatizadas pueden determinar rápidamente la capacidad de alguien para cumplir con ciertas reglas.

Asimismo, a partir de M-Pesa[33] en Kenia (ahora utilizado en varios países africanos), el dinero móvil ha comenzado a ser atractivo a los ojos de los nuevos clientes, incluida la población no bancarizada (Ramada-Sarasola, 2012). A este respecto, vale la pena señalar que, en algunos contextos, como en Perú, los usuarios mantienen los números de teléfonos móviles se durante toda la vida. En este caso, el procedimiento KYC también se cimienta en la verificación de la identidad a través de un identificador único emitido por el Estado, pero es mucho más simple configurar una cuenta para servicios financieros básicos como ahorrar dinero y hacer pagos y transferencias.

Po último, se está explorando una gama de tecnologías emergentes para el registro y la autenticación. Dichas tecnologías se inscriben en el centro de la agenda de tendencias de la autenticación sin contraseña, dado que combinan la autenticación multifactorial y la biometría (Foro Económico Mundial, 2020).[34] Gracias a formas alternativas[35] de establecer la singularidad de una persona, la innovación en el sector financiero puede facilitar las transferencias de efectivo, las remesas y los pagos digitales, al tiempo que garantiza el monitoreo financiero, contribuyendo así a la inclusión financiera de los no bancarizados. A su vez, en el sector financiero, las tecnologías de contabilidad distribuida alcanzan un mayor nivel de desarrollo que en cualquier otro sector.

Contextualizando la inclusión financiera en América Latina

Varios países latinoamericanos están implementando estrategias nacionales para la inclusión financiera (Villarreal, 2017). **Colombia, Perú y Uruguay se encuentran entre los países con mejor acceso financiero a nivel mundial.**

13 países de la región han preparado políticas y acciones integradas relacionadas con la distribución, la regulación y la educación en servicios financieros.

Además, algunos países (por ejemplo, Brasil, Chile, México) lanzaron sus estrategias de inclusión financiera hace más de una década (Banco Central do Brasil, 2009).

La región es considerada muy importante para el desarrollo de la industria de tecnología financiera (*fintech*, como se la conoce en inglés) y un mercado importante debido a la demanda de la población no bancarizada. Los bancos digitales se están volviendo cada vez más populares. En América Latina, existe un debate en evolución acerca de los marcos regulatorios, la resistencia de los bancos tradicionales y los problemas de ciberseguridad (Clavijo, S., et al. 2019). La falta de pruebas de identidad continúa siendo una barrera determinante para alcanzar una mayor efectividad en tales políticas. Sin embargo, se ha prestado poca atención pragmática a este tema (GAFI, 2019).[36]

Los riesgos de la identidad digital en el sector

La identificación digital por sí sola no es suficiente para remediar la exclusión financiera.

- Debido al perfil del sector financiero, basado en el riesgo, los procesos de KYC pueden requerir datos biográficos, biométricos e históricos adicionales a los clientes.[37]
- Más allá de la identificación de clientes y beneficiarios, la DDC exige obtener más información en situaciones de mayor riesgo para determinar la naturaleza de las actividades financieras (FAFT, 2014).
- La identificación combinada a los datos financieros presentan grandes riesgos para los usuarios en caso de incumplimientos (por ejemplo, ser excluidos socioeconómicamente de programas específicos o que se les denieguen créditos) y para la integridad del sistema financiero (por ejemplo, un aumento de la apropiación indebida de fondos públicos).
- Compartir datos de identificación entre instituciones financieras sin el consentimiento claro, informado y expreso de los usuarios también puede ser un motor de exclusión y discriminación, perpetuando así la pobreza en lugar de reducirla.[38]
- Cobrar al usuario tarifas por los servicios de verificación de identidad puede dar lugar a la exclusión socioeconómica.

- El proceso de verificación debe ser transparente y lo más económico posible.
- Para los servicios financieros básicos, debe haber procesos KYC simplificados física o digitalmente, así como deben resguardar la privacidad por diseño y por defecto.

Uso apropiado de la identificación digital en el sector

Como se mencionó, KYC constituye un procedimiento obligatorio, al igual que la verificación de identidad del usuario es un elemento clave para abrir cuentas bancarias o para la identificación de clientes y beneficiarios en determinada una transacción financiera. Por ello, es esperable que las entidades financieras soliciten recibos de pago para evaluar la capacidad de alguien para cancelar sus deudas contraídas por préstamos, por ejemplo. Sin embargo, no es razonable exigir y utilizar información financiera para determinar la singularidad.

A la vez, es fundamental cómo se establece el consentimiento del usuario para la recopilación y el intercambio de sus datos personales en la práctica. Para un uso apropiado de la identificación digital en el sector financiero, el acceso no autorizado a los datos de identidad de terceros debe ser abordado y comunicado públicamente.

Conclusiones fundamentales para un uso adecuado de la identificación digital en el sector

- Los requisitos básicos para reconocer al cliente idealmente deben ser gratuitos para garantizar la inclusión financiera de la población a la que se destinan y deben ser fáciles de cumplir. Es importante separar claramente los datos básicos utilizados para identificar a alguien en base a la información complementaria que es requerida para acceder a servicios específicos y la diligencia debida respecto del cliente.
- En tanto sector líder en identificación desde una perspectiva tecnológica, las compañías de tecnología financiera y los grandes bancos deberían apoyar y ser impulsores fundamentales de las tecnologías que garanticen la privacidad. Vale considerar a este respecto que la inexistencia de mecanismos de reparación y de reclamo para acceder al historial de los datos de uno mismo constituye un indicador importante de malas prácticas, si se tiene en cuenta el desarrollo tecnológico alcanzado por el sector.
- Los reguladores financieros deben trabajar en estrecha colaboración con las autoridades de identificación y protección de datos para garantizar la interoperabilidad con el sistema nacional de identificación.

Estudio de caso: **Perú y la inclusión financiera**

Perú es un caso de identidad muy particular. En 1995, el Gobierno peruano inició una extensa campaña de identificación mediante el establecimiento, constitucionalmente, del Registro Nacional de Identificación y Estado Civil (RENIEC). Como autoridad de identificación independiente, el RENIEC ha supervisado la emisión del Documento Nacional de Identidad (DNI).

El RENIEC fue creado inmediatamente después de un período de guerra civil, autoritarismo y persecución que dejó a millones de peruanos sin ninguna prueba de identidad legal. El estado autónomo de RENIEC está garantizado por los ingresos provenientes de la prestación de servicios de verificación de identidad y de autenticación a entidades privadas. Esto representó aproximadamente un tercio de los ingresos de RENIEC en 2015 y es probable que aumente, ya que casi toda la población tiene un DNI, pero no necesariamente un registro civil.

Desde 2015, Perú ha tenido una Estrategia nacional para la inclusión financiera que identifica la falta de identidad como una barrera determinante para el acceso (Comisión Multisectorial de Inclusión Financiera, 2015). Pagos Digitales Peruanos, un consorcio de bancos y empresas financieras, lanzó un sistema de pago móvil llamado BIM, que a menudo se ejemplifica como un caso de inclusión financiera basada en la identidad digital (Caruso, 2016)[39]. Es una réplica de los sistemas de dinero móvil oriundos de África.

BIM, una billetera digital, es una iniciativa sin fines de lucro que fue lanzada en 2011 y dirigida principalmente a las personas no bancarizadas, pero solo a aquellas en posesión de un teléfono móvil. Desafortunadamente, esto excluye a la mayoría de la población no bancarizada y que tampoco tiene acceso a un número de teléfono móvil (Center for Financial Inclusion, 2019). Aproximadamente 26 millones de peruanos no tienen acceso a servicios financieros, es decir, alrededor del 80 por ciento de la población. A pesar de ello, tanto los entrevistados del RENIEC como de las organizaciones sociales civiles están de acuerdo acerca del fracaso de la billetera móvil BIM, en lo que respecta a reunir una masa crítica de usuarios hasta ahora.

No solo se requiere un DNI para abrir una cuenta. En realidad, *"para tener un número de móvil, es necesario registrar el número de DNI".* (Miguel Arce, Gerente de ventas de Pagos Digitales Peruanos).

El KYC de la plataforma está garantizado por el código de identificación único proporcionado por el RENIEC y la verificación cruzada en una base de datos fotográfica como parte de su modelo económico[40]. La BIM se conecta con el RENIEC y obtiene los datos complementarios asociados con el DNI proporcionado por el cliente al registrarse en la aplicación. Si los datos no

coinciden, la cuenta se bloquea al día siguiente. La verificación cruzada es la misma para personas menores de edad o fallecidas. Según un ejecutivo a cargo de la BIM, los únicos datos que RENIEC proporciona en este caso son el nombre completo de la persona y el comprobante de edad legal. Una vez que se ha instalado la BIM, el usuario puede elegir qué proveedor de servicios financieros quiere usar.

Sin embargo, como argumentan los defensores de los derechos digitales, el perfil centralizado y poderoso del RENIEC plantea serios riesgos de privacidad. A diferencia del RENIEC, la Autoridad Nacional de Protección de Datos Personales[41] en Perú no es independiente. Además, no existe una compatibilidad clara entre la identificación digital y las normas de protección de datos. Considerando todos los países de América Latina, en Perú es particularmente fácil acceder a las fotos de identidad de los ciudadanos.

Con respecto al RENIEC, se ha observado que ***"desde la perspectiva de la sociedad civil,***[42] ***no me gusta esa autonomía. Una autonomía sin control, casi un poder absoluto"***. (Miguel Morachimo, director ejecutivo de Hiperderechos).

En lo que respecta a la legislación de identidad digital, no hubo una revisión o una consultoría para concebir normas, reglamentos, programas, aplicaciones, ya sea a través del Congreso, la Autoridad de Protección de Datos, el Ministerio de Justicia o la sociedad civil.

En términos de inclusión financiera, aunque todavía una parte importante de la población continúa no bancarizada, la BIM no tuvo un impacto significativo. Sin embargo, la integración entre la BIM y el RENIEC es justa desde la perspectiva de la usabilidad individual, la conveniencia de los proveedores de servicios financieros y los ingresos para la institución pública. Por otra parte, desde el punto de vista del manejo de datos, esta integración es preocupante debido al desequilibrio de poder de la autoridad de identificación sobre la protección de datos. Permitir la supervisión multisectorial sería una actitud muy proactiva por parte del RENIEC para fortalecer el sistema de identificación digital.

2.3. Asistencia sanitaria

El acceso a la atención sanitaria fue establecido como un derecho humano en virtud de la Declaración Universal de Derechos Humanos de 1948, como parte del derecho a un nivel de vida adecuado (art. 25). El derecho a la salud fue reconocido nuevamente como un derecho humano en el Pacto Internacional de Derechos Económicos, Sociales y Culturales de 1966. Además, el ODS 3.9 establece el objetivo de lograr una cobertura sanitaria universal *"que incluya protección contra riesgos financieros, acceso a servicios de asistencia sanitaria esenciales de calidad y acceso a medicamentos y vacunas esenciales seguros, efectivos, de calidad y asequibles para todos"*.

La identificación de individuos puede ser una herramienta para lograr dichos objetivos o, por el contrario, puede discriminar de forma errónea, impidiendo el acceso a la atención sanitaria por parte de aquellos que no están identificados. Las mencionadas potencialidades, tanto buenas como malas, se amplían en un sistema de identificación digital.

El rol de la identificación digital en la asistencia sanitaria

La identificación en el sector de la salud puede ser valiosa para la seguridad del paciente (OMS, 2007), la eficiencia en la prestación de servicios sanitarios y la gestión de la salud pública (Banco Mundial, 2018c). Además, un motor de identificación de pacientes puede ser importante para adicionar registros, generar estadísticas y organizar datos con el fin de mejorar la planificación de las políticas de salud.

