Autenticación Digital Ciudadana Argentina

Andrea Maciel [1], Georgina Etulain[2], Julián Ernesto Belistri[3] y Silvana Rica [4]

Dirección de Procesos e Integraciones
[1]maciela@jefatura.gob..ar; [2]etulaing@jefatura.gob.ar;
Dirección Nacional de Integración y Tramitación Digital Estatal
[3]julianb@jefatura.gob.ar; [4]ricas@jefatura.gob.ar
Secretaría de Innovación Tecnológica del Sector Público
Jefatura de Gabinete de Ministros
Buenos Aires, Argentina

Resumen. La evolución y las posibilidades generadas por el avance de las tecnologías de la información y la comunicación que se insertan en cada vez más actividades, y en el caso particular de Argentina, con su gran amplitud geográfica y una organización federal con múltiples niveles administrativos, conlleva a que la ciudadanía cuente con un promedio de 7 (siete) identidades digitales para interactuar con diversas aplicaciones, tanto públicas como privadas. Sólo el Estado Nacional entrega al menos 5 (cinco) identidades digitales diferentes como requisito para interactuar con sus plataformas.

La Plataforma de Autenticación Electrónica Central **PAEC/AUTENTICAR** es la aplicación del estado que se propuso concentrar y estandarizar en un solo lugar la verificación de la identidad digital de los ciudadanos contra los proveedores de identidad reconocidos oficialmente.

Esta experiencia permitió repensar y analizar nuevos conceptos, como el de Identidad Descentralizada en Blockchain (cadena de bloques), la aproximación a un Identificador Único para el ciudadano digital, la Identidad Transfronteriza como el reconocimiento y confianza mutua en identidades digitales de otros países, entre otras.

En este documento se presentan algunas de las ideas alcanzadas.

Palabras Claves: Identidad, Identidad Digital, Autenticación, Ciudadano Digital

1. Introducción

Con una mirada global, tanto los estados como el mercado necesitan contar con información abundante sobre la identidad digital de las personas y sus comportamientos en ambientes digitales para incluirlas eficientemente en sus políticas públicas o en la actividad privada. La escasez de esta información afecta en mayor medida a aquellas personas pertenecientes a sectores vulnerables como minorías, habitantes de parajes rurales, pueblos originarios, mujeres, niños, niñas y adolescentes, personas con discapacidad, adultos mayores, migrantes, pequeños emprendedores, personas excluidas de la economía formal, sin historial crediticio bancario o sin recursos económicos.

Cuando el mercado incluye a sectores de escasos recursos, lo hace a un costo más alto. Esto, que algunos teóricos llaman "penalidad de la pobreza"[1], se debe al mayor costo relativo que enfrentan las personas en situación de vulnerabilidad para acceder a bienes y servicios debido a la falta de identidad digital, o escaso empoderamiento o control sobre información personal.

La homologación de normativas en reconocimiento institucional de identidades, y en sistemas de autenticación, contribuirán en la reversión de este escenario, sobre todo para migrantes y grupos minoritarios.

Para el inicio de este trabajo nos planteamos varios interrogantes, en primer lugar, aquellos con definiciones concretas y claras en torno a la identidad de las personas en ambientes digitales:

¿Qué es la Identidad? ¿Qué es la Identidad Digital? ¿Qué es la Autenticación?

Según explicita la Real Academia Española, la **"Identidad"** es el conjunto de rasgos o características de una persona o cosa que permiten distinguirla de otras en un conjunto.

En el caso de nuestro país, el Registro Nacional de las Personas (RENAPER) es el organismo responsable de otorgar la identificación y la documentación de las personas con la potestad exclusiva de la emisión de Documento Nacional de Identidad y Pasaporte.

La **"Identidad Digital"**, también conocida como "Identidad 2.0", es la versión en internet de la identidad física de una persona. Está compuesta por todos los datos que proporcionan las personas usuarias de la red, entre ellos, e-mail y contraseñas, preferencias de consumo, fotos que publicamos o en las que nos etiquetan, comentarios, datos y actividad bancaria. Este tipo de acciones online crean una reputación digital, una opinión que los demás se forman acerca de nosotros con lo que ven publicado. Es el conjunto de información que nos identifica en el entorno online.

Se denomina "**Autenticación**" al procedimiento de validación de cualquier tipo de credenciales para operar con un sistema informático o red. Existe una amplia variedad de

métodos de autenticación, generalmente combinaciones de tres esquemas comúnmente descritos como “algo que sabemos, algo que tenemos, algo que somos”.

“Algo que sabemos” refiere a las contraseñas, pines o patrones de acceso; “algo que tenemos”: dispositivos USB físicos (memorias externas), teléfono móvil vinculado al recurso a acceder; “algo que somos”: aspectos biométricos, características físicas que nos distinguen de otras personas como las huellas dactilares o los puntos distintivos del rostro.

La autenticación en plataformas digitales del ámbito público tiene requerimientos adicionales a los de otros sistemas: es necesario verificar que quien accede a un recurso es una persona con determinados derechos y obligaciones, ya que las interacciones con el Estado tienen como objetivo, habitualmente, la obtención de un beneficio, el ejercicio de un derecho, o el cumplimiento de una obligación.

La Administración Pública tiene a su vez la responsabilidad de “preservar la confidencialidad, integridad y disponibilidad de la información, así como velar por los derechos de los titulares de datos personales o propietarios de información que gestiona” (Decisión Administrativa 641/2021 JGM, “Requisitos mínimos de Seguridad de la Información para Organismos”[2]).

Es en este punto en el que adquieren trascendencia las fuentes auténticas consultadas para autenticar personas, debiendo tener un reconocido respaldo institucional, con normas y procedimientos claros y confiables.

El segundo grupo de interrogantes parece más complejo de responder, y pretende actuar como disparador para enunciar las problemáticas y desafíos que surgen en torno a la identidad digital:

¿Cuáles son los elementos que definen la identidad digital de una persona? ¿Cuántas identidades digitales tiene hoy una persona? ¿Quiénes concentran y administran las identidades digitales de las personas?

