risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 22/06/2021
Aceitação/Acceptance: 28/08/2021

Un modelo de gestión de la Identidad Digital para el Estado Peruano

Alvaro Cuno[1], Yuri Aldoradín[2], Hedda Ganz[2], Fernando Veliz[2], Erik Papa Quiroz[3,4]

acunopa@unsa.edu.pe; {yaldoradín, hganz, fveliz}@pcm.gob.pe; erikpapa@gmail.com

[1] Universidad Nacional de San Agustín de Arequipa, Departamento de Ingeniería de Sistemas e Informática, Ciudad Universitaria, Arequipa, Perú.

[2] Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros, Lima, Perú.

[3] Universidad Privada del Norte, Departamento de Ciencias, Lima, Perú.

[4] Universidad Nacional Mayor de San Marcos, Facultad de Ciencias Matemáticas, Ciudad Universitaria, Lima, Perú.

Pages: 166-182

Resumen: Presentamos un modelo de gestión de la identidad digital para el Estado peruano, el cual ha sido diseñado considerando sus particularidades culturales, administrativas y legales. El modelo consiste de ocho constructos, cuatro procedimientos, tres niveles de seguridad y cuatro disposiciones operacionales. Su alcance es específico a las interacciones entre personas naturales y jurídicas con todas las entidades de la administración pública. El modelo fue diseñado de forma incremental, habiendo recibido retroalimentación de técnicos y especialistas en identidad digital. Su idoneidad ha sido evaluada contrastándolo con requisitos establecidos y con los principios propuestos por la Unión Internacional de Telecomunicaciones (ITU).

Palabras-clave: Identidad digital; Autenticación; Administración pública; Gobierno digital.

A digital identity management model for digital government in Peru

Abstract: We present a digital identity management model for digital government in Peru, which has been designed considering its cultural, administrative, and legal particularities. The model consists of eight constructs, four procedures, three security levels, and four operational provisions. Its scope is specific to interactions between natural and legal persons with all entities in the public administration. It has been developed incrementally, having received feedback from technicians and digital identity specialists. Its suitability has been evaluated by contrasting its regulatory provisions with established requirements and the principles proposed by the International Telecommunications Union (ITU).

Keywords: Digital identity; Authentication; Public administration; Digital Government.

1. Introducción

Investigadores del Banco Interamericano de Desarrollo (BID) han reconocido a la identidad digital como la piedra angular para la transformación digital de los países de América Latina y el Caribe (Pareja et al., 2017). En ese mismo sentido, la Organización para la Cooperación y el Desarrollo Económico (OECD) ha señalado a la identidad digital como una tendencia clave para la innovación del sector público (OECD, 2018). Así, considerando su importancia, diversos países alrededor del mundo han diseñado modelos (Australia, 2019; Canadá, 2020), estrategias y plataformas tecnológicas para la gestión de la identidad digital dentro de sus respectivas jurisdicciones. En dicha línea, no es menor advertir que diversos organismos internacionales han publicado estudios específicos y marcos de trabajo para la adecuada gestión de la identidad digital, por ejemplo, la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI o UNCITRAL por sus siglas en idioma inglés[1]), el Instituto Nacional de Estándares y Tecnología de los Estados Unidos (NIST por sus siglas en idioma inglés[2]) y el Foro Económico Mundial (WEF por su siglas en inglés[3]).

En el caso del Perú, la importancia de la identidad digital también ha sido reconocida por el Estado. En efecto, en la recientemente promulgada Ley de Gobierno Digital, aprobada con el Decreto Legislativo Nº 1412 del 12/09/2018, la identidad digital ha sido considerada como uno de sus componentes transversales. Sin embargo, debido a que esta ley fue publicada recientemente, diversas entidades públicas atendiendo a sus propias necesidades estuvieron entregando de manera desarticulada a los ciudadanos en general diferentes credenciales de autenticación de la identidad (i.e., usuarios y contraseñas) para el acceso a sus servicios digitales, ocasionando que los ciudadanos acaben teniendo una por cada entidad pública con la que interactúan. Esta situación ha producido no sólo una experiencia poco amigable en el uso de los servicios digitales gubernamentales, en la que se ven obligados a custodiar múltiples credenciales, poniendo su seguridad y privacidad en riesgo, sino que la inadecuada administración de tales credenciales no ha propiciado, y menos ha facilitado, los accesos a servicios digitales del Estado de manera ordenada y que, estimamos por la misma razón, tampoco se ha logrado masificar el uso de diferentes servicios digitales del Estado en la medida que no se ha allanado su apropiación digital[4].

Ante esto, se hace necesaria la definición de un modelo de gestión de la identidad digital que posibilite una efectiva implementación de una administración digital donde se favorezca la prestación de servicios digitales seguros y confiables por defecto centrados en los ciudadanos y personas en general que, a su vez, contribuya con el proceso de

[1] https://undocs.org/es/A/CN.9/WG.IV/WP.153
[2] https://pages.nist.gov/800-63-3/
[3] http://shorturl.at/rtuA5
[4] "[...] la apropiación no se descuenta del mero uso, sino que queda asociada directamente a las posibilidades de que ese uso resulte transformador de las realidades nacionales, sociales o personales. Desde este punto de vista, la apropiación adquiere un rol estratégico y, en ese sentido, instrumental: no es un fin en sí mismo, sino que se logra cuando el uso resulta fructífero en la búsqueda de una meta mayor." (Sandoval L.R., 2019).

transformación y gobierno digital[5] en ciernes en Perú. Para indagar sobre esta cuestión se plantea la siguiente pregunta de investigación: *¿Cuál sería el modelo idóneo de gestión de la identidad digital para la implementación del gobierno digital en el Perú*? Para responder se ha hecho uso del método de investigación denominado *Design Science*, se han tomado como referencia estándares reconocidos internacionalmente, se han revisado modelos desplegados en algunos países representativos y se han tenido en consideración particularidades jurídicas, administrativas, culturales y técnicas del Estado peruano[6].

Este artículo ha sido estructurado de la siguiente manera. En la Sección 2 se hace una revisión sucinta del marco conceptual relacionado. En la Sección 3 se presenta una revisión de experiencias de despliegue de la identidad digital en algunos países representativos. En la Sección 4, se describe el método de investigación, en la Sección 5 el modelo propuesto, en la Sección 6 se presenta la evaluación y en la Sección 7 la discusión. Finalmente, se presentan las conclusiones y los trabajos futuros en la Sección 8.

