BID
Banco Interamericano de Desarrollo

La gestión de la identidad y su impacto en la economía digital

Alejandro Pareja
Mari Pedak
Carlos Gómez
Alejandro Barros

Sector de Instituciones para el Desarrollo

División de Innovación para Servir al Ciudadano

DOCUMENTO PARA DISCUSIÓN Nº IDB-DP-529

Agosto de 2017

La gestión de la identidad y su impacto en la economía digital

Alejandro Pareja
Mari Pedak
Carlos Gómez
Alejandro Barros

Agosto de 2017

BID
Banco Interamericano de Desarrollo

http://www.iadb.org

Copyright © 2017 Banco Interamericano de Desarrollo. Esta obra se encuentra sujeta a una licencia Creative Commons IGO 3.0 Reconocimiento-NoComercial-SinObrasDerivadas (CC-IGO 3.0 BY-NC-ND) (http://creativecommons.org/licenses/by-nc-nd/3.0/igo/legalcode) y puede ser reproducida para cualquier uso no-comercial otorgando el reconocimiento respectivo al BID. No se permiten obras derivadas.

Cualquier disputa relacionada con el uso de las obras del BID que no pueda resolverse amistosamente se someterá a arbitraje de conformidad con las reglas de la CNUDMI (UNCITRAL). El uso del nombre del BID para cualquier fin distinto al reconocimiento respectivo y el uso del logotipo del BID, no están autorizados por esta licencia CC-IGO y requieren de un acuerdo de licencia adicional.

Note que el enlace URL incluye términos y condiciones adicionales de esta licencia.

Las opiniones expresadas en esta publicación son de los autores y no necesariamente reflejan el punto de vista del Banco Interamericano de Desarrollo, de su Directorio Ejecutivo ni de los países que representa.

Contactos: Alejandro Pareja, apareja@iadb.org.

LA GESTIÓN DE LA IDENTIDAD Y SU IMPACTO EN LA ECONOMÍA DIGITAL

BID
Mejorando vidas

Resumen

La identidad digital es la piedra angular de la transformación digital de América Latina y el Caribe (ALC). Es un aspecto cada vez más relevante en el sistema de identidad de las personas, cuyos cimientos son los registros civiles de calidad. Conforma un instrumento esencial para la inclusión y la reducción de costos de transacción en toda la economía, contribuyendo así a mejorar la calidad de los servicios tanto del sector público como del privado. Este documento brinda un panorama general de la identidad digital, mostrando costos/beneficios y ventajas/desventajas de las distintas alternativas de implementación. En particular, se incluye una mirada profunda de dos experiencias bastante distintas, la de Estonia y la de España.

Clasificaciones JEL: D02, D73, K23, L14, L81, L86, L88

Palabras clave: identidad digital, economía digital, gobierno digital, autenticación, biometría, certificado digital, firma digital, Estonia, España, Canadá, PKI, DNI electrónico

Índice

Índice 2
Prólogo 3
Resumen ejecutivo 4
Introducción 5
Gobernanza de los sistemas de identidad 9
Costo y financiamiento de los sistemas públicos de gestión de la identidad 10
Beneficios e impacto de la identidad digital 11
Estonia: del registro de población a la gestión de la identidad digital 13
Identidad 13
El registro de población como base de la gestión de la identidad 14
La identidad digital y sus ecosistemas 15
Documento de identidad digital 17
Usos de la identidad digital 20
Promoción del uso de la identidad digital 21
España: gestión de la identidad y economía digital 21
Inicios de la firma digital 22
La introducción del DNI-e 23
Acceso electrónico a los servicios públicos 23
Identificación en el marco de la Unión Europea 25
Lecciones aprendidas 26
Referencias bibliográficas 29

Prólogo

La identidad digital es la piedra angular de la transformación digital de América Latina y el Caribe (ALC). Para el año 2030, según los objetivos de desarrollo sostenible, todos los ciudadanos deberán contar con una identidad jurídica, incluido el registro de nacimiento. El poseer una identidad digital tiene el potencial de desencadenar una serie de beneficios de los que todo ciudadano debería gozar. La tasa de registro de la población en la región aumentó de 82% a 90%; sin embargo, a pesar de los avances, 1 de cada 10 ciudadanos no puede probar su identidad y, por lo tanto, no puede acceder a servicios básicos tales como educación, atención médica, beneficios sociales, acceso a capital u otro servicio financiero, ni tampoco votar, cruzar las fronteras legalmente o poseer bienes, entre otros.

El registro y la gestión de la identidad son instrumentos esenciales para la inclusión, ya que reducen los costos de transacción en toda la economía, permitiendo mejorar la calidad de los servicios para el sector público y privado. Este proceso enfrenta algunos desafíos; por ejemplo, la privacidad, por un lado, y el posible fraude, por el otro. Los retos de desarrollo actuales solo pueden ser sostenibles si el sector privado es también parte de la solución. Sin embargo, son los gobiernos los que establecen los cimientos para promover la inversión y generar prosperidad.

En esta dirección, el presente documento de discusión, elaborado en el marco de la agenda digital de la División Innovación para Servir al Ciudadano (ICS),[1] explora el potencial de la identidad digital en su transformación de los diferentes sectores de la economía a través de dos casos emblemáticos.

El Banco Interamericano de Desarrollo espera poder brindar a los países recursos financieros, conocimiento y soluciones innovadoras que promuevan la adopción de la identidad digital universal, empoderando a los ciudadanos para que mejoren su calidad de vida.

Luiz Ros
Asesor Especial en Innovación
Iniciativa de Economía Digital

[1] ICS integra el Departamento Instituciones para el Desarrollo (IFD). Tiene como misión mejorar vidas a través de mejores gobiernos (más efectivos, eficientes y transparentes). Sus áreas de intervención incluyen una agenda digital mediante la que se procura el desarrollo del gobierno digital y el fortalecimiento y la modernización de registros civiles y sistemas nacionales de identidad.

Resumen ejecutivo

Es muy difícil encontrar un resumen en español sobre el panorama de la identidad digital, que ponga en claro las decisiones que pueden o deberían tomarse, o que muestre costos/beneficios y ventajas/desventajas de las distintas alternativas disponibles a la hora de desarrollar un sistema efectivo de identidad digital. Este documento pretende contribuir a llenar este vacío, con lecciones generales que arroja la experiencia internacional así como con una mirada profunda de dos experiencias bastante distintas, la de Estonia y la de España. Los contenidos de este trabajo reflejan los temas tratados en el seminario "Gestión de la Identidad y su Impacto en la Economía Digital" realizado por el BID en octubre de 2016.[2] Durante el seminario se discutieron los aspectos más relevantes de la gestión de la identidad, tales como el valor de la confianza como habilitante del sistema, la necesidad o no de incluir biometría, los factores críticos de éxito, los sistemas en uso en el plano internacional y los roles del sector privado y el gobierno.

Posiblemente, la conclusión principal que pueda extraerse del seminario es que existe a nivel mundial una gran variedad de esquemas de identidad legal física, lo cual condiciona las alternativas que se toman en cuenta en cada país para el desarrollo de la identidad digital. Toda solución debe ser coherente con el contexto local. Los factores que llevan a cada país a adoptar un modelo son: i) culturales (por ejemplo, la captura rutinaria por parte del Estado de los datos biométricos de cada persona se hace con total naturalidad en algunos países mientras que en otros es algo inadmisible); ii) políticos o de tradición administrativa (por ejemplo, la existencia o no de un federalismo fuerte), y iii) técnicos (por ejemplo, las decisiones respecto a la unicidad u obligatoriedad de un documento nacional se toman después de realizar un análisis de costo-efectividad). En el cuadro 1 se pueden apreciar las principales dimensiones de estos esquemas y los países donde se aplican las distintas alternativas.

Cuadro 1. Distintos sistemas de identidad

Característica	Alternativas	Ejemplos
Documento Nacional de Identidad (único y obligatorio, válido en el ámbito nacional)	Sí	España, Hispanoamérica
	No	Estados Unidos, Reino Unido, Jamaica
Sistemas federados (emisores subnacionales con validez nacional)	Sí	Estados Unidos, Canadá
	No	Estonia, Hispanoamérica
Documento con biometría de huella o iris	Sí	Hispanoamérica, India
	No	Estonia, Estados Unidos
Documento con chip (identidad digital) obligatorio para mayores de edad	Sí	Estonia, Uruguay, España
	No	Estados Unidos

Fuente: Elaboración propia.

[2] El seminario fue organizado como parte de la agenda de conocimiento de la División ICS, en coordinación y con el apoyo del programa "Cutting Edge" del Sector de Conocimiento y Aprendizaje (KNL). El objetivo del seminario tuvo dos componentes: i) profundizar el conocimiento respecto del estado actual de las tecnologías relacionadas con la identidad, en cuanto a alternativas así como al grado de uso efectivo de las mismas, procurando comprender la variedad de situaciones alrededor del mundo, y ii) tomar conocimiento de experiencias internacionales avanzadas, abarcando no solo lo tecnológico sino también factores de implementación y sustentabilidad que pueden conducir a un esquema exitoso.

Una segunda conclusión es que el aprovechamiento por parte de cada persona de las oportunidades que ofrece la era digital depende básicamente de contar con: i) conectividad; ii) un dispositivo de conexión y conocimiento para utilizarlo, y iii) identidad digital.[3] Claramente, sin la tercera se podrá utilizar Internet y aprovechar algunas de sus ventajas, por ejemplo, el acceso a información. Sin embargo, no se podrán realizar transacciones que requieran verificación de identidad, incluidas muchas relacionadas con el gobierno digital y el sector financiero.

Una tercera conclusión surge de la comparación de los procesos de adopción en Estonia y España. Quizá un modelo centralizado, prácticamente obligatorio y basado en un número muy reducido de alternativas, simplifica y facilita la adopción. Ahora bien, puede ser difícil de aplicar en países con burocracias de larga y compleja trayectoria. El contexto estonio era propicio para este esquema pues se trata de un país pequeño cuya burocracia tuvo que reinventarse a principios de los años noventa.