Todos los atributos que figuran en la web asociados a la identidad de una persona, son elementos que integran su identidad digital, como ser los perfiles personales, las redes sociales generales (Facebook, Instagram, Twitter, Youtube) y profesionales (LinkedIn, Xing, Viadeo), y los portales de búsqueda de empleo. También los comentarios, contenidos digitales, contactos, las direcciones de correo electrónico e incluso la mensajería instantánea.

Asimismo, la acumulación de credenciales que, presentadas ante organismos públicos o privados, hacen posible validar a la persona ya que son atributos que componen su identidad digital (Certificado de Nacimiento, Título Universitario, Certificado de Discapacidad, Licencia de Conducir)

Una sola persona puede tener varias identidades digitales, dado que muchas plataformas poseen procedimientos de identificación y autenticación independientes unos de otros.

Generalmente se requiere crear un código y una contraseña para acceder a cada una de ellas, es decir, generar una nueva identidad digital en cada caso.

En este sentido, en nuestro país, la ciudadanía cuenta con un promedio de 7 (siete) identidades digitales para interactuar con diversas aplicaciones, éstas son emitidas y administradas por organismos públicos nacionales, provinciales o municipales, como así también en su gran mayoría por entidades privadas. Tal es así que grandes grupos tecnológicos (Microsoft, Facebook, Google) generan inversiones multimillonarias en infraestructura, concentrando la mayor cantidad de información de las personas.

En los últimos años, impulsadas por el avance de la tecnología, cada vez se generan más y más soluciones sistémicas y nuevas identidades digitales, causando una gran incomodidad para los seres humanos que operan estos sistemas.

La multiplicidad de identidades digitales, genera en sí misma riesgos por varios factores. En primer lugar, por la dificultad que genera recordar las distintas claves que se van creando, en segundo término, por la inseguridad generada al tener que anotarlas y gestionarlas, y, muchas veces por el uso de contraseñas sencillas, con robustez insuficiente. También, la proliferación de estas identidades digitales, generan vulnerabilidades que requieren soluciones con distintos niveles de seguridad.

A lo largo del artículo se irán recorriendo alternativas de respuestas, soluciones y enfoques en relación a los problemas de identidad digital en el mundo y en particular en la Argentina. Estudiar nuevos paradigmas alrededor de estas temáticas, es imprescindible para que la Secretaría de Innovación Tecnológica siga mejorando los sistemas de gestión de la identidad digital.

2. Plataforma de Autenticación Electrónica Central del Estado PAEC/AUTENTICAR[3]

Con el fin de resolver una gran parte de los problemas planteados, el Estado Nacional de nuestro país toma el compromiso de poner a disposición una única plataforma transversal para que los organismos públicos y privados simplifiquen la gestión de las identidades digitales. Esta plataforma aplica el concepto de "Autenticación Delegada", incorporando como proveedores de identidad a instituciones oficiales reconocidas a nivel nacional, poniendo en valor la fuente auténtica, es decir, respaldando la verificación de identidades digitales.

Propósito.

La Plataforma de Autenticación Electrónica Central del Estado (PAEC/AUTENTICAR) surge en 2016 ante la necesidad de permitir a las personas su autenticación para realizar distintos trámites en forma digital, haciendo, a su vez, un uso eficiente de los recursos existentes. Se partió en ese año de una situación previa: distintos organismos ya contaban con sistemas de registro de identidades digitales. El plan de innovación del Estado implicó la implementación de nuevas plataformas y aplicaciones, para las cuales no iba a ser eficiente

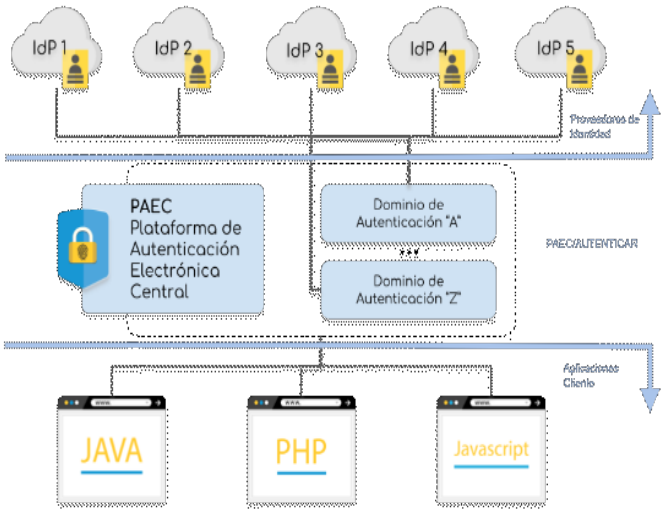
crear nuevos sistemas de registro de identidades, sino por el contrario, el desafío consistió en reutilizar los ya establecidos.

Se planteó entonces, como solución transversal, la construcción de una plataforma con la responsabilidad de resolver en un único punto la interacción entre tres actores: las **Aplicaciones Cliente** que requieren usuarios autenticados, las personas con **Identidades Digitales** registradas y las entidades llamadas **Proveedores de Identidad o IdP** (por las siglas en inglés de Identity Provider) que otorgan la identidad digital.

El propósito de PAEC/AUTENTICAR consiste en brindar una plataforma transversal para que otras aplicaciones gestionen identidades digitales de manera simple, ofreciendo con una sola integración la posibilidad de conectar con distintos proveedores de identidad para reconocer a la persona operando con dichos sistemas. Cualquier organismo que presente la solicitud, cumpla los requisitos y lleve adelante el trámite adecuado podrá utilizar el servicio de autenticación de la Secretaría de Innovación Tecnológica del Sector Público luego de ser dado de alta en la plataforma.

Funcionamiento.