2. Marco Conceptual

2.1. La identidad de las personas naturales

La identidad de una persona es el conjunto de atributos que permiten distinguirla de otras dentro de un determinado ámbito. Dependiendo del ámbito, el conjunto de atributos utilizados, así como sus valores pueden variar significativamente. Por ejemplo, para la inscripción de una persona en una universidad, usualmente se requiere la utilización del nombre, fecha de nacimiento y sexo tal como consta en su Documento Nacional de Identidad. Sin embargo, para la interacción dentro de un círculo o ámbito amical podría bastar el uso de un apodo o alias como nombre distintivo de la persona. De manera similar, cuando una persona crea su cuenta en la red social Facebook puede optar por utilizar un nombre distinto a los anteriores, así como una foto y una fecha de nacimiento ficticia.

Como puede observarse, los valores de los atributos de identidad difieren en función del ámbito en cuestión. Por ejemplo, en el ámbito del Estado peruano, el nombre, apellidos, la fecha y el lugar de nacimiento, son atributos definidos al momento de la inscripción del nacimiento de un recién nacido. Es decir, la persona (el recién nacido) no elige su nombre ni sus apellidos[7], tampoco puede tener más de una inscripción y no

[5] En el contexto del presente artículo, entiéndase por gobierno digital al uso estratégico de las tecnologías digitales para la creación de valor público, mediante la producción y acceso a datos, contenido y servicios en beneficio de las propias entidades públicas y de las personas naturales y jurídicas que interactúan con el Estado.

[6] Según Pareja et al. (Pareja, 2017), los países toman en cuenta los siguientes factores para adoptar un determinado modelo de gestión de la identidad digital: culturales (p. ej., 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), administrativos (p. ej., la existencia o no de un federalismo fuerte), y técnicos (p. ej., las decisiones respecto a la unicidad u obligatoriedad de un documento nacional se toman después de realizar un análisis de costo-efectividad).

[7] En el Perú, el nombre de una persona no puede ser modificado salvo por motivos justificados y mediante autorización judicial.

puede eliminarse del registro de nacimientos del Estado. Cuando una identidad es única e irremplazable se le denomina identidad básica (UNCITRAL, 2018). En contraste, en el ámbito de una red social, p.ej. Facebook, una persona elige el nombre con el que desea ser identificado, puede tener múltiples inscripciones (cuentas) con diferentes nombres, y las puede eliminar cuando lo desee.

2.2. Estándares ISO/IEC para la gestión de la identidad

Existen dos estándares ISO/IEC que abordan aspectos relacionados a la gestión de la identidad. El primero, el ISO/IEC 24760 *A framework for identity management*, tiene tres partes. La primera parte define conceptos fundamentales relacionados a la gestión de la identidad; la parte 2 provee directrices para la implementación de sistemas de información de gestión de identidades y establece los requisitos para la implementación de un marco para la gestión de identidades; y la parte 3 provee directrices para la gestión de la información de la identidad, asegurándose que éstas se encuentren en concordancia con las partes 1 y 2.

El segundo, el ISO/IEC 29115 *Entity Authentication Assurance Framework* (EAAF), establece un marco de trabajo para la gestión de la confianza de la autenticación de la identidad de una persona en un determinado contexto. El EAAF presenta los siguientes componentes: actores (entidades, proveedor de servicios de credenciales, autoridad de registro, partes que confían, verificador y terceros de confianza), procesos (enrolamiento, gestión de credenciales y autenticación), niveles de confianza (bajo, medio, alto y muy alto), directrices de gestión (provisión del servicio, cumplimiento contractual, provisiones financieras, gestión de la seguridad de la información, auditorías, servicios externos, infraestructura operacional y capacidades operativas), amenazas y controles de seguridad.

2.3. Esquemas para la gestión de la identidad digital

A nivel internacional, es posible encontrar una variedad de esquemas de gestión de los sistemas nacionales de identidad para el ámbito presencial, los cuales de acuerdo a su naturaleza pueden presentar limitaciones inherentes para el desarrollo de la gestión de la identidad digital. Por un lado, hay países en los que una entidad pública central tiene las competencias exclusivas en cuanto al registro civil de nacimientos, al enrolamiento en el sistema nacional de identidad y a la emisión del documento nacional de identidad. En estos países es el Estado el que provee la **identidad fundacional** (aquella que proviene de los registros civiles). En este grupo figuran casi todos los países de América Latina y buena cantidad de países integrantes de la Unión Europea (p.ej. Alemania, Estonia, España, Portugal, etc.). Por otro lado, hay países donde no existe una única entidad pública que enrole y emita un documento nacional de identidad; este es el caso de Canadá, USA, Reino Unido y varios países del Caribe. En estos países suele utilizarse documentos de **identidad funcionales**, por ejemplo, licencias de conducir, carnés del seguro social, pasaportes, etc. Estos documentos coexisten y le corresponde a cada organización definir cuál acepta o no como comprobante de identificación de una persona (Pareja et al., 2017).

2.4. Self-Sovereign Identity

Self-Sovereign Identity (SSI) es un término utilizado frecuentemente para referirse a los esquemas de gestión de la identidad digital basados en la tecnología de registros distribuidos (*Distributed Ledger Technology* - DLT), también conocida como Blockchain. La SSI no siempre es definida consistentemente, pero la mayoría de sus promotores coinciden en definirla como aquella que busca permitir que las personas posean y administren completamente su identidad sin tener que depender de un tercero (Dunphy et al., 2018).

Si bien, la justificación de la SSI está más orientada al ámbito no gubernamental, con la finalidad de contrarrestar la centralización de atributos de identidad que hacen diversas empresas (p.ej., Google, Facebook y Twitter) en Internet, hay algunas iniciativas gubernamentales que vienen estudiando su aplicabilidad, p. ej., *EU Blockchain Observatory and Forum*[8] de la Comisión Europea. Aunque últimamente se ha observado un notorio avance con la aparición de estándares (ISO, 2020a; ISO, 2020b), especificaciones, modelos, plataformas y software libre, todavía no es posible saber si el uso de las DLT para la gestión de la identidad digital puede dar resultados efectivos (Dunphy et al., 2018; Kubach et al., 2020; Liu et al., 2020), en particular en el ámbito gubernamental (Lindman et al., 2020) de aquellos países que se caracterizan por tener un gobierno unitario.

