UNIVERSIDAD
TORCUATO DI TELLA

Tipo de documento: Tesis de maestría

Maestría en Políticas Públicas

Identidad digital descentralizada y Gobierno: hacia un nuevo modelo de gobernanza de datos en el sector público

Autoría: *Gallo, Lucía*

Año de defensa de la tesis: *2022*

¿Cómo citar este trabajo?
Gallo, L. (2022) "*Identidad digital descentralizada y Gobierno: hacia un nuevo modelo de gobernanza de datos en el sector público*". [Tesis de maestría. Universidad Torcuato Di Tella]. Repositorio Digital Universidad Torcuato Di Tella
https://repositorio.utdt.edu/handle/20.500.13098/12070

El presente documento se encuentra alojado en el Repositorio Digital de la Universidad Torcuato Di Tella bajo una licencia Creative Commons Atribución-No Comercial-Compartir Igual 2.5 Argentina (CC BY-NC-SA 2.5 AR)
Dirección: https://repositorio.utdt.edu

Biblioteca Di Tella

UNIVERSIDAD TORCUATO DI TELLA

Escuela de Gobierno

Maestría en Políticas Públicas

IDENTIDAD DIGITAL DESCENTRALIZADA Y GOBIERNO: HACIA UN NUEVO MODELO DE GOBERNANZA DE DATOS EN EL SECTOR PÚBLICO

Alumna: Lucía Gallo

Tutor: Lucas Jolías

Diciembre, 2022.

Índice

Agradecimientos

A Eduardo Gallo y Alejandra López, por el esfuerzo y la libertad con la que me educaron. A Natalia Simonet, mi compañera de vida, y a mis amigas, Victoria Leo Murias e Ivanna Velisone: gracias a las tres por ser mi sostén y por hacer mi mundo inmensamente más feliz. A mi hermana Sara, por ser la persona tan especial que es y por alegrar mi vida.

A la Universidad Torcuato Di Tella, mi casa de estudios, por su excelencia y por abrirme un mundo de oportunidades. A mi camada de la Maestría en Políticas Públicas, por el compañerismo y el apoyo. Especial agradecimiento a Lucía Castañeda, por los días, tardes y noches de estudio y en especial por su amistad. También a Santiago Bestilleiro, quien además de ser mi amigo es un referente para mi.

Finalmente, quiero agradecer a la persona que hizo posible este trabajo: Lucas Jolías, tutor de este trabajo. Gracias a él por tener la mejor predisposición desde el primer día, por la generosidad y por sus enseñanzas.

1. Introducción

El advenimiento de nuevas tecnologías digitales ha generado una gran disrupción en todos los ámbitos de la sociedad. Industrias enteras se vieron transformadas, aparecieron nuevos modelos de negocios y también la posibilidad de una interacción mucho más personalizada y masiva de lo que se podría haber pensado apenas unas décadas atrás. Las consecuencias no sólo se sintieron en el sector privado sino también en la cotidianeidad de las personas, que incorporaron la tecnología en su forma de comunicarse, informarse, educarse e interactuar con terceros.

El sector público no estuvo exento de esto. En los últimos años, hemos visto impactos positivos en el funcionamiento interno de los gobiernos así como en su interacción con lxs ciudadanxs gracias a políticas de transformación digital. De acuerdo al BID, a partir de la digitalización, en América Latina los trámites se volvieron un 74% más ágiles[1]. A nivel económico, países como Brasil han generado ahorros de aproximadamente 350 millones de dólares por año, de los cuales el 75% representan ahorros para los usuarios, según datos del gobierno brasileño[2].

Si bien los avances hacia una transformación digital de las administraciones públicas son importantes y han generado un impacto positivo en la sociedad, los resultados han sido muy dispares según los países y jurisdicciones que se analicen. Desde una óptica teórica, lxs expertxs en la materia indican un horizonte que parece muy difícil de alcanzar: gobiernos con enormes estructuras, diferentes niveles de gestión y años de una tradición burocrática donde “el expediente manda”, deberían compartir información entre sí y con terceros de manera segura, rápida y eficiente, haciendo un uso inteligente de los datos para mejorar la prestación de servicios a la vez de impulsar la economía digital.

Aún con avances significativos, tanto la confianza en el sector público como la satisfacción por los servicios públicos se encuentran hace años en mínimos que parecen muy difíciles de revertir. Si bien la política de gobierno digital no es la razón principal de este descontento, sí es una de las caras más visibles de los gobiernos frente a sus ciudadanxs y, como tal, tiene un enorme potencial para mejorar la situación actual. El contraste con la realidad del sector privado es grande: este ha sacado un gran provecho de las nuevas

[1] Cetina, Camilo. 2022. *DIGIntegridad: La transformación digital de la lucha contra la corrupción*. Edited by Carlos Santiso. CAF, p.19. https://scioteca.caf.com/handle/123456789/1901.
[2] Ibidem, p. 76.

tecnologías para dar saltos de innovación más palpables por lxs usuarixs, lo cual puso más de manifiesto las falencias del sector público.

Al hablar de transformación digital, uno de los principales desafíos del sector público -aunque también del privado- es la interoperabilidad de sus sistemas para generar procesos más ágiles que beneficien a la ciudadanía pero también que permitan eficientizar el funcionamiento interno de lo público. La interoperabilidad es una de las bases fundamentales de la transformación digital justamente porque es la que permite que múltiples sistemas puedan hablar un lenguaje en común y generar así servicios eficientes y políticas de gobierno digital integradas y que creen valor para la sociedad.

Sin embargo, las administraciones públicas no sólo cargan con enormes estructuras burocráticas con sistemas que no dialogan entre sí: además existen conflictos y rivalidades entre ellas -e internas a la organización- así como una falta de protocolos de estandarización de datos que actúan en detrimento de un uso compartido de la información. Los incentivos y mecanismos burocráticos del Estado, hacen muy difícil que la interoperabilidad institucional y administrativa se expanda por toda la administración pública y entre los diferentes niveles de gobierno.

Como consecuencia, los gobiernos -en todos sus niveles- continúan delegando en la ciudadanía la responsabilidad de recolectar y proveer una y otra vez la misma información aunque sin permitirle la autogestión de esos datos personales. Aún más, en muchas ocasiones es el propio Estado el que emitió esa información en primer lugar, pero por la falta de interoperabilidad mencionada, el usuarix debe volver a solicitarla y/o presentarla reiteradamente. Por esa falta de integración y de protocolos en común, no sólamente las gestiones se vuelven ineficientes sino que se generan grandes brechas de seguridad en los procesos de validación de esos datos.

Dentro de esta problemática, la gestión de la identidad digital cobra una gran importancia ya que es, junto a la interoperabilidad, otro de los grandes pilares de las políticas públicas de gobierno digital: es la llave de acceso de todas las personas al mundo digital y el nexo de los diferentes servicios y proyectos que los gobiernos llevan adelante. Poder identificar de forma rápida, eficiente y segura a una persona para validar que es quién dice ser, es la base fundamental para poder escalar a una mayor cantidad y complejidad de trámites y servicios digitales.

Al respecto de la gestión de la identidad digital, cabe señalar, en primer lugar, que los modelos mayormente utilizados en la actualidad son de carácter centralizado y no ofrecen demasiadas garantías para la seguridad de lxs usuarixs. Según estimaciones del The Digital Trust Index (2022)[3], durante el 2021 el costo global del cibercrimen ha sido de 6 trillones de dólares, lo que representa más del 40% de toda la economía digital del mundo. Lo que es más preocupante es que para 2025 calculan que la economía digital tendrá un valor de $20,8 trillones, pero el ciberdelito tendrá un valor de $10,5 trillones.[4]

En segundo lugar, junto con las grandes innovaciones privadas han aparecido en los últimos años grandes monopolios que reúnen enormes volúmenes de información personal y sensible. Empresas como Google, Facebook, Twitter, entre otras, se convirtieron en habilitadores para operar digitalmente pero a un costo enorme para la seguridad y privacidad de los usuarios. No sólo hay una gran falta de transparencia sobre el uso de esos datos sino que existen ya numerosos casos de graves infracciones a las leyes de protección de datos personales[5].

Ante esta situación, surge con claridad una necesidad de repensar los modelos de gobernanza de datos actuales para así también rever las bases sobre las cuales apoyan las estrategias de gobierno digital. Asimismo, urge dar mayores y mejores garantías a la ciudadanía sobre el uso y seguridad de sus datos personales, y de esta manera comenzar a reconstruir la confianza ciudadana hacia el sector público.

En línea con esa necesidad, en los últimos años, el surgimiento y los avances en la adopción de tecnologías disruptivas como blockchain han permitido a distintos actores del ecosistema pensar en estrategias y protocolos que contribuyan a resolver este problema y a transformar la gestión de la identidad digital. Estas tecnologías implican, en muchos casos, una nueva lógica en la ideación de modelos de gestión de la información en general y de la identidad digital en particular, que tiene un gran contraste con el modelo tradicional adoptado por el sector público.

---

[3] Cebr. 2022. “The digital trust index: What is the value of digital trust?”, Londres. bit.ly/3Wyt5nh
[4] Hayat, Zia. 2022. “Why digital trust is key to building thriving economies.” The World Economic Forum.
https://www.weforum.org/agenda/2022/08/digital-trust-how-to-unleash-the-trillion-dollar-opportunity-for-our-global-economy/.
[5] Fowler, Geoffrey A., y Geoffrey Fowler. 2021. “Your privacy is the price of Facebook’s monopoly.” *The Washington Post*, August 29, 2021.
https://www.washingtonpost.com/technology/2021/08/29/facebook-privacy-monopoly/
La cuestión viene tomando relevancia desde hace ya una década. Ver más en:
https://www.forbes.com/sites/tamlinmagee/2014/01/31/social-id-raises-questions-on-data-ownership-privacy-monopoly/?sh=7668d2ec39a4

En este trabajo se explorarán los avances, tendencias y desafíos de las políticas de gobierno digital a nivel global, haciendo énfasis en las políticas de identidad digital, los modelos de gestión existentes y las nuevas propuestas que se apalancan en blockchain, entendiendo estas temáticas como centrales para el presente y futuro de la transformación digital del ámbito público. Finalmente, para entender la aplicación práctica de estos modelos, se analizará el protocolo impulsado por el Gobierno de la Ciudad de Buenos Aires, y creado de forma colaborativa y abierta, para una gestión descentralizada de la identidad digital.

El objetivo principal de este trabajo es aportar al conocimiento existente sobre dos temas sobre los cuales no abunda información. Por un lado, las implicancias de la identidad digital y la interoperabilidad para la transformación digital en gobierno; por otro lado, el uso de una tecnología como blockchain y de enfoques descentralizados para ello. Asimismo, se busca contribuir al análisis de casos prácticos en la región latinoamericana, entendiendo que existe sobre esta región un corpus bibliográfico aún menor y que América Latina posee características distintivas que no permiten extrapolar estudios de otras latitudes. Finalmente, se pretende abrir debates y nuevas investigaciones que profundicen sobre el estudio de los temas a tratar en este trabajo.

2. Hipótesis y metodología

El presente trabajo sostiene que la problemática principal de las políticas de transformación digital del sector público reside en la nula o baja interoperabilidad de sus áreas y que la implementación de modelos de gobernanza de datos descentralizados para la gestión de la identidad digital pueden ser una solución a este problema.

Ante esta situación, resulta esencial explorar nuevos modelos de gobernanza de datos del sector público que ataquen de raíz la problemática actual. En este sentido, la identidad digital es un pilar fundamental de la transformación digital del sector público ya que actúa como un "pasaporte" al mundo digital en su totalidad. Garantizar la autenticación de las personas y el acceso a sus credenciales de manera segura y eficiente es la base para una transformación digital del sector público sostenible, inclusiva y efectiva[6].

Como mencionamos anteriormente, la llegada de la tecnología blockchain habilitó un surgimiento más robusto de modelos descentralizados y abiertos para la gobernanza de datos. Estos, han dejado de ser teóricos para empezar a mostrar aplicaciones reales y potencialmente revolucionarias. En contraposición a los modelos actuales, la recuperación del control sobre su información por parte de la ciudadanía le devuelve también un rol activo en la administración de su información, dándole a las personas esa agilidad de la que los gobiernos carecen.

Es en estos nuevos esquemas donde reside la gran oportunidad para administraciones públicas de mejorar su gobernanza de datos para lograr así una verdadera transformación digital que ponga a lxs ciudadanxs en el centro.

Aunque el concepto de blockchain tiene algunas décadas, su aplicación tal como la conocemos hoy es reciente. Es recién en 2008, con la aparición del white paper sobre Bitcoin, bajo la autoría de "Satoshi Nakamoto"[7], que comienzan a surgir de forma muy incipiente las primeras aplicaciones, mayormente en el sector de las finanzas.

A la hora de analizar el desarrollo de políticas públicas que incorporen esta tecnología, encontramos un desarrollo más tardío e incipiente en la mayoría de países. Aún más, si nos

[6] Roseth, Benjamin. 2021. "Gobierno Digital: 5 pilares para tener servicios públicos sin salir de casa." Blogs iadb. https://blogs.iadb.org/administracion-publica/es/gobierno-digital-5-pilares-que-permiten-al-gobierno-ofrecer-servicios-sin-salir-de-casa/.

[7] Satoshi Nakamoto es un seudónimo y, si bien existen teorías sobre quién o quiénes están detrás del whitepaper, se desconoce su origen real.

circunscribimos únicamente a políticas para la gestión de identidad, dejando de lado aplicaciones financieras, los casos que pueden encontrarse se reducen ampliamente. Adicionalmente, algunas aplicaciones actuales de blockchain adoptan enfoques centralizados a través del uso de redes privadas o permisionadas; si bien esta cuestión se explorará más adelante, cabe mencionar que este tipo de enfoques se diferencian sustancialmente de los descentralizados y que muchas de los estudios publicados al día de la fecha se centran en ellos.

En consecuencia, la bibliografía sobre la temática surge mayormente a partir del año 2018, aumentando su volumen con el transcurso de cada año y los avances de la tecnología. Es importante destacar también que la mayoría de estudios existentes se concentran en casos fuera del sur global, siendo particularmente escasa la información disponible para entender la situación de América Latina en esta cuestión.

Por estos motivos, este trabajo adopta un enfoque exploratorio y descriptivo. En primer lugar, se busca contextualizar el desarrollo de las políticas de gobierno digital a nivel global y regional, para tener una imagen de los progresos y oportunidades que existen en la actualidad, en términos generales. En segundo orden, se hará foco en uno de los pilares de la transformación digital: las políticas de identidad digital. En particular, la atención se centrará en lo que respecta a los nuevos modelos de gestión descentralizados que han surgido en el último tiempo, apalancados en una tecnología como blockchain, y la relación de estos con la interoperabilidad en gobierno.

Para ello, se utilizarán distintas herramientas metodológicas y de relevamiento de información. Por una parte, se realizará un meta análisis de investigaciones cuali-cuantitativas que reúnen distintas teorías, metodologías, datos y conclusiones, con el fin de obtener una visión integral de la temática y generar nuevas interpretaciones de los temas a tratar en este trabajo. Se analizarán mayormente fuentes secundarias de diversa índole, tales como estudios, investigaciones, informes, policy papers, conferencias y publicaciones que puedan aportar al entendimiento de una temática novedosa en el ámbito de la gestión pública. Además, se realizará un análisis de la encuesta de E-government de la Organización de Naciones Unidas, una de las fuentes de información más importante sobre la materia.

Asimismo, para lograr comprender en profundidad este modelo innovador, se optó por el enfoque de análisis de caso. En concreto, se hará foco en Quark ID, un protocolo descentralizado para la gestión de la identidad digital que es impulsado por el Gobierno de

la Ciudad de Buenos Aires pero que tiene el apoyo de importantes actores del sector privado y de otros gobiernos latinoamericanos. A través de entrevistas a profesionales involucrados con el proyecto, se buscará echar luz sobre la visión, características y aspectos técnicos del proyecto. Los testimonios contribuyen a caracterizar a este proyecto y también entender las perspectivas futuras de los modelos descentralizados en otras latitudes.

Al ser una temática tan novedosa, este trabajo busca aportar a la generación de conocimiento, en particular sobre casos concretos de aplicación en América Latina, por lo que el objetivo principal no es contrastar hipótesis sino indagar de manera exploratoria un nuevo modelo de gobernanza de datos para el sector público. Asimismo, se pretende abrir camino a debates y futuras investigaciones sobre la transformación digital del sector público y sobre aspectos específicos de la incorporación de enfoques descentralizados de gestión de datos, el uso de tecnologías exponenciales, la interoperabilidad y la identidad digital en el ámbito público.

Finalmente, en línea con esa búsqueda de aporte de conocimiento, este trabajo incorpora un análisis de la base de datos de las Naciones Unidas sobre el desarrollo del e-government y la e-participation en el mundo realizado en lenguaje R y publicado en formato abierto en GitHub para que toda persona pueda descargarlo, analizarlo y reproducirlo, además de utilizarlo de base para realizar nuevas investigaciones[8]. También se encuentra una versión en formato HTML en R-pubs[9].