PAEC/AUTENTICAR implementa el concepto de "Autenticación Delegada", es decir que no gestiona ni conoce las credenciales a verificar, sino que actúa como plataforma intermediaria. Se le ofrece a la persona la posibilidad de seleccionar el proveedor de identidad, hecho lo cual se presentan las interfaces de autenticación habituales. Es el proveedor de identidad quien verifica dichas credenciales e informa a la plataforma si debe darse autorización a la persona usuaria para continuar. En caso de ser autorizada, PAEC/AUTENTICAR envía a la aplicación cliente los datos de la persona en forma estandarizada.



Proveedores de Identidad.

Un proveedor de identidad es una entidad que cumple el rol de brindar su servicio de autenticación de credenciales, y que por su normativa y facultades puede registrar identidades digitales oficialmente reconocidas. Cabe destacar que la plataforma PAEC/AUTENTICAR no integra proveedores de identidad "sociales", como ser las redes sociales privadas, por su bajo nivel de seguridad o nula verificación de documentación.

Se enuncian a continuación los principales proveedores de identidad dentro de la plataforma:

- **Registro Nacional de las Personas (RENAPER)**[4]: autenticación por Documento Nacional de Identidad (DNI) junto al número de trámite de la credencial.
- **Administración Federal de Ingresos Públicos (AFIP)**[5]: autenticación por Clave Única de Identificación Tributaria (CUIT) y Clave Fiscal.
- **Administración Nacional de la Seguridad Social (ANSES)**[6]: autenticación por Código Único de Identificación Laboral (CUIL) y Clave de Seguridad Social.
- **MiArgentina**[7]: autenticación credenciales de argentina.gob.ar
- **Nic.Ar**[8]**:** autenticación por credenciales de Nic Argentina.
- **Administración Pública Nacional**[9]**:** autenticación por credenciales otorgadas a agentes y funcionarios del Sector Público.

Estandarización.

Para simplificar la comunicación entre las aplicaciones cliente y PAEC/AUTENTICAR se utiliza el protocolo OpenID Connect[10] (especificación de APIs HTTP que utiliza Json como estructura de intercambio de datos), permitiendo que la implementación en la aplicación cliente sea uniforme. De esta forma, se hace transparente tanto para las personas usuarias como para las aplicaciones cliente la diversidad de mecanismos de conexión e intercambio (soap, servicios web xml, json) de los distintos proveedores de identidad.

Federación de identidades.

A su vez, se ha establecido **un identificador único de usuario** para todos los proveedores de identidad, lo que permite crear una federación de identidades, es decir unificar las identidades digitales de la misma persona independientemente del proveedor de identidad utilizado para su autenticación.

Single Sign On.

El usuario se beneficia del Single Sign On (SSO por sus siglas en inglés), puesto que PAEC/AUTENTICAR verifica si ya existe una sesión de usuario iniciada antes de solicitarle credenciales nuevamente. De esta manera la persona usuaria puede utilizar distintas aplicaciones cliente del ecosistema sin tener que validar su identidad en cada oportunidad.

Niveles de Seguridad.

Dada la variedad de proveedores de identidad y sus distintas normativas y procedimientos para establecer la correlación persona física - identidad digital, se utiliza el concepto de nivel de seguridad.

Los niveles de seguridad inferiores indican una verificación menor. A modo de ejemplo, toda persona con ciudadanía argentina y Documento Nacional de Identidad, más de 47 (cuarenta y siete) millones de personas según los resultados provisorios del "Censo Nacional de Población, Hogares y Viviendas 2022"[11], verifica una Identidad Digital con Nivel de Seguridad 1 (uno), cuyas credenciales son el número de documento y el número de trámite que figura en la credencial, lo que permite realizar tramitaciones simples.

Los niveles de seguridad aumentan a medida que las verificaciones documentales y biométricas de las personas son mayores.

Infraestructura.

Actualmente, PAEC/AUTENTICAR se despliega en 10 (diez) nodos/servidores para atender los reconocimientos de identidad recibidos, con 2 (dos) balanceadores de cargas para distribuir las peticiones según los siguientes criterios: el proveedor de identidad requerido y la carga instantánea de cada nodo. Existen proveedores de identidad más utilizados que otros, por distintas razones: mayor facilidad de acceso a las credenciales, mayor cantidad de tramitaciones "no críticas" que se admiten con el nivel de seguridad que otorgan. Uno de los más utilizados en nuestro país es RENAPER, al cual se le asignan 4 (cuatro) nodos dedicados en nuestra infraestructura. En segundo lugar, se encuentra el proveedor de identidad de los agentes y funcionarios de la Administración Pública, con 2 (dos) nodos dedicados. Los restantes 4 (cuatro) nodos no están dedicados a un solo IdP, sino que pueden gestionar cualquiera de ellos.

Esta infraestructura permite administrar los más de 12 (doce) millones de autenticaciones mensuales, que se concentran mayormente en los días hábiles y la franja horaria diurna, lo que implica aproximadamente 1.000 (mil) autenticaciones por minuto.

Marco Normativo.

Existen normativas que respaldan y dan apoyo legal aportando un marco de seguridad jurídica y de uso a la plataforma. Considerando la heterogeneidad de identidades digitales proponen alcanzar una solución de autenticación centralizada, que contenga un único proceso de reconocimiento de personas usuarias para tener acceso a los recursos de sistemas.

- **Decreto Nº 1265/2016**[12] Plataforma de Autenticación Electrónica Central.
- **Resolución 216/2018**[13] Autenticar, Procedimiento, Términos y Condiciones.
- **Decreto Nº 1759/1972**[14] Reglamento de Procedimientos Administrativos.
- **Decreto 1558/2001** Ley 25.326 de Protección de Datos Personales[15].