Desde la perspectiva de los proveedores de servicios, una vez que se conoce la identidad del paciente, es posible acceder al historial médico y de tratamientos, lo cual garantiza que se le brinde una atención adecuada y consistente. Desde el punto de vista del paciente, la documentación es importante para probar la inscripción en programas de seguro u otras redes de seguridad que cubren los gastos médicos. Con respecto al constructo de "seguridad del paciente", la identificación del paciente es uno de los elementos más relevantes presentados por las organizaciones internacionales de salud.[43]

Métodos de identificación y posibilidades en asistencia sanitaria

La emergencia de la identificación digital en el sector de la salud está vinculada a una proliferación de políticas de tecnología de la información sanitaria para implementar servicios de salud electrónicos, incluidos registros médicos electrónicos, registros de salud electrónicos, registros de salud

personales y recetas electrónicas, junto con iniciativas en expansión sobre la salud móvil (OMS y UIT, 2012).[44]

Los métodos actuales para la identificación del paciente generalmente implican el uso de un número de registro médico emitido y resguardado por el proveedor del tratamiento, que no siempre cuenta con un sistema compatible o interconectado. Por lo tanto, los pacientes pueden estar vinculados a varios números de registros médicos, cada uno emitido por la clínica u hospital que les brindó atención. El informe de ONUSIDA (ONUSIDA, 2014) apunta al hecho de que, dentro de un contexto más amplio, es prácticamente imposible, en función del número, determinar qué pacientes son iguales en todas las organizaciones o ubicaciones. Esta constatación desarmaría los beneficios descriptos anteriormente. A su vez, el método probabilístico de comparación de registros médicos puede ser otra forma de identificar pacientes (ONUSIDA).[45]

Para eliminar los múltiples mecanismos de registro de pacientes paralelos y desconectados, a menudo se considera la implementación de un identificador nacional digital de salud (NHDID, por sus siglas en inglés). Este consiste en un número único vinculado a la información de identificación provista por la autoridad de confianza. Cuando se emite un NHDID para un paciente, generalmente va acompañado de una tarjeta de identificación. El paciente puede usar la tarjeta para comunicar su NHDID a otras partes que necesiten usar la información del NHDID. Este proceso suele ir acompañado de una solicitud de documentación adicional y/o la recopilación de datos biométricos.

Contextualizando la asistencia sanitaria en América Latina

El modelo para la identificación y prestación de servicios de salud de manera centralizada en América Latina se construyó gradualmente en la década de 1990. Anteriormente, los sistemas de atención sanitaria habían estado vinculados a la seguridad social y todos los que no estaban vinculados a dicho sistema se dirigían a un servicio de “propósito general”. Dichos servicios se unificaron más tarde en la mayoría de los países latinoamericanos.

En el modelo anterior de prestación de servicios, no se almacenó información sobre el paciente, excepto en lo que atiene a los procedimientos realizados. Por lo tanto, la atención se centró en documentar y garantizar la facturación correcta de los servicios, principalmente para evitar el fraude por parte del proveedor descentralizado. En el modelo centralizado, en cambio, los pacientes y sus registros médicos son monitoreados para asegurar la continuidad del tratamiento. El cambio de paradigma requirió un sistema de identificación más sofisticado, que permitiera centrarse en la seguridad del paciente.

Los progresos realizados por los países latinoamericanos en el campo de los servicios electrónicos de salud *(e-health)* son múltiples. Los datos de los Estados Miembros de la OMS de la región, disponibles a través de su oficina regional, la Organización Panamericana de la Salud (OPS, 2016), muestran una visión general mixta de las prácticas relacionadas con la salud electrónica.

77.8 %
TENER UNA POLÍTICA O ESTRATEGIA NACIONAL PARA LA COBERTURA UNIVERSAL DE SALUD.

84.2%
INFORMARON TENER UNA POLÍTICA O ESTRATEGIA NACIONAL AL MENOS PARA UN SISTEMA DE INFORMACIÓN DE SALUD.

Por lo tanto, a pesar de su heterogeneidad, las políticas y tecnologías de salud electrónica han penetrado en los estados latinoamericanos. Un NHDID probablemente será la llave a través de la cual los ciudadanos accederán a las nuevas formas de brindar servicios de salud.

Riesgos de la identificación digital en el sector

Una identidad digital nacional para la atención sanitaria por sí sola no protegerá la privacidad y confidencialidad de la información del paciente, ni garantizará su identificación precisa.[46]

La digitalización de los registros y servicios de atención sanitaria y la aparición de nuevas tecnologías plantean preocupaciones acerca de la privacidad (protección de los datos de salud, incluida la biometría) y sobre la relación de confianza entre pacientes y proveedores a otro nivel. Por lo tanto, la integridad de los datos de salud comienza a convertirse en un problema de ciberseguridad.

- El acceso no autorizado o el mal uso de la información personal puede reducir la confianza, socavar los derechos de privacidad y, en algunos casos, poner a los grupos vulnerables en grave riesgo de daño (Banco Mundial, 2018c).[47]
- Los sistemas de salud electrónica pueden convertirse en la mayor colección de información sobre la ciudadanía de un país, convirtiéndose en un registro civil de facto. Los registros médicos pueden revelar el origen étnico o la afiliación religiosa de manera sistemática, lo que no es apropiado para un sistema de identificación nacional de propósito general.
- Compartir o vender datos personales para una variedad de propósitos

dudosos, incluida la discriminación antiética por parte de los proveedores de seguros de salud.

» Si esto no se planifica con cuidado, existen grupos de personas que pueden quedar excluidos del programa de asistencia sanitaria o de identificación en sí. Algunas personas, como los inmigrantes, las trabajadoras sexuales, los individuos pertenecientes a la comunidad LGBTQ+, los usuarios de drogas o las personas con enfermedades estigmatizadas, pueden ser reacias a identificarse; una decisión debe respetarse plenamente.

» Solicitar documentación adicional puede conducir a la exclusión. Dependiendo del país y de las diferentes condiciones locales de las comunidades rurales y autóctonas, puede haber una documentación formal mínima para ayudar a verificar la identidad de una persona. Además, en situaciones específicas se puede prescindir que parte de la población deba presentar documentos, como en el caso de desastres naturales, guerra u otras calamidades.

Usos apropiados de la identificación digital en el sector

Como se mencionó anteriormente, el acceso a los servicios de salud es un derecho humano reconocido internacionalmente. En este sentido, es necesario analizar en detalle si –y en qué ocasiones– la identificación del paciente es un paso hacia la realización de esos derechos o, por el contrario, si excluye aún más a grupos vulnerables del acceso a la salud. En última instancia, todos tienen derecho a recibir asistencia sanitaria urgente para salvar sus vidas o evitar daños irreparables a su salud, y esto debe proporcionarse independientemente de cualquier documento de identidad que se presente.[49]

» Los grupos en riesgo y aquellos con estigmas sociales son extremadamente dependientes del contexto y la cultura de cada región y, por esta razón, se deben diseñar políticas específicas para incluirlos. Para eso, es esencial comprometerse con los miembros de las poblaciones clave para que se puedan identificar y abordar las posibles preocupaciones.

» Es posible que se deban desarrollar métodos de identificación alternativos para garantizar la integridad del proceso de solicitud presentados ante sistemas nacionales que requieran identificación, como los programas de vacunación. Para ello, el propósito de identificación se puede satisfacer reuniéndose con un anciano de la aldea o tribu, un trabajador de salud de la población o comunidad, un líder religioso u otra fuente confiable.

» Además, la responsabilidad acerca de la privacidad debe cuidarse haciendo cumplir las leyes y regulaciones de privacidad que se centran en los derechos individuales, al tiempo que garantizan un acceso adecuado a los datos para satisfacer las necesidades de información de la salud pública (Banco Mundial, 2018c).[48]

Conclusiones fundamentales para un uso apropiado de la identificación digital en el sector

- Al establecerse una identificación nacional única para los servicios sanitarios, esta puede ser vinculada a una identificación fundacional. Sin embargo, este enlace no debe permitir el acceso a datos médicos confidenciales por parte de terceros. En caso de ser necesario acceder a ellos para satisfacer necesidades de información de interés para la salud pública, los datos deben ser anónimos, de forma que se evite que el paciente pueda ser reidentificado.
- El acceso a servicios médicos urgentes, no solo emergencias, nunca debe estar condicionado a la identificación. Este principio se aplica, consecuentemente, a la identificación digital.
- Es posible que resulte necesario desarrollar métodos de identificación alternativos para garantizar la integridad del proceso de solicitud de sistemas nacionales que requieren identificación (como los programas de vacunación). La identificación digital podría constituir en elemento que facilite dicho fin.

Estudio de caso: **Certificado electrónico de nacimiento y Cartilla electrónica de vacunación de México**

Actualmente, existen varios documentos oficiales para identificar ciudadanos en México. Entre los principales se encuentra la Clave Única de Registro de Población (CURP). Este registro es una combinación de letras y números asignados por el Consejo Nacional de Población a cada persona nacida en México o a extranjeros con permiso de residencia; sin embargo, aún no se ha traducido en una identificación nacional universal. Los certificados de nacimiento y el CURP sirven como identificaciones fundacionales que permiten a las personas obtener identificaciones funcionales, que se utilizan para votar y tener acceso a programas de seguridad social y servicios públicos de salud. Aunque la Coordinación de Estrategia Digital Nacional (CEDN), lanzada a fines de 2013, implementó recientemente importantes acciones de salud electrónica, el país no cuenta con una política o estrategia nacional integral en el campo.

En México, la identificación es un requisito para recibir atención sanitaria. Este hecho debe ser revisado, ya que potencialmente excluye a las personas que no tienen medios de identificación o que no quieren identificarse para acceder a los servicios de salud, ya sean públicos o privados. De todas formas, de acuerdo con los expertos entrevistados dentro del alcance del presente proyecto, las personas que no tienen medios de identificación pueden recibir tratamiento de emergencia, como fue predeterminado por la legislación.

Cada sistema de salud aún recolecta, almacena y procesa los datos de sus beneficiarios. Sin embargo, el gobierno implementó, como parte de la Estrategia Digital Nacional, el Certificado electrónico de nacimiento (CEN) y la Cartilla electrónica de vacunación (CEV), dos nuevas formas de documentación electrónica utilizadas en el sistema de salud.

El CEN es una versión electrónica del certificado de nacimiento[50] en un formato nacional único establecido por el Ministerio de Salud. Este documento es emitido a los recién nacidos por la institución de salud afiliada de su lugar de nacimiento. Puede tener una versión impresa y será el primer paso para una identidad digital única en el cuidado de la salud.[51]

La versión electrónica del certificado de nacimiento no es un requisito para obtener una copia impresa del certificado de nacimiento o del CURP, y la versión en papel todavía está en uso. Si bien la Ley General de Salud establece que es obligatoria desde 2015, aún no todas las instituciones la han implementado (México Digital, 2014). Según el gobierno mexicano, el sistema ya está en vigor en 21 estados y, para 2017, se habían emitido

más de 200.000 certificados electrónicos (México Digital, 2018). En algunos casos, el registro clínico electrónico ya se ha implementado (Comisión Nacional de Arbitraje Médico, 2018).

La CEV, establecida en 2014, tiene la misma funcionalidad de la Tarjeta Nacional de Salud que está actualmente en uso, pero aún queda trabajo por hacer para lograr la plena operatividad. Solo unas pocas ciudades la han implementado, y solo es obligatoria en los estados que ya han implementado el sistema. El proyecto también comprende una aplicación móvil, un panel de control, un administrador web y una tarjeta de vacunación con un chip. Los datos del certificado de nacimiento y el CURP se ingresan en el chip, y los datos de vacunación de cada persona se incluyen y almacenan electrónicamente y se respaldan con datos escritos a mano en la misma tarjeta.

La combinación de CEV, CEN y los registros clínicos electrónicos puede representar una ganancia para el gobierno porque no tendría que repetir los estudios clínicos varias veces, dado que ya fueron almacenados electrónicamente. Sin embargo, la base de datos mexicana agrega datos sensibles y biométricos del paciente y sus familias, aumentando el daño en caso de mal uso o fuga. Esto es preocupante porque hay interesados en tener acceso a dicho base de datos, como las compañías de seguros.[52]

La ley mexicana de protección de datos determina que debe existir un interés legítimo para recopilar datos. Sin embargo, no proporciona ninguna definición de "interés legítimo". Por lo tanto, en la práctica, la ley actual permite la recopilación de datos que algunos consideran excesivos.