Por último, casos exitosos como los de Estonia y Canadá muestran que los esfuerzos coordinados entre el sector público y el privado son clave para el desarrollo de sistemas de identidad digital sólidos. Debe tenerse en cuenta, sobre todo, el rol del sistema financiero como principal consumidor de servicios de identificación y autenticación de la economía. Un esquema acordado entre el sector público y el financiero no solo genera economías, sino que cataliza el proceso de adopción por parte de la población.

El seminario fue dirigido por Alejandro Pareja (Especialista de ICS), coordinado en conjunto con Carlos Molina (Especialista Líder de KNL), y contó con el apoyo técnico de Alejandro Barros (Consultor Experto en Innovación en el Sector Público). La experiencia de Canadá fue presentada por Joni Brennan (Presidenta, *Digital ID & Authentication Council of Canada* [DIACC]) y Rita Whittle (Directora Ejecutiva de Políticas de Gestión de la Identidad y Seguridad, *Treasury Board of Canada Secretariat*). También se contó con Mari Pedak (Consultora Senior de la *e-Governance Academy* de Estonia), Carlos Gómez Muñoz (Jefe del área informática en el Ministerio de Hacienda y Administraciones Públicas de España) y Paul Musser (Vicepresidente de Asociaciones Público-privadas, MasterCard).[4]

La edición de este documento estuvo a cargo de Alejandro Pareja, quien contó para su revisión con el apoyo de Ben Roseth (Especialista de ICS), Phil Keefer (Asesor Principal de IFD) y Estefanía Calderón y Florencia Serale (Consultoras de ICS). El documento está organizado del siguiente modo: primero se incluye una breve introducción donde se repasan los conceptos más importantes; seguidamente, se presentan las experiencias de Estonia y de España, a cargo de Mari Pedak y Carlos Gómez.[5]

---

[3] Las personas que satisfagan estas tres condiciones pueden considerarse ciudadanos digitales cabales.

[4] Este documento se complementa con cuatro videos con entrevistas a los panelistas: Joni Brennan (https://vimeo.com/223474418); Carlos Gómez (https://vimeo.com/223474381); Paul Musser (https://vimeo.com/223474614), y Mari Pedak (https://vimeo.com/223476203).

[5] Es importante aclarar que los textos de Pedak y Gómez reflejan sus respectivas visiones; es decir, no deben considerarse como análisis realizados por el BID ni debe asumirse, necesariamente, que el BID comparte sus visiones plenamente.

Introducción[6]

El significado más amplio del término "identidad" implica que la persona puede ser reconocida durante toda su vida. Las características que se utilizan para la identificación cambian con el tiempo de forma objetiva (atributos biométricos, cambios de nombre, etc.) o pueden ser cambiadas por la persona (nombre de usuario o contraseña, etc.). Un desafío importante en la actualidad es lograr manejar los atributos significativos de la identidad de una persona interfiriendo lo menos posible con su privacidad.

La identidad legal se plasma en lo que se conoce como **documentos de identidad fundamentales** (certificados de nacimiento para ciudadanos naturales, registros de inmigración para ciudadanos legales o residentes, o documento nacional de identidad en ambos casos). A partir de estos documentos se pueden generar los **documentos de identidad funcionales** (pasaporte, licencia de conducir, etc.) y las identidades digitales legales.

La criticidad de los sistemas de identidad ha ido en aumento por diversas razones. Por ejemplo, para el sector financiero, se pueden destacar las siguientes (Foro Económico Mundial, 2016): i) el creciente volumen de transacciones que requieren verificación de identidad derivado del incremento del uso de los canales digitales y de la conectividad entre entidades financieras; ii) requisitos de transparencia por parte de los reguladores, y iii) el riesgo de fraudes y daños reputacionales para las entidades.

Todo sistema de identidad cuenta con tres tipos de actores básicos (Deloitte, 2016): i) los **usuarios de servicios**, quienes obtienen una identidad a efectos de cumplir con la normativa y poder realizar transacciones; ii) los **proveedores de identidad**, quienes capturan y almacenan los atributos de la identidad de los usuarios, se aseguran de que sean verdaderos y llegan a completar transacciones en nombre de estos, y iii) los **proveedores de servicios** (básicamente, las empresas y el gobierno), quienes se apoyan en los proveedores de identidad a efectos de cumplir con el requerimiento KYC (del inglés “know your customer”, que podría traducirse como “sepa quién es su cliente”), en todos aquellos casos en los que las buenas prácticas lo aconsejen o la normativa lo requiera.

La gestión de estos sistemas de identidad combina procesos y tecnologías que potencian el uso de los datos identificatorios de las personas, y requiere: i) un **modelo de gobernanza y un modelo de negocio**; ii) un **marco legal** apropiado y actualizado; iii) la **simplificación y estandarización de procesos y sistemas**; iv) el establecimiento de mecanismos de **interoperabilidad** que faciliten la coordinación entre los diferentes organismos, y v) la promoción y coordinación del **ecosistema de uso de la identidad**.

Con el advenimiento de la **economía digital,**[7] las interacciones y transacciones que hasta ahora solo se realizaban en forma presencial están empezando a ejecutarse a través de sistemas de información interconectados y de la web. De allí surge la necesidad de tener en cuenta la **identidad digital** de cada persona, entendida como los elementos de hardware o software que permiten que una persona se identifique y sea autenticada, obtenga los permisos para acceder a determinados recursos de información o físicos (por

[6] Esta sección fue elaborada por Alejandro Pareja sobre la base del conocimiento reunido para el seminario.
[7] En el contexto de este documento se entiende por “economía digital” aquella donde la generación de valor se basa fuertemente en tecnologías de la información (o, dicho de otro modo, en el procesamiento digital de información).

ejemplo, el acceso a un área) y realice transacciones a través de Internet o redes privadas.

La identidad digital puede clasificarse en dos categorías:

1) **Identidad digital legal**: es la que requiere estar vinculada a la identidad legal de una persona física o jurídica. Es necesaria, por ejemplo, para realizar transacciones con el gobierno o con instituciones financieras reguladas.
2) **Identidad digital simple**: es aquella que no requiere estar vinculada a una identidad legal física. Se utiliza, por ejemplo, para conectarse a redes sociales.

Una de las formas más usuales de identidad digital es un nombre de usuario. En el caso de la identidad digital legal, es este nombre de usuario el que está vinculado a una identidad física. La vinculación se produce en el momento del enrolamiento.

La identidad digital suele tener validez en un determinado dominio: puede ser válida únicamente para interactuar con una institución o en una red social determinada o puede, en cambio, tener un reconocimiento más general (por ejemplo, en todo un país). Esto implica que una persona física puede tener más de una identidad digital, y utilizar cada una para una función o contexto diferentes. Lo que no puede suceder es que dos personas físicas tengan la misma identidad digital legal.[8]

Las personas y las organizaciones, tanto públicas como privadas, requieren para muchos tipos de interacción que se pueda verificar fehacientemente la identidad de la otra parte. En el mundo físico, el proceso de verificación de la identidad se basa en credenciales físicas, tales como la cédula de identidad, la licencia de conducir u otro tipo de documento, que acreditan la identidad de su portador de alguna forma.

En la economía digital es necesario identificar a las personas a distancia, sin mediar una interacción física, en la mayoría de los casos sin conocimiento previo de la otra parte y muchas veces siendo una computadora la encargada de ejecutar el proceso. Como consecuencia, la gestión de la identidad conlleva, por un lado, desafíos en cuanto a privacidad, protección de datos y nuevos riesgos de fraude y, por el otro, la necesidad de revisar y ajustar esquemas de gobernanza, marcos legales[9] y tecnologías que puedan estar quedando obsoletos.

En este nuevo contexto, el grado de complejidad del proceso de verificación de la identidad de las personas depende del objetivo final que se persiga. En particular, la complejidad depende del riesgo asociado a un posible error en la verificación. La comprobación de la identidad será tan fuerte como el mecanismo que se utilice para realizarla. Los sistemas de autenticación de usuarios fuertes son significativamente más caros.

[8] En este documento, a menos que se aclare lo contrario, de aquí en adelante se utilizará el término “identidad digital” para referirse a la “identidad digital legal”.
[9] Por ejemplo, las leyes que regulan la validez de una firma, en particular, la digital.

Los principales procesos de un sistema de identidad digital son los siguientes:[10]

1) Registro en un sistema de identidad digital. Se crea un usuario del sistema y se le asigna una credencial digital.[11] El enrolamiento puede ser presencial o en línea. En el primer caso, se suele firmar un compromiso de responsabilidad por el uso de la identidad digital. En el segundo caso, es común incluir un paso de confirmación a través de un enlace o una clave enviados al correo electrónico o teléfono del usuario.
2) Identificación y autenticación. Tiene lugar cuando se intenta acceder a algún sistema de información. Las personas se identifican mediante una credencial física o digital y, mediante la autenticación, se verifica que la persona sea quien dice ser.
3) Firma digital. Es un mecanismo informático que permite demostrar la autenticidad de un documento o mensaje.

La autenticación es un proceso clave en el mundo digital. Históricamente se ha sustentado en tres elementos (factores) que se utilizan para mejorar la robustez y seguridad del método, a saber:

1) Algo que la persona sabe: una clave o la respuesta a una pregunta personal.
2) Algo que la persona es: biometría dactilar, de iris, cara o voz.
3) Algo que la persona tiene: una tarjeta de identidad o de crédito, un certificado digital.[12]

Las buenas prácticas señalan que, para operaciones de riesgo alto, se debe utilizar una combinación de al menos dos de estos elementos.

La innovación en el terreno de la autenticación es constante. Entre las más recientes novedades se puede mencionar, para algunos servicios en línea, la adopción de mecanismos complementarios de seguridad de tipo adaptativo, basados en la historia de los usuarios (su perfil de navegación, geolocalización, perfil de uso de redes sociales, etc.).