3. Evolución de la plataforma PAEC/AUTENTICAR

Si bien PAEC/AUTENTICAR se comienza a difundir a partir del año 2016 con la promulgación de la normativa, desde el año 2020 y la pandemia de COVID19, la cantidad de personas que se autentican creció exponencialmente, dato que se observa en las métricas de nuestra plataforma. Esto se debe a que los organismos públicos avanzaron en el desarrollo de

soluciones digitales, en pos de brindar al ciudadano mayor cantidad de servicios y de acercar el Estado a las personas. La concurrencia presencial a las ventanillas de tramitación debió ser reemplazada por plataformas y sistemas que permitieran iniciar la solicitud y en algunos casos la tramitación completa.

Esta irrupción permitió repensar nuevamente los procesos en cada uno de los organismos que componen el mapa del estado y desencadenó el surgimiento de gran cantidad de aplicaciones sobre la red, con la necesidad de registrar e identificar a las personas, mediante una verificación de su identidad de una manera rápida, eficiente y oportuna.

Explosión en uso: personas usuarias y autenticaciones

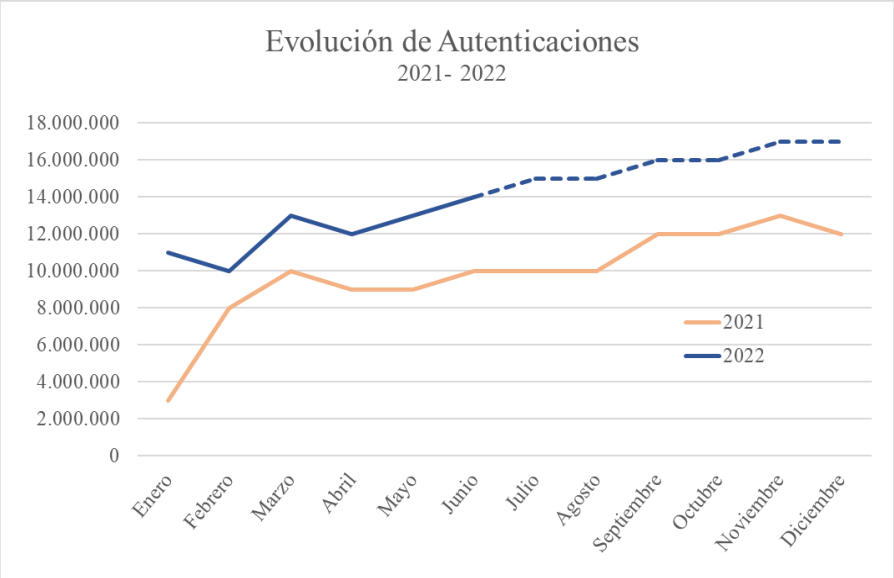
Al inicio de la pandemia, en los primeros meses del 2020, el uso de PAEC/AUTENTICAR ascendió a los **5 (cinco) millones de personas** verificando su identidad en la plataforma. El alto impacto en el consumo requirió revisiones en la infraestructura: la cual se amplió creando nuevos nodos de atención para satisfacer la creciente demanda.

Desde entonces, la cantidad de autenticaciones se mantiene en unos 10 (diez) millones de reconocimientos promedio mensuales, lo cual se traduce en que la plataforma recibe y comprueba aproximadamente 300.000 autenticaciones efectivas por día.

Este indicador sigue constantemente en crecimiento, alcanzando en el mes de mayo del 2022 un total de **13.164.216 interacciones.**

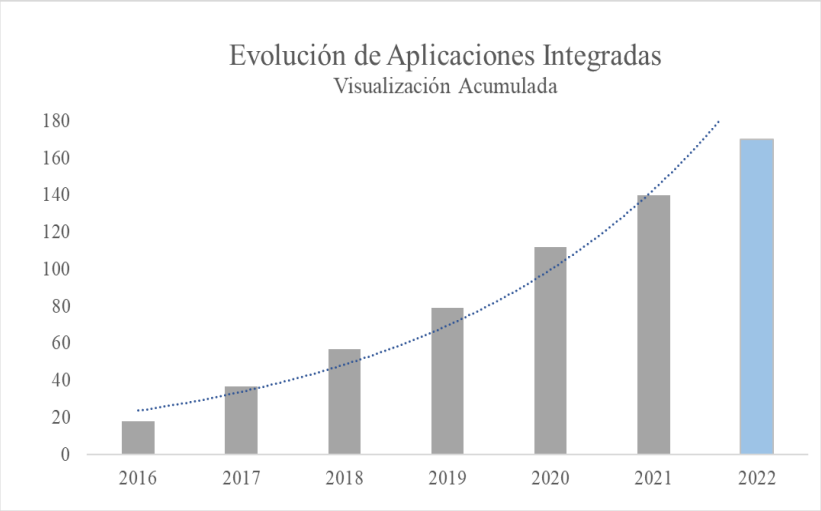
Crecimiento en aplicaciones cliente integradas

La plataforma PAEC/AUTENTICAR cuenta **con 144 (ciento cuarenta y cuatro)** aplicaciones cliente integradas que obtienen el servicio estandarizado de autenticación.



Algunos organismos del Sector Público Nacional que la utilizan son los Ministerio de Desarrollo Productivo, Agricultura Ganadería y Pesca, Turismo y Deporte, el Instituto Nacional de Semillas, Prefectura Naval Argentina, Comisión Nacional de Regulación de Transporte y Agencia de Administración de Bienes del Estado.

A nivel territorial, existen aplicaciones ya integradas de los gobiernos provinciales de Catamarca, Santiago del Estero, San Juan, Chaco y Santa Cruz, y también, a gobiernos municipales como Chivilcoy, Berisso, G.Pueurredón, Concordia, Maipú, Tandil, Saladillo, San Carlos de Mendoza, Catriel, Toluhin, Luján, La Matanza, Hurlingham y San Nicolás.