Según lo señalado por Dunphy et al. (Dunphy et al., 2018) y Kubach et al. (Kubach et al., 2020), las Blockchain tienen aún varios desafíos técnicos por superar, y ni qué decir de los desafíos legales. Por ejemplo, Naves et al. (Naves et al., 2019) afirman que la naturaleza descentralizada de la tecnología Blockchain hace que no sea posible determinar bajo qué marco legal se puede hacer uso de ella, en general, porque cada área legal establece las condiciones de aplicabilidad dentro de su dominio. Ellos inciden en que la dificultad de la determinación es mayor cuando se trata de operaciones transfronterizas.

2.5. Hoja de ruta de la ITU

La *International Telecommunication Union* (ITU) ha publicado un documento titulado *Digital Identity Roadmap Guide* (ITU, 2017), donde describen los principales aspectos que se necesitan abordar durante el diseño, desarrollo e implementación de un marco de identidad digital nacional (*National Digital Identity Framework* - NDIF). El documento es una herramienta práctica que: (1) establece quince principios (ver Tabla 1) que sientan las bases para diseñar, desarrollar e implementar un NDIF y (2) define aspectos operacionales críticos de un NDIF (modelo de gobernanza, modelo de adopción, modelo arquitectural y modelo de sostenibilidad).

Según la ITU, los principios fueron desarrollados teniendo en consideración estudios clave, experiencia regulatoria internacional, casos de estudio reales y estándares técnicos/operacionales reconocidos internacionalmente.

[8] https://ec.europa.eu/digital-single-market/en/eu-blockchain-observatory-and-forum

1. Visión y misión	9. Flexibilidad y escalabilidad
2. Enfoque integral	10. Interoperabilidad
3. Inclusión social	11. Velocidad de desarrollo
4. Prosperidad social y económica	12. Identidad como plataforma
5. Derechos humanos fundamentales	13. Unicidad de identificadores
6. Resiliencia	14. Tecnología robusta y resistente al futuro
7. Seguridad, privacidad y confianza	15. Calidad de datos
8. Sostenibilidad y optimización	

Tabla 1 – Principios de la ITU para un NDIF

3. Experiencias de despliegue de la identidad digital

A continuación, se revisa de forma breve algunos aspectos, en relación a la gestión de la identidad digital, de tres países con forma de gobierno federal (Canadá, Australia y Brasil) y cuatro países con forma de gobierno unitario (Uruguay, Chile, Estonia y Corea del Sur). Estos países fueron seleccionados en base a la disponibilidad de información pública en la web[9].

3.1. Países con Gobierno Federal

Canadá es una república federal de más de 37 millones de habitantes, está compuesta por 10 provincias y tres territorios. Canadá ha adoptado un esquema que provee a sus ciudadanos un mecanismo de acceso a sus sistemas de identidad de forma estandarizada. Consiste de un único Broker de Identidad (IdB) y múltiples Proveedores de Identidad (IdP). El IdB está a cargo de la empresa SecureKey Technologies Inc. y los IdP a cargo de siete entidades financieras: *Bank of Montreal*, *Canadian Imperial Bank of Commerce*, *Desjardins Financial Group*, *National Bank of Canada*, *Royal Bank of Canada*, *Scotiabank* y *Toronto Dominion Bank*. Los ciudadanos que pueden utilizar el sistema son todos los clientes de las entidades financieras, quienes utilizan sus credenciales bancarias, mediante una APP denominada Verified.Me para acceder a servicios de entidades de telecomunicaciones, financieras y tiendas en línea. Según el *Global Findex* del Banco Mundial, más del 97% de los canadienses se encuentran bancarizados.

Australia es una república federal de más de 26 millones de habitantes, compuesta de seis estados y dos territorios. Australia está adoptando un esquema federado acreditativo para la gestión de la identidad digital, el cual les permite a los ciudadanos y a las empresas acceder a los servicios en línea del gobierno utilizando un mecanismo único y seguro. En Australia, crear y utilizar una identidad digital es voluntario, las personas que no lo desean pueden acceder a los servicios de gobierno por medios tradicionales, tales como teléfono o de forma presencial. El esquema comprende seis roles (Australia, 2019)[10]: (i)

[9] Es de destacar que para una revisión detallada de la implementación de la identidad digital en América Latina se cuenta con el análisis de Barbosa et al. (2020).
[10] Mayor información sobre el *Trusted Digital Identity Framework* de Australia aquí: https://www.dta.gov.au/our-projects/digital-identity

Proveedores de Servicios de Identidad y Servicios de Credenciales, (ii) Proveedores de Servicios Digitales, (iii) Broker de Identidad, (iv) Servicios de Verificación de Atributos, (v) Proveedores de atributos y (vi) Autoridad para Autorización de Relaciones.

Brasil es una república federal compuesta por 26 estados que cuenta con más de 200 millones de habitantes. Según Torres et al. (Torres et al., 2017), en el 2017, Brasil no tenía un sistema nacional de gestión de identidades digitales en funcionamiento. Ellos consideraban que una de las razones principales es que su sistema nacional de identificación se encontraba fragmentado y era heterogéneo en cada uno de sus estados. Por tal motivo, propusieron una estrategia para la gestión de la identidad digital nacional en el programa e-Gov del Brasil que contemplaba cuatro partes: (i) Gestión de la infraestructura, (ii) sistema de gestión de la identidad digital, (iii) factores de autenticación y (iv) modelo de documento de identidad. No obstante, es importante destacar que, recientemente, Brasil ha desplegado un servicio centralizado de autenticación de la identidad digital del ciudadano, denominada *LoginUnico* integrado a la plataforma GOV.BR, que hasta abril del presente año, ya contaba con 100 millones de usuarios registrados[11]. El servicio fue creado por el Ministerio de Economía y por el Servicio Federal de Procesamiento de Datos. El concepto del servicio fue concebido mediante el proyecto de la Plataforma de Ciudadanía Digital instituido por el Decreto número 8.936, del 19 de diciembre de 2016.