Las firmas digitales se realizan a través de certificados digitales y permiten no solo dar consentimiento al contenido de un documento o mensaje sino asegurar su inviolabilidad y el no-repudio de la firma.

En el sector público de ALC, el grado de desarrollo de las transacciones en línea es muy bajo.[13] Por lo tanto, los mecanismos de autenticación digital son limitados y, en general, se restringen a usuario y clave. Varios países de la región han establecido una normativa

---

[10] A los que se detallan se pueden agregar la autorización para acceder a determinados recursos y los inherentes a la gestión (modificaciones y bajas del sistema).

[11] La credencial digital es un documento, archivo o identificador digital que en el mundo digital equivale a un documento de identidad físico. Al igual que en el mundo físico, los atributos de identidad contenidos en la credencial digital varían: pueden o no incluir biometría, firma, etc.

[12] Un certificado digital es un archivo digital que en el mundo digital cumple funciones similares a las de una tarjeta de identidad física que incluye la firma de la persona. Por lo tanto, el archivo contiene la identificación de la persona y su clave pública. Es parte del mecanismo que puede utilizar su dueño para firmar paquetes de información (documentos). Dicho de otra forma, el archivo dice quién es su dueño (identificación) a la vez que permite comprobar la firma digital que esa persona utiliza (autenticación). El archivo es emitido por un certificador autorizado cuya función es garantizar a terceros que la firma corresponde a la persona. El certificado puede estar grabado en el disco duro de una computadora, en el chip de un documento físico o en la nube.

[13] Véase un estudio sobre la calidad de los trámites en Pareja *et al.* (2016).

de firma digital, algunos hace más de 10 años; sin embargo, el nivel de uso es aún muy incipiente. Entre los principales factores causales de este bajo nivel de desarrollo se pueden mencionar: i) las escasas posibilidades de uso de los certificados, debido a la baja oferta de servicios que aceptan firmas digitales y al relativamente reducido número de casos de uso donde es necesaria una firma digital con certificado; ii) el costo para el usuario (considerable en sus comienzos); iii) la incomodidad que le representa al usuario tener que contar con un lector del dispositivo donde se almacena el certificado (*smartcard*, *token*-USB u otro), y iv) varios marcos normativos que pueden haber sido aprobados para emular a países avanzados, siguiendo una moda, más que teniendo en cuenta la situación local o manejando con realismo las expectativas de adopción.[14]

Gobernanza de los sistemas de identidad

Existen diversos modelos de gobernanza para los sistemas de identificación. Por un lado, hay países en los que una entidad pública central tiene las competencias exclusivas en cuanto a registro de nacimientos y al enrolamiento en el sistema nacional de identidad (junto a la correspondiente emisión del documento de identidad físico). En esta categoría figuran todos los países de América Latina.

Por otro lado, hay países donde no existe una única institución pública central que enrole y emita un documento nacional de identidad (por ejemplo, Canadá, Estados Unidos, Reino Unido y varios países del Caribe). En estos casos, suelen existir documentos de identidad funcionales. Por ejemplo, permiso de conducir, comprobante de registro en la seguridad social, pasaporte o documento electoral. Estos documentos de identidad coexisten y le corresponde a cada agente definir cuál acepta como comprobante de identificación de un individuo. En general, los ecosistemas con multiplicidad de documentos de identidad conllevan mayores riesgos de fraude. Por lo tanto, en estos casos se requiere una sólida coordinación entre los distintos emisores.

En algunos países, el número y el documento de identidad se emiten al momento del nacimiento, mientras que, en otros, se obtienen a la hora de abrir una cuenta bancaria, comenzar a estudiar, emprender una actividad económica, o para poder conducir o votar.

En cuanto a la identidad digital, hay países de la región donde la institución rectora del sistema de identidad también gestiona la identidad digital, sobre todo para su uso en la relación con el Estado. En ningún caso se trata de un proveedor exclusivo. Por el contrario, lo usual es que cada organismo implemente su propio mecanismo de autenticación. No obstante, algunos países de la región, como Chile y Uruguay, están avanzando en la implementación de un esquema *single sign-on*[15] para el sector público. Hay países donde el impulsor principal de la identidad digital única para el sector público es el organismo responsable del gobierno digital.

En el ámbito privado, en particular en el caso de las instituciones financieras, se observa una tendencia a desarrollar modelos propios de gestión de la identidad digital. Esto se debe a la criticidad y a los riesgos del proceso de autenticación para este tipo de

[14] Véase Andrews, Pritchett y Woolcock (2012). Los autores llaman a casos de este tipo "mimetismo isomórfico" (*isomorphic mimicry*).
[15] Con este esquema la persona se conecta con el mismo usuario y contraseña a cualquier sitio, en este caso, de gobierno. Un ejemplo que también cabe destacar es el de Francia: https://franceconnect.gouv.fr/.

instituciones e implica que haya pocas experiencias en las que una institución financiera contrate a otra empresa los servicios de autenticación de usuarios.

Costo y financiamiento de los sistemas públicos de gestión de la identidad

Las instituciones proveedoras de servicios de identidad se financian con una combinación de recursos provenientes del presupuesto nacional y de la venta de servicios. La proporción de ambas fuentes varía según el país.

Hay algunos servicios que suelen prestarse gratuitamente (como la emisión del certificado de nacimiento) y otros que no. Se suelen cobrar incluso servicios que son obligatorios para los ciudadanos (la renovación del documento de identidad, por ejemplo). También suelen venderse servicios a empresas (especialmente, a las del sector financiero), relacionados con la verificación de identidad.[16]

En cuanto a la identidad digital, habitualmente existe un bajo grado de conciencia respecto de los costos asociados (algo que también sucede en el sector privado), siendo muy común que se los incluya como parte del costo total de la gestión de las tecnologías de la información y, por lo tanto, no se los tenga cuantificados. Esto, en consecuencia, impide considerar alternativas con mejor relación costo-efectividad.

Los principales componentes del costo de gestión de la identidad digital son los siguientes:

1) Implementación y mantenimiento del soporte tecnológico, constituido por bases de datos, la plataforma PKI (por su sigla en inglés, *Public Key Infrastructure*),[17] el software de gestión de los datos de identidad y otras medidas de ciberseguridad.
2) Enrolamiento y revocación de certificados. Debido a su criticidad, en muchos casos es un trámite presencial, con el consiguiente alto costo tanto para la institución como para los ciudadanos.
3) Adquisición y mantenimiento de dispositivos que almacenan certificados (*tokens*, tarjetas, lectores, generadores de claves dinámicas, etc.).
4) Soporte a usuarios (por ejemplo, cuando olvidan su clave).

En el cuadro 2 se presenta, a modo de referencia, una estimación de los costos operativos de gestión de la identidad anuales por usuario:

[16] Por ejemplo, la solicitud de la filiación de una persona a partir de su huella dactilar.
[17] Se traduce como Infraestructura de Clave Pública y es la plataforma de generación, gestión y revocación de certificados digitales, que permite encriptar y desencriptar comunicaciones y documentos.

Cuadro 2. Costos operativos de la gestión de la identidad

Tipo de mecanismo	Costo anual por usuario (USD)
Usuario-clave	10 a 100[18]
Clave dinámica[19]	20 a 36[20]
Firma digital	50 a 180[21]

Estos costos, que son inevitables para que puedan realizarse transacciones a través de la web, podrían parecer significativos. Sin embargo, es bueno compararlos con los correspondientes a los otros canales de atención. En el caso del canal en línea, el costo operativo total incluye el costo de gestión de la identidad digital. En el cuadro 3 se presentan estos costos.[22]

Cuadro 3. Costos operativos por canal de atención (en USD)

Canal	Canadá	Reino Unido	Noruega	Australia
Presencial	7,42	15,32	14,01	19,61
Telefónico	4,57	5,89	7,01	7,66
En línea	0,11	0,44	0,53	0,46

Fuente: Elaboración propia sobre la base de Kernaghan (2012), Local Government Association (2014) y Deloitte (2015).

Beneficios e impacto de la identidad digital

Desde el punto de vista económico, se pueden considerar dos tipos de beneficios asociados con la identidad digital: i) los derivados directamente de la digitalización de procesos existentes que antes se ofrecían solo en forma presencial (por ejemplo, la verificación de identidad), y ii) los asociados al surgimiento de nuevos servicios y actividades económicas como resultado del uso de la identidad digital. El cuadro 3 presenta la ventaja desde el punto de vista operativo. A efectos de completar el análisis se deben considerar la reducción de costos transaccionales para los usuarios del canal en línea, básicamente por ahorro de tiempo y traslados. Esto arroja un impacto aún mayor, aunque difícil de determinar. De todos modos, parece razonable estimarlo en una hora-hombre (correspondiente a un ingreso medio) por transacción. Ahora bien, aun cuando el ahorro para los ciudadanos es claramente positivo, cabe resaltar que, al llevar los servicios a canales virtuales, se produce una externalización de costos hacia ellos. Esto se manifiesta, por ejemplo, en la necesidad de contar con un dispositivo para conectarse y en los costos de los certificados digitales, el servicio de conectividad y otros.

[18] Véase, por ejemplo, AT&T (2016).
[19] A las claves dinámicas se las denomina *one-time password* (OTP).
[20] Véase, por ejemplo, Lista de precios de Bitium (2017).
[21] Véase, por ejemplo, Productos y precios de DocuSign (2017).
[22] En el ámbito privado –es decir, en la industria financiera– se aprecian costos similares, entre canales presenciales y remotos.