Se enuncian a continuación tres casos emblemáticos de integración:

PREVIAJE[16], programa de preventa turística y reintegro de gastos para la promoción del turismo iniciado en noviembre de 2021 por el Ministerio de Turismo y Deporte. Su integración a la plataforma consistió en ofrecer el proveedor de identidad "MiArgentina" para las personas usuarias turistas y "AFIP" para los representantes de empresas prestadoras de servicios turísticos. Se gestionaron el acceso de los 5 (cinco) millones de suscriptores al programa, además de los representantes de las empresas, alcanzando el primer lugar en cantidad de personas usuarias entre las aplicaciones cliente de la plataforma.

TAD[17], la plataforma de Tramitación a Distancia del Estado, ofrece a sus más de 3 (tres) millones de personas usuarias registradas los 2412 trámites vigentes a la fecha.

GDD[18], el ecosistema de Gestión Digital Documental del Estado, multiplicó sus instalaciones en ambientes Cloud para su uso por parte de otros organismos a lo largo y ancho del territorio nacional, como solución rápida y eficiente para resolver la necesidad de realizar tramitaciones durante la pandemia, utilizando PAEC/AUTENTICAR como validador de

identidades. Esto permitió no sólo incrementar su uso sino también dar a conocer y trabajar de manera federal en todo el territorio, estandarizando las maneras de validar la identidad.

Incorporación de métodos y proveedores de identidad

La plataforma también debe evolucionar en su arquitectura, ofreciendo distintas alternativas para el reconocimiento de personas usuarias y sus identidades digitales.

En la actualidad es bastante cotidiano el acceso a aplicaciones sistémicas, usualmente utilizadas en dispositivos móviles, que basan su verificación de identidad sobre métodos biométricos y, aunque un poco menos frecuente, también reconocimientos con mecanismos sobre firma digital.

- **Verificación Biométrica**

La autenticación biométrica es un proceso para probar la identidad de las personas utilizando características biológicas únicas, como pueden ser las huellas dactilares o bien, rasgos faciales, patrones oculares, voz, entre otros.

En la Subsecretaría de Innovación Administrativa se está avanzado en la implementación de autenticación biométrica como otros mecanismos de autenticación, para potenciar la plataforma.

Autenticación por Huella Dactilar: la persona se autentica mediante el dispositivo de lectura de huella, la cual es tomada por la plataforma AUTENTICAR, para ser constatada y comparada con la oportunamente capturada al momento de gestionar el Documento Nacional de Identidad o el pasaporte (datos obrantes en RENAPER).

Autenticación por Identificación Facial: actualmente se cuenta con la autenticación mediante el proveedor de identidad MiArgentina, nivel 3, que permite la autenticación por reconocimiento de rostro, e identificar a una persona a partir de una imagen digital tomada por un dispositivo. La Subsecretaría de Innovación Administrativa tiene por objeto avanzar e incorporar este mecanismo dentro de sus servicios, asociándolo a la plataforma AUTENTICAR validando la imagen tomada con el Registro Nacional de la Personas (RENAPER), utilizando el servicio que este organismo aporta.

- **Autenticación con Plataforma de Firma Digital Remota**

Incorporar a la Plataforma de Firma Digital Remota (PFDR)[19] como un Proveedor de Identidad a PAEC/AUTENTICAR, implica un agregado/actualización de la plataforma, usando los servicios existentes que permite por medio de un mecanismo de comprobación de usuario garantizar que la persona es quien dice ser. La Dirección de Firma Digital es el organismo que tiene la competencia para otorgar certificados de firma digital a la ciudadanía. Lo realiza in situ o por medio de sus autoridades de registro desplegadas a lo largo y ancho del territorio nacional. En ambos casos se verifica presencialmente la identidad de las

personas, con la toma de datos biométricos y firma hológrafa. Estas verificaciones permiten que el nivel de seguridad otorgado a sus usuarios sea uno de los más elevados.

El registro de Firma Digital cuenta con 250.000 (doscientos cincuenta mil) firmas registradas, potenciales personas usuarias de la plataforma PAEC/AUTENTICAR con un nivel de seguridad 3 (tres).

4. Hacia un nuevo paradigma de Autenticación:

Identidad Centrada en el Ciudadano.

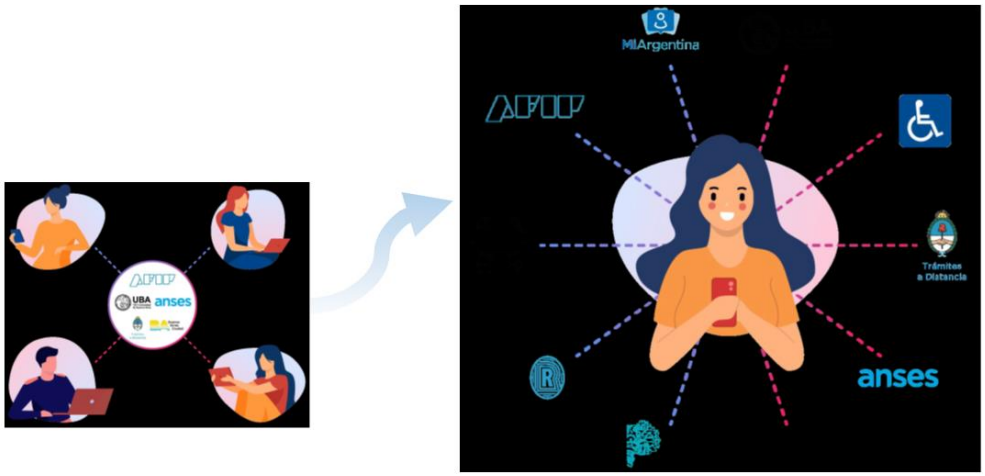
Hablar de un nuevo paradigma de Autenticación Digital Ciudadana nos obliga a abordar interrogantes desafiantes sobre la verificación de la identidad digital, basándose en nuevas tecnologías, tales como las cadenas de bloques, más conocida por su término en inglés "Blockchain".