"El cumplimiento de la legislación sobre protección de datos personales en poder de las compañías de servicios establecidas en México es mínimo, como resultado de la falta de familiaridad con la ley" (Enríquez, O. 2018).

A su vez, la ley no define el estándar correcto de almacenamiento de datos o las consecuencias por incumplimiento.[53] Es correcto afirmar que hoy México tiene una legislación consistente con respecto a la protección de datos personales, pero aún es poco conocida y se aplica de manera deficiente.

Evelyn Tellez, investigadora del INFOTEC (el centro público de investigación del Gobierno de México especializado en el desarrollo de tecnologías de información y comunicación), también reforzó ciertas cuestiones delicadas en relación con el almacenamiento y el procesamiento de datos personales por parte del gobierno. Por ejemplo, los datos de más de 80 millones de mexicanos fueron clonados recientemente.

Asimismo, el registro clínico es el segundo registro más importante en México (el primero es el instituto electoral nacional, INE). Una explicación de este fenómeno es que, para obtener una cita médica, los usuarios deben

presentar un comprobante de domicilio, credencial de votante y certificado de nacimiento a fin de satisfacer los requisitos de datos básicos. Además, se les solicita que proporcionen todas las huellas digitales del usuario y la familia del usuario (padres y/o hijos).

Existen vacíos en la legislación que impactan directamente en la protección de los datos de los ciudadanos mexicanos (OCDE, 2018), lo que se hace evidente en los análisis de casos de filtraciones masivas de datos, como señaló Tellez. Por lo tanto, existe una desconfianza real sobre la seguridad de los datos en poder del Estado mexicano[54], al tiempo que el robo de identidad ha sido un problema real para los mexicanos en los últimos años.[55] De hecho, según un proveedor de soluciones de TI y redes de alto nivel en México, aunque las credenciales como el INE son difíciles de falsificar, el sistema de identificación mexicano aún es deficiente en materia de seguridad de datos y protección contra la falsificación de identidades.

Por último, en la medida en que se solicita la tarjeta electrónica de vacunación y los registros médicos electrónicos para acceder a los servicios de salud, esta práctica se convierte en un punto que merece atención. Si los canales de acceso no están disponibles para todos, sin duda estaríamos frente a una mala práctica en el sistema de identificación.

2.4. Protección social

Más allá de los diferentes enfoques y definiciones, definimos la protección social como el sistema de programas, actores, políticas y acciones orientados a salvaguardar las poblaciones vulnerables, erradicar la pobreza y promover el bienestar y el trabajo digno (UNRISD, 2010). Entre los programas de protección social (PPS), existen sistemas contributivos y no contributivos (por ejemplo, transferencias monetarias condicionadas e incondicionales), principalmente abordados aquí.

La adopción o vinculación con las tecnologías de identificación digital es una tendencia emergente y en rápido crecimiento en los programas de protección social. Considerando el enfoque integral de los objetivos de desarrollo sostenible (ODS) de la ONU, está en foco la necesidad de una mejor coordinación entre los programas de protección social. En este sentido, una forma eficiente de identificar a las personas es esencial para garantizar la interoperabilidad, vincular datos entre programas, promover la participación social y mejorar la prestación de servicios.

El rol de la identidad digital en la protección social

Sin una prueba legal de identidad, una persona no puede ser incluida en casi ningún programa de ayuda. Este es un motor que estimula la demanda de documentación de identidad entre los pobres. Los estudios muestran que la inclusión social impulsó la demanda de registro civil e identificación en América Latina (Hunter, W. & Bril, R, 2016; Hunter, 2019)[56]. Además, los gobiernos han creado políticas para simplificar los servicios de identificación (Muzzi, 2010) y hacerlos más accesibles para la población vulnerable indocumentada.[57]

La adopción o vinculación con las tecnologías de identificación digital es una tendencia emergente y en rápido crecimiento en los programas de protección social.

En este sentido, una forma eficiente de identificar a las personas es esencial para garantizar la interoperabilidad, vincular datos entre programas, promover la participación social y mejorar la prestación de servicios.

Métodos de identificación y posibilidades de la protección social

Los sistemas de protección social exigen más información sobre la población que los sistemas de identificación ordinarios. Es necesario caracterizar a las personas en múltiples aspectos de sus condiciones (por ejemplo, la edad, los ingresos, el número de dependientes del jefe de hogar). Por lo

tanto, los PPS adoptan una amplia gama de métodos de identificación que varían según las capacidades del gobierno, la infraestructura de TIC del país, las características del programa y la población a la que se destinan. En la mayoría de los países, la inscripción de beneficiarios se realiza mediante identificaciones básicas tradicionales en papel.

Cuando el país tiene un sistema de identificación fundacional, se utiliza como fuente primaria para identificar a los beneficiarios de los sistemas de protección social. Sin embargo, cuando la cobertura de la identificación fundacional no es suficiente o no existe, es necesario establecer una forma alternativa de identificar a la población a la que se destinan los programas. Por lo tanto, muchos países llevan a cabo un proceso de registro específico para la población destinataria de PPS y emiten una tarjeta para identificar a los beneficiarios.

Un sistema de información de gestión típico (MIS, por su sigla en inglés)[58], como la columna vertebral para gestionar los PPS, tiene al menos tres pilares funcionales:

Inscripción e identificación	Focalización y definición de la calificación	Facilitar transacciones y prestaciones de servicio.

La interoperabilidad de los registros se combina con el uso de un sistema de identificador único para contribuir a una visión global de los beneficiarios, vinculados entre varios programas. Por ejemplo, las naciones en desarrollo han adoptado la identificación biométrica debido a su beneficio potencial para garantizar una identificación precisa

Contextualizando la protección social en América Latina

Los PPS tradicionales en América Latina solían estar vinculados a las políticas laborales. Como la principal innovación para la reducción de la pobreza, durante más de dos décadas, el uso de transferencias de efectivo de carácter no contributivas fue el foco de la investigación y la formulación de políticas.[59] Estos PPS tenían varios puntos en común, pero diferían en sus criterios de calificación de situaciones consideradas de pobreza.

En 2014:

20

PAÍSES DE LA REGIÓN TENÍAN UNA POLÍTICA DE TRANSFERENCIAS MONETARIAS CONDICIONADAS

25%

DE LA POBLACIÓN DE AMÉRICA LATINA Y EL CARIBE ESTABAN INSCRITOS EN UNA POLÍTICA DE TRANSFERENCIA MONETARIA (ECLAC, 2015).[60]

Altos niveles de desigualdad caracterizan las sociedades latinoamericanas (Ibarra y Byanyima, 2016). Una parte importante de la población no solo es pobre, sino también social, cultural y legalmente excluida. Con frecuencia, los más vulnerables y, por lo tanto, quienes necesitan asistencia, son, además, invisibles para El estado. Se los desconoce porque no tienen ninguna documentación personal formal y, en consecuencia, no son alcanzados por los programas de protección social.

Riesgos de la identificación digital en el sector

Asegurar la inclusión en la protección social es tan primordial como, a su vez, un tema complejo. Implica la identificación de individuos que son vulnerables y socialmente excluidos por defecto, a menudo no solo económicamente, sino también en otros aspectos de sus vidas.

- Sin condiciones materiales mínimas y acceso a la información, una persona no puede navegar por los procedimientos burocráticos para tener un documento de identidad, y mucho menos una identidad digital.
- El aspecto de vulnerabilidad implica que los beneficiarios potenciales pueden residir en viviendas precarias, poco resistentes al clima o no tener ninguna vivienda, por lo que a menudo no pueden guardar sus documentos. Se ha alentado ampliamente el uso de la biometría para enfrentar este desafío.
- Independientemente de la creciente adopción de la identificación biométrica (Carmona, 2019), los estudios realizados en el contexto indio[61] muestran que el riesgo de excluir a los grupos vulnerables es considerable (Drèze et al., 2017; Muralidharan, 2020).[62]
- La identificación en PPS recopila una amplia gama de datos personales. Esto significa que muchos datos confidenciales están expuestos a los riesgos comunes a cualquier esquema de identificación digital, como las fugas, pero que específicamente en el contexto de la protección social puede significar estigmatización y vergüenza.
- La brecha digital (incluyendo la alfabetización digital, la tecnología y el acceso a Internet) a menudo es intrínseca a la situación de vulnerabilidad de quienes dependen de la asistencia social, lo que conlleva un alto riesgo de exclusión.

- Esta difícil situación se ha enfrentado al crear programas de protección social que abordan simultáneamente ambos lados de la ecuación: proporcionar ingresos mínimos y acceso a servicios básicos y simplificar los procedimientos para obtener documentación personal básica.
- En este sentido, la protección de datos debe ser percibida como un elemento de protección social (Sepúlveda, 2019).
- Los identificadores de protección social no deberían estar vinculados a bases de datos biométricos.

» Cualquier falla del sistema puede acarrear graves consecuencias. Este es el caso, por ejemplo, si una persona no cuenta con la identificación digital exigida por las agencias gubernamentales o si su identificación digital está "incompleta" porque sus huellas digitales no se cargan en la base de datos nacional debido a la mala conectividad a Internet (Access Now, 2018).

Usos apropiados de la identificación digital en el sector

En el contexto de la protección social, la identificación de los beneficiarios es un componente esencial e integrado del esquema. Hacer que los individuos califiquen para recibir la protección social es una forma de incluirlos. Sin embargo, existen preocupaciones sobre los medios utilizados para llevar a cabo la identificación.

En América Latina, la adopción de la identificación biométrica obligatoria aún no está muy extendida. Sin embargo, las críticas sobre el fraude han presionado la adopción de la biometría en los programas de protección social. Esta debería considerarse cuidadosamente a través de una evaluación pública de riesgos, y los datos biométricos no deben ser obligatorios para la autenticación individual con el fin de obtener acceso a bienes y servicios.

Conclusiones fundamentales para un uso adecuado de la identificación digital en el sector

» Los gobiernos deberían crear un registro único para ofrecer protección social, adoptando una perspectiva inclusiva que permita mejorar su capacidad de llegar a la población vulnerable. Es crucial simplificar y hacer que los servicios de identificación sean más accesibles para la población indocumentada equilibrando los requisitos y las condiciones de los beneficiarios.

» La integración de los sistemas de información gerencial y los sistemas de identificación digital deben tener en cuenta el riesgo de excluir a la población más vulnerable, al tiempo que no deben perder de vista la efectividad de las políticas.

» La adopción de la tecnología biométrica con el objeto de proveer protección social debe ser precedida de una evaluación integral del sistema nacional de identificación, en la cual los marcos institucionales y legales sean evaluados a través de los lentes de promoción de la inclusión y los derechos, asegurando que los grupos de personas carenciadas y más vulnerables no resulten excluidos.

Estudio de caso: **Registro único para programas sociales de Brasil**

El registro único para programas sociales (CadÚnico) es un registro administrativo desarrollado en 2001 para apoyar los programas sociales integrados en Brasil, que respaldan varios programas de protección social, como el programa de transferencia condicional de efectivo Bolsa Familia (PBF) (Lindert et al., 2007; Hellmann, 2015).

El CadÚnico es la herramienta de identificación de beneficiarios, la cual diferencia las necesidades de las poblaciones a las que se destina el beneficio de acuerdo con las características de cada familia. El proceso de registro es gratuito y descentralizado dentro de los tres niveles federativos de gobierno. Se utiliza para la inscripción y para recopilar información sobre las familias más vulnerables, incluyendo las condiciones de trabajo, la composición familiar y la vivienda, entre otros. Más de 13 millones de hogares en todas las regiones del país, casi una cuarta parte de la población brasileña, han sido incluidos en el programa.

El Registro único también desempeñó un papel importante en la creación de demanda de registro de nacimientos e identificación civil. Es decir, facilita que las poblaciones invisibles califiquen como beneficiarias de las medidas de protección social. Ser una persona indocumentada en Brasil significa ser un ciudadano de segunda clase, quizás incluso peor: una persona que no tiene ningún documento de identificación puede sentirse deshumanizada.