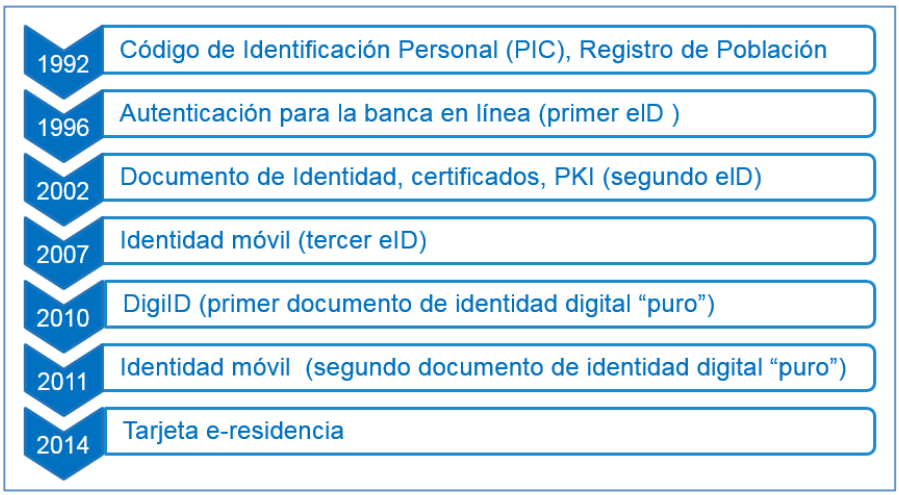
Respecto a las nuevas actividades económicas derivadas de la gestión de la identidad digital, se pueden mencionar las siguientes:

1) Ciberseguridad: necesaria para la protección ante fraudes, suplantación de identidad, etc.
2) Desarrollo de software específico para gestión de identidad que abarca las funcionalidades ya mencionadas.
3) Servicios privados de autenticación.
4) Gestión de certificados digitales por parte de organismos públicos y empresas emisoras de certificados.
5) Desarrollo y producción de dispositivos para autenticación y almacenamiento de certificados digitales.
6) Algunas actividades que se reducen o desaparecen, por ejemplo las asociadas a la atención presencial al público.

Estonia: del registro de población a la gestión de la identidad digital[23]

Estonia es uno de los países líderes en gestión de la identidad digital. Desde principios de los años noventa se fueron estableciendo algunos componentes esenciales de la gestión de la identidad en el marco legislativo (código de identificación personal, registro de población, etc.) (gráfico 1). En 1996, se inició el proceso de autenticación para la banca en línea. A partir de allí se produjo una evolución constante y en 2014 comenzó a emitirse la identidad digital para extranjeros que desean formar parte de la comunidad de residentes digitales de Estonia (*Estonia e-residents*).[24] Actualmente, el 98% de los residentes de Estonia cuenta con un documento de identidad que funciona como *token* para utilizar la identidad digital.

Gráfico 1. Hitos en la gestión de la identidad digital en Estonia



Fuente: Elaboración propia.

Identidad

En el corazón de la política de gestión de la identidad estonia se encuentran los siguientes principios: i) el Estado es el único responsable de identificar a las personas; ii) la gestión es centralizada; iii) cada persona debe contar con una y solo una identidad legal, y iv) el vínculo entre el documento físico y el certificado digital es inequívoco y verificable públicamente a través de un elemento fundamental en el sistema estonio: el código de identificación personal (PIC, por su sigla en inglés), que se puso en vigor en 1992.

En tiempos donde la identificación de la persona se limitaba al mundo físico, la presencia física de la persona, en gran medida, compensaba la necesidad de contar con un identificador único legal. Si bien muchos estados incluyeron un código numérico de identificación personal en los documentos de identidad, su ausencia no causaba ninguna

[23] La autora de esta sección es Mari Pedak, experta en identidad digital de la Academia de Gobierno Electrónico de Estonia (eGA). Véase la aclaración al final del resumen ejecutivo.
[24] Estonia lleva otorgadas 12.000 residencias digitales. Véase https://e-estonia.com/e-residents/about/.

consecuencia seria. El desarrollo de los servicios electrónicos ha cambiado completamente la situación: la existencia de un identificador único pasa a ser un requisito previo para el establecimiento de un marco de identificación fuerte.

El PIC es un número de 11 dígitos. Contiene información personal (género y fecha de nacimiento), a diferencia de otros países donde el número de identidad es completamente secuencial y, por lo tanto, no contiene ninguna información personal. El PIC se asigna cuando la persona se inscribe en el Registro de Población.

En culturas y contextos históricos diversos, la actitud respecto del número de identificación es diferente. En Europa hay países donde la asignación de números a las personas va en contra de su memoria histórica o social. Algunos países consideran que el número de identificación personal o los datos que contiene son sensibles y, aun cuando exista, su uso es muy limitado.

Muchas veces las discusiones sobre el identificador único se enfocan, precisamente, en si el mismo debe o no reflejar atributos de la persona, algo bastante irrelevante. El identificador único es necesario para asegurar una identificación inequívoca e incondicional de los consumidores de servicios electrónicos en procesos de autenticación segura y de intercambio de datos. Debido a que las tecnologías de la información modernas ofrecen nuevas formas de identificador único, se espera que la discusión sobre la forma que debe tomar el identificador ceda paso a un debate más sustantivo.

El registro de población como base de la gestión de la identidad

El registro de población en Estonia incluye los eventos cubiertos por el registro civil y otros, entre los cuales figura el registro del domicilio. El registro de población es el resultado de un proceso en el que la información sobre los acontecimientos de la vida, originalmente registrados en diferentes sistemas administrativos, se vincula automáticamente de forma continua.

Los distintos sistemas administrativos reciben datos de las personas y son, al mismo tiempo, una fuente de datos. El registro de población se nutre de las listas de votación, del censo, del proceso de emisión de documentos de identidad, de los sistemas de registro civil y del registro de residencia; es decir, que los datos para el registro de población son recolectados por el sector público al proveer distintos servicios.

Con la difusión de los registros digitales y el intercambio automatizado de datos, la relevancia de los datos o, en otras palabras, la calidad de los datos y su mantenimiento se han vuelto cruciales. Los datos obsoletos o inexactos se transmiten en tiempo real a lo largo del país, o incluso a través de las fronteras nacionales, lo que puede implicar consecuencias negativas para las personas.

Sobre la base de la experiencia de Estonia, a fin de garantizar la calidad de los datos se recomienda establecer una jerarquía de registros y asignar a diferentes instituciones la "propiedad" de subconjuntos de datos específicos. Sin esto, es probable que se produzcan superposiciones innecesarias de procesos y bases de datos, lo que conduce a una duplicación inútil del gasto en equipamiento y tecnología. Además, terminará almacenándose la misma información en diferentes formatos en diferentes registros, causando confusión y dificultando el desarrollo del sistema en su conjunto. El registro civil es una buena opción para mantener el conjunto principal de datos personales.

El establecimiento de tal jerarquía asegura que todos los procesadores de datos estén utilizando los datos correctos, suministrados por la institución oficialmente propietaria (exclusiva) de los mismos. Y si se descubren datos personales erróneos, las correcciones

solo pueden y deben realizarse por dicha institución propietaria, después de lo cual todos los procesadores de datos pueden utilizar el conjunto de datos corregido.

La identidad digital y sus ecosistemas

Los esquemas digitales de identidad pueden clasificarse en tres tipos: i) aquellos con bajo nivel de seguridad (por ejemplo, *passwords*); ii) aquellos basados en PKI (por ejemplo, documento electrónico), y iii) los que se basan en *blockchain*. A continuación, se describe cada uno de ellos y su uso en Estonia.

Esquema de identidad con bajo nivel de seguridad

Estos sistemas de identidad digital utilizan medios como tarjetas de contraseña y calculadoras de PIN.[25] A pesar de la inseguridad de estos esquemas, son los que predominan en el mundo digital. La autenticación de nombre y contraseña prevalece en las redes sociales. Lamentablemente, muchos países y grandes proveedores de servicios solo ofrecen esquemas de este tipo.

Incluso en Estonia, la sociedad de la información más avanzada, cerca de 25% de los usuarios del portal del Estado utilizan estos mecanismos de autenticación. Las razones detrás de la popularidad, derivadas de su éxito en el sector financiero, incluyen: i) el inicio relativamente temprano de la banca electrónica en Estonia (1996) que incluyó el suministro de servicios de autenticación a terceros; ii) un nivel muy alto de adopción de la banca electrónica por parte de las personas (cerca del 100%), y iii) la sencillez de su utilización (no se necesita un hardware especial, por ejemplo, un lector de tarjetas inteligentes, ni instalar ningún software).

Esquema de identidad basado en PKI

La seguridad de los esquemas de identidad digital basados en PKI se construye a partir de criptografía asimétrica. Se utiliza una clave criptográfica, la cual se divide en dos partes: la clave pública y la clave privada. La clave pública es administrada por el proveedor de identidad. Los sistemas difieren en los métodos de almacenamiento de claves privadas.

Los más comunes son los esquemas en los que la clave privada se encuentra en el chip de un documento de identidad digital o en una tarjeta SIM de teléfono celular (estos esquemas son los que se utilizan en Estonia). Esto asegura la protección de la clave por parte de su propietario.

Hay países como Dinamarca que no emiten documento nacional de identidad, donde las claves privadas son administradas centralmente por el gobierno, un sistema que se conoce como nemID.[26] Las claves privadas almacenadas centralmente también pueden guardarse con bastante seguridad usando medidas de seguridad técnicas y organizativas. Sin embargo, no están bajo el control de sus dueños. Tales soluciones son posibles en aquellos países donde las personas confían tanto en su gobierno que están dispuestas a

---

[25] La tarjeta de contraseña es una tarjeta física con una serie de números y en cada nuevo intento de inicio de sesión el sistema pide un número diferente de la tarjeta. La calculadora de PIN genera un nuevo código aleatorio en forma periódica (por ejemplo, cada 30 segundos). Originalmente, el usuario consultaba el PIN en un *token*. Más recientemente, la consulta se hace mediante una *app*. Ambos esquemas son implementaciones del modelo OTP, ya que la contraseña correcta es diferente y aleatoria en cada intento de inicio de sesión. Esto hace que el robo de contraseñas no tenga sentido.

[26] https://www.nemid.nu/dk-en/.

creer que se excluye el uso indebido de sus claves privadas. Dado que el uso de los servicios de identidad digital está directamente relacionado con la confianza,[27] es aconsejable dar prioridad a los esquemas en los que cada persona gestiona su propia clave privada.

