GESTIÓN DE LA IDENTIDAD Y SU IMPACTO EN LA ECONOMÍA DIGITAL

18 de octubre, 2016
Sala Andrés Bello 3

BID
Mejorando vidas

Gestión de la Identidad
y su impacto en la Economía Digital

Alejandro Barros[1], Alejandro Pareja[2]

Octubre 2016

Contenidos

Introducción.

El presente documento tiene por objeto exponer los temas que se abordarán en el seminario "La gestión de la identidad y su impacto en la economía digital". Consta de dos partes. En la primera, se hace una descripción de los principales aspectos de la gestión de la identidad y su impacto económico. En la segunda se indican cuáles son los desafíos y alternativas actuales, los cuales serán desarrollados durante el seminario.

La identidad legal y un **sistema nacional de identidad (SNI)** confiable son críticos para **acceder a diversos servicios**, tanto públicos (educación, salud, seguridad, justicia, beneficios sociales y gobierno electrónico en general) como privados (financieros, comerciales, etc.) Por otro lado, los SNI deben **contribuir a la reducción de costos**

[1] Alejandro Barros, Consultor Internacional, abc@alejandrobarros.com, www.alejandrobarros.com
[2] Alejandro Pareja, Especialista Modernización del Estado, División de Capacidad Institucional, Banco Interamericano de Desarrollo, apareja@iadb.org, www.iadb.org ,

transaccionales, a facilitar la ejecución de políticas públicas, a mejorar la calidad y satisfacción con los servicios públicos y al desarrollo del sector privado.

Los SNI abarcan no solo a todas las instituciones responsables de la oferta de los servicios asociados a la identidad sino, también, la consideración de todos los agentes que conforman la demanda de dichos servicios. Esta demanda la encarnan básicamente **tres actores: los ciudadanos, las empresas y el propio gobierno**.

La gestión de la identidad es la combinación de procesos y sistemas que potencian el uso y usabilidad de los datos identificatorios de las personas. La gestión y el uso deben ser eficientes, seguros, ciudadano-céntricos y respetuosos de las normas de protección de los datos personales. Esta gestión de la identidad requiere: 1) un **modelo de gobernanza y modelo de negocio**; 2) **marco legal** apropiado y actualizado; 3) la **simplificación y estandarización de procesos y sistemas**; 4) el establecimiento de mecanismos de **interoperabilidad** que faciliten la coordinación entre los diferentes organismos; y 5) la promoción y coordinación del **ecosistema de uso de la identidad**.

Con el advenimiento de la **economía digital**, interacciones y transacciones que previamente se realizaban presencialmente pasaron a ejecutarse en forma creciente a través de sistemas de información interconectados y la web. Esto ha hecho surgir la necesidad de considerar 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 y realice transacciones a través de internet o redes privadas.

Gestión de la identidad

Las organizaciones, tanto públicas como privadas, y las personas requieren para muchos tipos de interacción que se pueda verificar fehacientemente la identidad de la otra parte. Hasta hace algunos años, el proceso de identificación se basaba en credenciales físicas, tales como la cédula de identidad, licencia de conducir u otro documento, que de alguna forma acreditaban la identidad de su portador.

En el mundo de los sistemas de información que operan en red, este proceso de identificación se ha complejizado. En la actualidad, se requiere 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. Esto conlleva, por un lado, desafíos en cuanto a privacidad, protección de datos, posibilidad de fraude y, por otro lado, la necesidad de revisar y ajustar esquemas de gobernanza, marcos legales[3] y tecnologías que puedan estar quedando obsoletos.

En este nuevo y complejo contexto, el proceso de identificación de personas depende del objetivo final que se persiga, es decir, de la actuación y/o interacciones que se quiera realizar. En el siguiente cuadro se muestran los principales casos de uso.