Por ley, el acceso a los servicios públicos esenciales es gratuito para las personas desfavorecidas, pero la complejidad del ecosistema de identidad impone restricciones a las personas. Esto es así porque la regulación de los servicios requiere la presentación de documentos, como lo destaca Raquel Chrispino, una jueza en Río de Janeiro:

"Hay reglas brasileñas que imponen rutinas administrativas, por lo que estamos hablando de ordenanzas, resoluciones, estamos hablando de actos administrativos normativos que, para regular el servicio público, terminan obligando a los ciudadanos a ingresar algunos de sus números de identificación en determinado sistema" (Chrispino, 2019).

Históricamente, los procesos de inscripción para los grupos más excluidos son diferentes de los de la población general. De hecho, las personas indocumentadas se incluyen en el registro y reciben instrucciones para emitir el registro e identificación de nacimientos (Ministerio de Desarrollo Social de Brasil, 2015).

La mayoría de los beneficiarios de PBF son mujeres y personas negras o de raza mixta. El análisis de la composición familiar de los beneficiarios del beneficio de la PBF revela que los hogares monoparentales encabezados

por mujeres representan el grupo más grande (Campello y Neri, 2014). La investigación cualitativa muestra que la inclusión de las mujeres en la Bolsa Familia crea y expande oportunidades para las libertades personales de las personas, abriendo más posibilidades para empoderar a las mujeres en general (Campello y Neri, 2014). El papel esencial de los documentos personales para el empoderamiento ciudadano y el acceso a los servicios es claro.

A pesar del reconocimiento global del programa de transferencias monetarias condicionadas y su sistema de información de gestión, la inscripción en el programa se realiza bajo la condición previa de que los beneficiarios tengan sus datos completamente expuestos en el portal de transparencia gubernamental. Aunque la regulación brasileña de protección de datos determina la necesidad de consentimiento expreso e informado[63], los datos sensibles aún se muestran bajo consentimiento forzado, ya que es una condición para acceder a la PBF.


IMPRIMIR | BAIXAR | REMOVER/ADICIONAR COLUNAS | DETALHAMENTO DE BENEFÍCIOS AO CIDADÃO

DETALHAR	UF	MUNICÍPIO	CPF	NIS	BENEFICIÁRIO	VALOR DISPONIBILIZADO (R$)
Detalhar	CE	CATARINA	***.481.018-**	1.214	ADELINO	89,00
Detalhar	CE	CATARINA	***.268.023-**	1.613	ADRIANA	346,00
Detalhar	CE	CATARINA	***.896.003-**	1.614	ADRIANA	440,00
Detalhar	CE	CATARINA	***.898.933-**	2.031	ADRIANA	137,00
Detalhar	CE	CATARINA	***.030.691-**	1.616	ADRIANA	170,00
Detalhar	CE	CATARINA	***.044.408-**	2.003	ADRIANA	89,00
Detalhar	CE	CATARINA	***.460.293-**	1.60	ADRIANA	148,00
Detalhar	CE	CATARINA	***.000.000-**	1.613	ADRIANE	188,00

Fuente: *Portal de transparencia* - Portal con la información de los beneficiarios, Gobierno Federal de Brasil <www.transparencia.gov.br>.

Un aspecto positivo es que el identificador del programa de protección social no está directamente vinculado a una base de datos biométricos. Si el gobierno tiene la intención de implementarlo, esto debería hacerse con una evaluación clara y amplia del riesgo, menciones explícitas a las salvaguardas de protección de datos y mediante consultas populares.[64]

Finalmente, un punto clave es el uso del número de contribuyente como el identificador principal en Brasil, ya que se solicita no solo al jefe de familia, sino a todos sus dependientes. El identificador del contribuyente no es una identificación civil, y las irregularidades en los deberes electorales o fiscales han llevado a la exclusión de quienes más lo necesitan. Este requisito debe ser reconsiderado para los programas de protección social, o debe haber una reestructuración general del sistema de identificación.

Sección 3

Aprendizajes

Foto: Tales Duarte

3. Aprendizajes

La identidad toca el núcleo mismo de la dignidad humana. La identificación es un asunto que se remonta mucho más atrás que las agendas de transformación digital y manejo de datos. Sin embargo, los encargados de formular políticas aún no comprenden su complejidad. Esta faceta pasa a menudo por alto y los sistemas de identificación digital se implementan enfocando principalmente en objetivos centrados en el gobierno, en lugar de aplicar un enfoque centrado en el usuario; por lo que se repite lo que sucedió en la informatización de las bases de datos del gobierno en la segunda mitad del siglo pasado.

¿Cuáles son los usos apropiados de la identificación digital?

Varias ideas clave surgieron durante la investigación asociada al presente informe. Además de los ya destacados en los casos de uso sectoriales, esta sección presenta cuatro conjuntos de recomendaciones diseñadas para los responsables políticos y otras partes interesadas que, en última instancia, enfatizan que el uso de la identificación digital solo puede ser apropiado cuando es una herramienta que facilita el acceso a los derechos y servicios por el usuario. Esta sección destaca, asimismo, que dichos objetivos no pueden lograrse cuando el sistema de identificación digital no garantiza la inclusión, el valor del usuario, la privacidad y la seguridad, porque puede significar una barrera adicional –aumentando la exclusión– o transformarse en una herramienta de discriminación negativa. Tales parámetros y sus recomendaciones consecuentes son los siguientes:

1. Inclusión: La identificación digital solo puede ser considerada apropiada cuando promueve la inclusión.

» **Se debe estar atento a de no reproducir el problema de la exclusión actual digitalmente.** En todos los estudios de caso de los distintos países, la identificación es obligatoria, ya sea legal o de facto, para el pleno disfrute de los derechos y servicios. La exclusión del acceso a los servicios básicos debido a la falta de identificación puede ser un problema analógico que no debe transponerse o potenciarse digitalmente. Los principales documentos de identificación de Chile y Perú (RUT y DNI, respectivamente) son esenciales para que las personas lleven a cabo

acciones necesarias y cotidianas. Sin embargo, asegurar la Clave Única, la clave chilena para los servicios digitales del gobierno, no es posible sin el RUT. La iniciativa peruana para la inclusión financiera (cuya principal barrera es la falta de medios de identificación) se dirige solo a los que poseen un número móvil, pero para obtener un número móvil se necesita un número de DNI. México parece seguir el mismo camino, ya que la mayoría de los procedimientos públicos y privados no pueden realizarse sin identificación oficial, y también se requiere gradualmente la identificación digital.

» **El acceso a los derechos y servicios básicos no debe depender de la identificación digital.** Como se señaló, la identificación, cualquiera que sea el formato, no puede ser una barrera para acceder a servicios y derechos básicos. Esto vale, en consecuencia, para la identificación digital. Por lo tanto, comprender y considerar la desigualdad en el acceso a la infraestructura de las TIC y el contexto de división de la alfabetización digital es esencial al implementar dicho sistema. Muchos países latinoamericanos aún luchan con la desigualdad en el acceso a la tecnología y el analfabetismo digital. Por lo tanto, cualquier agenda que establezca la identificación digital como la única ruta de acceso es excluyente desde su matriz. El acceso multicanal es imprescindible en la región.

2. Valor para el usuario : Balance entre el interés individual e institucional.

» **Se debe asegurar de que los sistemas de identificación digital impulsan los derechos de las personas, sin sustentar sus libertades y derechos civiles.** En lo que respecta a los usos sectoriales, se ve reflejada la delgada línea entre la identificación como un derecho o como un medio de intrusión, vigilancia y un factor para el mayor desequilibrio de poder entre instituciones e individuos dentro de un sistema de identificación fundacional. Por ello, el sistema de identificación debe articular claramente sus usos previstos, tanto en el plazo inmediato como en escenarios futuros. Esto también significa que es primordial un marco de implementación que aborde la minimización de datos, el propósito claro y otras barreras de protección necesarias para salvaguardar a los usuarios de posibles abusos.

» **No se debe seguir la tendencia a expensas del valor efectivo para el usuario.** La adopción de tecnología llamativa, independientemente de su idoneidad para el contexto dado, muestra un interés predominante de la institución por parecer moderna en lugar de abordar las necesidades reales de sus usuarios. Por ejemplo, algunos usos sectoriales de la

identidad digital dentro de las propuestas del gobierno digital parecen ser principalmente una marca política, ya que en realidad la mayoría de los servicios ofrecidos no pueden ser 100% digitalmente alcanzables o, lo que es peor, pueden contribuir a aumentar la brecha digital y de acceso a los servicios.

» **Cuando la innovación aporta un valor real para el usuario y la inclusión, vale la pena adaptarlas.** En ciertos contextos y sectores de uso, la identificación digital puede aportar un valor real al usuario y contribuir a la inclusión. Por ejemplo, se observó que, en los usos sectoriales de la inclusión financiera y la protección social, la identificación digital proporcionó formas alternativas de establecer la singularidad de una persona, superando las barreras dadas. En el primer caso, la tecnología contribuyó a facilitar las transferencias de efectivo, las remesas y los pagos digitales, al tiempo que garantizaba el monitoreo financiero, contribuyendo así a la inclusión financiera de los no bancarizados. En el segundo caso, facilitó la inscripción en el programa de asistencia y, fuera de los estudios de caso latinoamericanos, también se ha documentado la concesión de beneficios en las actualizaciones de la base en tiempo real. Por ejemplo, los usuarios del sistema de identificación indio (Aadhaar) declararon que la identificación biométrica aumentó su control sobre sus finanzas y aseguró pagos regulares (Gelb, A. et. Al., 2017)

3. Privacidad: Priorizar las leyes de protección de datos que salvaguardan la privacidad y los datos personales.

» **Establecer un marco regulatorio apropiado y completo.** Los cuatro países estudiados cuentan con una ley de protección de datos.[65] Sin embargo, como lo han demostrado los estudios de caso en este informe, el marco legal de protección de datos debe ser apropiado y completo. La ley de protección de datos de México carece de claridad. Por ejemplo, el concepto impreciso de interés legítimo (que autoriza la recopilación de datos personales sin el consentimiento del interesado) dificulta la evaluación de la idoneidad de la recopilación de datos y, en consecuencia, la recopilación excesiva de datos, incluso de miembros de la familia, es una práctica común en el país. En Chile, la legislación actual permite a cualquier persona acceder legalmente a una gran parte de los datos personales derivados del número de identificación chileno (RUT), el cual es considerado legalmente información pública.

» **Asegúrese de que la legislación sea ampliamente conocida y aplicada.** Los casos de México y Perú ilustran cómo la falta de discusión y

publicidad de la legislación relevante para las partes interesadas también minimiza la efectividad de los derechos legalmente reconocidos. En el caso mexicano, una de las barreras para cumplir con la legislación es la falta de conciencia y de mecanismos de rendición de cuentas; mientras que en Perú existe resistencia debido a las formas, percibidas como autoritarias, de concebir e imponer dicha legislación. En Chile, la legislación de protección de datos personales no protege adecuadamente la privacidad de los datos: al no proteger el número RUT con un estado privado, cualquier persona puede acceder legalmente a otros datos, lo que compromete significativamente la privacidad de los usuarios.

4. Seguridad: Otorgar una Mirada integral a la seguridad y la privacidad desde el diseño.

» **Garantizar mecanismos robustos para salvaguardar la privacidad e integridad de los datos del usuario.** Sin un diseño tecnológico robusto, adecuado y seguro que garantice la capacidad del sistema para proteger los datos del usuario, la identidad digital no debería ser implementada. Los estudios de caso muestran explícitamente cómo los datos del individuo están extremadamente expuestos en la actualidad. Por ejemplo, hay un registro importante de fuga de datos de identidad bajo los auspicios del gobierno mexicano. El hecho de que los datos financieros y de salud requeridos en los usos sectoriales de la identificación digital son muy sensibles y que su mal uso o filtración puede conducir a la exclusión y la discriminación no debe pasarse por alto. Por nombrar solo algunos riesgos, la exposición del estado de una enfermedad o una situación de vulnerabilidad económica puede significar que al usuario se le niegue el crédito o que se enfrente a tasas de seguro de salud más altas; en consecuencia, se perpetua la pobreza y la exclusión del servicio en lugar de reducirlo, sin mencionar cómo estos también pueden convertirse en conductores de exclusión social y discriminación.