El documento de identidad estonio se basa en la tecnología PKI e incorpora dos certificados: uno para autenticación y otro para firmas digitales. Para usar las claves privadas es necesario usar un código PIN. Además, el chip contiene un archivo que replica los datos visibles en la tarjeta. No hay información biométrica electrónicamente utilizable en el documento.

La identidad móvil fue introducida en el mercado estonio en mayo de 2007 por la mayor operadora móvil (EMT) en cooperación con el centro de certificación SK. Para obtener una identidad móvil, el usuario debe reemplazar la tarjeta SIM por una que sea compatible con la PKI. A pesar de que el proceso de registro está a cargo del operador móvil, no puede considerarse lo suficientemente fiable. Por lo tanto, el usuario debe activar su identidad móvil en el entorno web. La identidad móvil no requiere un lector de tarjetas inteligentes conectado a la computadora ni instalar ningún software específico. Los certificados de identidad móvil contienen la misma información personal que los certificados del documento de identidad.

Blockchain

En los esquemas discutidos previamente siempre hay un tercero que funge como garante de identidad (por ejemplo, el gobierno). Las nuevas tecnologías permiten prescindir de este tercero, es decir, desintermediar. La tecnología más conocida en este sentido es *blockchain*, que ha ganado gran reputación como componente central de las criptomonedas. Si se usara *blockchain*, toda la comunidad sería la garante de la identidad de una persona, mientras que la clave privada sería administrada por los propios individuos usando una cartera digital o un papel. Ya existen servicios basados en *blockchain* que se ofrecen en el mercado estonio. Por ejemplo, la empresa GuardTime ofrece servicios de firma digital basados en *blockchain*.

Actores involucrados en el ecosistema de la identidad digital

Las partes interesadas del ecosistema abarcan las relacionadas con la producción de portadores de identidad, la atribución de identidad digital y la habilitación de su uso.

En Estonia hay principalmente dos ministerios involucrados en este tema:

1) El Consejo de Policía y Guardias Fronterizas, subordinado al Ministerio del Interior (MI), es directamente responsable de la emisión y el mantenimiento de los documentos de identidad personal y de las identidades electrónicas de los residentes en general. El Centro de Informática y Desarrollo, también subordinado

[27] Los sistemas de identidad y firma digitales, al igual que los sistemas físicos, requieren de un tercero que garantice a las partes que una persona o máquina es quien dice ser. En el mundo físico, para probar la identidad se muestra un documento de identidad. Quien quiera verificar esa identidad, basta con que observe la foto y otros datos personales que figuran en la tarjeta y los compare con la persona que tiene delante. Implícitamente, el verificador confía en los datos de la tarjeta porque confía en que el emisor de la misma ha hecho las verificaciones correspondientes y el documento es seguro (difícil de falsificar). En el mundo digital ocurre algo similar (véase la nota 12). Quien recibe un documento firmado coteja, con el certificador autorizado que otorgó el certificado al firmante, que la firma corresponde a la persona. Y confía en lo que diga dicho certificador ya sea por su prestigio o porque el gobierno (en tanto autoridad certificadora raíz) asegura que es confiable.

al MI, es responsable del mantenimiento y desarrollo de los correspondientes sistemas informáticos y bases de datos del registro de población y de los documentos de identidad.
2) La Autoridad Estatal de Sistemas de Información (RIA), subordinada al Ministerio de Asuntos Económicos y Comunicaciones (MEAC), es responsable de la coordinación gubernamental en el campo de las TI, el uso de la identidad digital y la seguridad de los ecosistemas digitales.

La visión en Estonia es que únicamente los gobiernos pueden crear el marco que proporcione el grado de armonización necesario para la gestión de la identidad digital a nivel nacional. El sector privado, por su lado, desempeña un papel significativo en el ecosistema estonio. La fabricación y la personalización de los documentos de identidad son subcontratadas a la empresa TRÜB Baltic AG. Los servicios de certificación y validación son proporcionados por la empresa SK. RIA y SK funcionan como un centro de excelencia para el uso electrónico del documento de identidad, proporcionando software para el uso de documentos de identidad electrónica –incluido el marco de software de firmas digitales–, soporte al usuario final y servicios a proveedores de servicios que utilizan el documento de identidad. En la actualidad, debido a su pequeño tamaño de mercado, solo hay una autoridad certificadora (emisor de certificados digitales) en Estonia.

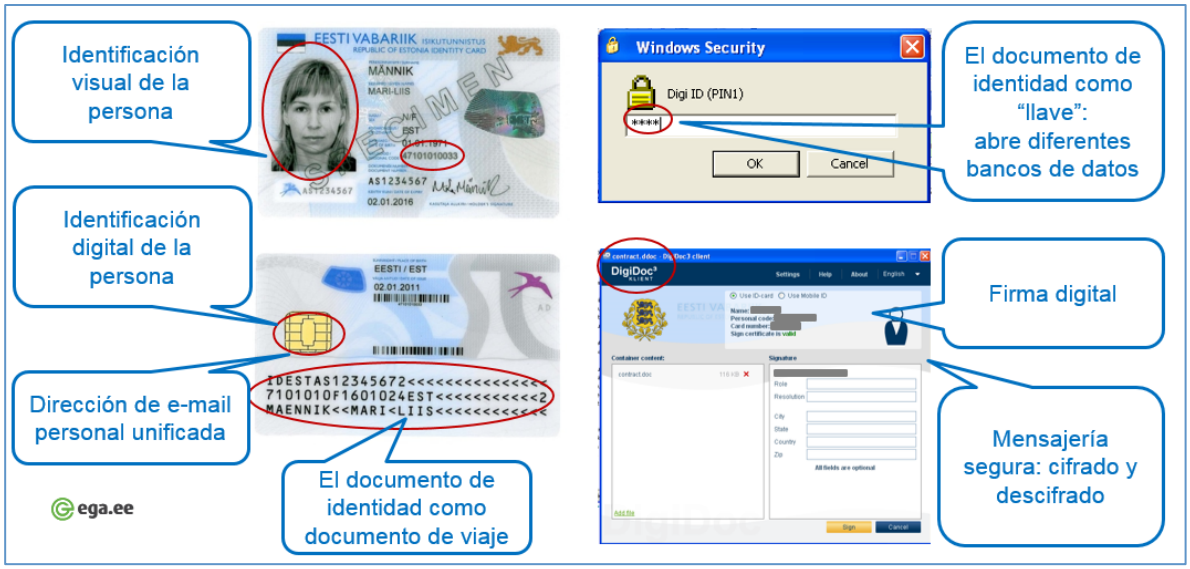
Documento de identidad digital

La puesta en marcha del documento de identidad en Estonia se inició en 2002 (gráfico 2). El despliegue se consideró terminado en octubre de 2006, cuando se superó el umbral de 1 millón de documentos expedidos. Desde entonces, el número de documentos activos se ha mantenido en torno a 1,1 millones. El documento de identidad es válido por un máximo de cinco años[28] y es obligatorio desde los 15 años de edad. Permite la identificación física, la identificación, autenticación y firma digitales, la encriptación y desencriptación de mensajes, y también es válido como documento de viaje dentro de Europa.

Tanto el documento de identidad como los certificados que contiene no son válidos hasta que se los activa. Esto se produce cuando se le entrega al usuario. Cuando se emite el documento, el receptor puede optar por mantener inactivos los certificados, es decir, por no tener una identidad digital. En ese caso, el documento solo se puede utilizar como un documento de identidad tradicional. Generalmente, esta opción es muy poco utilizada.

[28] La idea de vencimiento de los documentos de identidad está asociada, principalmente, a las variaciones de los atributos de identidad que se dan durante la vida de una persona (los cambios se dan en la fisonomía y en algunos datos personales que figuran en el documento, por ejemplo, el domicilio) y a la necesidad de reflejar esos cambios para que el documento pueda utilizarse para verificar identidad o residencia. Por otro lado, la evolución tecnológica, tanto en la producción de tarjetas de identidad como en la de certificados digitales, tendente a brindar mayor seguridad a los mismos y, en consecuencia, mayor confianza al sistema, también es un factor que lleva a aconsejar una duración limitada. Hay países, por ejemplo Estonia, donde los documentos tienen una vigencia de cinco años; en otros, de 10, y en algunos otros, como Brasil, los hay de duración ilimitada.

Gráfico 2. Documento de Identidad de Estonia



Fuente: Elaboración propia.

En octubre de 2010 se inició la emisión de una tarjeta de identidad exclusivamente digital (DigiID) (infografía 1). Tiene solamente la funcionalidad digital del documento de identidad principal y por lo tanto no se puede utilizar para la identificación física de una persona. Cada DigiID está asociada con un documento de identidad principal y contiene una segunda identidad digital. La tarjeta está hecha de PVC y no tiene características de seguridad.

El propósito de DigiID es permitir a las personas distinguir su identidad digital entre acciones privadas y acciones tomadas como miembros de una organización, por ejemplo, en cuanto empleados. DigiID se suele conservar y utilizar en el trabajo (maestros en la escuela, médicos en los hospitales, funcionarios del gobierno en sus oficinas, etc.), mientras que el documento de identidad principal se lleva consigo.

Infografía 1. Tarjeta de Identidad Digital (DigiID) de Estonia

Fuente: https://www.politsei.ee/et/nouanded/dokumentide-naidised/digi-id/kuni-30112014-valja-antud-digi-id.dot.

El documento de identidad estonio es multifuncional y se utiliza en todas las áreas de los servicios públicos. Así, por ejemplo, en Estonia no existe una tarjeta de seguridad social separada y no hay necesidad de llevar la licencia de conducir y los documentos del coche porque la policía de tráfico puede consultar las respectivas bases de datos en tiempo real a partir de la identificación contenida en el documento de identidad.

El uso de la biometría en los documentos de identidad digitales es un tema recurrente, especialmente en los países donde el nivel de alfabetización digital es bajo. El chip de los documentos de viaje seguros y modernos contiene características biométricas de la persona, que pueden compararse (por ejemplo, en las fronteras) con las características físicas de la persona capturadas en el momento (verificación uno a uno). El uso de la biometría en los documentos de viaje ha brindado mayor seguridad al movimiento transfronterizo de personas.