[3] Leyes que regulan el uso de la Firma Electrónica

Tipo de Interacción	Descripción	Ejemplo de mecanismo	Ejemplo de uso
Registrarse	Creación de un usuario en un nuevo sitio	En algunos casos el registro como usuario puede realizarse online mientras que en otros es un paso presencial. En el primer caso, suele utilizarse una clave dinámica (*one-time password*[4]), las cuales se envían al teléfono o casilla de correo del usuario. En el segundo caso, se recibe la clave personalmente y se asume la responsabilidad por la identidad digital.	Identidad digital en Chile – Sistema Clave Única[5]
Identificarse y ser autenticado	Tiene lugar cuando se intenta **acceder** a algún sistema de información	Usuario y clave.	Acceso a sitios web
Obtener **autorización** para acceder a un determinado recurso de información o servicio	Puede haber un esquema de permisos preestablecido según los distintos perfiles de usuario o puede requerirse para una instancia complementaria de autenticación cuyo objetivo sea incrementar el nivel de seguridad en operaciones con alto riesgo.	Generalmente se utilizan mecanismos de segunda clave o clave dinámica	Transferencia electrónica de fondos
Dar **consentimiento**	El usuario está otorgando el consentimiento en una actuación	Firma electrónica (certificados digitales)	Firma de contratos

Este proceso de gestión de identidad puede requerir múltiples actividades, algunas de ellas presenciales y otras en modalidad remota. La gestión de la identidad debe contemplar el proceso completo: 1) el registro del nacimiento; 2) el enrolamiento en un sistema de identidad con el correspondiente otorgamiento de su credencial, física o digital[6]; 3) el uso de la credencial digital en las plataformas para las cuales

[4] Un ejemplo de one-time password (OTP) es el código numérico que es enviado a algún dispositivo que tiene el usuario (teléfono móvil, mail, otro).

[5] Clave Única - https://www.claveunica.gob.cl/

[6] La credencial digital es un identificador utilizado por una persona para interactuar con un sistema de información. Por ejemplo: usuario y clave, certificado digital o información biométrica (huella, iris).

fue otorgada (incluyendo atributos y permisos); 4) la eventual revocación, producto de problemas de seguridad (suplantación); y 5) la baja del sistema. El sistema debe garantizar la seguridad y trazabilidad de la información, conforme a las regulaciones de la organización o incluso a normativas de ámbito nacional o internacional.

Enrolamiento en el Sistema Nacional de Identidad (SNI)

El enrolamiento es el proceso mediante el cual se registra la filiación de la persona y se le asigna un número único de identidad. En los países que cuentan con un documento nacional de identidad suelen registrarse también otros datos biométricos e imágenes de las huellas dactilares. Algunos países, como la India, han comenzado a registrar también imágenes de iris.

En algunos casos, se incorpora al documento[7] uno o más chips en los que se graba la información personal registrada (incluyendo las minucias de una huella dactilar a efectos de que pueda ser cotejada) y, eventualmente, un certificado digital para firmar electrónicamente. En estos casos, para poder hacer uso de la identidad digital grabada en el documento, la persona requerirá un dispositivo que permita leer el documento (lectura del chip).

Autenticación de la identidad digital

Con relación a la economía digital, la principal actividad del proceso de gestión de la identidad es la autenticación. Históricamente, la autenticación se ha sustentado en tres elementos (factores) que, dependiendo del nivel de riesgo del proceso a realizar, se utilizan para mejorar la robustez y seguridad del método. Estos tres factores son:

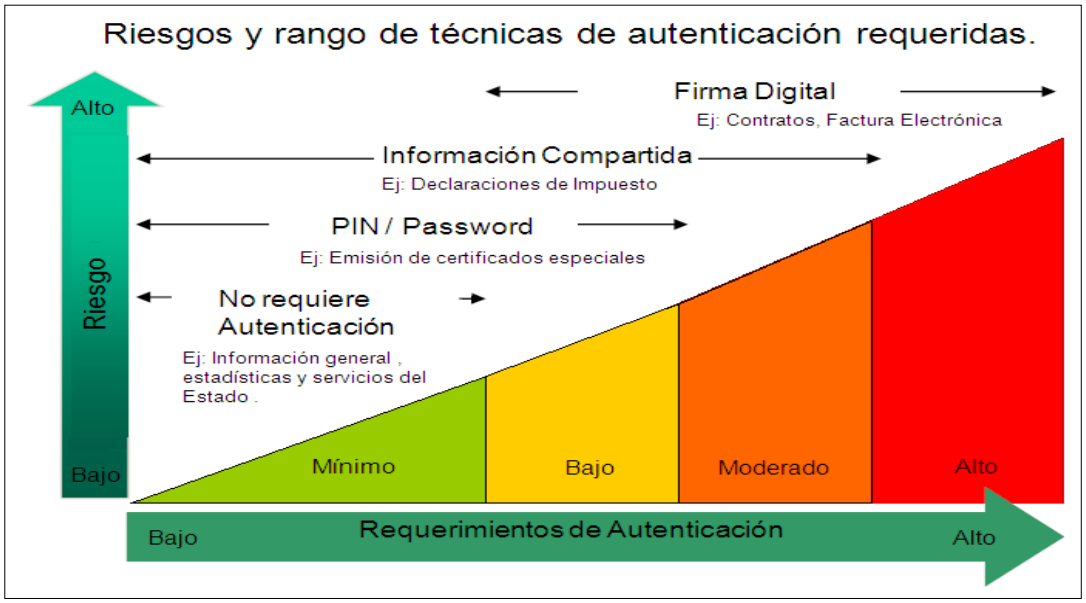
	Descripción	Ejemplos de Uso
Algo que la persona sabe	Se refiere a algo que la persona sabe, mantiene en secreto y usa al momento de identificarse.	• Usuario y clave o PIN (personal identification number) • Desafío (pregunta de respuesta secreta)
Algo que la persona es	Corresponde a algún atributo físico de la persona, generalmente conocido como característica biométrica.	• Huellas dactilares • Imagen de los iris • Forma de la cara • Voz
Algo que la persona tiene	Algún elemento físico o tecnológico que la persona posee	• Documento de identidad. En particular el electrónico (conocido como eID o eDNI)

[7] Habitualmente se conoce ese documento con Documento Nacional de Identidad (DNI) o Cédula Nacional de Identidad

		• Tarjeta inteligente (smart card). Por ejemplo, tarjeta de crédito. • Dispositivo tipo token. • Certificado digital instalado en un computador personal o en la nube • Certificado instalado en algún dispositivo (Smart card, token USB, teléfono móvil[8])

Las buenas prácticas señalan, que para operaciones de riesgo alto se debe utilizar una combinación de al menos 2 de estos factores. A efectos de definir el nivel de seguridad que corresponde en cada caso de uso, no sólo se debe tener en cuenta el riesgo intrínseco del mecanismo sino el tipo de interacción. En la siguiente imagen se presenta un esquema de las distintas posibilidades.

Ilustración 1: Gestión de Credenciales



Fuente: Elaboración propia

En el mundo público, al menos en la región, los mecanismos de autenticación digital son bastante básicos y, en general, se utiliza el mecanismo de usuario y clave. En cuanto a la firma digital, si bien muchos países de la región han regulado su uso por la vía de leyes de firma electrónica, su difusión y uso es aún muy incipiente. Probablemente esto sea producto de dificultades de usabilidad que dicho mecanismo tiene, derivado de la obligación de contar con un lector del dispositivo donde se almacena el certificado (smartcard, token-USB[9] u otro).

[8] En el caso del uso de los teléfonos móviles, esto se ha resuelto por la vía del uso de un segundo chip, el cual se utiliza como repositorio del certificado. Las compañías de telecomunicaciones en general no tienen un rol en la gestión de ese segundo chip.