» **La recopilación de datos confidenciales debe minimizarse.** Existen diferentes conjuntos de datos mínimos con respecto a propósitos específicos del sector. Sin embargo, la mayoría de ellos recopilan más datos para el registro que los necesarios para su propósito original. Esto compromete la seguridad porque la cantidad de datos recolectados es proporcional al riesgo de fuga de la misión y el daño potencial a la privacidad del usuario en caso de fuga de datos, uso indebido o uso compartido no autorizado. El caso de México ilustra los requisitos injustificados para que los datos se agreguen a los registros clínicos de los usuarios, como las credenciales de los votantes y las huellas digitales, tanto del usuario como de sus familiares.

Anexo I: Etapas de la investigación

En la primera etapa, realizamos una revisión sólida de la bibliografía sobre gestión de identidad desde una perspectiva cronológica, geográfica y multisectorial. Las principales fuentes de investigación fueron revistas, libros, sitios web y artículos. Entre ellos, es relevante resaltar las siguientes fuentes: Identification Revolution: Can Digital ID be Harnessed for Development? (Gelb y Metz, 2018); OECD Digital Government Reviews[66]; Access Now's assessment on National Digital Identities (2018)[67]; ITU's Roadmap for Digital Identity (2018)[68]; World Bank ID4D collection with a focus on the Practitioner's Guide and country diagnostics (2019)[69]; y el informe de McKinsey titulado Digital Identification: A key do inclusive growth (2019).[70] Realizamos, también, investigaciones bibliográficas específicas sobre usos sectoriales. Asimismo, evaluamos documentos de identificación históricos de América Latina para obtener una mejor comprensión del escenario regional.

En la segunda etapa, analizamos los casos de uso sectoriales. Nos centramos en los servicios gubernamentales digitales, la inclusión financiera, la atención sanitaria y la protección social. Esta elección se fundamentó en la precepción de que dichos sectores podrían proporcionar una visión general relevante de la identificación digital en términos de derechos fundamentales (asistencia sanitaria y protección social) y de servicios emergentes (gobierno digital e inclusión financiera). Cada uno de los casos de uso sectoriales fue acompañado por un estudio de caso.

En la tercera etapa, realizamos análisis específicos de cada país y una serie de entrevistas en cada país. Las opciones de estudio de caso se basaron en la discusión actual y los datos disponibles sobre dichos usos sectoriales en países latinoamericanos específicos. Descubrimos que sería apropiado enfocarse en México para la asistencia sanitaria dado su registro electrónico de vacunación; en Perú, para abordar la inclusión financiera, debido a que a menudo se lo considera un punto de referencia para las billeteras móviles con identificación digital; y, en Chile, por sus servicios de gobierno digital que cuentan un enfoque integrado para la identificación y una agenda avanzada de gobierno digital; finalmente, en Brasil, para tratar la protección social, ya que su programa de transferencias monetarias condicionadas y su sistema de información gerencial son reconocidos globalmente.

Notas

1. Una identidad establecida dentro de un sistema destinado a ser utilizado por otras entidades. Los Estados a menudo operan sistemas de identificación fundacionales a través de agencias de Registro Civil y Estadísticas Vitales (RCEV) con bases de datos centralizadas. El Aadhaar de India y el Número de Seguro Social de los Estados Unidos son ejemplos de identificaciones fundacionales. En algunos casos, los certificados de nacimiento, pasaportes y otras credenciales emitidas por el gobierno se usan como identificaciones fundacionales.
2. Además de los beneficios potenciales descritos, las organizaciones señalan tanto los riesgos inherentes de los sistemas de identificación digital como los desafíos y oportunidades más específicos del contexto de los países del sur global.
3. Para obtener más información acerca del movimiento Good ID, visitor el sitio https://www.good-id.org/en/about
4. El Aadhaar, en India, y el e-ID, en Estonia, son dos ejemplos recurrentes de identificaciones digitales fundacionales.
5. Los niveles de matrimonio infantil en la región se han mantenido alrededor del 25 por ciento en la última década, mientras que otras áreas del mundo han experimentado una disminución significativa, particularmente en el sur de Asia, donde los niveles de matrimonio infantil han caído de casi 50 por ciento a 30 por ciento en el mismo período. Para más detalles, visitar el sitio <https://www.unicef.org/press-releases/latin-america-and-caribbean-decade-lost-ending-child-marriage>
6. La cuestión de la facilidad de uso del sistema debe tener en cuenta los niveles de alfabetización digital, el idioma y la edad de los usuarios.
7. A diferencia del anterior, el objeto del método era identificar individuos en sus relaciones civiles con el Estado y con otros individuos.
8. La reflexión a la que hacemos es referencia es la siguiente: *"La identificación de todos los habitantes sin distinción, para garantizar, como lo he dicho, el derecho al nombre y contribuir eficaz y seguramente a que sea verdad el buen funcionamiento de las instituciones del Estado, para bien de la sociedad por ellas regida."*
9. El índice se compone de tres factores: el índice de servicios en línea, el índice de telecomunicaciones y el índice de capital humano.
10. La mayoría de los países latinoamericanos obtienen puntajes entre 0,45 y 0,65.
11. Aunque el uso de herramientas tecnológicas impulsa la mejora de la calidad del servicio, también es necesario contar con procedimientos claros y estandarizados, además de una identificación digital multipropósito para que el usuario pueda llevar a cabo el proceso de manera ágil y eficiente.
12. Un estudio realizado por el Banco Interamericano de Desarrollo (BID) muestra que entre los 20 países que brindan servicios de registro civil, 14 deben conservar copias impresas de los certificados de nacimiento o certificados procesados digitalmente (BID, 2019).
13. Por ejemplo, en 2016 el Banco Mundial estimó que una parte significativa de la población, principalmente en las zonas rurales, todavía no tiene acceso a la electricidad. Recuperado de la base de datos <Banco Mundial, Energía sostenible para todos (SE4ALL) del Marco de seguimiento global de SE4ALL dirigido conjuntamente por el Banco Mundial, la Agencia Internacional de Energía y el Programa de asistencia para la gestión del sector energético. https://data.worldbank.org/indicator/EG.ELC.ACCS.ZS?view=map>
14. Sociedad digital: brechas y desafíos para la inclusión digital en América Latina y el Caribe. Publicado en 2017 por la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (7, place de Fontenoy, 75352 París 07 SP, Francia) - UNESCO y la Oficina Regional de Ciencias de América Latina y el Caribe, Oficina de la UNESCO en Montevideo (Luis Piera 1992, Piso 2, 11200 Montevideo, Uruguay).
15. El término es empleado como un uso sectorial de la identidad digital en la bibliografía acerca de la identificación para el desarrollo (ID4D, por sus siglas en inglés) del Banco Mundial.
16. "Mudamos" es una aplicación móvil que permite a las personas apoyar los proyectos de ley que plasman iniciativas ciudadanas en Brasil mediante firmas electrónicas. Al utilizar el mecanismo constitucional de la democracia directa y garantizar los niveles de seguridad de la identidad digital inviolable, ha facilitado la participación cívica en los palacios legislativos de varias ciudades. Ver más en: <https://www.mudamos.org/>.
17. Varios gobiernos están experimentando enfoques novedosos, incluidas las identidades basadas en teconologías *blockchain*; de hecho, este es uno de los principales casos de uso en la infraestructura europea de servicios Blockchain. Ver: <https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=147458240>

18. En Reino Unido se adopta un sistema de garantía de identidad destinado a proporcionar un único inicio de sesión confiable en todos los servicios digitales del gobierno. Ver: <https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify>.

19. Un ejemplo de esta tendencia es mi GovID de la Commonwealth, que se está probando en Australia este año con una función de reconocimiento facial. Ver <https://www.mygovid.gov.au/>. Por otro lado, la evidencia empírica ha demostrado la existencia de sesgo de algoritmo en dicha tecnología, lo que lleva a la discriminación por edad, raza y origen étnico, lo que genera preocupación en su etapa prematura de adopción masiva. Ver <https://www.theverge.com/2019/12/20/21031255/facial-recognition-algorithm-bias-gender-race-age-federal-nest-investigation-analysis-amazon>

20. or ejemplo, los registros administrativos públicos brasileños y el sistema de identificación se encuentran muy fragmentados. Esto ha llevado a una creciente adopción del número de contribuyente como el identificador principal en el país. Ver <http://mapadainformacao.com.br/>.

21. Esto ocurre, por ejemplo, cuando la propuesta del gobierno digital es principalmente una marca política, pero, en realidad, la mayoría de los servicios ofrecidos no son 100% digitalmente acequibles.

22. Un ejemplo de esta tendencia es my GovID de la Commonwealth, que se está probando en Australia este año con una función de reconocimiento facial. Ver más en: <https://www.mygovid.gov.au/>. Por otro lado, la evidencia empírica ha demostrado la existencia de sesgo de algoritmo en dicha tecnología, lo que lleva a la discriminación por edad, raza y origen étnico, lo que genera preocupación en su etapa prematura de adopción masiva.Ver más en: <https://www.theverge.com/2019/12/20/21031255/facial-recognition-algorithm-bias-gender-race-age-federal-nest-investigation-analysis-amazon>

23. Es importante enfatizar que la forma de identificación digital que sea requerida debe garantizar la seguridad y privacidad del usuario y que, en tanto caso de utilidad pública, dicha identidad digital requerida debe ser accesible para todos los que quieran usarla; esto significa que debe ser libre de cargos y discriminación, así como fácil de asegurar.

24. Al considerar los métodos de autenticación, el sistema de identificación del Reino Unido puede servir de ejemplo, ya que utiliza diferentes niveles de garantía de identidad para acceder a los servicios gubernamentales en línea, en lugar de una identidad única considerada "estándar de oro". El marco para asegurar la identidad y los estándares desarrollados para determinar qué formas de evidencia de identidad cumplen con cada nivel de garantía de identificación no solo proporcionan una guía valiosa para otros países, sino que también pueden adaptarse fácilmente a diferentes contextos (Whitley, 2018).

25. La persona debe ir a las oficinas de Registro Civil e Identificación con la tarjeta de identidad, proporcionar un correo electrónico, registrarse en el sitio web y validar con el RUN.

26. Extraído de la instrucción presidencial sobre transformación digital. Ver más en: <https://digital.gob.cl/instructivo/acerca-de>.

27. https://www.leychile.cl/Navegar?idNorma=141599

28. Ver: <https://www.uncdf.org/financial-inclusion-and-the-sdgs>.

29. De acuerdo con el Banco Mundial, la calidad de vida se puede mejorar con el acceso a los servicios financieros, s se tienen en cuenta las inversiones potenciales, la gestión de riesgos y los seguros. Ver <https://www.worldbank.org/en/topic/financialinclusion/overview>.

30. Lo que difiere es el conjunto de datos requeridos. Los programas de inclusión financiera tienden a solicitar un número de identificación y un contacto telefónico, mientras que los bancos tradicionales solicitan información sobre los antecedentes financieros de alguien: de carácter biográfico, biométrico, evidencia de respaldo y metadatos.

31. En el centro de la DDC, como un subconjunto de KYC, está el proceso de asegurar la identificación, verificación y capacidad de cumplir con ciertas reglas en el sector financiero. El objetivo es monitorear y comprender la naturaleza de las transacciones.

32. Ver más en: <https://www.accessnow.org/whyid-letter/> y en: <https://privacyinternational.org/long-read/2237/sustainable-development-goals-identity-and-privacy-does-their-implementation-risk>.

33. Lanzado en 2007, el M-PESA, que realiza transferencias de efectivo a través de un SMS, es el caso más notorio de dinero móvil. Fue la realización de una importante compañía de telecomunicaciones del país (Safaricom) y una extranjera (Vodafone). Tras esta experiencia, el sector de las telecomunicaciones ha desarrollado billeteras digitales basadas en dispositivos móviles en todo el mundo.