[8] El repositorio con el código se encuentra disponible en: https://github.com/lushugallo/egovernment . Al respecto, en este trabajo se incorpora un breve análisis de las bases de datos mencionadas mientras que en GitHub se puede acceder a información más detallada.
[9] La versión en html del análisis puede consultarse en https://rpubs.com/lushugallo/egovernment

3. Nuevos paradigmas estatales en el mundo digital.

3.1. El camino al gobierno digital: de e-government a gobiernos de plataforma.

La irrupción de nuevas tecnologías digitales ha modificado radicalmente a la mayoría de las sociedades en un corto período de apenas 4 décadas. A finales del siglo XX, el incremento en el acceso a una computadora personal y a la conexión a internet creó nuevas posibilidades al mundo. Muchas de las innovaciones que surgieron durante el siglo XXI eran inimaginadas en ese entonces.

La llegada de la llamada Cuarta Revolución Industrial surge de la mano de la llegada de tecnologías digitales como internet de las cosas (IoT), la inteligencia artificial y el aprendizaje automatizado (machine learning), la robótica, la computación en la nube, blockchain, entre otras. Es la reciente combinación y convergencia de estas tecnologías la que dio lugar a innovaciones tan transformadoras que remiten a una nueva revolución industrial[10].

Si bien con variaciones en su acceso, cada vez más personas podían hacer un uso intensivo de ellas en casi todas las actividades cotidianas: acceder a la educación, a servicios públicos, comunicarse de forma rápida, acceder a -y generar- información con una llegada masiva, y la lista sigue. La enorme caída de los costos de acceso a componentes tecnológicos o en el almacenamiento de información permiten que hoy se vean niveles exponenciales de creación de información y nuevos conocimientos que circulan también con enorme velocidad.

La digitalización se ha producido de manera más acelerada en el sector privado[11], transformando industrias enteras y creando nuevos modelos de negocio. Allí, los procesos tendieron a ser cada vez más automáticos y eficientes, la provisión de servicios también creció en volumen y calidad, con una personalización de estos como nunca antes se había visto. Asimismo, la composición de los rankings de mayor capitalización empresarial se vieron alterados: actualmente son las empresas intensivas en tecnologías quienes están en la cabeza.

---

[10] Navarro, Juan Carlos. 2018. “El imperativo de la transformación digital: Una agenda del BID para la ciencia y la innovación empresarial en la nueva revolución industrial.” https://bit.ly/3C6g1gM, pp. 3-5.
[11] Neri, Antonio. 2022. “Public sector risks losing trust as digital transformation lags.” The World Economic Forum. https://www.weforum.org/agenda/2022/05/the-public-sector-must-accelerate-digital-transformation-or-risk-losing-sovereignty-and-trust/

Aunque más lentamente, desde el sector público también se han producido grandes avances en esa dirección. Las estrategias de incorporación de tecnologías en la administración pública no han sido unívocas sino que han ido variando a lo largo del tiempo de acuerdo al contexto de cada país y a las tecnologías disponibles. Factores como la capacidad de adopción e inversión tecnológica de cada gobierno, la voluntad política, la demanda ciudadana, las prácticas culturales y los procesos de contratación pública, entre otros, marcaron distintos rumbos en la modernización en el sector público[12].

Respecto a esa evolución, la digitalización fue concebida en sus comienzos como la incorporación de tecnologías de la información y las comunicaciones (TICs) para incrementar la eficiencia de las agencias gubernamentales, comunicar información y posteriormente, proveer servicios online[13]. En esta etapa, la tecnología era utilizada como un medio para digitalizar procesos analógicos preexistentes, con el fin de hacerlos más eficientes, pero no para introducir nuevas lógicas de gestión a partir de ella.

Más adelante, las políticas de gobierno digital buscaron dejar de centrarse en las tecnologías en sí para empezar a poner el foco lxs usuarixs y en los resultados de las innovaciones. A través del rediseño y reingeniería de procesos, pero sobre todo mediante el establecimiento de una nueva cultura digital por diseño, se buscó satisfacer la necesidad de lxs ciudadanxs[14]. En paralelo, la interacción del sector público con la ciudadanía y el sector privado se incrementó y mejoró en calidad, a la vez que se buscó habilitar la innovación en los procesos, servicios y productos de gobierno[15].

Es necesario subrayar que es usual encontrar un uso laxo o intercambiable de términos como “e-government” y “gobierno digital”, para referirse a distintos tipos de políticas de incorporación de tecnología en gobierno y/o procesos generales de digitalización o transformación digital. Esto no sólo ocurre en la bibliografía principal de esta temática o en ámbitos académicos sino también en la práctica de las políticas públicas: algunas políticas y estratégicas de digitalización son englobadas en varios países bajo el término

---

[12] Naciones Unidas. 2020. *United Nations E-Government Survey 2020*. Nueva York: Naciones Unidas. https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2020-Survey/2020%20UN%20E-Government%20Survey%20(Spanish%20Edition).pdf., p. 23;
Santiso, Carlos, y Idoia Ortiz de Artiñano. 2020. *Govtech y el futuro del gobierno 2020*. CAF y PublicTechLab de IE University de España. https://docs.ie.edu/publicteclab/GOVTECH_Y_EL_FUTURO_DEL_GOBIERNO.pdf., p. 17.

[13] United Nations. 2001-2022. *UN E-Government Survey*. https://publicadministration.un.org/egovkb/en-us/Overview.

[14] OCDE. 2019. *The Path to Becoming a Data-Driven Public Sector*. París: OECD Publishing. https://doi.org/10.1787/059814a7-en., p. 14.

[15] United Nations. 2001-2022. *UN E-Government Survey*.

e-government, mientras que en otros casos el mismo término se utiliza para definir a la etapa inicial o anterior a la de las políticas de gobierno digital[16].

3.1.1. Evolución de la estrategia de digitalización del sector público.

A pesar de los diferentes usos de la terminología, podrían establecerse cuatro grandes etapas del desarrollo de las estrategias de transformación digital del sector público. Estas son: gobierno analógico, gobierno electrónico, gobierno digital y gobierno inteligente[17].

Durante la etapa más incipiente, la de **gobierno analógico**, se comienza a incorporar tecnología para crear registros internos y estadísticas; el foco está en las operaciones y lógicas internas así como en procedimientos analógicos[18]. Con la estrategia de **gobierno electrónico**, a lo anterior se suma un uso de las TICs como herramientas de transparencia y comunicación con la ciudadanía[19]. Este momento coincide en varios países con la irrupción de internet y su primera etapa de desarrollo -también conocida como Web1- donde el foco estaba en la comunicación de información pero no en la interacción[20]. De esta manera, comienzan a verse páginas oficiales de gobiernos, con esporádicas publicaciones de información pública general, pero en las cuales la población no interactúa.

La etapa de **gobierno digital**, por su parte, va un paso más lejos: aquí los datos comienzan a ser más masivos -y en algunos casos abiertos-, y pasan a tener un rol más preponderante en la estrategia de modernización estatal con el fin de crear valor público, mejorar el diseño de las políticas públicas y promover la innovación. Se comienza a hablar de automatización de procesos a gran escala, integración de servicios y un salto en la eficiencia administrativa[21]. Este estadío tiene su análogo en el desarrollo de la internet actual, la Web 2, momento en el que el que la interacción y las transacciones pasan a ser protagonistas.

Finalmente, en la etapa de **gobierno inteligente**, se incorpora tecnología más avanzada para sacar el máximo provecho del conocimiento extraído de los datos; lxs ciudadanxs se consolidan como eje central de los procesos, el diseño y la implementación de políticas[22].

---

[16] United Nations. 2001-2022. UN E-Government Survey. p24.
[17] Santiso, Carlos, y Idoia Ortiz de Artiñano. 2020. *Govtech y el futuro del gobierno 2020*, pp. 25-27.
[18] Ibidem.
[19] Ibidem.
[20] Jolías, Lucas, Ana Castro, y Jesús Cepeda, eds. 2022. *Identidad Digital Descentralizada : una guía de implementación de blockchain en gobierno*. Bahía Blanca: GovTech Hub. https://plus.os.city/publicaciones/identidad-descentralizada.p. 25.
[21] Santiso, Carlos, y Idoia Ortiz de Artiñano. 2020. *Govtech y el futuro del gobierno 2020*, pp. 25-27.
[22] Ibidem.

Es en esta etapa donde se desarrollan e incorporan soluciones digitales integradoras que buscan evitar los típicos silos o compartimientos estancos característicos de modelos de gestión anteriores y generar una mayor articulación, comunicación e interoperabilidad entre agencias y dependencias de gobierno. Este enfoque suele denominarse Gobierno como Plataforma (GaaP) o de "todo el Gobierno" (Whole-of-Government approach o WGA)[23].

Tabla 1. Elementos de la transformación digital de los gobiernos[24].

	Gobierno analógico	Gobierno electrónico	Gobierno digital	Gobierno inteligente
Enfoque	• Operaciones cerradas y enfoque de lo interno. • Procedimientos analógicos.	• Transparencia y enfoques centrados en el ciudadano. • Procedimientos impulsados por TIC.	• Enfoques impulsados por la apertura al usuario y los datos. • Transformación de los procedimientos y operaciones.	• Aprovechamiento del conocimiento derivado de los datos para hacer del ciudadano el eje central.
Datos	• Estadísticas y registros administrativos	• Acceso a la información	• Analítica de datos, datos abiertos y masivos.	• Inteligencia artificial y análisis predictivo.

Es importante resaltar el hecho de que no todos los gobiernos han logrado avanzar de manera uniforme a través de estas etapas. Asimismo, las mismas son esquemáticas y reflejan, en la mayoría de los casos, los lineamientos que las políticas de digitalización deberían seguir de acuerdo a lxs expertxs y al corpus teórico. La mayor parte de los gobiernos no ha alcanzado aún un desarrollo que se encuadre totalmente dentro del esquema de GaaP y, en algunos casos, tampoco han alcanzado siquiera etapas anteriores.

3.1.2. Encuesta de Gobierno Digital de la Organización de Naciones Unidas

Como hemos mencionado, la bibliografía sobre la transformación digital en el sector público aparece con fuerza en los últimos 10 años y no existen demasiados estudios globales sobre la cuestión. Una fuente de referencia muy importante sobre la temática proviene de la Organización de Naciones Unidas, que lleva adelante dos encuestas que evalúan el nivel de desarrollo de las políticas de e-government y el grado de participación de la ciudadanía de 193 países. En ellas, el término de e-government se entiende en un sentido amplio y evoluciona con el paso del tiempo.

[23] Santiso, Carlos, y Idoia Ortiz de Artiñano. 2020. *Govtech y el futuro del gobierno 2020*, pp. 25-27.
[24] Ibidem, p. 27.

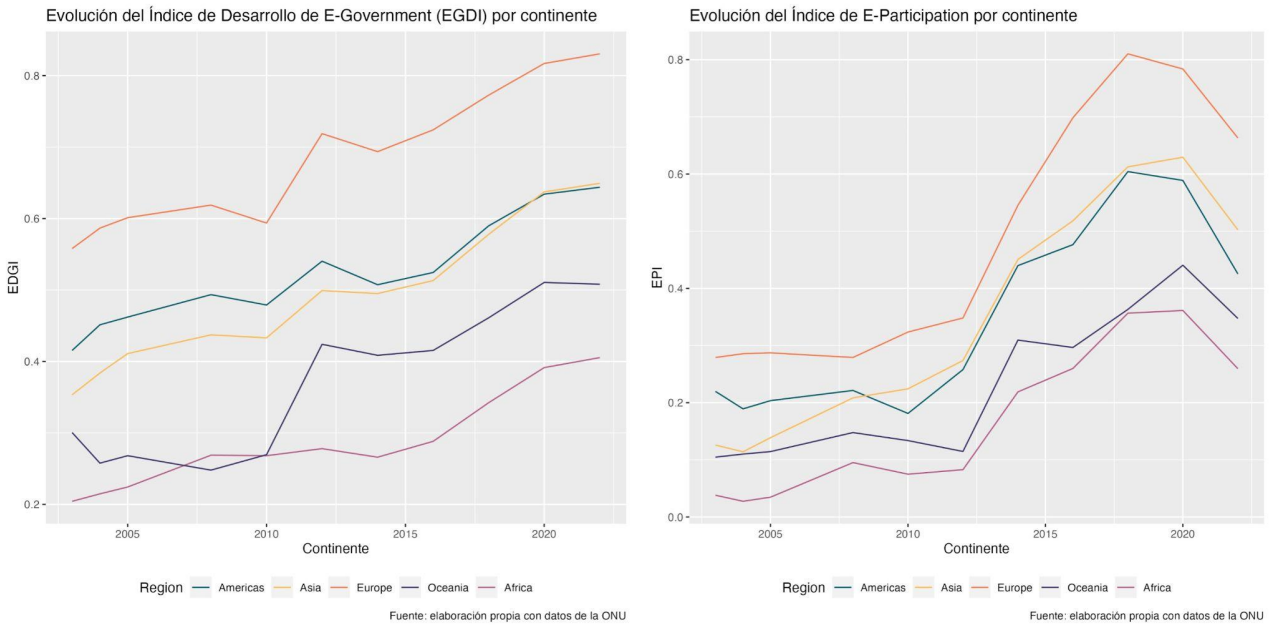
Con una primera medición en el año 2003 y una periodicidad promedio de 2 años[25], el índice de e-government (EGDI) mide el progreso de los países miembros de las Naciones Unidas en sus políticas de e-governement y la efectividad en la prestación de servicios públicos digitales. El índice se conforma por tres sub-índices de servicios online, capital humano y de infraestructura de las telecomunicaciones.El cuestionario a partir del cual se realiza el index, indaga sobre características de la prestación de servicios online, incluyendo el uso de enfoques Whole of Government, políticas de datos abiertos, participación electrónica, prestación de servicios multicanal, grado de aceptación y brechas digitales, la existencia de alianzas a través del uso de TICs, entre otros. El índice de e-participacion (EPI), por su parte, surge de una encuesta suplementaria que evalúa el grado de participación ciudadana en tres niveles: información, consulta y toma de decisiones electrónica

Los índices adoptan valores entre 0 y 1, siendo 1 la mayor calificación que se puede obtener, El estudio no apunta a una evaluación de la performance individual de cada país sino del nivel de desarrollo que presentan entre sí; esto responde al supuesto que adopta la ONU de que cada país debe decidir sobre el nivel y el alcance de sus políticas de acuerdo a sus propias prioridades nacionales. Adicionalmente, toda la información recogida por la encuesta está disponible también a nivel regional, continental y según nivel de ingresos de cada país y está disponibilizada de forma abierta en internet[26].

Del análisis de las encuestas surge que, desde 2003 al 2022, ha habido un gran progreso en el desarrollo de las políticas de gobierno digital a nivel global. Si el promedio mundial era de 0,36 en 2003, en 2022 alcanzó los 0,61. De igual modo, aunque partiendo de valores más bajos, la e-participación trepó del 0,15 al 0,44.

[25] Las primeras mediciones no contaban con una regularidad de 2 años, aunque en la última década esta periodicidad se ha respetado.
[26] Los criterios para la agrupación responden a criterios establecidos por el área estadística de la ONU y por el Banco Mundial. Más información en:
https://publicadministration.un.org/egovkb/en-us/About/Overview/

Gráfico 1. Evolución de índices EGDI y EPI por continente[27].

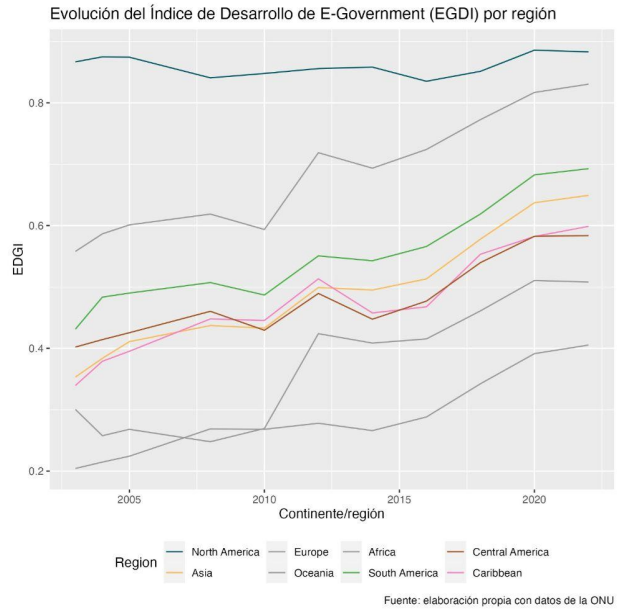


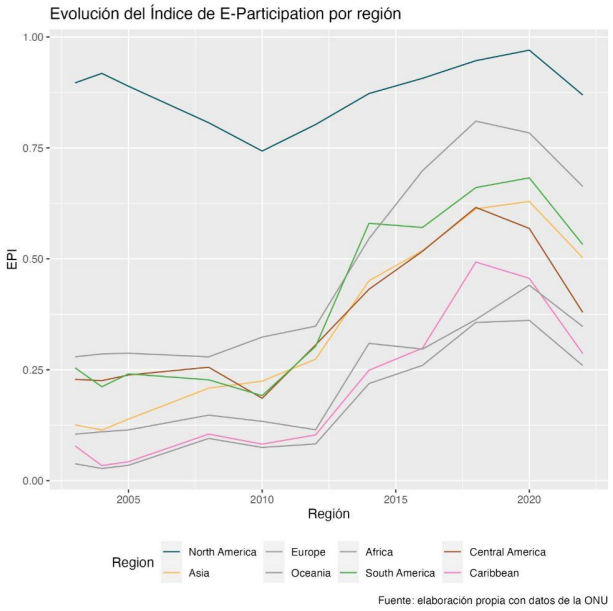
No todos los continentes evolucionaron de la misma manera; el derrotero de las políticas digitales varía de acuerdo a la geografía y al momento en el tiempo en el que se analice el caso. Como se observa en ambos gráficos, el índice EGDI crece a un ritmo estable y decrece levemente en 2022, mientras que el EPI se dispara recién en 2012 pero cae más abruptamente en el último período analizado.