3.2. Países con gobierno unitario

La República Oriental del **Uruguay** es el segundo país más pequeño de América del Sur, comprende alrededor de 19 departamentos y 112 municipalidades distritales, y tiene aproximadamente 1.5 millones de habitantes. Como parte de su Agenda Digital 2020, instrumento orientador y directriz del proceso de transformación digital del país, implementó el portal GUB.UY como único punto de acceso que centraliza la oferta de servicios públicos y orienta a los ciudadanos para su adecuada utilización. Asimismo, dispuso la obtención obligatoria de la Cédula de Identidad Digital, documento que acredita la identidad de un ciudadano uruguayo, el cual es proporcionado por la Dirección Nacional de Identificación Civil (DNIC). Además, y enfocándose en un entorno digital, la Agencia de Gobierno Electrónico y Sociedad de la Información y el Conocimiento (AGESIC), en su calidad de ente rector y a través de su servicio digital "USUARIO-gub.uy" (https://mi.iduruguay.gub.uy) ha habilitado también la posibilidad de que los ciudadanos acrediten su identidad a través de tres mecanismos: (i) Usuario y contraseña, (ii) Cédula de Identidad Digital y (iii) Identidad digital móvil.

La República de **Chile**, con una población de más de 19 millones de habitantes, ha instaurado un mecanismo centralizado de autenticación digital denominado "ClaveÚnica" que es proporcionado gratuitamente por el Servicio de Registro Civil e Identificación, a la luz de lo dispuesto en la Ley Nº 19.799 y su reglamento (Decreto Nº 181). ClaveÚnica busca proveer a los ciudadanos de una Identidad Electrónica Única (RUN y contraseña) para la realización de trámites en línea con el Estado. Es considerada una firma electrónica que puede emplearse en los procedimientos administrativos y

[11] https://www.gov.br/pt-br/noticias/financas-impostos-e-gestao-publica/2021/04/gov-br-alcanca-a-marca-de-100-milhoes-de-usuarios-cadastrados

en cualquier clase de acto jurídico (salvo algunas excepciones). De acuerdo al portal https://claveunica.gob.cl/, en la actualidad, más de 8 millones de ciudadanos cuentan con su clave única activa y 212 entidades públicas han integrado sus servicios con la plataforma de autenticación de la identidad. Para una revisión detallada de la identidad digital en Chile se recomienda el estudio titulado *Digital Government in Chile – Digital Identity* publicado por la OECD (OECD, 2019).

La República de **Estonia** es una república báltica situada en el nordeste de Europa, que cuenta con una población de alrededor de 1.3 millones de habitantes. Desde el 2004 forma parte de la Unión Europea y de la OTAN. A diferencia de otros países, el 98% de su población tiene una identidad digital emitida por el Estado en forma de una tarjeta inteligente (ID-Card). Adicionalmente, los estonios tienen la posibilidad de utilizar soluciones más modernas como la Mobile-ID y Smart-ID. Estonia diseñó e implementó su esquema nacional de identidad digital desde el año 2002, el cual está basado en la infraestructura de clave pública y puede ser utilizado tanto por el sector público y privado. Las entidades del sector público y aquellas del sector privado que prestan servicios públicos utilizan el servicio nacional de autenticación (TARA) provista por la Autoridad de Sistemas de Información (RIA).

La República de **Corea del Sur** es un país de Asia Oriental que cuenta con más de 51 millones de habitantes. A nivel mundial, es considerado uno de los países líderes en materia de gobierno electrónico. En el 2017, Corea diseñó e implementó *Digital One Pass*, un sistema integrado de autenticación de la identidad de los ciudadanos para el acceso a servicios digitales gubernamentales. Este sistema proporciona una variedad de métodos de autenticación, tales como, autenticación vía móviles (rostro, huella dactilar, patrones, PIN, certificados acreditados), certificados acreditados en computadoras personales y SMS. El sistema cuenta con dos niveles de seguridad: nivel alto (huella dactilar, patrones, PIN, certificado digital) y nivel bajo (SMS o contraseña). Una de las fortalezas del sistema es que un ciudadano puede utilizar una única credencial de identidad digital para acceder a centenas de servicios electrónicos gubernamentales provistos desde su portal GOV.KR.

4. Método

El método de investigación utilizado en este trabajo es el *Design Science*, el cual permite obtener conocimiento y entendimiento de un dominio mediante la construcción y uso de artefactos artificiales, los cuales, según Hevner et al., (2004), pueden ser: (i) constructos[12], (ii) modelos[13], (iii) métodos[14] o (iv) instanciaciones[15]. Para el proceso de investigación hemos utilizado la propuesta de Peffers et al. (2007), que está conformada

[12] Los **constructos** definen los conceptos básicos y el lenguaje con los cuales se definen y comunican los problemas y las soluciones.
[13] Los **modelos** utilizan los constructos para representar el problema o solución en el contexto del mundo real.
[14] Los **métodos** permiten transformar un modelo o representación en otra representación con la finalidad de resolver un problema o realizar una tarea.
[15] Las **instanciaciones** representan la operacionalización de los constructos, modelos y métodos.

por cinco actividades: (i) definición del problema, (ii) objetivos de la solución, (iii) diseño y construcción, (iv) demostración y (v) evaluación.

La definición del problema no ha ofrecido mayor dificultad ya que la gestión de la identidad digital es señalada como uno de los grandes desafíos que los países tienen que superar para llevar a cabo su transformación digital. En efecto, como consecuencia del despliegue de servicios digitales y ante la ausencia de un esquema oficial para la autenticación de la identidad digital, un buen número de entidades públicas del Estado peruano han venido desplegando servicios digitales haciendo uso del tradicional "usuario y contraseña" sin poner mayor atención a los problemas subyacentes que esto genera, por ejemplo: (1) multiplicidad de "usuarios", uno por cada entidad, pudiendo este ser un correo electrónico, un número de DNI, un número de RUC, un nombre arbitrario, etc., (2) diversidad de políticas de definición y recuperación de contraseñas y (3) la no adopción de protocolos de autenticación basados en estándares técnicos reconocidos. Otro desafío que se encontró fue la falta del reconocimiento formal del problema a nivel país. No obstante, producto de acciones de sensibilización y tomando en consideración las recomendaciones de organismos internacionales, fue posible incluir a la identidad digital como uno de los bloques fundamentales en la Ley de Gobierno Digital del Perú aprobada el 12 de diciembre de 2018.