[9] Ejemplo de Token USB - http://www.safenet-inc.es/multi-factor-authentication/authenticators/pki-usb-authentication/etoken-pro/

En la región las experiencias de documentos de identidad que incluyen elementos de identificación digital (certificados para firma, minucia de huella dactilar u otros datos personales), o bien son incipientes (por ejemplo Uruguay), o bien no han sido exitosas en su utilización (por ejemplo, Chile).

En la actualidad, para algunos servicios online, se han adoptado mecanismos complementarios para autenticar a las personas de tipo adaptativo, basados en la historia del cliente/usuario (su perfil de navegación, geolocalización, perfil de uso de redes sociales, etc.), esto como un elemento adicional de seguridad.

Por otro lado, es interesante destacar que algunas compañías han establecido modelos de negocio (complementarios a sus negocios habituales) asociados a la autenticación (proveedores de identidad). Tal es el caso de Google[10] y Facebook[11] y otros, los cuales están siendo utilizados por múltiples organizaciones públicas y privadas como mecanismos de autenticación.

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 están prácticamente todos los países de Hispanoamérica.

Por otro lado, hay países donde no existe una institución pública central que enrole y emita un documento nacional de identidad (por ejemplo, Canadá, Estados Unidos, Reino Unido[12] y varios países del Caribe). En estos casos, suelen existir documentos de identidad de facto. Se pueden citar como ejemplos: permiso de conducir, comprobante de registro en la seguridad social, pasaporte o documento electoral. Estos documentos de identidad coexisten y corresponde a cada actor definir cuál acepta como comprobante de identidad. En algunos casos la multiplicidad de emisores de identidad incrementa los riesgos de fraude, principalmente en los casos en los que la coordinación entre los distintos emisores es débil.

Tanto en el sistema hispanoamericano como en el de origen anglo-sajón los documentos de identidad aceptados se derivan de un registro de nacimiento (nacional o extranjero), el cual es siempre la piedra angular del sistema.

[10] Google Cloud Identity & Access Management - https://cloud.google.com/iam/
[11] Facebook Connect - https://developers.facebook.com/docs/facebook-login
[12] Linea de tiempo de lo que ha ocurrido con la Cédula de Identidad en el Reino Unido - http://www.bbc.com/news/10164331

En algunos países el número y documento de identidad se emite al momento del nacimiento. En otros ha de obtenerse, por ejemplo, cuando se desee abrir una cuenta bancaria, para comenzar a conducir o para votar.

En cuanto a la identidad digital, hay países hispanoamericanos donde la institución rectora del sistema de identidad gestiona también identidad digital, sobre todo para su uso en la relación con el estado. En ningún caso se trata de un proveedor exclusivo sino que la tendencia es más bien a 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*[13] para el sector público. En algunos casos el impulsor principal de la identidad digital para el sector público es el registro civil mientras que en otros lo es el organismo responsable del gobierno electrónico.

También en los países de tradición sajona la identidad digital se gestiona en forma distribuida (no existe un gestor exclusivo), habiendo casos con sistemas federados[14] y casos en los que los distintos emisores de identidad no están coordinados. En algunos casos, se externaliza parte de la gestión, tal es el caso de Chile en que la producción de cédula está entregada a un proveedor externo[15].

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 riesgos del proceso de autenticación para este tipo de instituciones e implica que haya pocas experiencias de tercerización del servicio.

Financiamiento de la gestión de la identidad

En cuanto a la identidad básica (la que se plasma en un documento de identidad), las instituciones proveedoras se financian con el cobro a los ciudadanos por el documento (aun en los casos en que el mismo es obligatorio) y con aportes presupuestales, en proporciones que varían según el caso. También suelen vender servicios relacionados con la identidad[16], tanto al sector privado (sobre todo la banca) como al resto del sector público.

Los sistemas de gestión de identidad en muchos casos son operados directamente por la institución del estado que tiene como mandato el registro de identificación[17] de las personas, tal es el caso de Uruguay; otros países han

[13] Este esquema consiste en que el usuario se conecta con el mismo usuario y contraseña a cualquier sitio, en este caso, de gobierno.