Aún más, las regiones que componen los continentes tampoco presentan la misma evolución. Tomando el caso del continente americano, podemos ver que su evolución tiene algunos outliers. Si se analiza el gráfico anterior del índice EGDI, pero desagregando América en regiones, América del Norte pasa a estar a la cabeza del desarrollo de e-government mientras que regiones como América Central y el Caribe descienden. América del Sur, por su parte, presenta valores superiores al resto de LAC[28], quedando tercera. Algo similar sucede al analizar el EPI, aunque con una mayor diferenciación de Norteamérica y una tendencia a la baja en los últimos dos años a niveles generales.

[27] United Nations. 2001-2022. *UN E-Government Survey*.
[28] América Latina y el Caribe.

Gráfico 2. Evolución de índices EGDI y EPI por continente, desagregado[29].





Para un análisis más pormenorizado sobre la cuestión, existe un repositorio anexo a este trabajo que puede consultar en https://github.com/lushugallo/egovernment, así como una versión en HTML del análisis, disponible en https://rpubs.com/lushugallo/egovernment .

3.2. La gobernanza de la digitalización: el rol de la interoperabilidad

Uno de los principales aprendizajes que se han obtenido luego de varios años de transformación digital en el sector público es -de acuerdo a la principal bibliografía- que esta debe ser abordada como una política pública integral. Esto es, que no solo se haga foco en la tecnología o en la mera digitalización de procesos preexistentes, sino que signifique una nueva manera de pensar, diseñar e implementar las políticas públicas de principio a fin.

En este paradigma, las nuevas tecnologías tienen que ser habilitantes de servicios públicos de mayor impacto y calidad, donde la ciudadanía está en el centro y su experiencia y conocimiento sean tenidos en cuenta tanto en el proceso de formulación como en la implementación de las políticas públicas[30].

[29] United Nations. 2001-2022. *UN E-Government Survey*.
[30] Ramírez Alujas, Álvaro, Jesús Cepeda, y Jolías Lucas. 2021. *GovTech en Iberoamérica : ecosistema, actores y tecnología para reinventar el sector público*. Bahía Blanca: GovTech Hub.

De acuerdo a la Organización de Cooperación y Desarrollo Económico (OCDE), un buen gobierno digital debería cumplir con los siguientes seis aspectos[31]:

1. **Ser digital por diseño**: el uso de la tecnología deberá estar al servicio de la simplificación y rediseño de procedimientos así como de la creación de nuevos canales de comunicación con la ciudadanía desde un principio.
2. **Estar basado en datos**: estos deben ser un activo estratégico y el gobierno debe contar con los mecanismos necesarios para que sean reutilizables, intercambiables y accesibles para mejorar la toma de decisiones.
3. **Actuar como plataforma**: deben garantizarse las condiciones para que lxs usuarixs puedan acceder a una amplia gama de servicios públicos.
4. **Ser abierto por defecto**: los datos, procesos de formulación y algoritmos deber estar disponibles, en la mayor medida posible[32].
5. **Estar centrado en lx usuarix**: el armado de procesos, servicios y políticas debe girar en torno a las necesidades de lx receptorx de la política.
6. **Ser proactivo**: el gobierno debe poder anticiparse a las necesidades de la ciudadanía y responder a ellas de forma proactiva, eliminando los procesos burocráticos y simplificando la interacción entre las partes.

Para garantizar que la digitalización cumpla con todos los elementos anteriores y llegue a buen puerto, el modelo de gobernanza digital pública por el cual se opte será determinante[33]. Asimismo, el grado de interoperabilidad gubernamental también jugará un rol clave[34].

Antes de adentrarnos en el rol de la interoperabilidad, es importante definir qué se entiende por gobernanza. Desde una perspectiva clásica, esta ha sido entendida como la forma en la que se ejerce el gobierno. En los últimos años, a raíz de la evolución de Estado pero sobre todo de las expectativas de la sociedad sobre este, su definición se amplió y puede explicarse como "*la forma de mejorar la relación (horizontal) entre una pluralidad de actores públicos y privados, tendientes a mejorar la toma de decisiones, la gestión y el desarrollo de*

https://www.trustfortheamericas.org/media/projects/attachments/en/Libro-Govtech-Iberoamerica-2021.pdf., p. 64.

[31] Naser, Alejandra (coord), ed. 2021. *Gobernanza digital e interoperabilidad gubernamental: una guía para su implementación*. Santiago de Chile: Comisión Económica para América Latina y el Caribe (CEPAL). https://repositorio.cepal.org/bitstream/handle/11362/47018/1/S2100258_es.pdf, p.17.

[32] Sobre este punto, se destaca la necesidad de que exista un equilibrio con el interés nacional y público y respeto de la legislación vigente.

[33] Naser, Alejandra (coord), ed. 2021. *Gobernanza digital e interoperabilidad gubernamental*…, p. 11.

[34] Ibidem, p. 9.

lo público y lo colectivo, con una marcada intención de integración y de interdependencia"[35]. Aplicada al ámbito digital, la gobernanza puede leerse como la manera de organizar y articular políticas públicas con diversos actores públicos con el fin de crear valor público, basándose en tecnologías digitales[36].

Como se señaló anteriormente, la llegada de la Web 2 tuvo una estrecha relación con el desarrollo de la etapa de Gobierno Digital. Este estadío de internet, trajo a la escena a nuevxs actorxs y a nuevas herramientas que tendieron a facilitar la gobernanza digital: la interacción entre personas y organizaciones se masificó y los distintos gobiernos cambiaron sus enfoques de digitalización, mejorando el acceso a servicios digitales y reduciendo la carga burocrática en muchos aspectos[37].

Sin embargo, a pesar de los avances, distó de ser una solución definitiva. La creciente complejidad de la transformación digital trajo aparejada nuevas problemáticas y nuevos desafíos en su abordaje. La administración pública, por su parte, adoptó mayormente un enfoque estado-céntrico, poniendo el foco en la resolución de sus problemas burocráticos -o de áreas en particular- y no necesariamente en la generación de intercambios y mejores prestaciones para tercerxs. Por otro lado, tampoco logró resolver la gobernanza interna de los nuevos desarrollos.

El resultado de este abordaje fue la creación de una multiplicidad de sistemas que responden a necesidades y estándares de áreas específicas, no dialogan entre sí y duplican información y procesos[38]. Es decir, de soluciones digitales inconexas y una gran falta de interoperabilidad.

Asimismo, otra tendencia que se observó es que muchos países adoptaron un modelo centralizado para el despliegue de sus estrategias de Gobierno Digital pero este demostró tener un mejor impacto en países chicos y unitarios, ya que, por su organización verticalista, la interoperabilidad resultaba más factible[39]. En países más grandes y federales, este modelo no demostró ser funcional a los objetivos de digitalización planteados en la teoría. Esto se debe a que los modelos centralizados requieren de una estandarización de información y una coordinación que en países con gobiernos subnacionales de gran

[35] Ibidem, p.11.
[36] Ibidem, p.14.
[37] Jolías, Lucas, Castro, Ana, y Cepeda, Jesús - Editores (2022). Identidad Digital Descentralizada - Una guía de implementación de blockchain en gobierno…, p. 26.
[38] Ibidem, p. 26.
[39] Ibidem, p. 27.

autonomía -como plantea el modelo federal- son mucho más difíciles de alcanzar. Por un tema de escala y de complejidad del volumen de información, las dificultades también se incrementan en países con mayor población.

El rol de la interoperabilidad para garantizar la gobernanza digital no es una novedad; la bibliografía comenzó enfatizar esta necesidad y los beneficios asociados de la creación de mercados o plataformas digitales únicas de manera temprana[40]. Una de las principales consecuencias negativas que trae la falta de interoperabilidad es la complejización de la administración pública y su funcionamiento interno, que también se traduce en una tensa relación con la ciudadanía, las empresas y demás instituciones.

La falta de fluidez de datos genera una comunicación lenta y poco productiva entre distintas áreas estatales, con un grado de cooperación muy bajo. Los procesos estatales se vuelven complejos, lentos y repetitivos, por lo cual también encontramos un coste de oportunidad en la asignación de recursos humanos[41], tecnológicos y logísticos "que resultan redundantes de manera parcial o total" y que podrían ser reubicados en áreas donde generarían más valor[42]. Adicionalmente, los procesos y trámites se multiplican ya que los abundantes datos públicos están desperdigados en lugar de ser reutilizados y destinados a la creación de valor público[43]. Esto tiene grandes costos que repercuten fuertemente en lxs ciudadanxs y contribuyentes.

Si el horizonte de la interoperabilidad en gobierno digital es el principio de "once-only" ("solo una vez", en español), lo que termina sucediendo es todo lo contrario. Este principio postula que nadie tenga que proporcionar al gobierno el mismo dato más de una vez. El Estado es el principal emisor de documentación personal, desde partidas de nacimiento, credenciales escolares, hasta certificados de propiedad, entre otros. Sin embargo, para realizar trámites y/o acceder a servicios, es muy común tener que presentar este tipo de documentación para ser verificada por un área gubernamental. El principio "once only" aboga por que distintas agencias y organismos públicos puedan proveer esa información internamente sin que el ciudadanx actúe de intermediario.

---

[40] Naser, Alejandra (coord), ed. 2021. *Gobernanza digital e interoperabilidad gubernamental…*, p. 25.
[41] Se hace referencia a la multiplicidad de personas dedicadas a una misma tarea, como pedir, analizar, procesar datos que podrían estar disponibles de existir interoperabilidad.
[42] Naser, Alejandra (coord), ed. 2021. *Gobernanza digital e interoperabilidad gubernamental…*, p. 27.
[43] Lau, Edwin. 2006. "E-Government and the Drive for Growth and Equity." Paper, Belfer Center for Science and International Affairs, Harvard Kennedy School.
https://www.belfercenter.org/publication/e-government-and-drive-growth-and-equity.

Esto no sólo dista de ser la realidad en muchos países sino que termina dándose un fenómeno inverso conocido como *Ciudadano Cadete*. Las personas, y también las empresas, son usualmente quienes deben adecuarse a las normas de cada organismo u área con la que tengan que interactuar y no al revés. En términos prácticos, lo que sucede es que estas deben solicitar y proveer información emitida por organismos estatales ante otros organismos estatales. De la misma manera, para interactuar con ellos, una persona debe crearse un sinfín de accesos digitales en cada sistema y teniendo que aportar la misma información en repetidas ocasiones[44], ya que los sistemas oficiales no dialogan entre sí.

Esta situación es muy tangible a la hora de realizar trámites. Al respecto, se debe destacar que las barreras de acceso a ellos repercuten a las personas de menores recursos. De acuerdo al BID, el acceso a trámites entre personas de menores ingresos difiere en 26 puntos porcentuales si se compara con la de mayores ingresos, siendo que el primer grupo es el que más podría beneficiarse de este acceso[45].

Estas falencias por parte del sector público no hacen más que acrecentar la desconfianza y el descontento con los gobiernos, en un contexto en el que las expectativas sociales respecto a los servicios en general -públicos y privados- han aumentado[46]. En particular en América Latina, la desconfianza hacia el sector público es mayor que en otras regiones. En contraposición, el sector privado ha sabido canalizar estas demandas mediante el uso de nuevas tecnologías pero esencialmente mediante un cambio cultural en el que el sector público ha mostrado grandes dificultades.

Apalancadas en tecnologías digitales, nuevas industrias han surgido y las preexistentes se han reinventado. Basados en análisis intensivos de los datos que fluyen entre áreas y organizaciones, se han creado servicios novedosos, personalizados y de gran calidad. La interoperabilidad -al menos a nivel interno- ha sido la base para la automatización de varios procesos, que han permitido ese gran salto de calidad y que no han tenido el mismo alcance en el sector público.

---

[44] Jolías, Lucas, Castro, Ana, y Cepeda, Jesús - Editores (2022). Identidad Digital Descentralizada…, p. 26.

[45] Roseth, Benjamin, Angela Reyes, y Carlos Santiso, eds. 2018. *El fin del trámite eterno: ciudadanos, burocracia y gobierno digital*. Banco Interamericano de Desarrollo (BID). http://dx.doi.org/10.18235/0001150, p. 22.

[46] Ramírez Alujas, Álvaro, Jesús Cepeda, y Jolías Lucas. 2021. *GovTech en Iberoamérica…,* p. 251.

En el contexto de este incremento y complejización de las expectativas, se ha sumado una dimensión ética, donde factores como la corrupción, el resguardo de la privacidad y la falta de acceso a ciertos sectores, tomaron mayor relevancia[47]. En sistemas interoperables, los datos presentan un menor riesgo de ser alterados o no estar bien ingresados ya que la información se replica bajo estándares en común y, de haber discrepancias en ellos, los errores se detectan más rápidamente Por ello, pueden ser gestionados de manera más transparente y eficiente, realizando cruces para validar transacciones, detectar situaciones irregulares y cumplimientos o no de políticas.

Ante esta situación, han surgido nuevos modelos de gobernanza de datos donde ya no son las organizaciones o instituciones quienes monopolizan la información sino cada individuo quien mayor autonomía sobre su información. Actualmente presenciamos el avance de una tendencia hacia modelos organizativos más horizontales y descentralizados, de la mano con el surgimiento de un nuevo modelo de internet, conocido como Web3, que propone protocolos y un esquema de organización radicalmente distinto al actual. A continuación profundizaremos en sus implicancias de su aplicación en el sector público.

3.3. La interoperabilidad como problema: ¿sobre qué bases se construye la transformación digital pública?

Los últimos 40 años vieron sucederse avances sin precedentes en el terreno tecnológico que le abrieron la puerta de acceso a una importante parte de la población a nuevos productos y servicios digitales más eficientes y personalizados. Como tendencia, estas nuevas prestaciones provinieron del ámbito privado pero generaron también un aumento en las demandas y expectativas ciudadanas respecto a los servicios públicos.

En paralelo, el sector público desplegó una serie de políticas públicas de transformación digital, apalancadas en las nuevas tecnologías, aunque conservando también un gran *legacy* tecnológico. A pesar de los grandes avances, la digitalización en el sector público ha demostrado varias deficiencias y no ha logrado responder correctamente a esas crecientes expectativas ciudadanas de tener un Estado más transparente, ágil y eficiente.

La falta de respuestas acordes a la demanda, se tradujo en un agravamiento de la crisis de confianza por parte de una ciudadanía que esta vez contaba con mayores herramientas

[47] Naser, Alejandra (coord), ed. 2021. *Gobernanza digital e interoperabilidad gubernamental*…, p. 11.

para manifestarse públicamente y, también, para coordinar esa manifestación de manera horizontal y logrando un mayor alcance[48]. Si esta situación comenzaba a acrecentarse en la segunda década del siglo XXI, la crisis sanitaria desatada por la irrupción del sars-cov-2 terminaría de poner en un primer plano la incapacidad estatal de brindar respuestas de calidad[49].

Desde el plano teórico, instituciones referentes, académicxs y los gobiernos vienen planteando desde hace varios años la importancia de avanzar hacia gobiernos de plataformas, donde los sistemas interoperables son la base. Sin embargo, ese intento de interoperabilidad no ha alcanzado los objetivos esperados y nos enfrentamos a gobiernos fragmentados, lentos, costosos y poco sostenibles.

El problema de la interoperabilidad no es una cuestión de digitalización o de tecnología; los gobiernos han creado una gran batería de sistemas digitales en los últimos años. Su problemática reside en que cada uno de ellos responde a áreas y procedimientos particulares, a resolver cuestiones burocráticas específicas, pero no dialoga con el resto. Esta falta de diálogo no sólo ocurre entre distintos niveles estatales sino también dentro de una misma administración pública y también entre organismos públicos y privados. Por ello, nos encontramos ante la necesidad de pensar nuevos esquemas que no busquen garantizar que la interoperabilidad provenga en su totalidad de la coordinación del sector público.