La solución que se propone para el problema es un modelo de gestión de la identidad digital específicamente diseñado para la interacción entre personas naturales y jurídicas con todas las entidades de la Administración Pública. En particular, para los siguientes escenarios: C2G (*citizen to government*), G2C (*government to citizens*), G2G (*government to government*), G2E (*government to employees*), y G2B (*government to businesses*). Debido a la complejidad de abordar el problema en toda su magnitud, se ha visto pertinente acotar su alcance, excluyendo interacciones C2B (*Citizens to Business*) y B2B (*Business to Business*), con la finalidad de darle viabilidad a la propuesta, lo cual no impide que en un futuro pueda ser ampliado. El modelo de gestión a adoptarse tendría que cumplir con los siguientes requisitos:

R1. Tomar como base los registros nacionales de identificación
R2. Encontrarse alineada a estándares y buenas prácticas reconocidas internacionalmente, en particular el NDIF de la ITU
R3. Contemplar consideraciones jurídicas, culturales, administrativas y técnicas del Estado
R4. Ser única frente a todo el Estado
R5. Ser segura y fácil de usar
R6. Ser de rápido despliegue.

Tabla 2 – Requisitos del modelo de gestión de la identidad digital para el Estado peruano

El diseño, desarrollo y demostración del modelo de gestión se realizó de manera incremental y cíclica. Fue desarrollado incrementalmente, poniendo a discusión versiones intermedias de manera regular, y fue mejorado constantemente hasta que todos los requisitos fueron satisfechos. La demostración del modelo fue realizada en workshops, reuniones con especialistas en identidad digital y entrevistas focalizadas.

5. El Modelo

El modelo está conformado por constructos, procesos, niveles de seguridad y disposiciones operacionales.

5.1. Constructos

Los constructos que conforman el modelo son los siguientes: Ciudadano Digital, Plataforma Nacional de Autenticación, Gestor de la Identidad Digital, Servicio Digital, Proveedor de Servicios Digitales, Proveedor de Atributos de Identidad, Credencial de Autenticación y Domicilio Digital Nacional. Una representación gráfica de los principales constructos se presenta en la Figura 1, y un ejemplo de interacción entre ellos es descrito a continuación. Cuando un ciudadano digital requiere acceder a un servicio digital para realizar un trámite (paso 1), éste delega la autenticación de la identidad hacia la plataforma nacional de autenticación (paso 2). Entonces, ésta última interactúa con un gestor de la identidad para efectuar la autenticación del ciudadano digital (paso 3). Una vez autenticado, el ciudadano digital realiza el trámite requerido. Una vez atendido el trámite, el servicio digital envía una notificación al domicilio digital nacional del ciudadano (paso 4), quién finalmente ingresa a su domicilio digital para acceder a la notificación (paso 5).

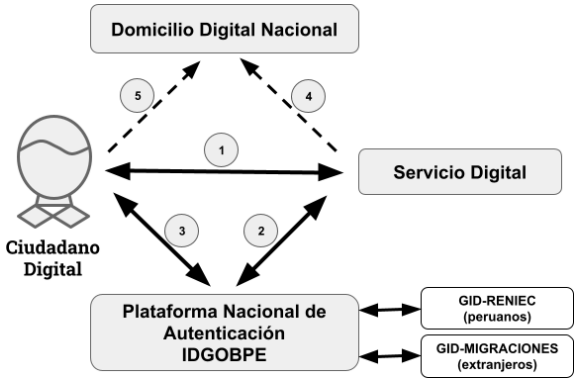

Figura 1 – Constructos del modelo de gestión de la identidad digital. Las flechas continuas representan una interacción síncrona y las discontinuas una interacción asíncrona.

Un **Ciudadano Digital** es aquel peruano o extranjero que cumple con los siguientes requisitos: (i) tiene atributos de identidad inherentes registrado en el Registro Nacional de Identificación y Estado Civil (RENIEC) o en la Superintendencia Nacional de Migraciones (MIGRACIONES), (ii) cuenta con su domicilio digital nacional y (iii) cuenta con credenciales de autenticación activas. Además, para el ejercicio pleno de su ciudadanía, el ciudadano digital requiere de conectividad, dispositivos (PC, tablet, smartphone, etc.) y capacitación.

La **Plataforma Nacional de Autenticación** (IDGOBPE), es aquella que permite autenticar en línea la identidad de un ciudadano digital mediante los servicios de autenticación de la identidad digital de los peruanos o extranjeros provistos por los

Gestores de la Identidad Digital. Esta plataforma es administrada por la Secretaría de Gobierno y Transformación (SGTD) de la Presidencia del Consejo de Ministros (PCM).

El **Gestor de la Identidad Digital** (GID), es aquel que provee el servicio de autenticación de la identidad digital de los peruanos o de los extranjeros en el Perú, a través de la plataforma IDGOBPE. Los GID son dos: (i) El RENIEC que gestiona el servicio de autenticación de los peruanos, y (ii) MIGRACIONES que gestiona el servicio de autenticación de los extranjeros.

Los **Proveedores Públicos de Servicios Digitales** (PPSD) son todas las entidades de la Administración Pública del Perú que proveen servicios digitales.

Los **Atributos de Identidad Digital** son aquellos datos que en su conjunto caracterizan a un ciudadano digital. Se clasifican en inherentes y complementarios. Los atributos inherentes son aquellos que permiten distinguir a un ciudadano digital cómo distinto de otros y que posibilitan el ejercicio de sus derechos fundamentales dentro del contexto del Estado peruano. Los atributos complementarios son aquellos que en conjunto con los inherentes permiten caracterizar a un ciudadano digital desde una determinada perspectiva (económica, social, tributaria, etc.).

Los **Proveedores de Atributos de Identidad** son todas las entidades de la Administración Pública que gestionan algún atributo de identidad de las personas. Ellos son responsables de mantener la veracidad, la exactitud y la vigencia de los valores de tales atributos.