Lo fundamental de este concepto es situar a los propios individuos en el centro de su Identidad Digital.

Siguiendo los principios de descentralización de blockchain, son las personas y no terceras partes, quienes crean y gestionan su identidad digital.

Se denominan **"identificadores"** a las credenciales que permiten acreditar atributos de identidad de la persona (título universitario, licencia de conducir, certificado de vacunación)

La **Blockchain o Cadena de Bloques** es una tecnología de registro distribuido (Distributed Ledger Technology o DLT), una combinación de tecnologías que permiten crear registros de información digitales, seguros, compartidos y sincronizados, que se actualizan de manera continua, anotando transacciones verificadas por sus participantes, a prueba de manipulación y, por tanto, inmutable, transparente e íntegro.



La “Identidad Centrada en el ciudadano” propone que los organismos (públicos o privados) emitan identificadores/certificados a nombre de la persona y los registren en la blockchain. De esta manera su verificación estará descentralizada en una red blockchain (no ya centralizada como en el modelo tradicional) y la persona los podrá almacenar en portadocumentos, billeteras digitales o wallets y presentarlos ante quien decida. De esta manera, es el ciudadano quien tiene el poder de decidir qué datos comparte.

La Subsecretaría de Innovación Administrativa se encuentra implementando una prueba piloto de aplicación de la tecnología blockchain para la generación identidad digital basada en el ciudadano. El objetivo de esta experiencia es integrar este tipo de identidad descentralizada a los sistemas y servicios que posee actualmente el Estado Argentino mediante su plataforma PAEC/AUTENTICAR.

El éxito de esta experiencia permitirá explorar soluciones en donde la persona ciudadana tenga total control sobre su información y completa autonomía respecto a su identidad digital. El Estado se encargará de verificar su identidad, pero una vez realizado este proceso la persona usuaria podrá autogestionar su propia información.

5. Experiencias en Argentina y en el Mundo

En la Secretaría de Innovación Tecnológica se vienen realizando experiencias variadas y pruebas de concepto sobre el reconocimiento de la identidad digital de las personas:

Gobierno Nacional Argentino junto a los Municipios de la Provincia de Buenos Aires de General Pueyrredón y Berisso: “Autenticación Ciudadana en Blockchain”

En General Pueyrredón se confeccionó un portal llamado “Identidad MDQ” como una ventanilla de trámites y servicios digitales que permite a los vecinos vincular su Identidad Digital y recibir en su porta documentos o wallet los documentos oficiales que el municipio emite bajo la tecnología blockchain. El programa tiene como premisa beneficiar al ciudadano marplatense en épocas de temporada de verano, con el fin de evitar las colas para poder acceder a una entrada para un evento y/o espectáculo, ser atendido prontamente ante un trámite con el municipio y disponer en su portadocumentos digital todas las credenciales emitidas por los organismos municipales.

El Municipio de Berisso plantea avanzar en una solución pensando en los sectores más vulnerables, sus isleños. Los residentes en las islas del Río de La Plata, dada por la geografía del lugar acceden al territorio continental por medio de lanchas, con horarios de ida y vuelta estipulados. Para realizar trámites en oficinas municipales o ser atendidos en hospitales requieren sacar turnos y/o hacer largas colas, llegando a no poder realizar el trámite o atención en el día cuando están por perder la última lancha de regreso a sus hogares. La propuesta es que estas personas tengan acceso a una identificación y credencial digital, que les permita ser atendidos con prioridad, para lo cual se avanzó en la confección de un portal para la autenticación y creación de la identidad descentralizada del ciudadano isleño. El programa fue acompañado de obras de infraestructura y conectividad en el territorio de las islas, condición necesaria para utilizar estas tecnologías.

República Argentina junto a la República Oriental del Uruguay rumbo al "Ciudadano Digital Rioplatense"

Con el fin de avanzar en el reconocimiento de identidades digitales entre países, se creó el grupo de trabajo "*Identidad Digital Rioplatense*", integrado por la Subsecretaría de Innovación Administrativa Argentina y la Agencia de Gobierno Electrónico y Sociedad de la Información y el Conocimiento (AGESIC) Uruguay, con el objetivo de establecer las bases técnicas y normativas para permitir a los ciudadanos de cada país validar su identidad en la plataforma de autenticación del país vecino.

De esta manera se ampliará el universo de identidades reconocidas en ambos países, permitiendo acceder a trámites y servicios estatales para los cuales no es necesaria la ciudadanía o incluso la residencia en territorio. Los 1,5 millones de ciudadanos uruguayos con identidad digital podrán acceder a los más de 2.400 (dos mil cuatrocientos) trámites digitales de Argentina, entre ellos la inscripción en la Universidad de Buenos Aires (UBA) o el inicio de un reclamo en la Dirección Nacional de Defensa del Consumidor y Arbitraje del Consumo.

Por su parte, la ciudadanía argentina accederá a la plataforma de servicios del país vecino, que cuenta a la fecha con 70 (setenta) aplicaciones en el sector público y 100 (cien) aplicaciones del sector privado.

Este proyecto se encara como una continuidad del **Acuerdo de Reconocimiento Mutuo de Certificados de Firma Digital del Mercosur entre Argentina y Uruguay**[20] de Agosto 2021, a través del cual se establece que las firmas digitales emitidas por personas físicas de ambos países son reconocidas como válidas, garantizando un intercambio transfronterizo seguro, confiable, transparente y eficiente.

A nivel internacional, pueden ser ejemplos a seguir en la planificación de programas de implementación de autenticación e identidad digital los siguientes avances en la materia:

Colombia[21] manifiesta que con la implementación de estrategias como el gobierno en línea y los servicios ciudadanos digitales, es necesario que la identidad que se tiene en el mundo físico tenga una representación en el mundo digital tanto para las personas naturales como para las jurídicas.