La falta de interoperabilidad en el ámbito público no sólo afecta la interacción entre instituciones, áreas de gobierno y el sector privado, generando ineficiencias, sino que perjudica esencialmente a lxs ciudadanxs cada vez que necesitan interactuar con el Estado. La falta de comunicación e intercambio de información genera que sean las personas quienes tengan que solicitarle al Estado información que en muchos casos este emitió, para poder presentarla ante otra área pública y así lograr avanzar en un trámite o acceder a un servicio. Este fenómeno, conocido como el del “ciudadano cadete”, fricciona aún más la tensa relación entre la sociedad y las administraciones públicas. Aún más, esta problemática afecta más a personas con menores recursos[50].

Es aquí donde reside la problemática principal de las políticas de transformación digital del sector público, en la nula o baja interoperabilidad de sus áreas. Esta, se explica en gran

[48] Ramírez Alujas, Álvaro, Jesús Cepeda, y Jolías Lucas. 2021. *GovTech en Iberoamérica…,* p. 61.
[49] Cetina, Camilo. 2022. *DIGIntegridad…,* p. 71.
[50] Roseth, Benjamin, Angela Reyes, y Carlos Santiso, eds. 2018. *El fin del trámite eterno*, pp. 22-23.

medida por su actual modelo de gobernanza de datos, de carácter centralizado, cerrado y piramidal, en donde cada área estatal, por más pequeña que sea, almacena y gestiona la información de manera aislada. Los distintos gobiernos han intentado atacar el problema de la falta de interoperabilidad siempre utilizando una misma lógica y han tenido grandes dificultades para lograrlo. Esta gestión en compartimentos estancos, impide generar bases sólidas para una digitalización sostenible y escalable a la vez que produce servicios lentos, costosos e ineficientes. No sólo la ciudadanía sufre directamente los costos asociados a estas ineficiencias sino que se pierden oportunidades de impulsar el crecimiento del sector privado[51]. La crisis de agilidad que enfrenta el sector público alimenta la falta de confianza institucional, dando como resultado democracias desgastadas[52].

En este sentido, la gestión de la identidad digital cumple un rol fundamental ya que, como mencionamos, es un pilar para la transformación digital. Además, como veremos a continuación, también es un área con un enorme potencial para mejorar las brechas de desigualdad y el acceso a derechos. La identidad digital -entendida de manera amplia como el conjunto de credenciales que acreditan varios aspectos administrativos de una persona- actúa hoy como un “pasaporte” al mundo digital en su totalidad pero no ha sido un foco de atención a la hora de desarrollar soluciones online. Sin embargo, es la pieza clave para garantizar una transformación digital del sector público sostenible, inclusiva y efectiva[53].

La solución de esta problemática quiere la exploración de nuevos paradigmas en los modelos de gobernanza digital del sector público. Como se mencionó anteriormente, con la llegada de tecnologías como Blockchain y de la Web3, comenzaron a surgir nuevos modelos de gobernanza de datos descentralizados que pueden ser una gran aporte para la solución a este problema. Estos, han dejado de ser teóricos para empezar a mostrar aplicaciones reales y potencialmente revolucionarias.

En contraposición a los modelos actuales, la recuperación del control sobre la información por parte de la ciudadanía le devuelve también un rol activo en la administración de su información, dándole a las personas esa agilidad de la que los gobiernos carecen. El hecho de que sean lxs ciudadanxs quienes poseen y otorgan permisos para acceder a su documentación, descomprime al Estado de realizar esta tarea, permitiéndole reasignar recursos para seguir mejorando en temas más estructurales.

---

[51] Naser, Alejandra (coord), ed. 2021. *Gobernanza digital e interoperabilidad gubernamental…*, p. 27.
[52] Jolías, Lucas, Ana Castro, y Jesús Cepeda, eds. 2022. *Identidad Digital Descentralizada…*, p. 40.
[53] Roseth, Benjamin. 2021. “Gobierno Digital: 5 pilares para tener servicios públicos sin salir de casa...”.

Asimismo, por las características de blockchain, permite una mayor escalabilidad de estas soluciones para que otras entidades -tanto públicas como privadas- comiencen a utilizar este tipo de modelos de gestión de datos. Esta posibilidad se incrementa si las soluciones son pensadas y disponibilizadas en formato abierto, para reducir las barreras de acceso a gobiernos o instituciones con menores recursos y eliminar las fricciones de índole política que puedan surgir.

En las siguientes páginas se analizará de qué manera los modelos descentralizados basados en Blockchain ofrecen nuevas posibilidades para lograr una modernización exitosa del sector público y la generación de servicios de calidad, pero poniendo a las personas como protagonistas autónomas y activas.

Para poder comprender esta problemática, primero se indagará sobre la importancia de la identidad digital y los posibles modelos para su gobernanza. Luego, se revisarán los conceptos más importantes sobre Blockchain, su funcionamiento y para finalmente echar luz sobre los posibles beneficios y desafíos que traería su aplicación. Con el fin de profundizar en aspectos prácticos de la aplicación de nuevos modelos descentralizados de gobernanza en identidad digital, se analizará el protocolo impulsado por el Gobierno de la Ciudad de Buenos Aires, QuarkID.

Cabe volver a destacar que si bien hay una tendencia creciente, la utilización de la tecnología blockchain en el sector público no deja de ser incipiente. Es por eso que este trabajo tendrá un enfoque descriptivo y exploratorio para echar luz sobre la temática y abrir la puerta a futuras investigaciones una vez haya una mayor implementación de modelos descentralizados.

4. Identidad digital en la administración pública

4.1. El acceso a la identidad como problema amplio.

Como se ha señalado anteriormente, la identidad digital es uno de los pilares fundamentales para el desarrollo de transformaciones digitales exitosas. Sin embargo, para comprender la identidad digital resulta necesario revisar primero el concepto de identidad en un sentido amplio -no solo digital- y las problemáticas asociadas a su acceso.

El acceso a la identidad y la inscripción de los niños y niñas al momento del nacimiento son derechos consagrados en la Declaración Universal de los Derechos Humanos y por la Convención de los Derechos del Niños, respectivamente. Sin embargo, de acuerdo a datos del Banco Mundial, en el mundo existen aproximadamente 1000 millones de personas que no pueden demostrar su identidad[54].

Además de un derecho, el acceso a la identidad es un elemento clave para el desarrollo de las sociedades. Los Objetivos de Desarrollo Sostenible (ODS) de la ONU, incluyen en sus metas garantizar el acceso a la identidad jurídica para todas las personas para el año 2030, según reza la meta 9 del ODS N 16[55], dado que “para las personas, la identificación es un derecho, un instrumento de protección y un portal de acceso a servicios, beneficios y oportunidades”[56].

La identidad puede definirse de distintas maneras, entre ellas, como el “conjunto de rasgos propios de un individuo o de una colectividad que los caracterizan frente a los demás”[57]. Estos rasgos pueden estar sujetos a cuestiones identitarias, subjetivas, culturales, entre otros. En este trabajo, sin embargo, se adoptará una definición de identidad desde una mirada estatal, es decir, centrada en los aspectos y credenciales que dan carácter identitario a una persona ante los sistemas de identificación oficiales. Estos, reconocibles principalmente por los gobiernos, son determinantes a la hora de interactuar con la administración pública y contribuyen a hacer efectivos derechos básicos y fundamentales así como acceder a servicios.

---

[54] Banco Mundial, ed. 2021. *Principios Sobre la Identificacion para el Desarrollo Sostenible…* Dato para 2018.

[55] Naciones Unidas. “Objetivo 16: Promover sociedades justas, pacíficas e inclusivas.” UN.org. Accessed Diciembre, 2022. https://www.un.org/sustainabledevelopment/es/peace-justice/.

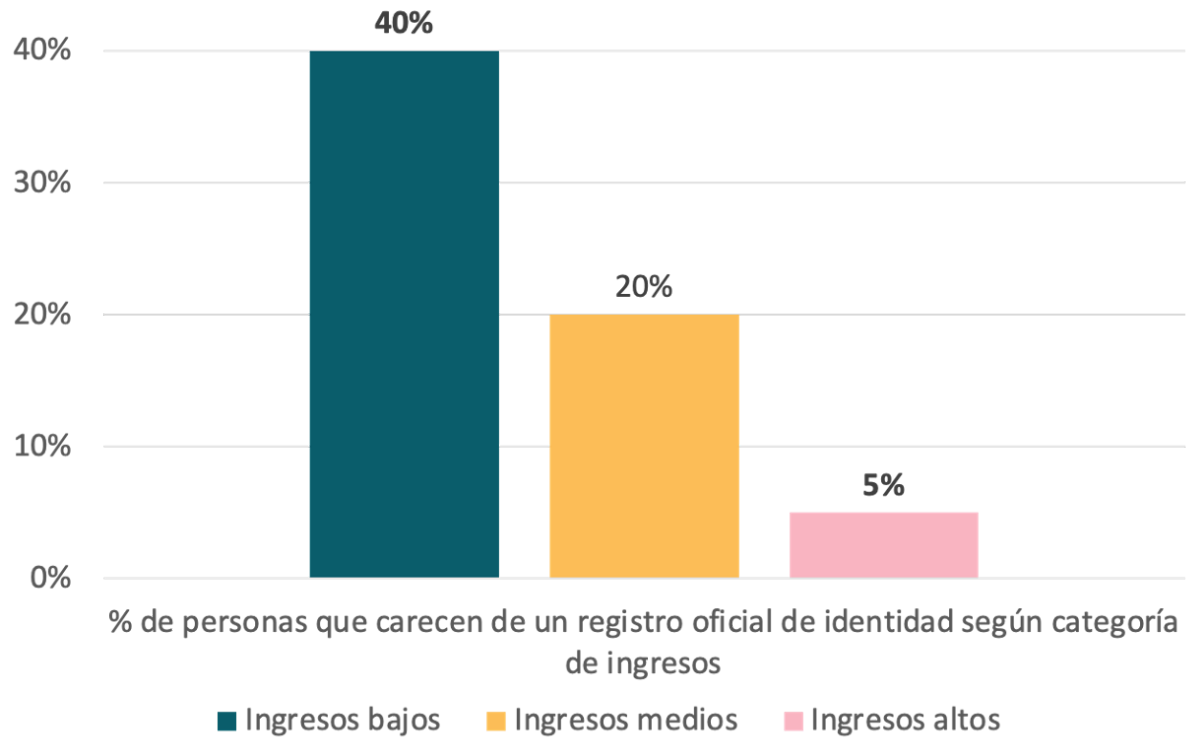
[56] Banco Mundial, ed. 2021. *Principios Sobre la Identificacion para el Desarrollo Sostenible : Hacia la Era Digital*. Banco Mundial. https://documentos.bancomundial.org/es/publication/documents-reports/documentdetail/371801496861423208/principles-on-identification-for-sustainable-development-toward-the-digital-age, p. 5.

[57] “identidad | Definición | Diccionario de la lengua española | RAE - ASALE.” 2022. Diccionario de la lengua española. https://dle.rae.es/identidad.

Como mencionamos anteriormente, a pesar de ser un derecho, una gran proporción de la población no puede acreditar su identidad. Este hecho trae aparejado una falta de acceso a servicios básicos, como la educación, la justicia, el empleo, servicios financieros, entre otros[58].

Es importante resaltar que la falta de acceso a la identidad se distribuye heterogéneamente de acuerdo a factores como la ubicación, el nivel de ingresos, el género de las personas, entre otros. Como se puede observar en el siguiente gráfico, los países de menores ingresos son los que mayor porcentaje de personas sin documentación oficial presentan.

Gráfico 3. Acceso a un registro de identidad según ingresos[59].



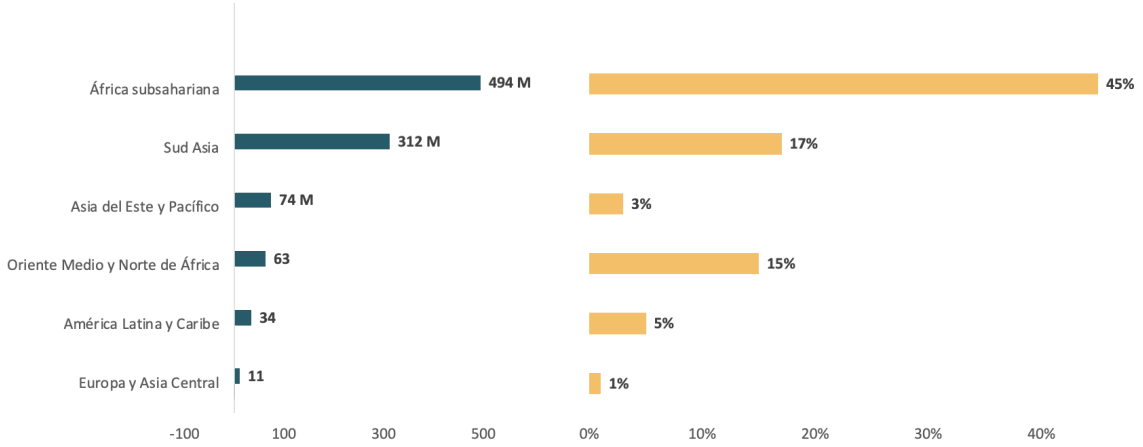
En números absolutos, la mayoría de las personas que no cuentan con acceso a una identidad oficial vive en países de ingresos medios bajos, habiendo para 2018 un estimado de 623 millones de personas de esa categoría de ingresos sin una identificación. En cuanto al grupo de ingresos altos, el número alcanzaría los 63 millones. Dentro de la categoría de

[58] Banco Mundial, ed. 2021. *Principios Sobre la Identificacion para el Desarrollo Sostenible…,* p. 5.
[59] Realizado en base a datos del Banco Mundial. "Data | Identification for Development." ID4D. Accessed Mayo, 2022. https://id4d.worldbank.org/global-dataset.

ingresos bajos, el número ascendería a 278 millones; a pesar de ser menos que en las de ingresos medios, sí tienen una propensión más alta a no acceder a ella, como se observa en el gráfico anterior.

A nivel regional, África subsahariana y el sur de Asia presentan los mayores porcentajes de personas con una falta total de acceso a credenciales identitarias oficiales, componiendo el 81% del total, y un acumulado de 806 millones de personas.

Gráfico 4. Personas que carecen de un registro de identidad según región, en términos totales (izquierda) y porcentuales respecto a la población total[60].



Asimismo, los datos sugieren que las políticas de identificación requieren un foco en la infancia: el 47% de las personas que no cuentan con una prueba oficial de identidad están por debajo de la edad nacional de identificación. Adicionalmente, observamos que la problemática afecta mayormente a los países pobres: 63% de los afectados viven en economías de ingreso mediano-bajo y el 28% en economías de ingreso bajo[61]. Dentro del grupo de países de ingresos bajos, 1 de cada 2 mujeres no tiene una identidad oficial.

A nivel general, la distribución de acceso es heterogénea por género pero las mujeres siempre tienen una mayor probabilidad de carecer de una prueba de identidad oficial. Esta chance se incrementa en países de bajos ingresos, como ya se mencionó, donde se encuentran brechas de un promedio de 15 puntos porcentuales. En promedio, mientras que

[60] Realizado en base a datos del Banco Mundial. “Data | Identification for Development.” ID4D. Accessed Mayo, 2022. https://id4d.worldbank.org/global-dataset.
[61] Diofasi, Anna, Jing Lu, y Vyjayanti T. Desai. 2018. “El desafío mundial de la identificación: ¿quiénes son los 1000 millones de personas que no tienen un documento de identidad?” World Bank Blogs. https://blogs.worldbank.org/es/voices/quienes-son-los-1000-millones-de-personas-que-no-tienen-una-identificacion.

el 30% de los varones mayores de 15 años carecen de una identificación, en las mujeres este número asciende al 45%.

Por otro lado, en la región latinoamericana, si bien existe un alto nivel de acceso en términos relativos, se estima que el 5% de la población aún no posee una identificación básica[62]. Además, no solo se observan disparidades de país en país sino también internamente, de acuerdo al sector socioeconómico de las personas: los grupos de bajos recursos económicos o que enfrentan alguna situación de vulnerabilidad son quienes componen mayormente ese 5%.

Ante esta situación, a la hora de abordar políticas de identidad digital resulta esencial contemplar las complejidades y distintas realidades de cada país y/o región/municipio para poder priorizar necesidades, buscar soluciones acordes y diseñar políticas públicas eficientes e inclusivas.

Sin embargo, tener acceso a algún tipo de identificación no es garantía de calidad; aún existen enormes oportunidades de mejora en este aspecto. Lo mismo sucede con los sistemas de identificación: no todas las formas existentes de autenticación o identificación son seguras y/o fiables ante proveedores de servicios. Algunos países sólo ofrecen modalidades de identificación no reconocidas internacionalmente, que no se adaptan a la era digital y/o ni protegen los derechos y datos de las personas, es decir, no adoptan protocolos mínimos comunes con otros Estados. En este sentido, puede hablarse no sólo de una problemática de falta de identificación sino de deficiencias en la identificación de las personas[63].