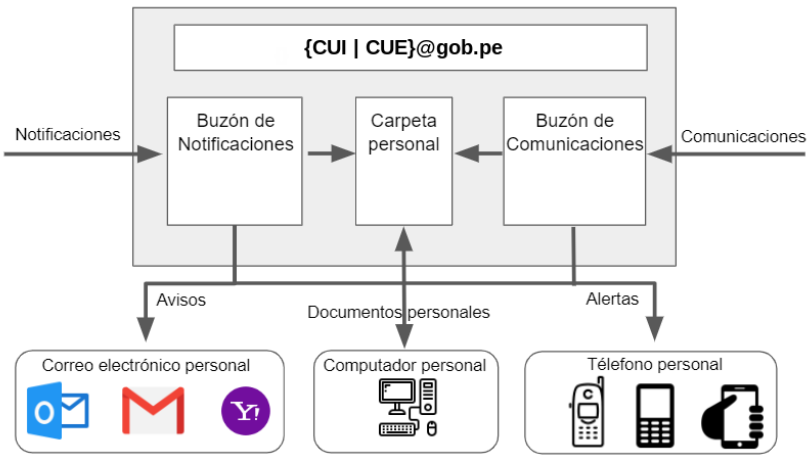

Figura 2 – Domicilio digital nacional: componentes e interacciones

Una **Credencial de Autenticación** es aquella representación de la identidad digital utilizada por un ciudadano digital para demostrar que es quién dice ser. Es emitida, entregada, activada y/o revocada por un GID.

El **Domicilio Digital Nacional** ostenta equivalencia funcional y jurídica con el domicilio habitual y sirve para recibir comunicaciones y/o notificaciones remitidas por

las entidades de la Administración Pública a los ciudadanos digitales. Es asignado a todos los ciudadanos digitales y está conformado por los siguientes componentes: (i) dirección electrónica única (CUI | CUE@gob.pe), (ii) buzón de notificaciones, (iii) buzón de comunicaciones y (iv) carpeta personal. Una representación gráfica de estos componentes se presenta en la Figura 2. La plataforma Domicilio Digital Nacional es administrada por la SGTD de la PCM.

5.2. Procedimientos

El modelo contempla cuatro procedimientos: enrolamiento, credencialización, autorización y autenticación.

El **enrolamiento** es el procedimiento mediante el cual se hace una inscripción en los registros oficiales del Estado peruano. Para el caso de los peruanos, comprende a la inscripción de nacimientos y a los procedimientos de actualización de datos de forma periódica (obligatoria cada 8 años o voluntaria cuando el ciudadano lo solicite) en el Registro Único de Identificación de Personas Naturales (RUIPN). Para el caso de los extranjeros corresponde a su inscripción en el Registro de Información de Migraciones (RIM) administrado por la Superintendencia de Migraciones. Este procedimiento es desarrollado por los GID en el marco de sus funciones y competencias.

La **credencialización** es el procedimiento mediante el cual se crean, activan o entregan credenciales de autenticación de identidad digital a los peruanos y extranjeros. Es desarrollado por los GID atendiendo las disposiciones establecidas por la plataforma IDGOBPE.

La **autenticación** es el procedimiento que permite autenticar en línea la identidad de un ciudadano digital mediante el uso de credenciales de autenticación. Es realizado por la plataforma IDGOBPE a través de los servicios provistos por los GID: RENIEC (para peruanos) y MIGRACIONES (para extranjeros). Ambos servicios incorporan tres niveles de seguridad. Este procedimiento es desarrollado por los GID atendiendo las disposiciones establecidas por la plataforma IDGOBPE.

La **autorización** es el proceso realizado por los PPSD, que se sigue después de una autenticación exitosa, mediante el cual se determinan los recursos permitidos o restringidos al ciudadano digital autenticado.

5.3. Niveles de seguridad

Los niveles de seguridad del modelo describen el grado de confianza en la autenticación de la identidad digital. Se han definido los siguientes tres niveles, considerando los factores que hay de por medio para su autenticación:

- **Nivel 1:** Provee un nivel de seguridad "básico" respecto de la identidad de un ciudadano digital autenticado. Para este nivel se requiere el uso de por lo menos un (01) factor de autenticación.
- **Nivel 2:** Provee un nivel de seguridad "razonable" respecto de la identidad de un ciudadano digital autenticado. Para este nivel se requiere el uso de dos (02) factores de autenticación diferentes entre sí.

- **Nivel 3:** Provee un "alto" nivel de seguridad respecto de la identidad de un ciudadano digital autenticado. Para este nivel se requiere el uso de dos (02) factores de autenticación diferentes entre sí, debiendo uno de ellos estar basado en un módulo criptográfico resistente a manipulaciones.

5.4. Disposiciones operacionales

En la Tabla 3, se presentan las disposiciones operacionales que se han definido para cada uno de los procedimientos de gestión de la identidad digital.

	Enrolamiento	**Credenciamiento**	**Autenticación**
Gobernanza	RENIEC y MIGRACIONES	RENIEC y MIGRACIONES	*Identity Broker*: SGTD y *Identity Providers*: RENIEC y MIGRACIONES
Adopción	Obligatoria	Obligatorio: DNI electrónico (DNIe) o DNI digital (DNId) Opcional: otras credenciales	Obligatorio: servicios digitales totalmente en línea
Arquitectura	RENIEC y MIGRACIONES	RENIEC y MIGRACIONES	Un *Identity Broker* (SGTD) y dos *Identity Providers* (RENIEC y MIGRACIONES)
Sostenibilidad	Pagado por persona natural	Gratuito	Gratuito: personas naturales y sector público Pagado: sector privado

Tabla 3 – Disposiciones operacionales

6. Evaluación

La evaluación de la idoneidad del modelo ha sido efectuada por los autores, contrastándolo con los requisitos establecidos en la Tabla 2. Con respecto al requisito R2, en la siguiente tabla se sustenta el cumplimiento de cada principio del NDIF de la ITU.

