Alejandro Barros
@abarros

Identificación digital (eID) y sus principios

Un desafío para la región

Son muchos los países en América Latina que actualmente se encuentran implementando sistemas nacionales de Identidad Digital, comúnmente denominados eID (Electronic Identification). Sin embargo, más allá de los problemas vinculados al soporte tecnológico necesario para su desarrollo y operación, probablemente el principal desafío sea la adopción de un conjunto de de principios y prácticas para su gobernanza.

Un buen ejemplo de ello es la iniciativa GoodID, un estudio liderado por Alexandre Barbosa del Instituto de Tecnología y Sociedad (ITS) de Brasil, que busca develar los retos y posibilidades del uso de la identificación digital en Latinoamérica en diferentes sectores, mediante un exhaustivo análisis de los sistemas ya existentes, con especial énfasis en lo que ocurre en México, Chile, Perú y Brasil. Asimismo, se proponen reglas y buenas prácticas que estos sistemas de eID deben contemplar, especialmente cuando se aplican a ciertas áreas, a saber:

1. Servicios gubernamentales digitales

Deben abarcar, como primer paso, un sistema de identificación ampliamente accesible que aporte valor al usuario, simplificando los procedimientos, reduciendo los costos directos e indirectos y habilitando los servicios de transacción.

Por otro lado, 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 los marcos legales de privacidad y protección de datos personales o, en su ausencia, siguiendo las mejores prácticas internacionales.

Aunado a lo anterior, es importante tomar en cuenta que 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 todos los ciudadanos.

2. Inclusión financiera

Los requisitos básicos para reconocer al usuario deben ser idealmente gratuitos, pues sólo así será posible garantizar la inclusión financiera de la población a la que se destinan. Además, es importante separar claramente los datos básicos utilizados para identificar a alguien con base en la información complementaria que es requerida para acceder a servicios específicos y la diligencia debida respecto del cliente.

Por otra parte, en tanto sector líder en identificación desde una perspectiva tecnológica, las compañías de tecnología financiera y los grandes bancos deberían convertirse en impulsores fundamentales de las tecnologías que garanticen la privacidad. Vale considerar a este respecto que la inexistencia de mecanismos de reparación y reclamo para acceder al historial de los datos constituye un indicador importante de malas prácticas, si se tiene en cuenta el desarrollo tecnológico alcanzado por el sector.

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

3. Salud

Al establecerse una identificación nacional única para los servicios de salud, ésta 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 manera que se evite que el paciente pueda ser reidentificado.

Adicionalmente, el acceso a servicios médicos urgentes, no sólo de emergencia, 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). En ese caso, la identificación digital podría constituir un elemento que facilite dicho fin.

4. Protección social
Los estados debieran crear un registro único para ofrecer protección social, adoptando una perspectiva inclusiva que permita mejorar su capacidad para 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.

De igual forma, 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 públicas.

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

Más allá de los problemas vinculados al soporte tecnológico necesario, el más grande desafío es la constitución del conjunto de reglas para la gobernanza de la Identidad Digital

El caso británico

El Reino Unido, por su parte, fue más lejos y definió un conjunto de principios que sus sistemas de Identidad Digital (eID) deben adoptar, los cuales resultan universales y cualquier política pública en materia de eID debiera contemplar.

1. Privacidad
El sistema debe garantizar la confidencialidad y privacidad de los datos de identificación de las personas que utilizan dicho mecanismo.

2. Transparencia
Cuando se acceden a los datos de identificación de las personas, los "dueños" (ciudadanos) deben contar con la información de su uso, las razones y finalidad del mismo.

3. No discriminación
Todos los ciudadanos deben poder acceder a la Identidad Digital, sin barreras de ningún tipo (edad, género, etnia u otra).

4. Interoperabilidad
El soporte tecnológico debe estar basado en estándares tecnológicos no propietarios que permitan la interoperabilidad entre plataformas.

5. Proporcionalidad
Las necesidades del usuario y otras consideraciones, como la privacidad y seguridad, se equilibrarán para que la Identidad Digital se pueda utilizar con la debida confianza.

6. Buen gobierno
Los estándares de ID estarán vinculados a las políticas y leyes gubernamentales. Cualquier regulación futura será clara, coherente y se alineará con el enfoque estratégico más amplio del gobierno para la regulación digital.

Avances en LATAM

Muchos países en Latinoamérica están desarrollando soluciones nacionales de eID a partir de la revisión de soluciones ya implementadas. Por ejemplo:

México, con su esfuerzo por crear un archivo digital que permita realizar trámites y servicios ante el Gobierno de la República, es decir, la e.firma.

Perú, que también pone a disposición una plataforma para la autenticación de la Identidad Digital a fin de acceder a múltiples servicios del Estado.

Chile, que cuenta con un portal ciudadano dedicado a la Clave Única ciudadana digital.

Paraguay, que ofrece un portal para la creación y registro de la identidad electrónica.

Uruguay, que, como primer esfuerzo, ha desarrollado una plataforma para la autenticación ciudadana. Sin embargo, sólo es posible acceder a ella mediante la Cédula de Identidad Digital física.

Llama la atención que los principios y buenas prácticas señalados por GoodID o el gobierno inglés no sean referenciados de forma explícita en los términos de uso y las políticas de estos mecanismos.

De la lectura de algunos de estos términos de uso se aprecia más un enfoque de carácter operacional del uso del mecanismo y no de las responsabilidades que el Estado asume a la hora de gestionar identidades digitales de los ciudadanos. Incluso algunos van más lejos, entregándole toda la responsabilidad al ciudadano.

A pesar de los avances logrados por América Latina en materia de eID, llama la atención que algunos gobiernos no terminan de hacerse responsables de la gestión y tratamiento de los datos

Alejandro Barros

Consultor Internacional y Académico Asociado del Centro de Sistemas Públicos de la Universidad de Chile. Ha sido consultor de organismos internacionales como el Banco Mundial, BID, PNUD y CAF, así como de varios gobiernos y empresas en América Latina y África. Autor de múltiples publicaciones, incluyendo el libro *Polis Digital*, dedicado a políticas públicas de desarrollo digital.