34. Con respecto a la autenticación sin contraseña, conceptos como Zero-Knowledge Proof y Proof Bullets también forman parte del núcleo de la identidad digital basada en la tenconología *blockchain*. Permite, por ejemplo, que una persona sepa si otra persona cumple con reglas específicas sin que revele dicha información.

35. Varios bancos digitales confían en el reconocimiento de imágenes de documentos oficiales, registros de video e incluso transmisiones en vivo como prueba de identidad.

36. En este sentido, el Grupo de Acción Financiera Internacional (GAFI) lanzó un borrador de consulta a fines de 2019 con el objeto de relevar la importancia de la identificación digital para garantizar la eficiencia, confiabilidad, seguridad e inclusión.

37. El procedimiento KYC supone identificar y recopilar una serie de datos de clientes de uno o más servicios financieros, así como asegurar ciertas características sobre dichos datos, en base a principios como la puntualidad: la capacidad de realizar todos los procedimientos de mitigación de riesgos en un período determinado y suficiente tiempo para que se tome una decisión. Veracidad: la capacidad de pronunciar la verdad (considerando que la información engañosa y algunas omisiones son moralmente equivalentes a las mentiras), y la integridad.

38. Dado el crecimiento de los servicios financieros digitales, el consentimiento se está convirtiendo en un tema central para la identidad digital en el sector (Loufield y Vashish, 2020).

39. El sistema está habilitado por una forma simplificada de establecer un proceso de KYC a través de la validación de identidad por parte de una autoridad estatal central en función de una Ley específica de dinero electrónico, que regula las características básicas del dinero electrónico como instrumento de inclusión financiera. Ley del Dinero Electrónico 2013 (Perú). Ver más en: <https://www.bcrp.gob.pe/docs/Transparencia/Normas-Legales/ley-29985.pdfl>.

40. El representante de la BIM argumentó que a pesar de que quieren ser completamente digitales en 2020 y usar datos biométricos, el costo para acceder a la base de datos del RENIEC es comparativamente más alto que en otros países, incluso para abrir cuentas bancarias. Un equivalente a 50 centavos de soles peruanos por persona, lo que puede ser costoso si se considera un escenario de cientos de miles de billeteras que se abren todos los días.

41. Desde 2011, Perú cuenta con una ley de protección de datos personales y una Autoridad Nacional de Protección de Datos Personales (ANPDP). Sin embargo, no es un organismo independiente y funciona bajo los auspicios del Ministerio de la Mujer y la Justicia. De conformidad con el Artículo 7 de la Ley Orgánica de RENIEC, la entidad es responsable de "garantizar la privacidad de los datos personales". A pesar de que el ANPDP ha estado vigente durante casi diez años, confían profundamente en RENIEC para garantizar la protección de datos. Ver <http://www.minedu.gob.pe/otd/pdf/normas/01-ley-26497-ley-organica-del-reniec.pdf>

42. Manifestó esto al destacar que RENIEC supervisa el cumplimiento de sus propias normas y que no ha implementado mecanismos para permitir la participación y los mecanismos de revisión. Algunos defensores de la privacidad afirman que los empleados de la autoridad de identificación apoyan la idea de la "cultura del secreto".

43. El Centro Nacional para la Seguridad del Paciente del Departamento de Asuntos de Veteranos (VA) de los Estados Unidos citó la identificación errónea de pacientes en más de 100 análisis, desde enero de 2000 hasta marzo de 2003. Fuente: Estudio de identificación errónea de pacientes de Mannos D. NCPS: un resumen de la causa raíz análisis. VA NCPS. Temas en seguridad del paciente. Washington, DC, Departamento de Asuntos de Veteranos de los Estados Unidos, junio – julio de 2003 (http://www.va.gov/ncps/TIPS/Docs/TIPS_Jul03.doc, consultado el 11 de junio de 2006) + Alianza Mundial para la Seguridad del Paciente (2004 , OMS); Nueve soluciones de seguridad para pacientes (2007, OMS).

44. Los servicios de salud electrónicos (eHealth, como se los conoce en inglés) también pueden concebirse como el uso de Internet y otras tecnologías relacionadas en el sector de la salud para mejorar el acceso, la eficiencia, la efectividad y la calidad de los procesos clínicos y comerciales utilizados por organizaciones de salud, médicos, pacientes, y consumidores, con el objetivo final de mejorar el estado de salud de los pacientes. Ver: Eysenbach G. ¿Qué es la salud electrónica? J Med Internet Res 2001; 3 (2): E20.

45. El proceso de correspondencia debe estar vinculado al sistema de indexación del paciente y puede requerir una potencia computacional significativa, una infraestructura de comunicación ampliamente disponible y recursos considerables para implementarlo en línea. Además, el uso de algoritmos está sujeto a problemas de exactitud y consideraciones acerca de su precisión.

46. Eso depende de las medidas de seguridad, como la seguridad de acceso basada en roles, las comunicaciones seguras y la infraestructura tecnológica adecuada. Además, también se requieren controles adecuados sobre el acceso a la información en los sitios web de asistencia sanitaria.

47. Si bien dichas preocupaciones son válidas para cualquier sistema de identificación, se intensifican en el sector de la salud, particularmente si los identificadores únicos están vinculados a registros de salud o a otros datos potencialmente confidenciales.

48. Por ejemplo, los datos confidenciales deben ser anonimizados, evitando así que el paciente sea reidentificado.

49. Esta es una recomendación reconocida en varios documentos internacionales, como la Convención internacional sobre la protección de los derechos de todos los trabajadores migratorios y de sus familiares (art. 28) y el Reporte especial sobre la salud de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (OHCHR) de las Naciones Unidas.

50. Es generado por el Sistema Electrónico Establecido (e-SINAC). De acuerdo con el gobierno mexicano, el sistema ya se implementó en 21 estados, y para 2017 se habían emitido más de 200 mil certificados electrónicos. Ver más en: <https://www.gob.mx/mexicodigital/articulos/certificado-electronico-de-nacimiento-142911>.

51. Ver más en: <https://www.gob.mx/mexicodigital/articulos/certificado-electronico-de-nacimiento>.

52. De acuerdo a lo manifestado por un entrevistado, existe un problema relacionado con el tráfico clandestino de datos de identidad e, incluso, se han producido filtraciones masivas de datos en posesión del Instituto Nacional Electoral (INE); todo lo cual ha hecho que el control de las personas sobre su identidad sea problemático.

53. En comparación con el Reglamento general de protección de datos (GDPR), que tiene una multa clara por incumplimiento, de parte de una empresa, del 4% de sus ingresos anuales.

54. En 2015, se publicó en línea una base de datos que contenía registro de los votantes, exponiendo así la información personal de 93.4 millones de ciudadanos mexicanos. En 2016, se produjo una importante fuga de datos de la aplicación de alquiler de automóviles Uber. En octubre de 2017, se reveló que MoneyBack, la compañía responsable de devolver el impuesto al valor agregado a los turistas extranjeros que visitaron México, dejó una base de datos no segura en Internet con 400 GB de archivos de información personal confidencial, como números de pasaporte, tarjetas de crédito e identificaciones oficiales de ciudadanos extranjeros. Ver más en: <https://privacyinternational.org/state-privacy/1006/state-privacy-mexico>.

55. En 2016, el Banco de México estimó el valor del fraude relacionado con el robo de identidad en 108 millones de pesos, lo que coloca al país en la octava posición mundial en este tipo de delitos. En 2017, el fraude con tarjetas bancarias, el robo de identidad, así como el acceso no autorizado o el mal uso de la información personal fueron las principales preocupaciones de los consumidores mexicanos, de acuerdo con el Índice de Seguridad de Unisys más reciente. Ver más en: <https://mundocontact.com/preocupa-a-mexicanos-robo-de-identidad/>; <https://mundocontact.com/robo-de-identidad-y-fraude-bancario-angustia-a-mexicanos/>.

56. No es posible afirmar que existe una causalidad entre la reducción de la pobreza y el acceso a la documentación personal, pero podemos afirmar que las estrategias que combinan estos dos elementos crearon condiciones propicias para mejorar ambos problemas.

57. El continente ha estado logrando resultados valiosos. En veinte años, los países latinoamericanos lograron un progreso significativo con respecto a la cobertura del registro de nacimientos. En 2000, el continente tenía 76 por ciento de cobertura para niños menores de cinco años y, ahora, según un informe reciente de UNICEF, ese porcentaje ha crecido a 94 por ciento. Ver <https://www.unicef.org/reports/birth-registration-every-child-2030>.

58. Un Sistema de Información de Gestión se define como el conjunto de tecnologías, procesos y actores involucrados en la gestión de la información para políticas y programas sociales. Un SIG juega un papel crucial en la protección social. Tiene funciones, como promover la divulgación a los beneficiarios para incluirlos, y múltiples funciones administrativas, como proporcionar información gerencial, integrar y controlar información, y proporcionar transparencia.

59. Algunos ejemplos son Chile Solidario, Prospera (México), Más Familias en Acción (Colombia), Juntos (Perú).

60. A pesar de ello, algunos beneficiarios aún se encuentran en situaciones vulnerables (UNU-WIDER, 2016).

61. El caso de Aadhaar es emblemático porque recopiló datos biométricos de más de mil millones de personas, proporcionando así una identificación digital única para casi toda la población. No obstante, hay algunos casos de negación de raciones de alimentos debido a fallas en la autenticación del sistema y a la discriminación de los grupos marginados. Ver <https://www.hrw.org/news/2018/01/13/india-identification-project-threatens-rights>.

62. La biometría puede hacer que las personas “se sientan observadas, rastreadas, etiquetadas y perfiladas, y eso tendrá consecuencias por la forma en que constituyen su política y su expresión. La vulnerabilidad de la pobreza exacerba esta amenaza a la libertad. Por supuesto, habrá alguien en algún lugar que dirá que los pobres no tienen ningún uso para la libertad “, como destacó Ramanathan (2014).

63. El Ministerio a cargo también pone a disposición en línea bases de datos desidentificadas para fines de investigación. Sin embargo, el gobierno debe aclarar cómo evitan la reidentificación de las inferencias de datos.

64. Surgen problemas adicionales de protección de datos a partir de las ordenanzas ejecutivas de crear un registro de datos unificado con vistas a favorecer la interoperabilidad entre las bases de datos del gobierno, pero sin publicar, en su caso, la evaluación del riesgo de los datos e involucrar a la sociedad civil. Las OSC se sorprendieron con la medida. Ver <http://www.in.gov.br/en/web/dou/-/decreto-n-10.046-de-9-de-outubro-de-2019-221056841>

65. La legislación brasileña de protección de datos se aprobó en 2018, pero los efectos de muchas de sus disposiciones, en particular la aplicación y las sanciones aplicables, que debían entrar en vigencia en enero de 2020, se han pospuesto hasta 2021.

66. La OCDE tiene un conjunto de diagnósticos por país acerca del gobierno digital, que clasifica un marco de identidad digital como elemento fundacional. En este proyecto, utilizamos principalmente las revisiones de Brasil, México, Perú y Chile. La información se recuperó de <http://www.oecd.org/gov/digital-government/>.

67. Access Now analizó, como representante del tercer sector, algunas identidades digitales nacionales específicas y entregó recomendaciones específicas sobre el uso de datos biométricos. Documento recuperado de <https://www.accessnow.org/national-digital-identity-programmes-whats-next/>.

68. La hoja de ruta de la Unión Internacional de Telecomunicaciones (UIT) sobre la guía de identidad digital proporciona el diagnóstico de los países y recomendaciones sobre las mejores prácticas y estándares. Recuperado de <https://www.itu.int/pub/D-STR-DIGITAL.01-2018>.

69. Lanzado oficialmente a mediados de 2019, este informe es una guía extendida para quienes deban tomar decisiones y los profesionales de operaciones, a fin de que desarrollen una estrategia de identidad digital, teniendo en cuenta el status quo del contexto dado, sus particularidades, el conjunto de políticas, el diseño y las opciones tecnológicas, e implicaciones. Recuperado de: <http://documents.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-Guide-Draft-for-Consultation.pdf>.