Sin embargo, las opiniones difieren significativamente cuando se trata de la inclusión de biometría en documentos de identidad para su verificación frente a bases de datos (verificación uno a muchos). Por ejemplo, el chip del documento de identidad de Estonia no contiene datos biométricos y, al mismo tiempo, se utiliza desde 2002 de forma segura tanto para la autenticación como para la firma digital. **La experiencia de Estonia demuestra que el uso de la biometría no es necesario para crear un ecosistema seguro en un país con alfabetización digital avanzada**. Cuando a finales de 2014 se preparó la adquisición para la próxima generación de documentos de identidad y se realizaron consultas con expertos en seguridad cibernética y protección de datos, ninguno de ellos apoyó la introducción de biometría en el documento de identidad, ya que la consideran una solución insegura. El uso de biometría solo fue apoyado para una solución *match-on-card*, análoga a los documentos de viaje. Ahora bien, este ejemplo no debe sobreestimarse ya que en países donde el nivel de alfabetización digital es bajo (lo que conlleva una necesidad mayor de verificaciones de identidad presenciales), la utilización de biometría en la comprobación de identidad puede ser la única opción viable.

Usos de la identidad digital

La legislación estonia distingue entre autenticación y firma digital, dejando la autenticación fuera del ámbito de aplicación de la ley. Esto quiere decir que no existe regulación respecto a la jerarquía de los diferentes sistemas de autenticación. Los reglamentos que sí existen suelen restringirse a aplicaciones o áreas específicas. Los métodos de autenticación basados en PKI son los preferidos en el sector público. Existen tres métodos de autenticación: mediante el documento de identidad, la identidad móvil o la identidad bancaria.[29] Todos se utilizan ampliamente en los servicios que requieren identidad legal, tanto en el sector público como en el privado. Por ejemplo, los estonios usaron el portal de servicios estatales @eesti.ee más de 3,5 millones de veces en 2015. El 54% se autenticó con documento de identidad, el 38%, con identidad bancaria y el 8%, con identidad móvil.

En cuanto a la firma digital, tras 15 años de uso se ha convertido en el sistema de firma digital más fiable y utilizado del mundo. Hoy en día se generan en Estonia aproximadamente 7 millones de firmas digitales por mes.[30] En realidad, una de las principales razones de la introducción del documento de identidad era que los estonios pudieran contar con un medio que les permitiera firmar digitalmente. Desde el inicio se vienen distribuyendo herramientas gratuitas para usuarios finales e integradores de sistemas. Como resultado, los estonios comparten una visión común sobre lo que son los documentos firmados digitalmente, los cuales son ampliamente aceptados, incluso por los tribunales. Este desarrollo ha dado lugar a un uso masivo de firmas digitales, reemplazando totalmente a las firmas manuscritas. En la banca electrónica se usan masivamente, ya que todas las transacciones deben estar firmadas digitalmente (siempre que el usuario haya iniciado sesión con un documento de identidad o una identidad móvil).

Aunque no debería, la introducción de nuevas tecnologías y nuevos métodos en ocasiones plantea la cuestión de las ganancias en términos de eficiencia. Se ha estimado que la introducción de una firma digital ahorra en promedio 20 minutos por transacción[31] y que, también en promedio, una persona realiza una transacción que requiere firma cada tres días. Esto equivale a aproximadamente una semana de trabajo por año. Por lo tanto, Estonia ahorra anualmente 2% de su PIB por ser una sociedad sin papeles.[32]

El despliegue de la autenticación digital y la firma digital también habilitaron la optimización de servicios públicos. Algunos servicios específicos experimentaron ahorros de tiempo incluso mayores. Por ejemplo, el registro de empresas acumuló ahorros de tiempo para el empresario que son 17 veces mayores que el promedio.

La autenticación y la firma digital son servicios de plataforma, que pueden ser utilizados por cualquier servicio electrónico. Una variedad importante de servicios de identificación se puede construir sobre los servicios de plataforma, tales como el acceso a edificios, los pagos electrónicos, la fidelización de clientes etc. (Electronic Identity, 2015).

---

[29] La identidad bancaria es un método basado en certificados digitales provistos por los bancos, que asumen así un rol de garantes de la identidad de las partes de una transacción digital.
[30] http://www.id.ee/?lang=en&id.
[31] World Development Report 2016: Digital Dividends.
[32] https://e-estonia.com/facts/.

Promoción del uso de la identidad digital

El papel crítico de la confianza en el contexto de la administración electrónica no puede sobreestimarse. La confianza no se deriva únicamente de una infraestructura técnica segura, que es en la que se han centrado la mayoría de los países. Es preciso generar confianza. Y los mejores resultados se obtienen cuando existe colaboración entre el sector público y el privado. Pero tan importante como la confianza es la sensibilización de los ciudadanos. Lamentablemente, este aspecto se mantuvo en un segundo plano en todos los países pioneros, incluida Estonia.

Al introducir la identidad digital, los países se enfrentan a la situación clásica del huevo y la gallina. Por un lado, los servicios electrónicos no comienzan a desarrollarse hasta que haya un número suficientemente grande de consumidores que justifiquen los costos. Al mismo tiempo, apenas reciben un documento de identidad digital del gobierno, las personas comprensiblemente desean comenzar a utilizarlo con entusiasmo. Esto implica que, durante el despliegue, hay un desajuste entre demanda y oferta, el cual debe gestionarse para que el proyecto no se descarrile y la confianza no se deteriore. En Estonia, esta situación duró cuatro años. Los proveedores de servicios comenzaron a hacer esfuerzos para desarrollar servicios recién cuando se llegó a 1 millón de identidades digitales. En este sentido, las campañas de sensibilización son esenciales en esta etapa para poder mantener informada a la población respecto de lo que cabe esperar de la identidad digital, cuáles serán sus beneficios y cuándo se los podrá disfrutar.

En Estonia, las campañas de formación y sensibilización comenzaron con el proyecto en 2002 y aún continúan, y abarcan: i) cursos de alfabetización digital (especialmente para adultos mayores); ii) cursos de comportamiento seguro en Internet y uso seguro de dispositivos inteligentes, y iii) apoyo y promoción de actividades extracurriculares relacionadas con informática para jóvenes, con el fin de aumentar el número de jóvenes que eligen estudiar ciencias o TI.[33]

España: gestión de la identidad y economía digital[34]

La identidad digital, y muy vinculada a ella, la firma digital, han estado presentes de manera continua en las políticas públicas españolas destinadas al desarrollo de la sociedad de la información y el conocimiento, como elementos fundamentales para garantizar la confianza en las transacciones en línea. En su condición de Estado miembro de la Unión Europea, estas políticas públicas en España siempre se han enmarcado en el contexto más amplio de las políticas de la UE, en las que la identidad y la firma digitales se han considerado de manera usual como habilitadores esenciales para llevar a cabo el mercado único europeo y para facilitar la movilidad de ciudadanos y empresas. Estas políticas están plasmadas en la Agenda Digital europea y su Plan de Acción de Administración Electrónica (2011-15), el Programa de Trabajo ISA de servicios de interoperabilidad para las Administraciones, y la Directiva Europea sobre Servicios Electrónicos.

---

[33] http://www.vaatamaailma.ee/en/.

[34] El autor de esta sección es Carlos Gómez Muñoz, Jefe de Informática de la Dirección de Tecnologías de la Información y las Comunicaciones del Ministerio de Hacienda y Función Pública de España. Véase la aclaración al final del resumen ejecutivo.

En el caso español, el plan España.es (2003–05) contemplaba varias medidas para garantizar la seguridad y confianza en las redes digitales, entre las que se encontraba el desarrollo del Documento Nacional de Identidad electrónico (DNI-e) y el establecimiento de un marco legal para la firma digital. Esta preocupación por la seguridad y confianza en línea tuvo su continuidad en los planes posteriores Avanza (2006-10) y Avanza 2 (2011-15), y en la actual Agenda Digital para España, que prevé medidas para facilitar los mecanismos de identificación y autenticación frente a la Administración, y para impulsar los servicios de confianza en el mundo digital.

Si bien las políticas mencionadas han tenido su desarrollo en los primeros años del siglo XXI, las primeras medidas para implantar en España sistemas de identificación y firma digital con carácter general (es decir, que puedan utilizarse en varios servicios electrónicos de proveedores diferentes) datan de finales del siglo XX, con la puesta en marcha del proyecto CERES (CERtificación ESpañola).

Inicios de la firma digital

El proyecto CERES fue iniciado en 1996 por la Fábrica Nacional de Moneda y Timbre de la Real Casa de la Moneda, en un momento en el que comenzaban a desplegarse las primeras PKI. El objetivo del proyecto era constituir un Prestador de Servicios de Certificación de carácter público, que garantizara la autenticidad, la integridad, la confidencialidad y el no repudio de las transacciones electrónicas que realizan los ciudadanos, las empresas y las Administraciones Públicas. Para fomentar su adopción, se definió un modelo de negocio en el que los certificados digitales serían gratuitos para los ciudadanos, financiándose el sistema con las contribuciones de los proveedores de servicios electrónicos que utilizaban ese sistema de identificación y firma digital.

La primera experiencia de utilización generalizada del sistema tuvo lugar en 1999, cuando la Agencia Estatal de Administración Tributaria permitió el uso de la certificación digital en la presentación telemática del impuesto sobre la renta de 1998, cuando se realizaron más de 20.000 declaraciones por este medio. Desde entonces, se ha ido ampliando el conjunto de servicios públicos en los que se pueden utilizar los certificados emitidos por CERES, así como el número de ciudadanos y empresas que disponen de dichos certificados, hasta llegar a cerca de 4 millones de certificados de persona física activos en 2014.