Visión: Personas identificadas con acceso a servicios digitales del Estado peruano de forma segura y fácil. **Misión:** ID basada en los registros nacionales de identificación. Múltiples niveles de seguridad de la autenticación y obligatoriedad de implementación de los servicios digitales totalmente en línea.
Enfoque integral: El modelo ha partido de un análisis global del entorno digital (uso de estándares internacionalmente reconocidos y la revisión de casos de algunos países federados y no federados) y de las circunstancias (marco jurídico peruano) y prioridades del país (sector público).
Inclusión social: El modelo ha sido diseñado de manera que sus servicios se puedan proporcionar a toda la comunidad que requiere interactuar con los servicios digitales de las entidades públicas (peruanos y extranjeros). Las personas con habilidades especiales, en estado de vulnerabilidad o de comunidades nativas no están obligadas a tener una identidad digital. Ellos pueden seguir haciendo uso de su identidad convencional si lo desean, lo cual les permitirá continuar disfrutando de las políticas de inclusión digital que tanto el RENIEC como MIGRACIONES tienen ya establecidas para estos casos.
Prosperidad social y económica: El modelo fomenta la prosperidad económica de las personas con los ahorros esperados al hacer uso de trámites en línea, así como con la obtención gratuita de las credenciales de autenticación.
Derechos humanos fundamentales: El modelo propuesto respeta y es coherente con los derechos humanos fundamentales de las personas porque está construido dentro del marco jurídico establecido para la gestión de la identidad en entornos presenciales.

Resiliencia: En la propuesta se ha dispuesto un enfoque de gestión de riesgos eficiente con la finalidad de asegurar un nivel adecuado de resiliencia.
Seguridad, privacidad y confianza: El modelo garantiza salvaguardas adecuadas (en conformidad con las normas nacionales) para la privacidad de los ciudadanos digitales y garantiza un nivel adecuado de seguridad de la información para ganar un alto nivel de confianza entre ellos y las partes interesadas.
Sostenibilidad y optimización de costos: Para garantizar la sostenibilidad del modelo, se ha propuesto un enfoque que no es totalmente gratuito ni completamente pagado. Los peruanos pagan una tasa para obtener su DNI (US $9) o por su DNIe (US $10), pero no por las otras credenciales de autenticación. De forma similar, los extranjeros pagan por el Carné de Extranjería una tasa de aproximadamente US $12. Las entidades públicas no pagan por utilizar los servicios de la plataforma IDGOBPE, salvo aquellas que lo hacen para la obtención de ingresos exclusivos.
Flexibilidad y escalabilidad: El modelo propuesto es flexible a actualizaciones y cambios debido a su modularidad y escalabilidad, pudiendo ser modificado o actualizado de manera rápida y efectiva cuando sea necesario.
Interoperabilidad: La interoperabilidad entre sistemas de identificación no es necesaria puesto que se ha adoptado el uso de los registros nacionales que son únicos, tanto para peruanos como para extranjeros. La interoperabilidad del servicio está garantizada debido a la adopción de protocolos de autenticación interoperables.
Velocidad de despliegue: Se ha propuesto que el despliegue de la plataforma sea en el corto plazo para los peruanos, y para los extranjeros en el mediano plazo. También se ha propuesto que la adopción sea incremental, empezando por las entidades públicas más grandes y finalizando con aquellas de menor envergadura..
Identidad como plataforma: La propuesta ha sido diseñada para ser la plataforma de autenticación oficial del Estado, con alcance nacional y con capacidad para interoperar con los servicios digitales provistos por todas las entidades públicas.
Unicidad de identificadores: Cada persona tiene un único identificador (CUI para los peruanos y CUE para los extranjeros) que las distingue de otras, aunque pueden tener múltiples credenciales de autenticación. La unicidad del identificador está garantizada por la adopción de los registros nacionales fundacionales de identificación (RENIEC y MIGRACIONES). Además, la seguridad de los registros se basa en el uso de herramientas biométricas y en su depuración valiéndose de las mismas.
Tecnología robusta y resistente al futuro: El modelo es robusto en el sentido de que está basado en los registros nacionales de identificación, en el uso de estándares internacionalmente reconocidos para garantizar su exactitud, integridad y seguridad. Para evitar la obsolescencia se ha previsto disposiciones para llevar a cabo acciones de mejora continua.
Calidad de datos: La calidad de los datos de identidad y su exactitud han sido asegurados mediante la adopción de los registros nacionales correspondientes.

Tabla 4 – Argumentación del cumplimiento de los principios definidos por la ITU

7. Discusión

Se han identificado cuatro aspectos que podrían ser atribuidos como limitaciones del modelo propuesto. El primero es que, a simple vista, no se contempla la participación del sector privado. Sin embargo, debe observarse que si bien la gobernanza (SGTD) y la operación de los procedimientos de autenticación (RENIEC y MIGRACIONES) se encuentran a cargo de organismos del sector público, nada impide que estos puedan contratar servicios del sector privado para su implementación, por ejemplo, servicios TIC, plataformas, hardware, software, interfaces de programación (APIs), tarjetas de identificación, etc.

El segundo aspecto se refiere a la incompatibilidad con los principios de la identidad auto-soberana (SSI). Respecto a este aspecto debe recordarse que, para el caso del Estado peruano, los atributos de identidad y sus valores no pueden ser creados o modificados a discreción ("soberanamente") por los ciudadanos, sino que estos son gestionados en exclusividad por los organismos públicos designados para esta tarea; con la finalidad de garantizar la seguridad jurídica de los actos de las personas cuando interactúan digitalmente con el Estado.

El tercer aspecto se refiere al hecho de no haber contemplado el consentimiento del ciudadano en el intercambio de atributos de identidad entre las entidades de la administración pública (proveedores de atributos, proveedores de identidad y proveedores de servicios digitales). Al respecto, es menester señalar que, en el caso del Perú, el Estado es único e indivisible, por lo tanto, no existe propiamente dicho "intercambio" entre entidades públicas, puesto que los atributos ya se encuentran "dentro" del Estado.

Un cuarto aspecto está referido a su alcance. Si bien se tienen muchas ventajas al hacer regulaciones únicamente para el sector público (p. ej., para evitar la sobre-regulación del sector privado, la creación de un esquema acreditativo para IdPs, etc.), se perciben también algunas desventajas (p. ej., la dificultad que tienen algunas organizaciones privadas de cumplir regulaciones mínimas de seguridad, así como la existencia de innúmeras credenciales de autenticación de servicios del sector privado en las manos del ciudadano). Sin embargo, consideramos que regular únicamente al sector público responde a una cuestión estratégica de índole progresiva.