70. El Instituto Global McKinsey lanzó, en la primera mitad de 2019, un informe extendido que también examinó diferentes fuentes de creación de valor mediante el uso de la identificación digital. Destacó el enorme potencial del aumento del PIB hasta 2030, tanto en países desarrollados (3%) como en desarrollo (6%), en promedio. Recuperado de <https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth>.

Bibliografía

Aadil, A., Gelb, A., Giri, A., Mukherjee, A., Navis, K., Thapliyal, M. (2018). Digital Governance: Is Krishna a Glimpse of the Future?. Center for Global Development Notes. Retrieved from <https://www.cgdev.org/sites/default/files/digital-governance-krishna-glimpse-future-working-paper.pdf>.

Access Now. (2018). National Digital Identity Programmes: What's next?. Retrieved from: <https://www.accessnow.org/cms/assets/uploads/2018/06/Digital-Identity-Paper-2018-05.pdf>.

ACP. (2019). Extreme poverty and digital welfare: New report from UN Special Rapporteur on extreme poverty raises alarm about the rise of a digital welfare dystopia. Retrieved 30 March, from: <https://www.apc.org/en/news/extreme-poverty-and-digital-welfare-new-report-un-special-rapporteur-extreme-poverty-raises>.

Appaya, S., Varghese, M. (2019). Digital ID – a critical enabler for financial inclusion. Retrieved 28 March, from: <https://blogs.worldbank.org/psd/digital-id-critical-enabler-financial-inclusion>.

Banco Central do Brasil. (2009). Perspectivas e desafios para inclusão financeira no Brasil: visão de diferentes atores. Brasília. Retrieved from: <https://www.bcb.gov.br/Nor/Deorf/projincfin/livro_inclusao_financeira_internet.pdf>.

Baya, V. (2019). Digital Identity: Moving to a decentralized future. Retrieved 30 March, from: <https://www.citi.com/ventures/perspectives/opinion/digital-identity.html>.

Barca, V., Makin, P & Bamezai, A. (2018). Integrating digital identity into social protection. An Analysis of potential benefits and risks. Discussion Paper. Oxford Policy Management.

Bhadra, S. (2019). Five Surprisingly Consequential Decisions Governments Make About Digital Identity. Retrieved 30 Msfrom: <https://www.omidyar.com/blog/five-surprisingly-consequential-decisions-governments-make-about-digital-identity>

Centre of Excellence for CRVS Systems. (2020). Gender Equality. Retrieved 30 May from: <https://crvssystems.ca/gender-equality>.

Center for Financial Inclusion (2019). Digital Financial Inclusion in Peru; A Promising Trend to Watch. Retrieved from: <https://www.centerforfinancialinclusion.org/digital-financial-inclusion-in-peru-a-promising-trend-to-watch>.

Chirchir, R., Barca, V. (2020). Building an integrated and digital social protection information system. Retrieved from: <https://socialprotection.org/sites/default/files/publications_files/GIZ_DFID_IIMS%20in%20social%20protection_long_02-2020.pdf>.

The Bureau of National Affairs. (2015). Privacy in Latin America and the Caribbean. Retrieved from: <https://www.bna.com/uploadedFiles/BNA_V2/Legal/Pages/Custom_Trials/PVRC/Privacy_Laws_Latin_America.pdf>.

Campello, T., Neri, M. C. (2014). Bolsa Família Program: a decade of social inclusion in Brazil. Brasília. Ipea.

Carmona, S. C. (2019). Biometric technology and beneficiary rights in social protection programmes. International Social Security Review. 4 (72), 3-28.

Caruso, C. (2016). Digital Financial Inclusion in Peru; A Promising Trend to Watch. Retrieved 30 March, from: <https://www.centerforfinancialinclusion.org/digital-financial-inclusion-in-peru-a-promising-trend-to-watch>.

Center for Global Development. (2017a).

Identification Revolution: Can Digital ID Be Harnessed for Development?. Retrieved from: <https://www.cgdev.org/sites/default/files/identification-revolution-can-digital-id-be-harnessed-development-brief.pdf>.

Center for Global Development (2017b). Identification as a National Priority: The Unique Case of Peru. Retrieved from: <https://www.cgdev.org/sites/default/files/identification-national-priority-unique-case-peru.pdf>.

Center of Excellence for CRVS Systems. (2020). Gender equality. Retrieved 30 March, from: <https://crvssystems.ca/gender-equality>.

Clavijo, S., Vera, N., Londoño, J., Beltrán, D. (2019). Digital Financial Services (FINTECH) in Latin America. Retrieved from: <https://www.anif.com.co/sites/default/files/investigaciones/anif-fintech-wpaper0219.pdf>.

Chrispino, R. (2019, September). Identidade como acesso à cidadania. (COSTA. J, Interviewer).

Comisión Multisectorial de Inclusión Financiera. (2015). Estrategia Nacional de Inclusión Financiera. Retrieved from: <http://www.mef.gob.pe/contenidos/archivos-descarga/ENIF.pdf>.

Comisión Nacional de Arbitraje Médico. (2018). El expediente clínico electrónico universal en México. Mexico. Retrieved from <http://www.conamed.gob.mx/gobmx/boletin/pdf/boletin18/expediente.pdf>.

Cortés, R. A. (2019). El nuevo entorno regulatorio de la protección de datos personales en Chile. Retrieved 30 March, from: <https://iapp.org/news/a/el-nuevo-entorno-regulatorio-de-la-proteccion-de-datos-personales-en-chile/>.

Dreze, J., Khalid, N., Khera, R., Somanchi, A. (2017). Pain without gain? Aadhaar and food security in Jharkhand.Economic and political weekly. Vol. 52, Issue No. 50. Retrieved 30 March, from: <https://www.epw.in/journal/2017/50/special-articles/aadhaar-and-food-security-jharkhand.html>.

Domínguez, M. (2018). Access and use of information and communication technologies in Mexico: determining factors. PAAKAT: Revista De Tecnología Y Sociedad. Vol. 8 No. 14. Retrieved 30 March, from <http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S2007-36072018000200002&lang=pt>.

ECLAC (2015). Inclusive social development: The next generation of policies for overcoming poverty and reducing inequality in Latin America and the Caribbean. Santiago de Chile. Retrieved from: <https://repositorio.cepal.org/bitstream/handle/11362/39101/4/S1600098_en.pdf>.

Enríquez, O. (2018). Marco jurídico de la protección de datos personales en las empresas de servicios establecidas en México: desafíos y cumplimiento. Revista IUS, 12(41), 267-291. Retrieved 10 December 2019, from <http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-21472018000100267&lng=es&tlng=es>.

Escócia, F. (2019a). Invisíveis: uma etnografia sobre identidade, direitos e cidadania nas trajetórias de brasileiros sem documento. Retrieved from: <http://www.mprj.mp.br/documents/20184/151138/escossiafernandameloda.invisiveis_umaetnografiasobreidentidade.pdf>.

Escóssia, F. (2019b, September). Identidade como acesso à cidadania. (COSTA. J, Interviewer). Retrieved 30 March, from: <https://www.youtube.com/watch?v=8yK3FHEnpnA>.

FAFT. (2014). Guidance for a Risk-Based Approach The Banking Sector. Retrieved from: <https://www.fatf-gafi.org/media/fatf/documents/reports/

Risk-Based-Approach-Banking-Sector.pdf>.

FATF. (2019). Public consultation on FATF draft guidance on digital identity. Retrieved 30 March, from: <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/consultation-digital-id-guidance.html>.

Ferrari, M. G. Marcas de identidad. Juan Vucetich y el surgimiento transnacional de la dactiloscopia (1888-1913). Rosario: Prohistoria Ediciones, 2015.

Gelb, A., Metz, A. D. (2018). Identification Revolution: Can Digital ID Be Harnessed for Development? Center for Global Development. Washington, DC.

Gelb, A., Mukherjee, A., Navis, K., Thaplyal, M., Giri, A. (2017). What a New Survey of Aadhaar Users Can Tell Us About Digital Reforms: Initial Insights from Rajasthan. Center for Global Development. CGD Notes. Retrieved 30 March, form: <www.cgdev.org/publication/what-a-new-survey-aadhaar-users-can-tell-us-about-digital-reforms-initial-insight>.

Gelb, A., Mukherjee, A., Navis, K., (2020). How Can Digital ID and Payments Improve State Capacity and Effectiveness? Center for Global Development Notes. Retrieved from <https://www.cgdev.org/sites/default/files/citizens-and-states-how-can-digital-id-and-payments-improve-state-capacity.pdf>.

Gobierno Digital Chile. (2019). División de Gobierno Digital. Retrieved 30 March, from <https://digital.gob.cl/plan/identidad-digital>.

Gobierno Digital Chile. (2018). Estrategia de Transformación Digital del Estado: Estado al Servicio de las Personas. Retrieved from: <https://digital.gob.cl/doc/estrategia_de_transformacion_digital_2019_.pdf>.

GSMA. (2016.) Digital identity as a key enabler for e-government services. Retrieved from: <https://www.gsma.com/identity/wp-content/uploads/2016/02/MWCB16-Digital-Identity-as-a-Key-Enabler-for-eGovernment-Services-Marta-Ienco.pdf>.

GSMA. (2016). Digital Identity: a prerequisite for Financial Inclusion?. Retrieved 30 March, from: <https://www.gsma.com/mobilefordevelopment/country/global/digital-identity-a-prerequisite-for-financial-inclusion/>.

Hellmann, A. G. (2015). How does Bolsa Familia work?: Best practices in the implementation of conditional cash transfer programs in Latin America and the Caribbean. IADB. Retrieved 30 March, from: <https://publications.iadb.org/en/how-does-bolsa-familia-work-best-practices-implementation-conditional-cash-transfer-programs-latin>.

Hunter, W., Brill, R. (2016). “Documents, Please”: Advances in Social Protection and Birth Certification in the Developing World. World Politics, 68(2), 191-228. doi:10.1017/S0043887115000465

Hunter, W. (2019). Identity Documents, Welfare Enhancement, and Group Empowerment in the Global South. The Journal of Development Studies, 55(3), 366-383, doi: 10.1080/00220388.2018.1451637

IADB. (2017). La gestión de la identidad y su impacto en la economía digital. Retrieved from: <https://www.alejandrobarros.com/wp-content/uploads/2016/04/Gestion-de-la-identidad-y-su-impacto-en-la-economia-digital.pdf>.

IADB. (2019). Registros civiles y oficinas de identificación: Análisis y fichas de país. Retrieved from: <https://publications.iadb.org/publications/spanish/document/Registros_civiles_y_oficinas_de_identificaci%C3%B3n_an%C3%A1lisis_y_fichas_de_pa%C3%ADs_es.pdf>.

Ibarra, A. B., Byanyima, W. (2016). Latin America is the world’s most unequal region. Here’s how to

fix it. Retrieved 30 March, from: <https://www.weforum.org/agenda/2016/01/inequality-is-getting-worse-in-latin-america-here-s-how-to-fix-it/>.

ITU News. (2019). Unique, legal and digital: Three characteristics of ID crucial to financial inclusion. Retrieved 30 March, from: <https://news.itu.int/unique-legal-digital-id-financial-inclusion/>.

Laval, C. E. P. (2018). Utopías de control detrás de la identificación civil: los proyectos de identificación de Clodomiro Cabezas Cabezas. Chile, 1927-1938, Revista Historia y Justicia. Retrieved 30 March, from: <https://doi.org/10.4000/rhj.1260>.

Lindert, K., Linder, A., Hobbs, J., Briere, B. (2007). The Nuts and Bolts of Brazil's Bolsa Família Program: Implementing Conditional Cash Transfers in a Decentralized Context. World Bank Group. Retrieved from: <http://documents.worldbank.org/curated/pt/972261468231296002/pdf/398530SP1709.pdf>.

Loufield, E., Vashisht, S. (2020). Data Consent: Let's Share the Burden for Effective Consumer Protection. Center for Financial Inclusion. Retrieved 30 May from: <https://www.centerforfinancialinclusion.org/data-consent-lets-share-the-burden-for-effective-consumer-protection>.