También en 1999 se aprobó la Directiva europea sobre firma digital,[35] que tenía como objetivo facilitar el comercio electrónico en el mercado único, para lo cual establecía un marco regulatorio para el mercado de prestadores de servicios de certificación. Al tratarse de una Directiva, su contenido debía ser desarrollado a nivel nacional, lo que ocurrió en España con la trasposición de la Directiva en la Ley de Firma Electrónica.[36] Esta Ley constituye un fundamento básico ya que otorga a la firma digital plena validez jurídica, reconociendo la equivalencia funcional entre la firma digital reconocida[37] y la manuscrita.

[35] Directiva 1999/93/CE del Parlamento Europeo y del Consejo.
[36] Ley Nº59/2003.
[37] Es la que se realiza con un dispositivo seguro, utilizando certificados electrónicos emitidos con las máximas garantías previstas.

La introducción del DNI-e

La Ley de Firma Electrónica, además de regular el mercado de prestadores de servicios de certificación en España,[38] previó la existencia del DNI-e como medio de identificación y firma, en conjunto con el programa España.es.

El DNI-e se hizo realidad en 2006, cuando comenzaron a emitirse las primeras unidades que incorporaban un chip en la tradicional tarjeta del DNI. El chip, además de los datos biométricos y de identificación, contenía dos certificados digitales, uno de autenticación y otro de firma. Desde entonces se ha ido sustituyendo a los antiguos DNI sin chip por los nuevos DNI-e, hasta cubrir hoy en día a prácticamente toda la población española, que está obligada a portar un DNI.

Si bien el DNI es obligatorio para todos los ciudadanos españoles mayores de 14 años, no ocurre lo mismo con su uso como medio de identificación y firma digitales, que es totalmente voluntario. La identidad digital incluida en el DNI-e requiere la activación por parte del ciudadano para poder utilizarse. Por otro lado, el usuario debe disponer de un lector de tarjetas. Estos aspectos, sumados a la aparición de problemas de compatibilidad con algunas plataformas y la escasa oferta de servicios que lo aceptan en el sector privado, han motivado que el uso real esté por debajo de las expectativas.

Se espera que el nuevo DNI-e 3.0, vigente desde enero de 2015, ayude a superar las barreras que obstaculizan el uso, al incorporar entre sus mejoras la posibilidad de acceder al chip sin necesidad de tener un lector de tarjetas, mediante la tecnología NFC[39] presente en muchos smartphones y tabletas.

Acceso electrónico a los servicios públicos

En 2007 se aprobó la Ley de acceso electrónico de los ciudadanos a los servicios públicos.[40] Su objetivo era impulsar el desarrollo de la administración electrónica en España, para lo cual otorgó a los ciudadanos el derecho a relacionarse electrónicamente con las Administraciones Públicas, que, a su vez, estaban obligadas a proveer los medios para posibilitar la relación. Como resultado de su aprobación, se desarrollaron la mayor parte de las infraestructuras de administración electrónica que actualmente funcionan en España.

En lo que respecta a la identificación digital, la mencionada ley consolidó un modelo en el que los ciudadanos disponían de tres opciones para identificarse electrónicamente frente a la Administración: i) utilizar su DNI-e, cuya aceptación es universal en los servicios públicos; ii) utilizar uno de los certificados electrónicos admitidos por la Administración en particular con la que se relaciona, o iii) utilizar un sistema de identificación no basado en certificado (por ejemplo, usuario y contraseña), específico del servicio al que se quiere acceder.

Debido al elevado número de prestadores de servicios de certificación existentes en España, el uso de certificados para el acceso a los servicios públicos planteaba un problema práctico, pues cada Administración debía establecer conexiones con cada uno de los prestadores. Además, la variedad de algoritmos y formatos de firma existentes

---

[38] Este mercado en la actualidad es uno de los más desarrollados de Europa, con más de 50 prestadores, de los cuales 25 están cualificados.
[39] *Near Field Communication* es una tecnología que habilita transacciones y pagos de bienes y servicios.
[40] Ley Nº11/2007.

multiplicaba la complejidad de la gestión de los documentos firmados. Para solventar este problema se desarrolló la plataforma @Firma, que actúa como intermediador entre las Administraciones y los prestadores. Así, la plataforma permite la validación de identificaciones y firmas realizadas con un certificado emitido por cualquier prestador reconocido por el Ministerio de Industria, Energía y Turismo (entre ellos los del DNI-e), simplificando enormemente el despliegue de aplicaciones de administración electrónica. @Firma también proporciona aplicaciones y componentes para realizar firmas (en PC o dispositivos móviles) y servicios de sellado de tiempo para formatos de firma longeva.

Por otra parte, la alternativa que esta ley permitía a cada servicio público de utilizar sus propios sistemas de identificación no basados en certificados llevó a que muchas entidades optaran por esta solución, lo que condujo a una situación ineficiente tanto para los propios ciudadanos, que se veían obligados a registrarse y a gestionar sus credenciales de manera independiente en cada servicio, como para las propias Administraciones, que debían dedicar recursos para el desarrollo y mantenimiento de estos sistemas.

Para corregir esta situación, en 2014 se puso en marcha el proyecto Cl@ve, destinado a implantar una plataforma común para la identificación, autenticación y firma electrónica mediante el uso de claves concertadas. El objetivo de este sistema era unificar todas las soluciones existentes, habilitando sistemas de identificación no basados en certificados electrónicos que pueden usarse en todos los servicios públicos. Para ello se apoyaba en dos sistemas ya existentes, uno de la Agencia Tributaria, que daría lugar al sistema Cl@ve PIN (para uso ocasional), y otro de la Seguridad Social, que daría lugar al sistema Cl@ve Permanente (para uso frecuente).

El sistema Cl@ve se complementa con Cl@veFirma, una solución de firma digital en la que los certificados digitales residen en un servidor. Con Cl@veFirma se evitan los problemas asociados con la gestión y el acceso a los certificados en el dispositivo del usuario, manteniendo todas las ventajas del uso de la firma digital.[41] Estos certificados de firma son emitidos por la Dirección General de la Policía, igual que los del DNI-e. El acceso al certificado para firmar se produce con la Clave Permanente del usuario, en la modalidad de nivel de seguridad reforzado.

Para poder utilizar el sistema Cl@ve es necesario que el ciudadano se haya registrado previamente, con una verificación previa de su identidad. Este registro puede realizarse: i) de manera presencial; ii) en línea con un certificado electrónico, y iii) en línea, sin certificado, pero proporcionando información que solo conocen el ciudadano y la Administración (esta modalidad habilita solamente a acceder a servicios de nivel de seguridad básico).

Aunque el alcance inicial del sistema Cl@ve se correspondía con el ámbito de la Administración estatal, donde es obligatorio su uso, desde el principio se abrió el sistema al resto de las Administraciones, que podían utilizarlo de manera voluntaria. No obstante, esta situación cambió recientemente con la puesta en vigor de la Ley del Procedimiento Administrativo Común de las Administraciones Públicas,[42] que exige que todas las Administraciones Públicas españolas acepten los sistemas de identificación usados por la Administración del Estado.

---

[41] Compárese con el caso de Estonia.
[42] Ley Nº39/2015.

Esta ley y la Ley de Régimen Jurídico del Sector Público[43] conforman el nuevo marco legal para la actuación administrativa en España, y dan el impulso definitivo a la administración electrónica, al establecer que la actividad de la Administración, tanto en sus relaciones internas como externas, debe ser digital.

Las principales novedades de la ley tienen que ver con la clara separación de la identificación y la firma, la simplificación del uso de ambas y la reducción de los actos en los que es necesario la firma. Además, la Ley está plenamente alineada con el Reglamento europeo eIDAS,[44] el cual define el marco general para la identificación electrónica y los servicios de confianza digital en la Unión Europea, y está destinado a ser uno de los referentes fundamentales de la identificación electrónica en el futuro.

Identificación en el marco de la Unión Europea

El Reglamento eIDAS consta de dos partes diferenciadas, una dedicada a la identificación electrónica transfronteriza, y otra, a los servicios de confianza.

En lo que respecta a la identificación electrónica, aunque el alcance del reglamento afecta únicamente a la identificación electrónica transfronteriza, su impacto también se está dejando notar a nivel nacional, donde los Estados miembros están alineando sus estrategias nacionales de identificación electrónica con las disposiciones del reglamento. Para ello, se están implantando sistemas de identificación de alcance nacional y categorizando los sistemas de identificación y los servicios que hacen uso de ellos de acuerdo con los niveles de seguridad que marca el reglamento; a su vez, se está estudiando cómo habilitar el acceso del sector privado a estos sistemas de identificación, pues el reglamento prevé su utilización de manera opcional.

En lo que respecta a los servicios de confianza, el reglamento persigue la creación de un mercado único, de manera que los servicios de identificación proporcionados por un prestador ubicado en cualquier país de la Unión Europea puedan ser utilizados en el resto sin ninguna limitación. De esta forma, se procura resolver los problemas causados por la Directiva de Firma, cuya trasposición a nivel nacional se realizó de forma heterogénea dando origen a una falta de interoperabilidad de los sistemas de firma nacionales. Además de la firma electrónica, el reglamento incluye otros servicios que anteriormente no estaban regulados a nivel europeo: i) los sellos electrónicos (medio equivalente a la firma para las personas jurídicas); ii) los sellos de tiempo electrónicos; iii) la entrega electrónica certificada, y iv) la autenticación de sitios web. A su vez, en línea con la Directiva de Firma, distingue entre servicios cualificados (aquellos sujetos a una supervisión más estricta y que otorgan el máximo nivel de garantías en su prestación) y no cualificados.

Merece mención especial la novedad que introduce el reglamento eIDAS respecto de la firma en servidor: al igual que el sistema Cl@veFirma, permite que tenga el mismo valor que la incorporada en el dispositivo y que, por tanto, pueda utilizarse para realizar firmas cualificadas. Con ello se persigue eliminar las barreras para la adopción generalizada de este tipo de soluciones, mucho más usables.

[43] Ley Nº40/2015.
[44] Reglamento (UE) Nº910/2014 del Parlamento Europeo y del Consejo que deroga la Directiva 1999/93/CE.