Dentro de estas deficiencias, observamos también que los mecanismos de identificación y autenticación que ofrecen los estados no suelen ser 100% fiables. Aún hoy, la modalidad presencial suele ser la más elegida aunque sólo consista en, por ejemplo, una comparación visual entre la foto registrada en un documento y la cara de la persona que la presenta. Quien verifica tiene pocas o nulas herramientas para verificar la autenticidad de dicho documento y rara vez se realiza una verificación biométrica[64]. La falta de tecnologías

[62] En total sería 34 millones de personas, de acuerdo a Cetina, Camilo. 2022. *DIGIntegridad(…)*.
[63] Banco Mundial, ed. 2021. *Principios Sobre la Identificacion para el Desarrollo Sostenible : Hacia la Era Digital*. Banco Mundial. https://documentos.bancomundial.org/es/publication/documents-reports/documentdetail/371801496861423208/principles-on-identification-for-sustainable-development-toward-the-digital-age, p. 3.
[64] Allende López, Marcos. 2020. *Identidad digital auto-gestionada. El futuro de la identidad digital: auto-gestión, billeteras digitales y blockchain*. Banco Interamericano de Desarrollo (BID). http://dx.doi.org/10.18235/0002635, p. 6.

acordes trae aparejada la persistencia de la falsificación o usurpación de identidades, la pérdida de documentación y la indocumentación de las personas. Esta falencia genera una situación de total desprotección, en particular para las personas en situación de vulnerabilidad[65], pero también actúa como un limitante a la digitalización de servicios.

Como veremos a continuación, con el advenimiento de la digitalización, poder acreditar la identidad de forma digital y segura se volvió significativamente más importante para las personas. Hoy el mundo cuenta con mayores y mejores herramientas para hacerlo, pero esto no se ha traducido necesariamente en una aplicación prácticas de las mismas: saber con seguridad que la persona o institución con la que estamos interactuando es quien dice ser y no un tercero (humano o generado de forma artificial) suplantando una identidad aún no es posible.

4.2. Irrupción de la identidad digital.

Hablar de identidad digital es hablar de la llave de acceso al mundo digital. Implica que un organismo estatal o privado pueda comprobar que esa persona es quien dice ser para acceder a una serie de prestaciones, a interactuar con terceros, y la lista sigue.

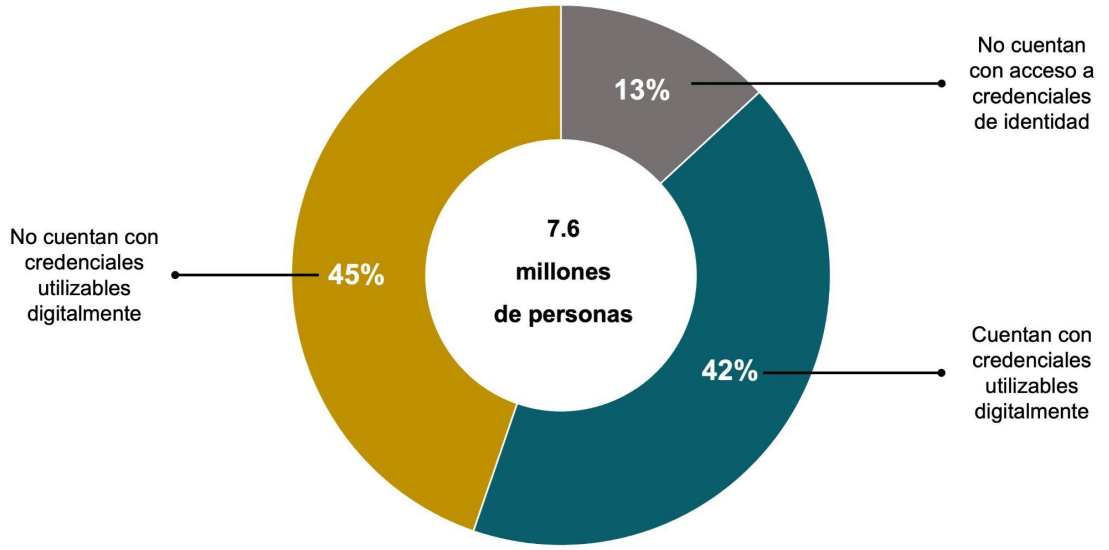
Cabe remarcar que no existe una distinción entre la composición de la identidad como tal en el mundo físico y en el digital: la identidad de una persona es la misma sin importar el contexto donde se está validando. Sin embargo, la decisión de nombrarlas por separado responde a una necesidad de explicar y analizar las particularidades de cada una en su operatoria, para entender también en mayor profundidad sus desafíos y oportunidades en lo relativo a las políticas públicas de gobierno digital.

De acuerdo a un estudio realizado por la consultora McKinsey, alrededor de 3.4 mil millones de personas poseen algún tipo de credencial identitaria pero con limitaciones para utilizarla en el mundo digital[66]. En contraposición, una porción menor de la población, 3.2 mil millones de personas, sí contaría con acceso a un ID utilizable digitalmente. En línea con esta información, se desprende que el 58% de la población mundial no puede acceder en forma total o parcial a una identidad digital.

---

[65] Ibidem, p. 6.
[66] Mckinsey. 2019. *Digital identification: A key to inclusive growth*. https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/digital%20identification%20a%20key%20to%20inclusive%20growth/mgi-digital-identification-report.pdf.

Gráfico 5. Acceso a credenciales identitarias digitales[67]



Con una tendencia a la digitalización en aumento, la falta de acceso a credenciales digitales de identidad representa un enorme traba para un pleno ejercicio de derechos. De allí, la importancia de repensar modelos robustos, seguros e incluyentes para su gestión. En los últimos años surgieron nuevos desarrollos que engloban tecnologías, lineamientos y protocolos para convertir el acceso a la identidad en algo seguro, escalable y de bajos costos.

Si bien es cierto que la irrupción de la digitalización tuvo su repercusión en los sistemas de identificación y se generaron mejoras, este tema no fue un foco de preocupación en los desarrollos realizados dentro del modelo de Web 2. Las innovaciones que sí existieron abrieron un abanico de posibilidades: en comparación con los sistemas tradicionales en papel, los sistemas de identificación digitales permitieron crear e implementar modelos de gestión y protección de datos más seguros, inclusivos y fáciles de utilizar. Además, demostraron incrementar la exactitud y confiabilidad de los datos.

Asimismo, la posibilidad de acreditar una identidad en entornos digitales y de forma remota permitió a una mayor cantidad de personas acceder a servicios digitales globales[68]. En

[67] Fuente: elaboración propia en base a Mckinsey. 2019. *Digital identification: A key to inclusive growth*., p. 34.
[68] Allende López, Marcos. 2020. *Identidad digital auto-gestionada…,* p. 12.

términos de inclusión, esto significó nuevas oportunidades para acortar brechas de acceso. Durante la pandemia por el sars-cov-2, por ejemplo, aquellos países que se valieron de identificadores digitales para realizar pagos gubernamentales, lograron alcanzar a un 39% más de beneficiarios que los que no lo hicieron[69].

Sin embargo, por una falta de priorización de los sistemas de identificación digital hoy en día es común tener que generar una identidad online para acceder a cada servicio o para interactuar con instituciones específicas. Es decir, no hubo un desarrollo coordinado y centrado en la eficiencia, la seguridad y la interoperabilidad, suficiente para crear bases sólidas al proceso de transformación digital.

Una buena gestión de la identidad digital tiene el potencial de mejorar la creación de valor público. En cuanto a lxs potenciales grandes beneficiarixs, encontramos principalmente tres: las personas usuarias, el sector público y el sector privado. Para el primer grupo, las principales ventajas se encuentran en la reducción de tiempo y costes asociados, una mejor experiencia de usuario al utilizar y gestionar credenciales y en la posibilidad de incluir a más sectores. Como se mencionó anteriormente, la falta de acceso a la identidad y a trámites afectan en mayor medida a personas de menores recursos.

Que las instituciones puedan validar la identidad de una persona y generar credenciales a distancia, sin necesidad de que la persona se presente físicamente en una oficina, permite que ya no sea necesario ausentarse del trabajo o viajar grandes distancias. Esto, en particular, beneficia a personas de menores ingresos, quienes suelen vivir en zonas más alejadas y tener menos flexibilidad horaria que grupos de mayores ingresos. Al hacer foco en los trámites presenciales, en América Latina, requieren en promedio 5,5 horas y al menos dos viajes a una oficina estatal; además, tienen una alta tasa de corrupción asociada. Sin embargo, en su versión digital, el acceso a servicios públicos es un 74% más rápido y le cuestan a las instituciones públicas un 95% menos[70].

El sector público, por su parte, puede beneficiarse de una gran reducción de costos al implementar modelos de identidad digital eficientes, en particular en el área de recursos humanos y de almacenamiento físico. Además, abre la puerta a una mejora considerable en la prestación de servicios, fomentando la transparencia y la seguridad. Finalmente, las administraciones públicas tendrían una mayor disponibilidad de datos mejor potencialmente

[69] Puliti, Riccardo. 2022. “La inclusión digital hace posible una recuperación más resiliente para todos.” World Bank Blogs. https://blogs.worldbank.org/es/voces/la-inclusion-digital-hace-posible-una-recuperacion-mas-resiliente
[70] Roseth, Benjamin, Angela Reyes, y Carlos Santiso, eds. 2018. *El fin del trámite eterno*, pp. 91-92.

mejor preparados para ser analizados y crear valor a partir de ellos. En este sentido, la posibilidad de, por ejemplo, automatizar procesos a partir de la estandarización de datos no sólamente los agiliza sino que habilita nuevos escenarios de innovación[71]. Del lado del sector privado, este tipo de mejoras en el sector público tiene un potencial impacto en la generación de nuevas oportunidades comerciales y de tener una interacción más fluida y productiva con clientes y socixs.

Además de los beneficios particulares de cada grupo, la identidad digital contribuye a que la ciudadanía, los gobiernos y las empresas interactúen más activamente en la economía digital. La importancia de sentar bases sólidas en la gobernanza de la identidad digital reviste también en las oportunidades económicas que promueve. Se estima que el potencial económico de la identidad digital podría generar entre el 3% y el 13% del PBI para 2030[72]. Sólo por mencionar un ejemplo, permitiría el acceso a servicios financieros de 1700 millones de personas.

No obstante, la implementación de la identidad digital también crea nuevas demandas y desafíos. En particular, hay cuatro áreas que se destacan en importancia y que, a su vez, están fuertemente interrelacionadas: la seguridad, el acceso, la tecnología y la regulación.

Desde el lado de la seguridad, la población pasó a tener una necesidad mayor de contar con medios idóneos para demostrar su identidad sin comprometer la integridad de datos sensibles y también de poder tener la certeza de estar interactuando con la persona o institución que es quien dice ser. La falta de respuestas acordes de gobiernos, proveedores y validadores de identidad aumentó el riesgo de vulneración de los datos, de suplantaciones de identidad y otros tipos de estafas.

En cuanto al acceso, no sólo existen cuestiones relacionadas a la calidad de acceso en la identidad digital; el factor de internet también se presentó como un limitante en algunas regiones. No todas las geografías accedieron a él con la misma celeridad y calidad y aún hoy existen muchas áreas sin cobertura o con un acceso deficiente. Además, en aquellas zonas donde puede considerarse que el acceso a internet es alto, cabe reparar en su distribución. En términos de género, sólo el 57% de las mujeres acceden a internet, mientras que en varones ese porcentaje asciende al 62%. En áreas urbanas, el número de usuarios de internet duplica al de zonas rurales. También se encuentran diferencias por rango etario, donde lxs jóvenes tiene un mayor acceso: el 71% de la población entre 15 y 24

[71] Banco Mundial, ed. 2021. *Principios Sobre la Identificacion para el Desarrollo Sostenible…,* p. 3.
[72] Allende López, Marcos. 2020. *Identidad digital auto-gestionada…,* p. 13.

usa internet, mientras que el resto de los grupos etarios alcanzan sólo el 57%[73]. Es importante volver a señalar que una mala implementación de estos sistemas afecta mayormente a sectores vulnerables; por ello hay un potencial riesgo de que se incremente las brechas de desigualdad.

De la mano con el acceso, está la cuestión tecnológica: no todos los países implementaron y/o pudieron acceder a las tecnologías más sofisticadas y acordes para los distintos desafíos de la transformación digital. La falta de herramientas idóneas para identificar a las personas y ciertos atributos sobre ellas contrarrestó las oportunidades para prestar servicios de forma eficiente y segura[74]. También debe tenerse en cuenta que para que la transformación digital sea exitosa, se necesita poseer un conocimiento específico sobre la tecnología -entre otros aspectos. En el caso del sector público, por ejemplo, uno de los potenciales beneficios es el ahorro en costos de almacenamiento de información. Sin embargo, para que esto suceda se deben poder implementar sistemas más eficientes y seguros que suplan esta necesidad. Por ello, aquí no sólo entra en juego una falta de acceso por un costo económico directo sino también por la existencia de una mayor barrera relativa al conocimiento.

Finalmente, aparece la cuestión de la legislación. Si bien la temática es amplia, basta mencionar que, por un lado, parte del corpus legal actual de muchos países proviene de tiempos donde los procesos de gestión de la información estaban muy lejos de los modelos actuales, con un bajo uso de tecnología y un alto uso de papel. Por otro lado, las nuevas tecnologías digitales traen grandes saltos en la forma de gestionar la información por lo cual la legislación debería seguir muy de cerca estos cambios en pos de ajustarse a la actualidad. Esto es un desafío porque la ley suele ir detrás del cambio y no al revés.

Como consecuencia del panorama actual, nos encontramos aún con una falta de acceso total a la identidad digital para algunas personas pero también ante una calidad deficiente para quienes sí acceden. Puede afirmarse que hoy abundan las identidades digitales fragmentadas: para interactuar con cada institución u organización, una persona debe crear tantas cuentas como instituciones con las que requiera acreditarse, y proveer la misma información de forma manual una y otra vez.

[73] Banco Mundial. “Desarrollo digital.” Banco Mundial. Accessed Mayo, 2022. https://www.bancomundial.org/es/topic/digitaldevelopment/overview.
[74] Banco Mundial, ed. 2021. *Principios Sobre la Identificación para el Desarrollo Sostenible…,* p. 5.

Como mencionamos, la calidad de protección de los datos, las tecnologías implementadas y la interoperabilidad entre los distintos sistemas es también sumamente variada, por lo cual los beneficios de la acreditación digital de la identidad no alcanzan hoy su potencial. Por último, aunque no menor, todas las credenciales y datos que componen la identidad no quedan bajo el dominio de las personas sino de dichas instituciones o empresas[75] que no son transparentes ni claras con las acciones que realizan con ellas.

Sin embargo, recientemente han surgido innovadoras propuestas que buscan superar muchos de los desafíos anteriormente mencionados. A continuación, abordaremos la situación de los modelos de gobernanza actuales y nuevos.

4.3. Modelos de gobernanza de la identidad digital.

La gestión de la identidad digital ha sido abordada de distintas maneras y sin seguir un único modelo. Además, dentro de cada país o jurisdicción, el tipo de modelo escogido pudo ir variando conforme al paso del tiempo, la disponibilidad tecnológica y de recursos y el enfoque de las políticas de transformación digital, entre muchos otros factores.

De acuerdo a la experiencia internacional, en términos generales pueden establecerse tres modelos[76] o etapas de gestión de la identidad digital: identidad centralizada, identidad federada e identidad descentralizada[77]. Estos modelos, como tales, son esquemáticos y en la realidad podemos encontrar situaciones más híbridas. Por otra parte, actualmente encontramos diferentes estadíos de desarrollo en los distintos países.

En el **modelo de identidad centralizada,** la gestión de la identidad está a cargo de un único organismo que la otorga, válida y puede revocar credenciales y permisos. La ciudadanía no tiene autoridad sobre su propia identidad y tampoco tiene control sobre la información personal que se comparte. Este modelo *top-down* suele generar fricción en particular en países federales, ya que los usuarios tienen que crear tantas identidades digitales como organismos con los que quieren interactuar, dado que cada gobierno tiene una lógica interna propia y/o a que el organismo centralizador no disponibiliza la información internamente[78].

---

[75] Jolías, Lucas, Ana Castro, and Jesús Cepeda, eds. 2022. *Identidad Digital Descentralizada,* p. 41.
[76] Allen, Christopher. 2016. “The Path to Self-Sovereign Identity.” Life With Alacrity. http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html.
[77] Ramírez Alujas, Álvaro, Jesús Cepeda, y Jolías Lucas. 2021. *GovTech en Iberoamérica…,* p. 71.
[78] Ibidem, p. 72.

El siguiente modelo, de **identidad federada**, presenta algunos avances y ventajas por sobre el anterior. A saber, la identidad es gestionada por varios organismos lo cual permite que lxs usuarixs usen una misma identidad para acceder a distintos servicios o plataformas, facilitando la interacción con el Estado. Por otra parte, en algunos casos se implementan mejoras en la experiencia del usuario y se incorpora cierto nivel de consentimiento sobre el uso de sus datos. Sin embargo, ciertos problemas permanecen: la identidad e información asociada sigue sin estar bajo el control de lx ciudadanx y la integración de servicios continúa siendo dificultosa[79].