Masiero, S. (2017). Digital governance and the reconstruction of the Indian anti-poverty system. Oxford Development Studies, 45 (4), 393-408.

Masiero, S. (2019). The Digitalization of Anti-poverty Programs: Aadhaar and the Reform of Social Protection in India. Digital Economies at Global Margins. Ed. Mark Graham. MIT Press Direct.

Mastercard. (2019a). Digital Identity: Restoring Trust in a Digital World. Retrieved from: <https://www.mastercard.us/content/dam/mccom/en-us/issuers/digital-identity/digital-identity-restoring-trust-in-a-digital-world-final-share-corrected.pdf>.

Mastercard. (2019b). Examining the Latin American and Caribbean E-commerce Market. Retrieved from: <https://newsroom.mastercard.com/latin-america/files/2019/12/Whitepaper-Digital-Security-mastercard-ENG-simples-FINAL2.pdf>.

McKinsey Global Institute (2019). Digital identification: A key to inclusive growth. Retrieved 30 March, from: <https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth>.

Mexico Digital. (2018). Certificado Electrónico de Nacimiento. Retrieved 13 December 2019, from: <https://www.gob.mx/mexicodigital/articulos/certificado-electronico-de-nacimiento-142911>.

Mexico Digital. (2014). Certificado Electrónico de Nacimiento. Retrieved 13 December 2019, from: <https://www.gob.mx/mexicodigital/articulos/certificado-electronico-de-nacimiento>.

Ministry of Social Development Brazil. (2015). Guia de Cadastramento de Famílias Indígenas. MDS. Brasília.

Muralidharan, K., Niehaus, P., Sukhtankar, S (2020). Identity Verification Standards in Welfare Programs: Experimental Evidence from India. National Bureau of Economic Research Working Paper, 26744

Muralidharan, K., Niehaus, P. & Sukhtankar, S. (2016). Building state capacity: Evidence from biometric smartcards in India. American Economic Review 106 (10), 2895-2929.

Murthy, G. & Medine, D. (2018). Data Protection and Financial Inclusion: Why Consent Is Not Enough. Blog Series: Data Privacy and Protection. Consultative Group to Assist the Poor. Retrieved

30 March, from: <http://cgap.org/blog/data-protection-and-financial-inclusion-why-consent-not-enough>.

Muzzi, M. (2010). Good Practices in Integrating Birth Registration into Health Systems (2000-2009). Unicef. Retrieved from: <https://www.unescap.org/sites/default/files/UNICEF-birth-registration-in-health-systems.pdf>.

OEA. (2008). Diagnóstico del marco jurídico-institucional y administrativo de los sistemas de Registro Civil en América Latina. PUICA. Retrieved from: <http://www.oas.org/sap/docs/puica/diagnostico_legal_administrativo.pdf>.

OECD. (2001). Understanding the Digital Divide. OECD Digital Economy Papers, No. 49, OECD Publishing, Paris, page 5. Retrieved 30 March, from: <https://doi.org/10.1787/236405667766>.

OECD. (2009). The Role of Digital Identity Management in the Internet Economy: A Primer for Policy Makers. OECD Digital Economy Papers. (Report No. 160). OECD Publishing, Paris. Retrieved 30 March, from <https://doi.org/10.1787/20716826>.

OECD. (2019a). Shaping the Digital Transformation in Latin America: Strengthening Productivity, Improving Lives, OECD Publishing, Paris. Retrieved 30 March, from: <https://doi.org/10.1787/8bb3c9f1-en>.

OECD. (2019b). Harnessing the Digital Transformation to Boost Productivity in Latin America and the Caribbean. Retrieved 30 March, from: <https://www.oecd.org/about/secretary-general/harnessing-digital-transformation-to-boost-productivity-in-lac-colombia-october-2019.htm>.

OECD. (2019c). Digital Government in Chile – Digital Identity. Retrieved from: <https://www.oecd-ilibrary.org/sites/9ecba35e-en/index.html?itemId=/content/publication/9ecba35e-en&mimeType=text/html>.

OECD (2019d). Strengthening Digital Government. Retrieved from: <https://www.oecd.org/going-digital/strengthening-digital-government.pdf>.

OECD (2019e). Digital Government in Chile – A Strategy to Enable Digital Transformation, OECD Digital Government Studies, OECD Publishing, Paris. Retrieved from: <https://doi.org/10.1787/f77157e4-en>.

Pan American Health Organization (PAHO). (2016). eHealth in the Region of the Americas: breaking down the barriers to implementation. Retrieved 30 March, from: <https://iris.paho.org/bitstream/handle/10665.2/31286/9789275119259-eng.pdf?sequence=6&isAllowed=y>.

Peirano, M. (2009). O paradoxo dos documentos de identidade: relato de uma experiência nos Estados Unidos. Retrieved from: <http://www.mprj.mp.br/documents/20184/151138/peirano,mariza.oparadoxodosdocumentosdeidentidade.pdf>.

Privacy International. (2012). Medical privacy and security in developing countries and emergency situations. Retrieved from: <https://privacyinternational.org/sites/default/files/2018-11/Privacy_International_Medical_Privacy.pdf>.

Privacy International. (2018). Liliana: "If you don't have RUT, you can't do it.". Retrieved 30 March, from: <https://privacyinternational.org/case-study/2545/liliana-if-you-dont-have-rut-you-cant-do-it>.

Ramada-Sarasola, M. (2012). Can Mobile Money Systems Have a Measurable Impact on Local Development?. Retrieved 30 May from: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2061526>.

Ratcliffe, R. (2019). How a glitch in India's

biometric welfare system can be lethal. Automating poverty Series. The Guardian. Retrieved 30 March, from <https://www.theguardian.com/technology/2019/oct/16/glitch-india-biometric-welfare-system-starvation>.

Ramanathan, U. (2014). Biometrics Use for Social Protection Programmes in India Risk Violating Human Rights of the Poor. Retrieved 30 March, from: <http://www.unrisd.org/sp-hr-ramanathan>.

Sepúlveda, M. (2019). Data Protection is Social Protection. Retrieved 30 May from: <https://www.project-syndicate.org/commentary/social-protection-biometric-data-privacy-by-magdalena-sep-lveda-2019-04?barrier=accesspaylog>.

Tase TH, Lourenção DCA, Bianchini SM, Tronchin DMR (2013). Patient identification in healthcare organizations: an emerging debate. Rev Gaúcha Enferm.;34(2):196-200.

UN. (2018). E-Government Survey: Gearing e-government to support transformation towards sustainable and resilient societies. Retrieved from: <https://publicadministration.un.org/Portals/1/Images/E-Government%20Survey%202018_FINAL%20for%20web.pdf>.

UN Secretary-General. (2019). Secretary-General's opening remarks to the High-level Event on "10 Years of Financial Inclusion - Vast Progress and Challenges Ahead". Retrieved 30 March, from: <https://www.un.org/sg/en/content/sg/statement/2019-09-25/secretary-generals-opening-remarks-the-high-level-event-10-years-of-financial-inclusion-vast-progress-and-challenges-ahead-delivered>.

UNAIDS. (2014). Considerations and guidance for countries adopting national health identifiers., Geneva, 17 April 2014. Retrieved from: <https://www.unaids.org/sites/default/files/media_asset/JC2640_nationalhealthidentifiers_en.pdf>.

UNCDF. (2020). Financial Inclusion and the SDGs. Retrieved 30 May from: <https://www.uncdf.org/financial-inclusion-and-the-sdgs>.

UNESCO and the Regional Bureau for Sciences in Latin America and the Caribbean (2017). Sociedad digital: brechas y retos para la inclusión digital en América Latina y el Caribe. Retrieved 30 March, from: <https://unesdoc.unesco.org/ark:/48223/pf0000262860>.

UNESCO. (2009). Regional overview: Latin America and the Caribbean. Retrieved from: <https://en.unesco.org/gem-report/sites/gem-report/files/178428e.pdf>.

UNICEF. (2018). Latin America and the Caribbean: a decade lost in ending child marriage. Retrieved 30 May from: <https://www.unicef.org/press-releases/latin-america-and-caribbean-decade-lost-ending-child-marriage>.

UNRISD. (2010). Combating Poverty and Inequality: Structural Change, Social Policy and Politics. Retrieved from: <http://www.unrisd.org/80256B3C005BCCF9/(httpAuxPages)/92B1D5057F43149CC125779600434441/$file/PovRep%20(small).pdf>.

UNU-WIDER. (2016). Cash transfers in Latin America: Effects on poverty and redistribution. Retrieved 30 May from: <https://www.wider.unu.edu/publication/cash-transfers-latin-america>.

Villarreal, F. G. (ed.). (2017). Inclusión financiera de pequeños productores rurales, Libros de la CEPAL, N° 147 (LC/PUB.2017/15-P), Santiago, Comisión Económica para América Latina y el Caribe (CEPAL), 2017. Retrieved 30 March, from: <https://repositorio.cepal.org/bitstream/handle/11362/42123/S1700277_es.pdf?sequence=1&isAllowed=y>.

Vucetich, J (1916). Comment in the Creation of the Identity Law of (Ley de Registro de Identidad de

las Personas). Registro General de Identificación. Argentina.

Whitley, E. A. (2018). Trusted Digital Identity Provision: GOV.UK Verify's Federated Approach. CGD Policy Paper. Washington, DC: Center for Global Development. Retrieved 30 March, from: <https://www.cgdev.org/publication/trusted-digital-identity-provision-gov-uk-verify-federated-approach>.

World Bank (2016). Identification Principles for Sustainable Development: toward the digital age. Retrieved from World Bank ID4D website <http://documents.worldbank.org/curated/en/213581486378184357/pdf/112614-REVISED-English-ID4D-IdentificationPrinciples-Folder-web-English-ID4D-IdentificationPrinciples.pdf>.

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

World Bank. (2018b). Global ID Coverage, Barriers, and Use by the Numbers: Insights from the ID4D-Findex Survey. Retrieved from: <http://documents.worldbank.org/curated/en/953621531854471275/Global-ID-Coverage-Barriers-and-Use-by-the-Numbers-Insights-from-the-ID4D-Findex-Survey.pdf>.

World Bank (2018c). The Role of Digital Identification for Healthcare: The Emerging Use Cases. Washington, DC: World Bank License: Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO); Retrieved from World Bank ID4D website <http://documents.worldbank.org/curated/en/595741519657604541/The-Role-of-Digital-Identification-for-Healthcare-The-Emerging-Use-Cases.pdf>.

World Bank. (2018d). Guidelines for ID4D Diagnostics. Retrieved from: <http://documents.worldbank.org/curated/en/370121518449921710/Guidelines-for-ID4D-Diagnostics.pdf>.

World Bank (2019a). Inclusive and Trusted Digital ID Can Unlock Opportunities for the World's Most Vulnerable. Retrieved 13 December, from: <https://www.worldbank.org/en/news/immersive-story/2019/08/14/inclusive-and-trusted-digital-id-can-unlock-opportunities-for-the-worlds-most-vulnerable>.

World Bank (2019b). ID4D Practitioner' Guide, Version 1.0 (October 2019). Washington, DC. Retrieved from: <http://documents.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf>.

WHO. (2007). Patient Identification. Retrieved from: <https://www.who.int/patientsafety/solutions/patientsafety/PS-Solution2.pdf>.

WHO & ITU. (2012). National eHealth Strategy Toolkit. Retrieved from: <https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-E_HEALTH.05-2012-PDF-E.pdf>.

World Economic Forum (2018). The appropriate use of Customer Data. Retrieved from: <http://www3.weforum.org/docs/WP_Roadmap_Appropriate_Use_Customer_Data.pdf>.

World Economic Forum. (2020). Passwordless Authentication: The next breakthrough in secure digital transformation. Retrieved 30 March, from: <https://www.weforum.org/whitepapers/passwordless-authentication-the-next-breakthrough-in-secure-digital-transformation>.

Financiado por

OMIDYAR NETWORK

Encuéntranos

itsrio.org