Lecciones aprendidas

Una de las primeras lecciones del caso español es la importancia de **separar la identificación y la firma electrónica**. Debido a que las primeras experiencias de despliegue de infraestructuras de identificación electrónica de carácter generalista se realizaron por medio de certificados electrónicos, se tendió a considerar a ambas de manera conjunta. Sin embargo, aunque frecuentemente se dan en el contexto de una misma transacción, no imponen los mismos requisitos ni requieren las mismas tecnologías. Como la identificación y autenticación es un proceso más sencillo que la firma, tiene sentido que también se apoye en mecanismos tecnológicos más amigables, sobre todo para el usuario.

Otra de las lecciones que se puede extraer es la **importancia de un marco legal adecuado**, que garantice la validez legal de las operaciones realizadas en línea, otorgue confianza suficiente a las partes que intervienen en las mismas, impulse la administración electrónica y sea consistente con las prácticas de identificación existentes en el mundo físico, de forma que ambos mundos, en línea y en persona, estén alineados. Por otro lado, debe tenerse en cuenta la identificación de personas jurídicas, que en muchas ocasiones son los principales usuarios de servicios digitales. Esto implica establecer reglas para la gestión de poderes y capacidades de representación de las personas físicas que las representan.

La **neutralidad tecnológica** es otro de los principios que debe respetarse a la hora de diseñar el marco general para la identificación electrónica y los servicios de confianza, ya que las tecnologías que lo sustenta cambian rápidamente con el tiempo. Es por ello que es muy recomendable adoptar un enfoque basado en los resultados que se desean conseguir, más que en las tecnologías que se van a utilizar. Esto es, por ejemplo, lo que hace el reglamento eIDAS a la hora de especificar los requisitos de los diferentes niveles de seguridad en la autenticación que prevé (básico, sustancial y alto). La adopción de estándares, como ISO/IEC 29115:2013 sobre el marco para el aseguramiento de la autenticación, o SAML 2.0, OpenID y Oauth para la federación de identidades, contribuye también a minimizar el riesgo derivado de la obsolescencia tecnológica.

El **principio de proporcionalidad** debe tenerse en cuenta en el diseño de un marco global de identificación. Por regla general, cuanto mayor es la seguridad de un mecanismo de identificación, más difícil resulta utilizarlo. Es por ello que se debe buscar un compromiso entre seguridad y usabilidad, exigiendo un nivel de seguridad en la autenticación adecuado a la naturaleza del servicio y de la información que maneja, lo que implica una evaluación de los riesgos del sistema de información. Lo mismo ocurre con el uso de la firma electrónica, cuya complejidad motiva a que solamente se exija cuando es necesario dejar constancia fehaciente de la voluntad del usuario.

Otra de las lecciones aprendidas es la existencia de diferentes perfiles de usuario, en función de la edad, la formación, la actividad profesional, los conocimientos de tecnologías de la información y las comunicaciones, la frecuencia de uso de los medios digitales, etc. Cada colectivo tiene sus preferencias en cuanto a sus medios de relación, por lo que es una buena práctica **dejar al ciudadano elegir** si quiere relacionarse por medios electrónicos, y en particular qué mecanismos usar. En este sentido, resulta relevante la experiencia de la Agencia Tributaria española; a pesar de que era posible acceder a sus servicios electrónicos identificándose con certificado electrónico desde 1999, en 2010 se observó que se había tocado techo, por lo que se planteó la habilitación de un nuevo mecanismo de acceso más sencillo destinado a todos aquellos que no disponían de certificados. Esto dio lugar a los servicios de confirmación del borrador de la

declaración de la renta, y al sistema de identificación Clave PIN, que aumentaron notablemente el nivel de tramitación electrónica respecto del que existía anteriormente.

En relación con la variedad de perfiles, resulta conveniente plantearse también la oportunidad de establecer una obligación de relacionarse con la administración por medios exclusivamente electrónicos para aquellos colectivos que disponen de los medios suficientes. En el caso de España, la Ley 39/2015 establece esta obligación para personas jurídicas, entidades sin personalidad jurídica, determinados colectivos profesionales y empleados públicos. Dinamarca va incluso más allá y ha extendido esta obligación a toda la ciudadanía, asegurando, eso sí, la posibilidad de que aquellos que no cuenten con los medios o los conocimientos para ello puedan recibir la asistencia necesaria.

Un aspecto relevante es también el **proceso de registro de los usuarios y de entrega de la credencial**, ya que el nivel de seguridad de un mecanismo de autenticación depende fuertemente de dicho proceso. En este sentido, el registro asegura la vinculación entre la identidad física y la identidad digital, por lo que es muy importante la verificación de la identidad que tiene lugar en ese momento, la cual será tanto más segura en tanto se utilicen documentos y datos existentes en registros oficiales. Generalmente, esta verificación adquiere la máxima garantía legal cuando la realiza una entidad administrativa, lo que le otorga un gran valor tanto para el propio sector público como para el sector privado. Además de un escenario de uso donde el sector privado admite credenciales emitidas por el sector público (como el DNI-e en España), existe la posibilidad de escenarios alternativos en los que las credenciales emitidas por el sector público se utilicen como base de confianza para generar credenciales propias del sector privado.

De gran importancia resulta también la **definición del modelo de financiación**, que debe ser sostenible, para lo cual es necesario establecer cuál es la contribución de cada actor a la financiación del sistema. Se debe tener en cuenta que si el costo recae en el ciudadano, se puede obstaculizar su adopción y con ello la demanda de servicios digitales, mientras que si recae en el proveedor del servicio electrónico que usa el mecanismo de identificación, lo que se obstaculiza es la incorporación de este al sistema y se frena la oferta de servicios en los que el mecanismo de identificación es admitido. También es posible que la financiación se realice con los presupuestos del Estado. Evidentemente, existe la posibilidad de definir modelos mixtos en los que el sistema se financie con contribuciones de todas las partes.

Por otra parte, es importante considerar los costos no tan visibles, como la infraestructura para la distribución de credenciales, o la integración de los servicios electrónicos con el sistema de identificación. Por último, se debe prestar especial atención a la posible competencia que se establezca entre el sector público y el sector privado en cuanto a la provisión de los medios de identificación, ya que la participación de esquemas de identificación de carácter público puede distorsionar la lógica de mercado. En este sentido, una posible aproximación puede ser que el sector público se encargue exclusivamente de la identificación de carácter legal, y el sector privado de la provisión de servicios de valor añadido vinculados a esa identificación, como pueden ser la certificación de atributos adicionales, la incorporación de garantías adicionales, o la utilización de mecanismos más convenientes y usables. No obstante, esta aproximación debe siempre contrastarse con el marco jurídico y la cultura existente respecto a los roles que deben desempeñar ambos sectores.

Por último, se debe tener conciencia de la importancia cada vez mayor que tiene la **dimensión transfronteriza de la identificación electrónica**. Con un comercio electrónico que tiene alcance global, y con una amenaza de cibercrimen también de carácter global, la necesidad de otorgar seguridad a las transacciones electrónicas que se producen entre ciudadanos y empresas de otros países es cada vez más perentoria. En este sentido, la experiencia de la Unión Europea con el reglamento eIDAS resulta paradigmática, aunque también es relevante la iniciativa MobileConnect, un nuevo estándar de seguridad impulsado por GSMA –asociación internacional que agrupa a más de 800 operadores de telefonía móvil del mundo entero– que permite la autenticación en los servicios en línea solo con un número de teléfono móvil a donde se envía un código que luego el usuario deberá introducir. Un marco adecuado para la identificación electrónica transfronteriza simplifica las relaciones con los ciudadanos y las empresas extranjeras, aumenta la facilidad para hacer negocios en el país y ayuda a atraer el talento tanto de estudiantes como de trabajadores.

Referencias bibliográficas

Andrews, M., L. Prichett y M. Woolcock. 2012. "Escaping Capability Traps through Problem-Driven Iterative Adaptation (PDIA)." Center for Global Development. Documento de Trabajo No. 299. Disponible en: https://www.cgdev.org/publication/escaping-capability-traps-through-problem-driven-iterative-adaptation-pdia-working-paper.

AT&T. 2010. "AT&T Healthcare Community Online: On-Demand Identity Management." Disponible en: http://www.corp.att.com/healthcare/docs/hco_identity_management.pdf.

Bitium. 2017. Lista de precios. Disponible en: https://www.bitium.com/site/pricing/.

Deloitte. 2016. "Picture Perfect: A Blueprint for Digital Identity." Disponible en: https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/financial-services/deloitte-nl-fsi-blueprint-for-digital-identity.pdf.

Deloitte Access Economics. 2015. "Digital Government Transformation." Deloitte Commissioned by Adobe. Disponible en: https://www2.deloitte.com/content/dam/Deloitte/au/Documents/Economics/deloitte-au-economics-digital-government-transformation-230715.pdf.

DocuSign. 2017. Productos y Precios. Disponible en: https://www.docusign.com/products-and-pricing.

e-Estonia. Disponible en: https://e-estonia.com/e-residents/about/.

Electronic Identity (eID). 2015. "Application Guide: where, why, how." Disponible en: https://eid.eesti.ee/index.php/EID_application_guide.

Foro Económico Mundial. 2016. A Blueprint for Digital Identity. Disponible en: http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf:

France Connect. s/f. Disponible en: https://franceconnect.gouv.fr/.

Kernaghan, K. 2012. "Transforming Local Public Services Using Technology and Digital Tools and Approaches." Universidad de Brock.

Local Government Association. 2014. "Transforming Local Public Services." Disponible en: https://www.local.gov.uk/sites/default/files/documents/transforming-public-servi-2a5.pdf.

Pareja, A., C. Fernández, B. Blanco, K. Theobald y A. Martínez. 2016. Simplificando vidas: calidad y satisfacción con los servicios públicos. Banco Interamericano de Desarrollo. Monografía No. 487. Disponible en: https://publications.iadb.org/handle/11319/7975.