Por último, una limitación a destacar es la referida a la evaluación de la idoneidad del modelo, puesto que la contrastación con los requisitos de la Tabla 2 pudiese ser calificada como subjetiva, lo cual podría menguar su credibilidad (a pesar que el modelo fue construido incrementalmente y con la participación de expertos en identidad digital). Por lo que una evaluación menos subjetiva sería una realizada en base a una implementación del modelo.

8. Conclusiones y trabajos futuros

En respuesta a la pregunta de investigación planteada, concluimos que el modelo de gestión de la identidad digital más idóneo para el despliegue del gobierno digital en el Perú es aquel conformado por: (i) ocho constructos (ciudadano digital, plataforma nacional de autenticación, gestor de la identidad digital, servicios digitales, proveedores de servicios digitales, proveedores de atributos de identidad, credenciales de autenticación y domicilio digital nacional), (ii) tres procedimientos (enrolamiento, credenciamiento y autenticación), (iii) tres niveles de seguridad (básico, razonable y alto) y (iv) cuatro disposiciones operativas (gobernanza, adopción, arquitectura y sostenibilidad). Este modelo ha sido diseñado teniendo en consideración el sistema nacional de identificación existente en el país, que para el caso de los peruanos (incluyendo mayores y menores de edad) tiene más del 98% de cobertura. Además, se ha tenido en cuenta aspectos jurídicos, culturales, administrativos y técnicos propios del Estado peruano, recomendaciones de organizaciones internacionales reconocidas (ISO/IEC) y experiencias de algunos países

federados y no federados (con gobiernos unitarios). La idoneidad del modelo ha sido evaluada mediante la verificación del cumplimiento con los requisitos de la Tabla 2, en particular, con los principios transversales del framework de identidad digital de la ITU.

Entre los posibles trabajos futuros destacamos los siguientes: (i) la evaluación de la idoneidad del modelo con otras alternativas, (ii) la implementación del modelo, (iii) la activación de cuentas, (iv) la inclusión de organizaciones del sector privado como GID, (v) el análisis para soportar operaciones C2B (*Citizens to Business*) y B2B (*Business to Business*), y (vi) su extensión para alcanzar la interoperabilidad a nivel transfronterizo con países de la región y de otras latitudes.

Referencias

Australia, (2019). Australia D. T. A. Trusted Digital Identity Framework: Architecture Overview. https://www.dta.gov.au/our-projects/digital-identity/trusted-digital-identity-framework.

Barbosa et al., (2020). Barbosa, A., Carvallho, C., Machado, C., and Costa, J. Good ID in Latin America. https://itsrio.org/wp-content/uploads/2020/07/ReportGoodIDENG.pdf.

Cheesman, (2020). Cheesman, M. Self-sovereignty for refugees? the contested horizons of digital identity. Geopolitics, pages 1–26.

Dunphy et al., (2018). Dunphy, P., Garratt, L., and Petitcolas, F. Decentralizing digital identity: Open challenges for distributed ledgers. In *2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 75–78. IEEE.

Canada, (2020). D. and of Canada, A. C. Pan-Canadian TrustFramework Model. https://diacc.ca/trust-framework/.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS quarterly*, 75-105.

ISO (2020a). Blockchain and distributed ledger technologies —privacy and personally identifiable information protection considerations. Standard ISO/TR 23244:2020, Geneva, CH.

ISO (2020b). Blockchain and distributed ledger technologies— vocabulary. Standard ISO 22739:2020 (en), Geneva, CH.

ITU (2018). Digital Identity Roadmap Guide. ITU, Geneva. Unión Internacional de Telecomunicaciones.

Kubach et al., (2020). Kubach, M., Schunck, C. H., Sellung, R., and Roß-nagel, H. Self-sovereign and decentralized identity as the future of identity management? Open Identity Summit 2020.

Lindman et al., (2020). Lindman, J., Berryhill, J., Welby, B., and Barbieri, M. P., 2020. The uncertain promise of blockchain for government.

Liu et al., (2020). Liu, Y., He, D., Obaidat, M. S., Kumar, N., Khan, M. K.,Choo, K.-K. R., et al. Blockchain-based identity management systems: A review. Journal of Network and Computer Applications, page 102731.

Naves et al., (2019). Naves, J., Audia, B., Busstra, M., Hartog, K. L., Yamamoto, Y., Rikken, O., and van Heukelom-Verhage, S. Legal aspects of blockchain. Innovations: Technology, Governance, Globalization, 12(3-4):88–93.

OECD, (2019). Digital Government in Chile: Digital Identity. https://doi.org/10.1787/9ecba35e-en.

OECD, (2018). Embracing innovation in government global trends 2018. https://www.oecd.org/gov/innovative-government/innovation2018.htm

Pareja et al., (2017). Pareja, A., Pedak, M., Gómez, C., and Barros, A. La gestión de la identidad y su impacto en la economía digital. Technical report, Discussion Paper No. IDBDP-529. Washington, DC: BID.

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. Journal of management information systems, 24(3), 45-77.

Reuben, W. and Carbonari, F. (2017). Identification as a national priority: the unique case of Peru. Technical Report, Center for Global Development.

Sandoval, L. R. (2019). La apropiación de tecnologías en América latina: una genealogía conceptual. Virtualis, 10(19):1-19.

Torres et al., (2017). Torres, J., Verzeletti, G., Távera, R., de Sousa Júnior, R. T., and de Mello, E. A national identity management strategy to enhance the Brazilian electronic government. CLEI Electronic Journal, 20(3):8–1.

UNCITRAL, (2018). Cuestiones jurídicas relacionadas con la gestión de la identidad y los servicios de confianza (A/CN.9/WG.IV/WP.153). Asamblea General de las Naciones Unidas Comisión de las Naciones Unidas para el Derecho Mercantil Internacional. Grupo de Trabajo IV (Comercio Electrónico) 57o periodo de sesiones. https://undocs.org/es/A/CN.9/WG.IV/WP.153. 2018.

Zwitter et al., (2020). Zwitter, A., Gstrein, O. J., and Yap, E. Digital identity and the blockchain: Universal identity management and the concept of the 'self-sovereign' individual. Front. Blockchain, 28.