[14] Fedarated Identity: los individuos pueden utilizar la misma identificación personal para identificarse en redes y sistemas de diferentes áreas o instituciones - https://en.wikipedia.org/wiki/Federated_identity

[15] La empresa francesa Morpho

[16] Por ejemplo, la solicitud de la filiación de una persona a partir de su huella dactilar.

[17] Registro Civil

externalizado algunas de las actividades del proceso, tal es el caso de Chile, que ha externalizado, la producción de cédulas y pasaportes la cual es realizada por un proveedor externo[18].

En cuanto a la identidad digital, habitualmente existe poca conciencia de los costos involucrados asociados a la gestión de la identificación, tanto en el mundo privado como público. Es muy común que se los incluya como parte del costo total de la plataforma tecnológica. Esto dificulta la visualización de alternativas con mejor relación costo-efectividad.

[18] Morpho - http://www.morpho.com/

En el siguiente cuadro se presentan los principales componentes de costo de la gestión de la identidad digital.

Ítem de costo	Descripción
Enrolamiento y revocación	Para servicios de riesgo bajo, el enrolamiento puede hacerse remotamente y en forma automatizada y, en consecuencia, con costo bajo. Sin embargo, cuando el servicio requiere mecanismos de alta seguridad, es muy probable que el enrolamiento deba hacerse en forma presencial, para que el usuario presente su documento de identidad, foto o huella y firme un contrato de uso. Esto implica costos importantes tanto para la institución como para el usuario (oficinas de atención, tiempos, traslados, mecanismos de verificación y otros). En los casos en los que la identidad digital se incluye en el documento de identidad, el proceso de enrolamiento queda subsumido en el de obtención del documento. En cuanto a la revocación, se deben asignar recursos a la atención de incidentes que ameriten el bloqueo y posible revocación de certificados digitales, como consecuencia de suplantaciones de identidad, fallecimiento, etc.
Gestión de la información	Corresponde al soporte tecnológico utilizado, bases de datos, proceso de encriptación y gestión de certificados (plataforma PKI[19]), software de gestión de los datos de identidad, otras medidas de ciberseguridad.
Dispositivos	Corresponde a los costos de dispositivos en los que se almacenan las credenciales (*tokens*, *smart cards)*, lectores de dispositivos o el servicio que suministra las claves dinámicas.
Soporte a usuarios	Call center para dar soporte a los usuarios finales, por ejemplo, cuando se olvida la clave.

En el siguiente cuadro se presenta, a modo de referencia, una estimación de los costos operativos de gestión de la identidad anuales por usuario, los valores corresponden a diferentes estudios realizados para instituciones financieras y bancos en la región (estas estimaciones incluyen los diferentes ítems de costos identificados en tabla anterior):

Tipo de mecanismo	Costo anual por usuario (US $)
Usuario-clave	10
Clave dinámica (one time password)	20
Firma Electrónica (incluye el costo del certificado y del dispositivo para almacenamiento)	50

Fuente: Elaboración propia a partir de datos de industria financiera

[19] *Public Key Infrastructure* es la plataforma de generación, gestión y revocación de certificados digitales que permite encriptar y desencriptar comunicaciones y documentos, con seguridad para las partes intervinientes.

Impacto Económico de la identidad digital

Desde el punto de vista económico, se pueden considerar impactos de dos tipos asociados a la identidad digital: por un lado, los derivados directamente de la digitalización de procesos existentes que previamente se ofrecían únicamente en forma presencial; y, por otro, los asociados al surgimiento de nuevos servicios y actividades económicas como consecuencia del uso de la identidad digital.

La identidad digital es un requisito básico para poder llevar a cabo transacciones en línea. Por lo tanto, todos los beneficios que trae consigo la modalidad en línea, tanto en eficiencia como en calidad percibida por los usuarios, son posibles gracias a un sistema confiable de identidad digital.