El tercer modelo, de **Identidad descentralizada** y sobre el cual desarrollaremos más adelante, apunta a que sean los usuarios quienes tengan en su poder las credenciales de identidad y que las gestionen, sin la intervención de terceros[80]. Esto no significa que el individuo pase a ser un emisor de identidad sino que se vuelve el administrador total de ella[81]. Este modelo rompe con la lógica tradicional al darle una mayor autonomía a lxs usuarios, planteando la existencia de repositorios personales y portátiles donde almacenar datos de manera segura[82]. En el plano tecnológico, incorpora tecnología Blockchain y dos innovaciones principales: las billeteras o wallets digitales (repositorios) y los registros descentrados de información[83], sobre los cuales nos detendremos más adelante. Con ellos, se elimina la necesidad de terceros de recurrir a la entidad emisora para comprobar la validez de una identidad.

La identidad descentralizada se sostiene en 10 principios, de acuerdo a Christopher Allen[84], referente en la materia.

1. Una **existencia** independiente del Estado donde la persona es el centro y quién autoriza el acceso al Estado a algunos datos que componen a su identidad toda.

2. El **control** del ciudadano sobre su identidad. La persona es máxima autoridad de sus datos sin detrimento de que pueda recibir reclamos sobre su identidad o aspectos de ella.

---

[79] Ramírez Alujas, Álvaro, Jesús Cepeda, y Jolías Lucas. 2021. *GovTech en Iberoamérica…,* p.73.
[80] Ibidem, p. 73; GCBA et al. 2022. “Identidad-digital - Whitepaper.”.
[81] Allende López, Marcos. 2020. *Identidad digital auto-gestionada…,* p. 7.
[82] Ibidem, p. 28.
[83] Ibidem, p. 7.
[84] Allen hace referencia a este concepto bajo el nombre de identidad auto-soberana. Como fue mencionado anteriormente, la terminología para referirse a soluciones basadas en blockchain para una gestión descentralizada de la identidad digital es variada. Los términos más comunes son identidad autosoberana, identidad autogestionada e identidad descentralizada, entre otros. Allen, Christopher. 2016. “The Path to Self-Sovereign Identity.”...

3. El **acceso** y conocimiento total del ciudadano sobre toda la documentación que conforma su identidad.

4. La **transparencia** y apertura en los sistemas y algoritmos con los que se gestiona y valida la identidad digital.

5. La **persistencia** de la identidad a lo largo del tiempo sin que ello entre en conflicto con el derecho al olvido. Lo que cambian son las claves y ciertos datos, pero no la identidad como un todo.

6. La **portabilidad** de toda la documentación que acredita una identidad sin ataduras a fronteras, regímenes políticos o entidades de terceros que puedan impedir o restringir su acceso.

7. La mayor **interoperabilidad** para garantizar su valor/validez, sin limitantes fronterizos.

8. El **consentimiento** expreso del ciudadano a la hora de utilizar su identidad digital, siendo la persona quien autorice o no el acceso a datos concretos.

9. La **minimización** en la divulgación de datos concretos de la identidad a través de técnicas de conocimiento cero (zero knowledge proof).

10. La **protección** y preservación de las libertades y derechos de los usuarios sobre las necesidades de los sistemas o redes utilizadas. La independencia, descentralización y resistencia a la censura de los algoritmos resulta clave.

Por sus características, la identidad descentralizada parte de un enfoque completamente novedoso. Sin embargo, su implementación dista de ser generalizada y sólo algunas administraciones públicas están avanzando hacia ella. Podemos encontrar algunas pruebas piloto y proyectos en fases iniciales de implementación, como el caso que analizaremos en este trabajo.

Antes de ello, aunque este trabajo no tenga como objetivo un análisis técnico de blockchain ni de la operatoria de la identidad digital en ella, resulta necesario comprender ciertos conceptos y aspectos específicos con el fin de lograr un mejor entendimiento de la

problemática como de las soluciones propuestas. A continuación, nos detendremos en este punto.

4.4. Identidad digital descentralizada en blockchain

La identidad descentralizada, se basa en novedosos estándares promovidos por el World Wide Web Consortium (W3C) y se apalanca en la tecnología Blockchain. Blockchain se traduce al español como “cadena de bloques”. Su nombre suele estar comúnmente asociado a las criptomonedas y al mundo financiero, pero sus usos van mucho más allá de este sector. Tan es así que esta tecnología se perfila como una infraestructura clave en el desarrollo digital de -si no todas- una gran cantidad de industrias.

Blockchain se puede definir como una base de datos con características distintivas respecto a las tradicionales, lo que la hace exponencialmente más segura. En primer lugar, es un tipo de base de datos distribuida (DLT). Esto quiere decir que la información no es almacenada por una autoridad central sino que todos los usuarios o nodos[85] que utilizan la red poseen una copia y contribuyen a su mantenimiento. Por ello, toda la información se encuentra validada en las copias que tienen millones de personas y, por ello, no puede alterarse.

Dentro de las DLT existentes, blockchain se distingue por su organización de la información en bloques. En esta arquitectura reside su parte de su distintiva seguridad. Cada transacción es registrada en un bloque que contiene una marca o código -conocida como hash[86]- del bloque predecesor y del actual. Cada bloque almacena una serie única de transacciones y, una vez emitido, queda encadenado cronológicamente a la serie histórica, de manera que resulta imposible de modificar o eliminar[87].

Volviendo a su carácter descentralizado, toda la información emitida queda registrada y se distribuye en tiempo real hacia todos los nodos que participan de esa red. Adicionalmente,

---

[85] Por nodo se entiende a un usuario o computadora que corre software en la blockchain. Existen tres tipos principales de nodos. Los “full nodes”, quienes tienen como principales funciones recibir, almacenar, validar y transmitir datos de otros nodos; los “mining nodes”, quienes además de las funciones anteriores publican nuevos bloques; y los “lightweight nodes”, generalmente operativos en dispositivos con bajo poder de procesamiento, que no mantienen copias completas de la red sino que envían su información a full nodes para ser procesada y validada. Berryhill, Jamie, Théo Bourgery, y Angela Hanson. 2018. *Blockchains Unchained: Blockchain Technology and its Use in the Public Sector*. Paris: OECD Publishing. https://doi.org/10.1787/3c32c429-en, p. 11.

[86] El hash es una función criptográfica que emite un código de un largo fijo que varía de acuerdo al input que recibe (transacciones).

[87] Cualquier modificación de la red requiere un consenso de la mayoría de los nodos que la integran. La imposibilidad de edición recae en nodos únicos o grupos minoritarios. Berryhill, Jamie, Théo Bourgery, y Angela Hanson. 2018. *Blockchains Unchained…,* pp. 10-11.

para ser emitido, el bloque y sus transacciones asociadas deben ser aceptadas por toda la red. Aquí reside uno de sus aspectos más innovadores: para realizar una modificación en la información no sólamente habría que convencer a los millones de personas que poseen copias de esa gran base de datos sino alterar una cadena de bloques de un tamaño que demandaría un poder de cómputo que haría imposible su realización. Por ello, se considera que la blockchain no puede ser hackeada[88].

Finalmente, es importante destacar otra característica distinta de las transacciones en Blockchain: su encriptación. Con ello nos referimos al hecho de que los datos se convierten a un formato de código alfanumérico que evita que pueda ser leído por actores no autorizados. La manera de desencriptar esta información es a partir de una llave (key), que es un código privado que solo se revela a actores autorizados para que lean y comprueben cierta información[89]

El registro de información en la blockchain puede realizarse por distintas redes o capas. Como no es el foco de este trabajo realizar un análisis técnico de esta tecnología, bastará decir que no todas las redes permiten una descentralización total. Algunas, pueden ser creadas y manejadas por empresas privadas o incluso gobiernos, y las personas pueden no disponer libremente de su información.

Existen aplicaciones de modelos de identidad digital en blockchain mediante este tipo de redes, llamadas privadas o permisionadas. Uno de los casos más destacados es el de Estonia, país de vanguardia en lo que respecta a la gobernanza digital. En 2001, con el lanzamiento de X-road, el célebre entorno tecnológico y organizativo creado para una gestión de la información estatal de forma segura e interoperable, puedo comenzar a realizar una verdadera transformación digital. De acuerdo a fuentes oficiales del país, por cada año que el sistema estuvo operativo, generando intercambios de información, Estonia ahorró 844 años de trabajo -o 240 horas cada tres minutos trabajados-[90]. Además de ser el primer país en implementar soluciones en blockchain en sectores estratégicos, como la

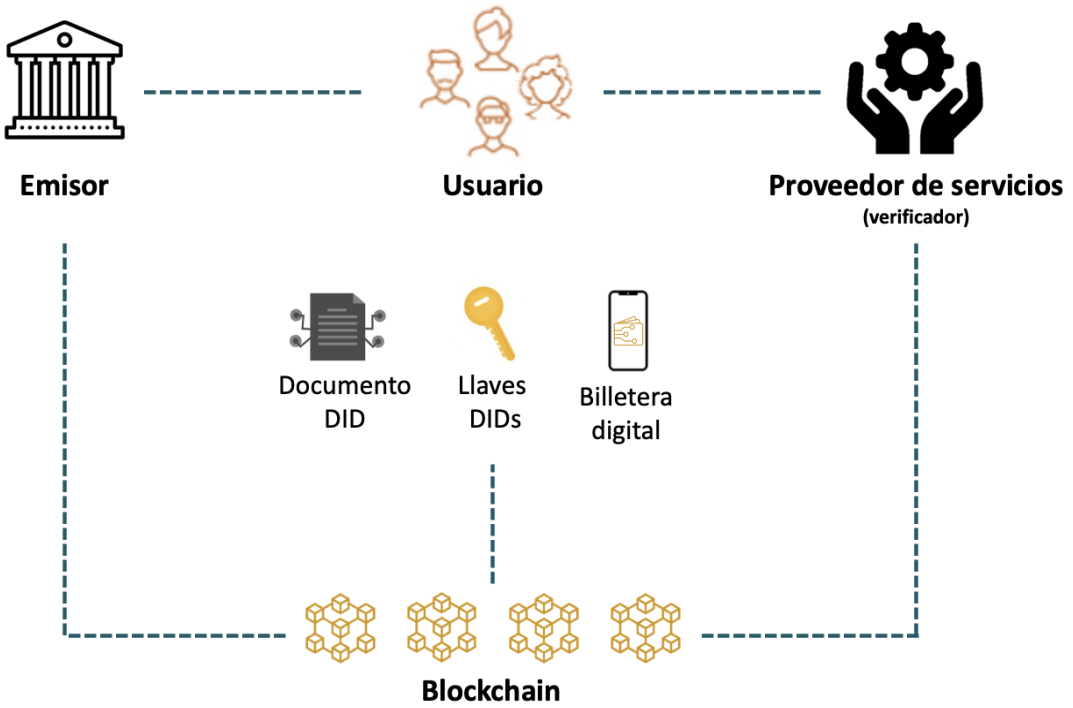
[88] Jolías, Lucas, Jesús Cepeda, y Ana Castro. “4 tendencias en el uso de blockchain en el Estado.” OS City. Accessed Octubre, 2022. https://plus.os.city/blog-os-city-plus/posts/4-tendencias-en-el-uso-de-blockchain-en-el-estado.
[89] Berryhill, Jamie, Théo Bourgery, and Angela Hanson. 2018. *Blockchains Unchained…,* pp. 10-11.
[90] Cetina, Camilo. 2022. *DIGIntegridad…; Apolitical. 2017. “El intercambio de datos de Estonia le permite pagar sus impuestos en cinco minutos.” Apolitical. https://apolitical.co/solution-articles/es/plataforma-de-intercambio-de-datos-que-convierte-a-estonia-en-lider-de-gobierno-digital.*

Justicia y la Salud, el país posee desde 2017 “embajadas blockchain” con el fin de salvaguardar su información si la seguridad del país se viera amenazada[91].

Sin embargo, la red que utilizan para compartir la información es privada y es el gobierno estonio quien tiene la custodia y la gestión de la información[92]. Esto hace que su enfoque se aleje bastante del espíritu del modelo de auto-gestión de la identidad digital. Diferentes arquitecturas pueden llevar a diferentes resultados en la aplicación de identidad digital, en particular en términos de utilidad y transparencia.

El modelo de identidad descentralizada, se basa en una filosofía más abierta, con la utilización de redes no permisionadas que permiten dar una verdadera autonomía a la ciudadanía. Para ilustrar su funcionamiento, el siguiente esquema simplificado puede resultar de gran ayuda.

Gráfico 6. Esquema simplificado de la Identidad Descentralizada[93]



[91] PwC. “Estonia – the Digital Republic Secured by Blockchain.” PwC. Accessed Junio, 2022. https://www.pwc.com/gx/en/services/legal/tech/assets/estonia-the-digital-republic-secured-by-blockchain.pdf.
[92] Semenzin, Silvia, David Rozas, y Hssan Samer. 2022. “Blockchain-based application at a governmental level: disruption or illusion? The case of Estonia.” Policy and Society 41, no. 10 (Abril). 1093/polsoc/puac014, p. 12 ; PwC, 2019. Estonia – the Digital Republic Secured by Blockchain.
[93] Allende López, Marcos. 2020. *Identidad digital auto-gestionada…,* p. 52.

Por un lado, encontramos que sigue habiendo emisores de credenciales. El gobierno -y todas las áreas específicas a cargo de la generación de documentación identificatoria - pueden cumplir este rol pero también pueden hacerlo instituciones privadas. Por ejemplo una institución del ámbito educativo o de la salud podría emitir certificados que acrediten la realización de un curso o un esquema de vacunación, por sólo nombrar algunas aplicaciones.

Sea quien sea quien actúa como emisor, este envía la información al usuarix a través de la Blockchain de manera encriptada. Esta credencial que se genera, al emitirse bajo los estándares internacionales del W3C, pasa a ser una credencial verificable[94]. El usuario recibirá sus documentos DID en una billetera virtual, entendiéndose por DID un identificador "persistente y globalmente único que no requiere una autoridad de registro centralizada porque se genera y/o registra utilizando plataformas descentralizadas"[95]. Las llaves DIDs, se encontrarán bajo dominio del ciudadanx y a través de ellas estx autorizará o no el acceso a información de entidades que se la requieran.

Las billeteras, por su parte, son softwares diseñados para "almacenar y acceder de forma segura a claves privadas, credenciales y otros secretos o materiales confidenciales pertenecientes a un sujeto"[96]. En otras palabras, son repositorios portables de carácter personal donde almacenar y administrar información de manera segura[97]. Su nombre surge de la similitud del uso de billeteras en el mundo analógico, donde guardamos carnets de identificación, tarjetas, dinero en efectivo, etc. De esta manera un usuarix puede almacenar en un sólo lugar toda la documentación que hace a su identidad y que fue emitida por distintas fuentes.

Es importante destacar que existen distintos tipos de wallets y que no todas gestionan la misma información ni lo hacen de la misma manera, por lo cual la interoperabilidad entre las ellas no es algo dado. También existen diferencias respecto a la tenencia de las llaves privadas que protegen la información -de manera similar a lo que sucede en blockchain públicas en contraposición con las privadas o permisionadas.
Además, existe una cuestión relacionada al tipo de uso principal que tienen las distintas billeteras existentes. Mayormente, este uso es financiero, por lo cual la interfaz de usuarix suele ser técnica y estar pensada para resolver cuestiones específicas del mundo financiero. Las wallets para la gestión de la identidad, en cambio, tienen otro foco y deben

[94] Ibidem, p. 52.
[95] GCBA et al. 2022. "Identidad-digital - Whitepaper."
[96] Ibidem.
[97] Allende López, Marcos. 2020. *Identidad digital auto-gestionada…,* p. 23.

apuntar a un público más amplio que no necesariamente tenga conocimientos específicos sobre blockchain. Por ello, en la implementación de políticas de identidad descentralizada resulta central que las billeteras tengan un diseño que permita una experiencia satisfactoria para todo tipo de usuarixs.

En el gráfico 5, se pueden observar grandes diferencias con respecto al modelo tradicional. Principalmente, el usuario pasa a actuar como administrador central de su identidad; se elimina el proveedor de identidad y queda sólo un proveedor de servicio: el emisor deja de ser administrador de esa información. El uso de las credenciales estará sujeto a los permisos provistos por las llaves DIDs, que estarán en manos de cada usuario. Para interactuar con otra institución que requiera verificar la información, la persona conectará directamente su wallet sin necesidad de cargar datos de forma manual y reiterativa.

Esos terceros con quienes un usuarix comparte información actúan como verificadores dado que necesitarán verificar datos o atributos. El usuario será quien elija sí compartir información y qué datos mostrar. De hecho, en muchos casos es posible que la persona no tenga que mostrar un dato específico sino que un atributo se cumpla o no. Cabe aclarar que el emisor puede modificar información sobre la credencial, pero al estar registrado en la blockchain quedará la huella de esa modificación, de modo que agrega mayor transparencia al sistema.