El proyecto de "Autenticación Digital", mediante el apoyo de herramientas tecnológicas, permite identificar a una persona para obtener una credencial única con la cual puede interactuar digitalmente con cualquier entidad del Estado.

El proyecto de "Carpeta ciudadana" habilita a las entidades que prestan funciones públicas el acceso a repositorios documentales electrónicos de las entidades administrativas para consultar los datos e información de las personas ciudadanas.

Unión Europea[22]: cuenta con un conjunto de normas para la Identificación Electrónica y los Servicios de Confianza en el ámbito de las transacciones digitales del Mercado Único Europeo. Ese reglamento, conocido como eIDAS, por sus siglas en inglés "Electronic IDentification, Authentication and trust Services", establece un marco legal que permite a

todos los Estados miembros de la UE reconocer mutuamente los sistemas de identificación de los demás.

Para el cumplimiento de la reglamentación mencionada, los gobiernos integrantes del bloque posibilitan a los ciudadanos de otros países, integrantes de la misma comunidad política, el uso de identificaciones electrónicas propias para acceder a sus servicios en línea.

España[23]: aprueba el primer estándar mundial sobre identidad digital descentralizada en blockchain, bajo la resolución de la norma española UNE 71307-1, en la que se establece el marco de referencia para la Gestión de Identidades Descentralizadas con tecnología blockchain.

Esa identidad es utilizada ante cualquier entidad privada u oficial, y posibilita escenarios que ya están planteados en Europa, uno de ellos es que cualquier europeo pueda, por ejemplo, matricularse en un colegio en Alemania, acabar sus estudios en Holanda, ser contratado por una empresa en España y recibir ayudas públicas para fundar su propia empresa en Italia, sin necesidad de que las diferentes administraciones deban solicitarse información.

Jamaica, Grecia, Pakistán, Serbia y Turquía[24] han comenzado o están planeando comenzar nuevas fases en sus respectivos programas de implementación de identidad digital.

Grecia anunció, a través de su ministro de Gobernanza Digital, Kyriakos Pierrakakis**,** el lanzamiento de la billetera de identificación digital destinada a facilitar la forma en que los ciudadanos llevan consigo sus credenciales. Mediante esta porta-documentera los usuarios de teléfonos inteligentes del país, acceden, por ejemplo, a sus tarjetas de identificación y licencias de conducir.

Jamaica[25] afirma que los jamaiquinos que vivan en cualquier parte del mundo podrán obtener la tarjeta de identificación biométrica nacional de nueva generación, que será de alta seguridad, y se reconocerá como única prueba de identidad para los titulares, a los que se les permitirá tener acceso a una amplia gama de servicios públicos.

Pakistán ha actualizado su centro de producción de tarjetas inteligentes para alinearlos con los estándares internacionales. El centro de producción de tarjetas inteligentes, tiene una capacidad de 1.200 tarjetas por hora y 125.000 por día, está equipado para cumplir con normas de calidad y pruebas de cumplimiento para cada envío. El lanzamiento de la billetera digital está destinado a facilitar la forma en que los ciudadanos llevan consigo sus credenciales de identificación. Se podrá acceder, por ejemplo, a licencias de conducir desde una billetera digital.

Serbia y Turquía han celebrado un acuerdo que permitirá a los ciudadanos ingresar a los respectivos países con solo una tarjeta de identificación biométrica válida en lugar de visas y pasaportes. El objetivo es mejorar y facilitar la circulación de personas y mercancías entre ambos Estados, así como fomentar las visitas turísticas que son comunes entre ellos.

Singapur[26] lleva tiempo trabajando en el desarrollo de un ecosistema nacional de identidad digital denominado **Singpass**, plataforma que permite realizar transacciones con el gobierno y empresas privadas. Escaneando un QR y con la huella dactilar o ingresando el código en

forma manual, se pueden realizar diferentes operaciones, sin introducir contraseñas. Singpass permite acceder a múltiples identificadores, y a todo tipo de credenciales digitales otorgadas por organizaciones estatales o privadas, haciendo posible todo tipo de trámites con esas instituciones. Incluye desde número de pasaporte y clave bancaria, hasta billetes de avión.

6. Conclusiones y Acciones Futuras

Un mundo más interconectado plantea desafíos en relación a la **Gobernanza de Datos**, para que los distintos Estados puedan concentrar información, identidades digitales, y posibilidades de autenticaciones, que garanticen que la persona sea quien dice ser.

La **Homologación de Normativas**, mediante acuerdos bilaterales, regionales, o internacionales, en materia de Autenticación Digital Ciudadana es vital para que las personas usuarias puedan realizar sus trámites y gestiones, con documentos que tengan la misma validez en un país que en otro.

Actualmente, las personas usuarias de la web generan y reproducen permanentemente identidades e información digital, sin saber dónde quedan almacenados todos esos datos. Los sistemas unificados de autenticación han planteado soluciones a este tipo de temas.

También la realidad virtual invade cada vez más nuestra vida diaria. El surgimiento del Metaverso[27] obliga a abordar nuevas problemáticas sobre las autenticaciones y las identidades digitales.

Avanzando en la búsqueda de un **Identificador Digital Único** para el ciudadano, apoyado en las nuevas tecnologías, la Subsecretaria de Innovación Administrativa pone en valor el concepto de autogestión por parte de la persona en la administración sus credenciales digitales, para que se empodere de sus propios documentos e identificaciones que conforman su identidad digital y las comparta de acuerdo a sus necesidades.

Interrogantes en relación a la identidad digital y su reconocimiento continúan encontrando soluciones y nuevos desafíos constantemente. Han de considerarse casuísticas cómo la de validar credenciales entre los distintos países, recientemente muy notorio ante los certificados de vacunación emitidos por los distintos estados. Habrá que enfrentarse a numerosos retos que mantengan a las personas usuarias libres de cualquier riesgo, hasta incluso garantizar que una identidad digital corresponde a la persona que asegura estar detrás, de manera unívoca y fidedigna.