Resulta por tanto relevante analizar los costos asociados a los diferentes canales de atención, tanto para la institución como para los usuarios. En el siguiente cuadro se presentan los costos por canal de atención (presencial, telefónico y en línea) para algunos estados, expresados en dólares por transacción[20].

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

Fuente: K. Kernaghan – Universidad de Brock (2012), Transforming local public services using technology and digital tools and approaches – Local Government Association (2014), Digital government transformation – Deloitte Commissioned by Adobe (2015)

Se puede apreciar una diferencia muy significativa entre los costos del canal en línea y el presencial. A efectos de completar el análisis de impacto se debe considerar el ahorro para los usuarios en los canales online, básicamente por ahorro de tiempo y traslados. Esto arroja un impacto aún mayor. Es muy difícil determinar este ahorro pero sin duda se podría estimar en una hora-hombre (correspondiente a un ingreso medio) por transacción.

Ahora bien, aun cuando el ahorro para los ciudadanos es claramente positivo, se debe hacer la salvedad de que al llevar los servicios a canales virtuales, se está produciendo una externalización de costos hacia ellos, por ejemplo por la necesidad de contar con un dispositivo para conectarse, costos de los certificados digitales, servicio de conectividad y otros.

[20] En el ámbito privado, esto es, industria financiera, se aprecian costos similares, entre canales presenciales y remotos.

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

- Ciberseguridad, corresponde a todos los mecanismos y sistemas necesarios (software, hardware) para asegurar un buen nivel de seguridad de los procesos de identificación.

- Desarrollo de software, asociado a la implementación de plataforma de identificación, tal es el caso de los desarrollos de plataformas de single sign-on anteriormente mencionadas.

- Establecimiento de servicios privados de autenticación, como los mencionados anteriormente (Facebook Connect, Google y otros). Operación tecnológica de plataformas de autencticación

- Desarrollo y producción de dispositivos de autenticación (tokens, smart cards y sistemas de claves dinámicas).

- En el caso de los certificados digitales, aparecen otras actividades asociadas, tales como proveedores de certificados, empresas emisoras de certificados[21] y dispositivos para su almacenamiento (token, smart cards).

- Algunas actividades se reducen o desaparecen, tales como todas las asociadas a los procesos de atención de público (ventanilla, personal, etc.). Producto de la interacción online, también debo redimensionar la cantidad de puntos de atención (oficinas) y sus costos asociados.

Desafíos y temas a desarrollar en el seminario

Una vez repasado el contexto actual de la gestión de la identidad, se desarrollarán en esta sección los principales desafíos, los cuales serán analizados durante el seminario. Algunos de los aspectos que deben abordarse al momento de definir un modelo de eID son:

- Respecto al **enrolamiento para la identidad básica** (la que se plasma en el documento de identidad) y en aquellos casos en los que se capturan datos biométricos, nuestra región se ha basado en las huellas dactilares, inicialmente de uno o dos dedos y con una tendencia clara al registro de los 10 dedos. Por otro lado, el proyecto Aadhaar[22] de la India realiza el enrolamiento tomando, además de las 10 huellas, la imagen de los iris. Se podría discutir cuál será la tendencia futura y **si será necesario o conveniente que nuestros países implementen enrolamientos que**

[21] En algunos países hay proveedores de certificados, tanto empresas privadas como emisores públicos
[22] https://uidai.gov.in/beta/

incluyan imágenes de iris u otro elemento biométrico (ventajas y desventajas). Además de las consideraciones técnicas propias del proceso de autenticación, habría que contemplar aspectos de privacidad y usabilidad.

- Respecto a los **documentos de identidad**, considerando que, al menos teóricamente, la autenticación biométrica podría realizarse directamente, sin que los datos tengan que estar grabados en una tarjeta (mediante un escáner que capture la imagen que luego se transmita al ABIS[23]), la pregunta es **si es posible y conveniente avanzar hacia sistemas de identidad sin documento físico (ventajas y desventajas)**.