Toda esta interacción se realiza sin tener que el emisor tenga que convalidar la información ni intervenir de ningún modo. De la misma manera, al estar toda la información registrada de forma segura e inalterable, no es necesaria la intervención de agentes legales o notariales. Este modelo no sólo minimiza el riesgo de fraude sobre los datos personales sino que reduce el costo asociado a los terceros -que dejan de ser necesarios- así como de tiempos de validación que puede requerir un trámite[98].

[98] Ibidem, p. 53.

5. Modelos de identidad descentralizada en acción: el caso del Gobierno de la Ciudad Autónoma de Buenos Aires.

5.1. Gobierno e identidad digital en la Ciudad Autónoma de Buenos Aires.

El Gobierno de la Ciudad de Buenos Aires (GCBA) viene trabajando en la mejora de sus capacidades de gobierno digital; el inicio de esta estrategia puede datarse en 2009, con la llegada al poder del partido actualmente gobernante[99]. En este punto, comenzó a delinearse una estrategia de digitalización del sector público, eliminando los trámites en papel y poniendo el foco en la mejora de servicios.

Hasta ese momento, la página oficial del GCBA tenía como uso principal la comunicación de información para su lectura, en un esquema que podría inscribirse dentro de una etapa de política de e-government[100]. En 2009, la página oficial del GCBA se reconvierte y la comunicación con la ciudadanía comienza a ser más interactiva, con la aparición de nuevos canales y sistemas para ello. Además, se dan algunas mejoras a nivel de los sistemas internos y las áreas del estado pueden comenzar a operar en un sistema unificado con firma digital llamado SADE, empezando a dejar atrás el uso del papel.

En los últimos años, ya con una base de digitalización más firme, el GCBA profundizó su estrategia buscando adoptar un enfoque de gobierno de plataforma. No solamente avanzó con nuevas políticas sino que reorganizó y cambió su organigrama, creando nuevas áreas dentro de la organización que tienen como objetivo específico impulsar y afianzar la transformación digital de manera integral y coordinada[101].

Entre las principales políticas de los últimos años, cabe mencionar la ampliación del sistema de datos abiertos (BA data), el lanzamiento de mapas abiertos sobre distintas temáticas, como el mapa del delito u oportunidades comerciales, así como Ciudad 3D, iniciativa premiada internacionalmente. En cuanto a los trámites, se amplió la oferta de servicios y los canales por los cuales poder realizarlos.

---

[99] El PRO comenzó a gobernar la Ciudad Autónoma de Buenos Aires en 2009. En renovaciones electorales posteriores, lo hizo de la mano de alianzas que sumaron otros partidos políticos, bajo el nombre de Cambiemos y luego Juntos por el Cambio.
[100] Santiso, Carlos, y Idoia Ortiz de Artiñano. 2020. *Govtech y el futuro del gobierno 2020*, pp. 25-27.
[101] Filer, Tanya, Antonio Weiss, y Juan Cace. 2019. *From City to Nation: Digital government in Argentina, 2015-2018*. Cambridge: Bennett Institute. https://www.bennettinstitute.cam.ac.uk/publications/argentina/.

Otra política importante fue la creación de Boti, un chatbot que utiliza inteligencia artificial y que brinda información de diversas temáticas a la ciudadanía. La oferta va desde poder realizar reclamos o solicitudes de acceso a la información pública, a consultar dónde es posible estacionar. Boti cumplió un rol importante durante la pandemia de COVID-19, siendo un medio de consulta ante sintomatología, turnos y demás cuestiones relativas a crisis sanitaria. En el primer tercio de 2022, tuvo 26 millones de conversaciones[102].

Como se ha mencionado, la identidad digital es central en toda política integral de transformación digital. Actualmente, el GCBA emplea un sistema tradicional de logueo, donde lxs usuarixs deben crearse una cuenta personal para iniciar sesión y acceder a sus servicios. Esa cuenta puede crearse haciendo uso de las integraciones con otros sistemas como AGIP o, en algunos casos, otros servicios privados como Google. No obstante ello, muchas veces es necesaria una carga y validación extra de datos, que ya se encuentran en otros sistemas.

Asimismo, el GCBA posee más de un sistema a través del cual lxs ciudadanxs pueden realizar trámites o acceder a servicios. De esta manera, es necesario crear varias cuentas para interactuar con un mismo gobierno. No todos los sistemas poseen la misma variedad de opciones para el logueo; algunas incluso requieren la creación de una cuenta directamente en esa página.

A pesar de los enormes avances y de liderar los rankings de transformación digital del país[103], aún queda un enorme camino por recorrer, siendo la interoperabilidad uno de los principales temas pendientes: muchas áreas siguen sin contar con los mecanismos para intercambiar información y lxs ciudadanxs continúan actuando como cadetes para proveer los datos en forma reiterativa cada vez que quieren realizar un trámite o interacción con el GCBA. En este sentido, la experiencia digital continúa siendo aquella de un gobierno fragmentado[104].

---

[102] GCBA. 2022. “Boti, el chatbot porteño, superó las 26 millones de conversaciones.” Buenos Aires Ciudad. https://www.buenosaires.gob.ar/jefaturadegabinete/innovacion/noticias/boti-el-chatbot-de-la-ciudad-supero-las-26-millones-de.
Para más información sobre Boti ver Banegas, Fernando. 2022. *Estados ágiles en América Latina: la experiencia de Buenos Aires en el uso de canales digitales con ciudadanos.* Caracas: CAF. https://scioteca.caf.com/handle/123456789/1879.

[103] Filer, Tanya, Antonio Weiss, y Juan Cace. 2019. *From City to Nation…*

[104] Esta situación también se da a nivel nacional. OCDE. 2019. *OECD Digital Government Studies Digital Government Review of Argentina: Accelerating the Digitalisation of the Public Sector*. París: OECD Publishing. https://doi.org/10.1787/354732cc-en.

Para dimensionar la problemática, es importante tener en cuenta que la Ciudad de Buenos Aires es la más grande del país. Además de su población de casi 3 millones de habitantes, se estima que por día la visitan más de 3 millones de personas más, la mayoría provenientes del Gran Buenos Aires, con motivos laborales[105]. Como tal, cuenta con una gran estructura burocrática, con una amplia diversidad de áreas que poseen información sensible y valiosa sobre lxs ciudadanxs y las actividades que suceden en la Ciudad, pero que no está disponibilizada para un uso más eficiente entre distintas reparticiones.

La tarea de coordinar y garantizar una comunicación interna y fluida en tamaña estructura es, sin dudas, compleja. Como consecuencia, se puede señalar un alto costo de oportunidad en la cantidad y calidad de información que se utiliza para la toma de decisiones, el diseño, implementación y monitoreo de políticas públicas.

Sumado a esto, la existencia de múltiples identidades digitales -o bien de identidades fragmentadas- trae aparejado el problema de la validación de la identidad. Los procedimientos actuales muchas veces requieren validar credenciales físicas; por la falta de protocolos en común esto debe hacerse de forma manual lo que no sólo genera una menor agilidad sino una mayor propensión a falsificaciones y suplantaciones de identidad. Del mismo modo que la administración pública sufre las ineficiencias de modelos de gestión subóptimos, lo hacen los ciudadanxs a la hora de querer acceder a servicios públicos.

Esta situación ha de entenderse -además- en un contexto de avance exponencial de la digitalización, donde las tecnologías y las necesidades y demandas ciudadanas avanzan más rápido que la respuesta estatal. A la vez, y como consecuencia de esa situación, garantizar un intercambio de datos de forma segura y eficiente entre áreas y organismos estatales -aunque también del sector privado- se vuelve aún más esencial no sólo para poder seguir construyendo la transformación digital pública sino para no quedarse atrás en ella. Aquí no sólo está en juego la seguridad y eficiencia del gobierno sino la calidad de los servicios que este provee y, como consecuencia, el grado de satisfacción de la ciudadanía.

Sin embargo, dentro de las iniciativas para mejorar la interoperabilidad y los problemas que está tiene aparejados tanto para lxs ciudadanxs como para el propio gobierno, el GCBA impulsa la creación de Quark ID[106], un novedoso protocolo que opera sobre blockchain y

[105] Valores pre-pandemia. Fuente: Consejo Económico y Social de la Ciudad de Buenos Aires (CESBA).
[106] Quark ID surge inicialmente bajo el nombre de TANGO ID. Por ello, en parte de la bibliografía y/o notas sobre él aparece con un nombre distinto al actual.

propone un nuevo modelo de gobernanza de datos para la gestión de la identidad digital radicalmente opuesto al anterior.

5.2. Un ecosistema cripto fuerte: primeros pasos hacia la descentralización.

Para entender el surgimiento de Quark ID es necesario primero remontarse a los antecedentes sobre identidad digital descentralizada en la Ciudad de Buenos Aires y también conocer el estado del ecosistema cripto en Argentina.

Por un lado, cabe señalar que Quark ID no es el primer acercamiento de la Ciudad de Buenos Aires -ni de Argentina- a la tecnología blockchain. El primer proyecto de identidad descentralizada en Argentina nació en 2016, bajo el nombre de Proyecto DIDI y aún continúa operativo. A diferencia de Quark ID, su propósito principal estaba orientado en generar un impacto positivo en grupos vulnerables; una de sus primeras aplicaciones fue en el Barrio Padre Carlos Mugica[107], un asentamiento informal de la CABA sobre el cual el Gobierno puso un gran foco para su integración y urbanización.

La manera de hacerlo era a través de la creación de una identidad digital confiable, accesible y relevante a personas del Barrio Mugica y de la generación de herramientas para que esas identidades pudieran consolidarse y así aumentar el acceso a bienes y servicios. En palabras de Proyecto DIDI, buscaban “mejorar los niveles de confianza y derribar algunas de las barreras socioeconómicas y financieras que impiden el acceso a bienes y servicios de calidad en poblaciones vulnerables”[108].

Con ello, buscaban en definitiva reducir la penalidad de pobreza, es decir, de ese mayor costo relativo que las personas de menos recursos enfrentan para acceder a ciertos bienes y servicios, utilizando nuevas tecnologías. Este costo, que surge por la información asimétrica del mercado que no cuenta con información confiable sobre la identidad y comportamiento de las personas, redunda en una exclusión de ciertos grupos o una inclusión a un costo muy alto para esas personas. Esta situación se da, en particular, en el acceso al sistema financiero, donde el proyecto tenía el foco.

Un factor importante de este antecedente para entender el posterior impulso de un protocolo para toda la ciudadanía tiene que ver con el equipo que llevaba adelante la integración del

[107] El actual Barrio Carlos Mugica fue históricamente conocido como “Villa 31” y luego como “Barrio 31”.
[108] Web oficial de DIDI. https://didi.org.ar/quienes-somos/

Barrio 31. En ese entonces, Diego Fernandez estaba al frente de la Secretaría de Integración Social y Urbana, cuya misión era coordinar el plan integral de reurbanización del Barrio Mugica. Actualmente él -y parte de su equipo- lideran la Secretaría de Innovación y Transformación Digital que además de estar a cargo del desarrollo de soluciones innovadoras en la Ciudad y de la modernización de sus sistemas, tiene bajo su órbita la Dirección General de Ciudadanía Digital, que impulsa Quark ID. Una posible explicación a cómo llega a la agenda del Gobierno de la Ciudad la Identidad Descentralizada, tiene que ver con la experiencia previa del actual Secretario de Innovación con respecto a la tecnología blockchain.

Además de haber un antecedente concreto de aplicación de identidad digital descentralizada en el GCBA, con un equipo que impulsaba su adopción y tenía conocimientos sobre la materia, el surgimiento de Quark ID debe entenderse también por la fuerza del ecosistema cripto en Argentina.

El país es considerado uno de los hubs cripto más importantes a nivel mundial. En materia de aplicación financiera, Argentina es uno de los países con más personas operando con criptomonedas. Probablemente impulsado por la inestabilidad económica, la cantidad de argentinxs que poseen conocimientos para operar con criptomonedas es ampliamente superior al promedio regional y global[109].

Las altas tasas de adopción van de la mano con un gran volumen de empresas y startups generando soluciones en blockchain. Con una particular inclinación hacia el sector fintech, pero con cada vez mayores aplicaciones en otros sectores e industrias, esta masa crítica disponibiliza recursos para construir soluciones robustas que no sólo aporten conocimientos técnicos sino una expertise en las necesidades de lxs usuarixs. Gracias a este ecosistema, el gobierno pudo apoyarse en él para el desarrollo pero también para tener una validación y un feedback con expertxs en la materia.

Parte de la apuesta del GCBA es apoyar ese ecosistema, que es visto por el Gobierno como un potencial atractivo para inversiones y generador de nuevos desarrollos con alto impacto[110].

---

[109] Sherlock communications. 2021. INFORME BLOCKCHAIN LATAM 2021. Sherlock communications. https://mcusercontent.com/4b2c98cfb207cdaae9e24e227/files/c62efd21-e66a-9942-8f50-2353d4c27e89/Sherlock_Communications_Ebook_Blockchain_LATAM_ES.pdf.

[110] Entrevista a Fabio Moto. 2022.

5.3. QuarkID, un protocolo para gestión de la identidad digital.

Quark ID es un protocolo descentralizado, público, no permisionado, abierto, extensible y capaz de interoperar con otros protocolos similares, que el Gobierno de la Ciudad de Buenos Aires impulsa pero sobre el cual no tiene ningún derecho de propiedad o licencia. El proyecto se ideó bajo un enfoque colaborativo: el GCBA convocó a lxs principales actores del ecosistema para construir, de manera consensuada con la comunidad, un sistema de interacciones digitales descentralizado.

De acuerdo al White Paper, uno de los objetivos principales del nuevo protocolo es devolverle autonomía a la ciudadanía: “se trata de un nuevo paradigma que va a permitir transacciones más simples y eficientes, devolviendo a las personas la soberanía sobre su información, el acceso, manejo y control de sus datos y documentación”[111]. Quark ID permitiría a lxs usuarios contar con sus credenciales en un único lugar, en una wallet a elección que le permita interactuar con organismos públicos y privados.

Al ser consultado al respecto, Fabio Moto, Project Manager de Quark ID del GCBA, destaca este punto como uno de los aspectos principales del protocolo y agrega que este problema, que es de carácter global, no implica sólo una falta de posesión de los datos por parte de las personas sino que estos estén en manos de empresas que comercian y usufructúan con ella[112].

Además de la falta de autonomía de las personas con respecto a sus datos, la motivación surge de otros tres elementos. El primero es la existencia de identidades fragmentadas en distintas plataformas que restan agilidad pero también otorgan información privada a terceros. El segundo elemento es la baja interoperabilidad entre organismos, que favorece la reproducción del fenómeno del *ciudadanx cadete*. Finalmente, la tercera problemática es la existencia de sistemas de validación obsoletos que aún requieren credenciales físicas para funcionar y que además de ser ineficientes, presentan grandes brechas de seguridad.

Un aspecto a destacar para entender la naturaleza del proyecto es que su creación no tiene como objetivo principal desarrollar identidades digitales para habitantes de la Ciudad de Buenos Aires sino impulsar un protocolo abierto y colaborativo para que tanto la Ciudad como cualquier otra organización -pública o privada- pueda hacer uso de ella y crear nuevas aplicaciones a partir de esa base. Desde el GCBA también destacan el impacto positivo que el proyecto puede tener en las empresas; según Moto, las sociedades que primero puedan

[111] GCBA et al. 2022. “Identidad-digital - Whitepaper.”.
[112] Entrevista a Fabio Moto. 2022.

implementar este tipo de sistema masivamente, podrían crecer entre un 4% y 15% de su PBI, por la simplificación, aceleración y seguridad que produce en trámites.

En la visión del GCBA, su rol como gobierno es facilitar la creación y el uso de nuevas herramientas que aporten valor a la sociedad. De acuerdo al Secretario de Innovación y Transformación Digital, una de sus responsabilidades es hacer que aquellos que lideran gobiernos enteros entiendan “que hay una oportunidad fenomenal pero no para el gobierno, para la sociedad”[113].

El protocolo actúa entonces como una infraestructura pública que el gobierno disponibiliza para que cualquier personas -física, jurídica, pública, privada, local o internacional- pueda adoptar con bajas barreras por la disminución del costo de desarrollo inicial y sobre la cual pueda además construir nuevas soluciones. En palabras de Diego Fernandez: “creemos que lo importante es que Quark ID funcione como una infraestructura pública, para que cualquiera pueda construir valor, y para transformar y simplificar la manera en que el Estado y la sociedad se relacionan, al mismo tiempo que empoderamos a las personas”[114].

Como se mencionó, Quark ID parte de un proceso de co-creación que reunió a actores del ecosistema local pero también del ámbito internacional. La mayoría de los participantes -como Extrimian, OS City, BEON tech, X capit, IOV labs y Starknet- provienen del ámbito privado. Sin embargo, también participaron instituciones públicas como el gobierno de Vicente López y de Luján de Cuyo. Desde el GCBA destacan el rol de empresas extranjeras en la provisión de cuestiones de alta tecnología que en Argentina aún no están disponibles; tal es el caso de Starknet, una empresa israelí que incorpora pruebas de conocimiento cero en su blockchain[115].