Referencias

[1] BID – Banco Interamericano de Desarrollo “Regulación de blockchain e identidad digital en América Latina | El futuro de la identidad digital”, 2020 *https://publications.iadb.org/publications/spanish/document/Regulacion-de-blockchain-e-identidad-digital-en-America-Latina-El-futuro-de-la-identidad-digital.pdf*

[2] Argentina. Decisión Administrativa 641/2021 JGM

"Requisitos mínimos de Seguridad de la Información para Organismos".
https://www.boletinoficial.gob.ar/detalleAviso/primera/246104/20210628

[3] Plataforma Electrónica de Autenticación Central PAEC/AUTENTICAR.
https://autenticar.gob.ar

[4] RENAPER. Registro Nacional de las Personas. Ministerio del Interior de la Nación Argentina
www.renaper.gob.ar

[5] AFIP. Administración Federal de Ingresos Públicos de Argentina
www.afip.gob.ar

[6] ANSES. Administración Nacional de la Seguridad Social de Argentina
www.anses.gob.ar

[7] MiArgentina. Jefatura de Gabinete de Ministros de Argentina.
Secretaría de Innovación Tecnológica. Subsecretaría de Servicios y País Digital.
www.argentina.gob.ar

[8] Nic.Ar - Dirección Nacional del Registro de Dominios de Internet. Subsecretaría Técnica. Secretaría Legal y Técnica. Presidencia de la Nación Argentina
www.nic.ar

[9] Administración Pública Nacional. JGM Argentina.
portal.gde.gob.ar

[10] OIDF OpenID Foundation. Protocolo OpenID Connect
openid.net/connect

[11] Resultados provisorios del Censo Argentina 2022. Instituto Nacional De Estadísticas y Censos.
https://www.indec.gob.ar/indec/web/Institucional-GacetillaCompleta-355

[12] Argentina. Decreto Nº 1265/2016 - Plataforma de Autenticación Electrónica Central
https://www.boletinoficial.gob.ar/detalleAviso/primera/155874/20161216

[13] Argentina. Resolución 216/2018
https://www.boletinoficial.gob.ar/detalleAviso/primera/181807/20180417

[14] Argentina. Decreto Nº 1759/72
http://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=21715

[15] Argentina. Decreto Reglamentario (1558/2001) a la Ley 25.326 y sus modificatorias.
www.boletinoficial.gob.ar/detalleAviso/primera/7220500/20011203?busqueda=1

[16] Ministerio de Deporte y Turismo de Nación Argentina
previaje.gob.ar

[17] Plataforma de Tramitación a Distancia del Estado Nacional. JGM Argentina.
tramitesadistancia.gob.ar

[18] Ecosistema de Gestión Digital Documental de la Administración Pública Nacional.
https://cas.gde.gob.ar/

[19] Plataforma de Firma Digital del Estado Nacional JGM Argentina.
https://www.argentina.gob.ar/jefatura/innovacion-tecnologica/innovacion-administrativa/firma-digital

[20] Acuerdo de Reconocimiento Mutuo de Certificados de Firma Digital del Mercosur entre Argentina y Uruguay
https://www.argentina.gob.ar/noticias/argentina-y-uruguay-ratifican-el-acuerdo-de-reconocimiento-mutuo-de-certificados-de-firma

[21] Ministerio de Tecnologías de la Información y las Comunicaciones. Colombia

https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/211009:El-Ministerio-TIC-publica-la-resolucion-que-establece-la-regulacion-para-la-habilitacion-de-los-Servicios-Ciudadanos-Digitales-Especiales
https://www.mintic.gov.co/portal/inicio/Sala-de-Prensa/Noticias/161813:Con-la-guia-de-Blockchain-el-Ministerio-TIC-le-apuesta-a-la-innovacion-publica-a-traves-de-la-transformacion-digital-de-sus-entidades
Centro de Estudios en Derecho Informático Facultad de Derecho - Universidad de Chile.
https://www.scielo.cl/scielo.php?pid=S0719-25842021000200251&script=sci_arttext

[22] eIDAS – Wikipedia Sistema europeo de reconocimiento de identidades electrónicas
https://es.wikipedia.org/wiki/eIDAS
Legal IT Insider, United Kingdom.
https://web.archive.org/web/20180117234338/https://www.legaltechnology.com/latest-news/understanding-eidas-all-you-ever-wanted-to-know-about-the-new-eu-electronic-signature-directive/
eID, Electronic Identification España. Reglamento europeo de identificación digital
https://www.electronicid.eu/es/blog/post/eidas-nuevo-reglamento-de-firma-electronica-en-europa

[23] Telefónica S.A. BlogThinkbig
https://empresas-blogthinkbig-com.cdn.ampproject.org/c/s/empresas.blogthinkbig.com/espana-aprueba-el-primer-estandar-mundial-sobre-identidad-digital-descentralizada-en-blockchain/amp/
España. Resolución a la norma de la Asociación Española de Normalización- UNE 71307-1. Disposición 413 del BOE núm. 9 de 2021
https://www.boe.es/boe/dias/2021/01/11/pdfs/BOE-A-2021-413.pdf

[24] Biometrics Research Group, Update.com
https://www.biometricupdate.com/202206/jamaica-greece-advancing-digital-id-plans-with-biometrics-capture-pilot-digital-wallet

[25] CNW Caribbean National Weekly
https://www.caribbeannationalweekly.com/news/caribbean-news/jamaica-targeting-diaspora-members-for-nids-rollout

[26] Government of Singapore
Singpass is your trusted digital identity for all the secure transaction needs in your everyday life.
www.singpass.gov.sg
Using the SingPass Mobile app to log in within seconds!
https://www.youtube.com/watch?v=f4di4HPgaRY

[27] Cointelegraph, en español
https://es.cointelegraph.com/news/digital-identity-the-only-sure-factor-that-will-represent-you-in-the-metaverse