- En la medida que se han ido desarrollando los sistemas de identidad digital, tanto las instituciones públicas como las empresas mantienen bases de datos con **datos personales de los usuarios**. Más allá de los riesgos de hurto de esa información, existen riesgos de uso inapropiado de la misma. La pregunta es **si es posible dar a los usuarios la posibilidad de controlar parcial o totalmente a quienes guarden datos de su identidad junto con la capacidad de autorizar qué datos se pueden compartir con cuál organización y bajo qué condiciones**. Se necesitaría saber qué normativa se requiere y cuál sería la mejor forma de implementar un mecanismo de este tipo.

- ¿Cuál es **la institucionalidad más apropiada**, en términos de eficiencia y calidad de servicio, para la gestión de la identidad digital? ¿Cuáles son las ventajas y desventajas de mantener un proceso descentralizado (incluso de actores no coordinados) respecto a uno más centralizado (con uno o con un conjunto reducido de gestores de identidad digital, eventualmente con el establecimiento de un marco de confianza entre ellos)?

- **¿Debería el Estado obligar a que todo ciudadano tenga una identidad digital?** ¿Cuáles son las ventajas? ¿Por qué, entre los países con gran desarrollo de la sociedad de la información, hay tanto quienes imponen la obligación como aquellos donde no existe ninguna regulación al respecto? El hecho de que una persona tenga identidad digital, ¿contribuye al desarrollo del gobierno electrónico y la sociedad de la información o no altera los niveles de uso de servicios digitales?

- ¿En cuáles **procesos de la gestión de la identificación** para actuar con el sector público hay espacio para la **colaboración con el sector privado**? **¿Qué procesos sería posible o conveniente tercerizar?** ¿Dónde el sector privado puede agregar más valor que el público? Aspectos normativos y técnicos que habría que considerar.

[23] Automated Biometric Identification System. Son los sistemas que cotejan una imagen biométrica contra un banco de imágenes a efectos de verificar con cuál se corresponde. En el caso de huellas dactilares se llama AFIS (Automated Fingerprint Identification System).

- Respecto a los **marcos normativos**, qué cambios se están requiriendo. Por ejemplo, a efectos de contemplar la gestión apropiada y segura de bases de datos que contengan datos personales de usuarios o a efectos de contemplar las nuevas posibilidades tecnológicas en cuanto a certificados digitales para firma.

- ¿Cuáles son en el ámbito mundial los niveles reales de uso de la firma digital? ¿Cuáles son las modalidades de **firma digital** más utilizadas y cuáles son las tendencias en este aspecto?

- **Fraude y suplantación**: ¿cuáles son los mayores riesgos de fraude y suplantación que pueden afectar el proceso de identificación de las personas? ¿Cómo se mitigan?

- ¿Deben los gobiernos intervenir en la extensión del uso de la identidad digital? ¿Cuáles son las políticas y proyectos a desarrollar?[24]

- **Procesos de adopción de la identidad digital universal, lecciones aprendidas:** hay varios ejemplos de proyectos de difusión masiva de la identidad y firma digital (en general asociada al documento de identidad) que no fueron acompañados por la adopción esperada por parte de los ciudadanos y las empresas. En otros casos más exitosos, la adopción ha sido muy paulatina. ¿Cuáles son las lecciones aprendidas al respecto? ¿Qué habría que haber hecho diferente en cada caso? ¿Cuáles son las expectativas razonables al respecto?

- ¿Qué nuevos servicios podrían surgir en torno a la identidad? ¿Hay servicios que quedan obsoletos?

- **Análisis de costos**: es importante que se identifiquen los costos asociados a la gestión de la identidad digital. Este análisis puede ser un insumo importante para la estrategia nacional, el diseño institucional y la actualización normativa.

[24] https://www.theguardian.com/technology/2014/nov/06/govuk-quietly-disrupts-the-problem-of-online-identity-login