Para llegar a un consenso, se realizaron workshops en donde se discutieron los distintos aspectos del protocolo. El Secretario de Innovación y Transformación Digital fue compartiendo versiones preliminares con el público a través de sus redes sociales[116]. Sin

[113] LABITCONF. 2022. “QuarkID - La construcción de una Identidad Digital Auto Soberana para Argentina.”
[114] Gobierno de la Ciudad de Buenos Aires. 2022. “La Ciudad estuvo presente en Labitconf con todos los detalles sobre Quark ID.” Buenos Aires Ciudad. https://www.buenosaires.gob.ar/jefaturadegabinete/innovacion/noticias/la-ciudad-estuvo-presente-en-labitconf-con-todos-los-detalles.
[115] Entrevista a Fabio Moto. 2022.
[116] Fernández, Diego. 2022. “Publicación sobre Workshop.” LinkedIn. https://www.linkedin.com/posts/dhfernandez_tangoid-blockchain-identidaddigital-activity-6941042024200441856-D1B7/?utm_source=share&utm_medium=member_desktop https://www.linkedin.com/posts/dhfernandez_tecnologia-innovacion-identidaddigital-activity-69280578.

dudas, esta estrategia contrasta con el modelo tradicional donde las soluciones se idean de forma cerrada en el sector público. Usualmente, ante una necesidad de estas características, el estado idearía un sistema de uso interno y privado, el cual desarrollaría a través de proveedor o bien directamente in-house. El lenguaje de desarrollo sería el estándar de la organización -no necesariamente compatible con otros sistemas externos o de otras áreas de un mismo gobierno- y su arquitectura respondería a las necesidades de ese uso específico.

En esta lógica cerrada reside, en gran parte, el problema de la interoperabilidad. ¿Cómo hacer que las áreas compartan información y la usen de una manera virtuosa si los sistemas que usan no hablan el mismo idioma? El principal enfoque para intentar alcanzar la interoperabilidad gubernamental ha sido el diseño de enormes sistemas que tenían que ser adoptados por todas las áreas de un gobierno y que reemplazaran a las anteriores.

En este sentido, la ideación colaborativa de este protocolo es otra señal de la intención del Gobierno de la Ciudad de Buenos Aires de incorporar miradas que no surjan solamente de lo público sino que aborden la problemática de una manera integral y de fomentar que ese protocolo pueda ser adoptado por otros sectores. Diego Fernandez declaró que con estos enfoques “no buscan reinventar la rueda” sino que apuntan a identificar consensos establecidos internacionalmente para poder sumarse a ellos y fomentar que otrxs también lo hagan, y de este modo asegurar una compatibilidad mayor con otros sistemas[117].

5.4. La implementación de una solución colaborativa.

Como se señaló anteriormente, QuarkID es, ante todo, un protocolo creado en forma colaborativa que el Gobierno de la Ciudad de Buenos Aires impulsa y cuyo código fuente estará disponible para su uso y adaptación en forma libre.

A la fecha[118], el proyecto se encuentra en fase de MVP (minimum viable product o producto mínimo viable, es español) y se esperan las primeras implementaciones en el Gobierno de la Ciudad de Buenos Aires para enero de 2023. De acuerdo al project manager de Quark ID del GCBA “como sucede con toda tecnología disruptiva” la implementación tendrá sus

[117] LABITCONF. 2022. “QuarkID - La construcción de una Identidad Digital Auto Soberana para Argentina”.
[118] Noviembre de 2022.

complejidades; por ello se hará de forma gradual y buscarán, con el tiempo, ir reemplazando “modalidades y formas más antiguas”[119].

En línea con ello, y de acuerdo a declaraciones de Diego Fernandez, se realizará un primer testeo de forma interna, en el Gobierno de la Ciudad de Buenos Aires. Luego, se realizará una selección de trámites que requerirán la creación de una identidad digital descentralizada para su realización a comienzos de 2023, generando un primer onboarding masivo. Antes de escalar su uso al resto de trámites, se realizará un monitoreo sobre el grado de adopción y el surgimiento de posibles pain-points que puedan surgir, de manera de poder perfeccionar el protocolo. Se prevé la creación de entre 300 mil y 500 mil identidades digitales descentralizadas para el 2023[120]. Esta primera implementación busca alcanzar a una masa crítica de usuarios, impulsando una adopción masiva, para que el sector privado -aunque también organizaciones del sector público- cuenten con una base mayor de usuarios y puedan escalar nuevas soluciones.

En cuanto a los aspectos técnicos, Quark ID es blockchain-agnóstico, es decir, que puede operar en más de una blockchain. En un primer momento, el protocolo comenzará a operar en las redes de Starknet y Rootstcok, pero se espera que pueda escalar a otras como ethereum, polygon o RSK[121]. En las primeras instancias, no incorporará zero-knowledge proof pero esperan hacerlo más adelante. Este protocolo fue destacado tanto por el equipo del GCBA como de Extrimian como una valor agregado importante en este tipo de soluciones[122].

Al ser consultado por el proceso de desarrollo de Quark ID, Mosquella destacó que uno de los mayores temores de las instituciones es la implementación y que el grado de dificultad de hacerlo varía de acuerdo al nivel de transformación digital previo con el que cada área cuenta y a la arquitectura de sus sistemas. En ese sentido, Mosquella afirma que “muchos gobiernos creen que deberán cambiar mucho de sus sistemas”, pero que esto no es necesariamente así. Desde el lado tecnológico, observa que las integraciones son posibles pero que la verdadera dificultad está en “cambiar el mindset” de los gobiernos, para que entiendan que se están embarcando en un sistema completamente distinto al que tenían[123].

[119] Entrevista a Fabio Moto. 2022.
[120] LABITCONF. 2022. “Bases de las Identidades Digitales Auto Soberanas - Presentación de los ganadores del Hackathon.” YouTube. https://www.youtube.com/watch?v=qQf_o8Mj4XU
[121] Gobierno de la Ciudad de Buenos Aires. 2022. “La Ciudad estuvo presente en Labitconf…”
[122] Entrevista a Fabio Moto. 2022; Entrevista a Pablo Mosquella. 2022.
[123] Entrevista a Pablo Mosquella. 2022.

Entre los principales desafíos, destaca también la necesidad de estandarizar datos -una práctica poco usual en gobierno- y de permitir que las capas de seguridad preexistentes se adapten a las integraciones vía API con soluciones en blockchain. Este último punto es visto con particular temor por algunas áreas. Adicionalmente, ve una necesidad de revisar el corpus jurídico para ver cómo este se adapta al nuevo modelo de gestión, así como de actualizar y reformar lo que sea necesario para la operatoria y un mejor resguardo de datos[124].

Gracias a su formato abierto, la ciudad de Buenos Aires no es la única que está implementando este protocolo. Su adopción avanza en territorios como Gibraltar, Nueva León y Monterrey en México, Gobierno de Colombia, Provincia de Salta, Provincia de Entre Ríos, Ciudad de Vicente López y Mar del Plata en Argentina. Para el Gobierno de la Ciudad de Buenos Aires, estos primeros casos de adopción del protocolo son sumamente promisorios ya que el protocolo se encuentra aún en fase de MVP. En un futuro, cuando incorpore aprendizajes de una implementación y la usabilidad en gobierno, esperan una adopción aún mayor[125]. Al ser consultado por la necesidad de una adopción mayor por parte de otros gobiernos o empresas para que Quark ID funcione en el GCBA, Moto Indicó que aún sin otras implementaciones el funcionamiento dentro de la Ciudad está garantizado aunque el mayor valor vendría que haya una gran adopción por otras entidades.

A priori, las palabras *blockchain*, *descentralización* y *gobierno* no parecen no ir de la mano. De hecho, Diego Fernandez ha comentado que la dificultad de generar cambios desde el gobierno es grande y que el puesto de Secretario de Innovación en un Gobierno puede ser visto como un oxímoron. Sin embargo, Mosquella destaca que la recepción de otros gobiernos e instituciones ante las propuestas de modelos descentralizados fue “sorprendentemente positiva”. En un primera instancia, lo ven como una herramienta más para su transformación digital pero considera que es tal vez el hecho de que la propuesta venga de la mano con una premisa tan potente como “devolverle la autonomía a las personas” lo que es el gran atractivo para los gobiernos. Sin embargo, destaca la necesidad de “educar” a lxs actores interesadxs más que con modelos tradicionales. Desde el GCBA también destacan este aspecto como muy importante, siendo centrales la educación, la comunicación y la difusión, en particular con la ciudadanía. Ambos coinciden en que el desafío mayor “es educativo y no tecnológico”[126].

---

[124] Ibidem.
[125] LABITCONF. 2022. “QuarkID - La construcción de una Identidad Digital Auto Soberana para Argentina.”
[126] Entrevista a Fabio Moto. 2022; Entrevista a Pablo Mosquella. 2022.

Además de Quark ID, hay otros proyectos de identidad digital en curso. Proyecto DIDI, mencionado anteriormente, está trabajando en implementaciones con el gobierno de la Provincia de Misiones y la Municipalidad de General Pueyrredón para la gestión digital de gobierno, y también con productores rurales y comunidades originarias de la región del Gran Chaco en proyectos de inclusión financiera. Estas aplicaciones son desarrolladas en conjunto con partners que también participaron en la ideación e implementación de Quark ID, como es el caso de la empresa govtech OS City[127].

5.5. Una nueva oportunidad para mejorar la gobernanza de datos

Los casos de uso de modelos descentralizados que se basen en tecnologías como blockchain se encuentran en un estadío de desarrollo muy incipiente, sobre todo en lo que se refiere a identidad digital. Este contexto hace que sacar conclusiones sobre su impacto en el funcionamiento de los gobiernos sea apresurado. Sin embargo, la aparición de este tipo de enfoques muestran señales positivas para alcanzar una verdadera transformación digital en el ámbito público.

En primer lugar, protocolos como Quark ID proponen un abordaje completamente distinto al que los gobiernos han adoptado sucesivamente para intentar resolver la cuestión de la interoperabilidad. De acuerdo al testimonio del COO de Extrimian, existe hoy un interés genuino y un gran entusiasmo por parte de los gobiernos de diferentes geografías en conocer sobre este tipo de soluciones y en avanzar en desarrollos e implementaciones.

Asimismo, el GCBA no está abordando la problemática de la interoperabilidad únicamente a través de Quark ID. Según Moto, la Secretaría de Innovación y Transformación Digital desarrolla también otros proyectos de integración interna. Para finales de 2023, la Ciudad tiene como objetivo haber integrado la mayor parte de sus sistemas, tanto de gestión interna como de cara al vecino[128]. En paralelo, trabajan en la simplificación de trámites, detectando y eliminando los procesos que se repiten para agilizarlos[129]. De esta manera, buscan atacar el problema desde varios frentes.

---

[127] Proyecto DIDI. 2021. “Identidad y blockchain: presentan nuevos proyectos de gobierno digital e inclusión financiera en….” Proyecto DIDI. https://proyectodidi.medium.com/identidad-y-blockchain-presentan-nuevos-proyectos-de-gobierno-digital-e-inclusi%C3%B3n-financiera-en-d9a134f569c8.
[128] Entrevista a Fabio Moto. 2022.
[129] Entrevista a Fabio Moto. 2022.

Adicionalmente, el hecho de que un gobierno impulse un protocolo de manera abierta y que este no lleve su logo en la imagen de marca es todo un gesto. De acuerdo a Pablo Mosquella, esta elección tuvo que ver con una búsqueda de disminuir la desconfianza que la presencia de un gobierno puede generar.

En línea con ello, el carácter open-source del protocolo es, tal vez, su aporte más significativo para la interoperabilidad. Por un lado, el gobierno disponibiliza una infraestructura o bien público al alcance de todo el mundo para ser adoptado y utilizado como una base sobre la cual seguir construyendo. Por otro lado, el código está disponible para que pueda ser revisado y adaptado a necesidades puntuales, otorgándole un nivel de transparencia y, por consiguiente, confianza, para nada usual en la actualidad.

El protocolo, a su vez, sigue estándares internacionales y su diseño no responde a necesidades internas y específicas de un gobierno. Así, cualquier actor que desee adoptar Quark ID, no deberá tener que mediar con un gobierno y adaptarse a su modelo de gestión sino sumarse a un estándar internacional. De esta manera, las fricciones de índole política o técnica que puedan surgir se ven disminuidas ampliamente y se allana el camino para establecer un lenguaje común y con menores costos transaccionales.

Esto beneficia a lo que puede llamarse una interoperabilidad “backend”, es decir, una comunicación más fluida dentro de una misma organización o entre organizaciones. De hecho, como señala Mosquella, las soluciones de identidad digital descentralizada bien pueden implementarse a una escala menor con el objetivo puntual de mejorar la interoperabilidad interna de una misma organización. Sin embargo, también tiene un gran impacto de cara a lxs usuarixs, en lo que puede denominarse interoperabilidad “frontend”.

Como se ha mencionado, con los modelos actuales de gobernanza, lxs ciudadanxs terminan actuando como “cadetes” de los gobiernos recolectando y presentando la misma información una y otra vez. En cambio, con este tipo de modelo de gestión como el que propone Quark ID, la persona pasa a tener la custodia de su información en todo momento, pudiendo presentar los datos requeridos de manera instantánea a una organización que esté integrada al sistema durante las 24 horas del día.

Este giro reconoce la falta de capacidad estatal de gestionar de manera interna la interoperabilidad pero lo resuelve devolviendo a las personas la autonomía sobre su información y, con ello, el tiempo que actualmente pierde al tener que estar supliendo esa falencia. Es notable que el enfoque de este modelo deja un lado la centralidad estatal para

poner a la ciudadanía en el centro. Si las implementaciones logran ser exitosas, tienen un enorme potencial de comenzar a devolverle a la ciudadanía la confianza en lo público que, como se ha destacado, está en crisis a nivel global.

Otro punto no menor es la capa de seguridad que este protocolo agrega. Actualmente, se dan principalmente tres situaciones de gran relevancia. Por un lado, existen aún mecanismos de validación obsoletos que obligan a utilizar credenciales físicas. Este tipo de validación manual tiene un bajo nivel de seguridad y fomenta la posibilidad de delitos de suplantación de identidad o falsificación de documentos.

Por otro lado, en los sistemas actuales, cuando una persona presenta documentación personal está otorgando más información que la solicitada. Por ejemplo, un pedido de mostrar un DNI para demostrar que una persona es mayor de 18 años, otorga no solamente la edad exacta de la persona sino datos sobre su lugar de residencia, número de trámite, foto, etc. A través de protocolos de zero knowledge proof, es posible validar un dato sin conocerlo exactamente. Retomando el ejemplo anterior, un algoritmo podría validar que la edad sea mayor a 18 pero sin mostrarle al solicitante del dato el número exacto.

Lo que sucede es que en los modelos actuales, toda la información obtenida no es almacenada de forma 100% segura. Sobre este último punto, Diego Fernandez hizo referencia a los múltiples ciberataques que recibe el Gobierno de la Ciudad de Buenos Aires en forma diaria a sus sistemas. Esta situación es común a todos los gobiernos y, a medida que avanza la tecnología crecen las posibilidades de que más ataques sean efectivos. Las vulneraciones a bases de datos de gobiernos -aunque también privados- son una realidad hoy y ya afectan la seguridad de las personas.

La utilización de bases de datos descentralizadas elimina la eficacia de los ataques dado que para hacerse de la información es necesario atacar a un enorme cantidad de nodos y no a un objetivo único. Además de sumar una capa de seguridad, le quita costos operativos de almacenamiento y protección de enormes cantidades de datos que, a su vez, se encuentran repetidos en varias bases de datos.

La autonomía y seguridad hacia lxs usuarixs no solamente se da a nivel del sector público sino también de cara a las empresas tecnológicas que hoy poseen millones de datos sensibles sobre las personas y monopolizan el acceso a la identidad digital. Sumado a las posibles vulneraciones de seguridad y resguardo de datos, si una empresa decidiera

prohibir el acceso a una cuenta que es la llave para realizar un login ante otras instituciones, le estaría también revocando el derecho a esos accesos.

Por último, ha de señalarse que el enfoque de código abierto permite alcanzar un impacto más amplio, bajar las barreras de acceso y habilitar la intervención de nuevos talentos y nuevos mercados. A su vez, crea y facilita nuevas oportunidades para el sector privado de una manera más segura, sostenible y escalable[130]. Por ello, el potencial de implementación de este tipo de modelos excede la finalidad principal que pueda tener, como es en este caso la gestión de la identidad digital.

[130] UNICEF. “CryptoFund.” CryptoFund UNICEF. Accessed Julio, 2022. https://cryptofund.unicef.io/home/.

6. Conclusiones.

La transformación digital en el sector público ha mostrado enormes avances en los últimos años pero su desarrollo dista de ser el ideal. En primer lugar, existen muchas desigualdades entre países aunque también entre los distintos niveles de gobierno e incluso entre las distintas áreas que componen una misma administración. A nivel global, los índices de gobierno digital promedio se encuentran muy por debajo de su potencial.

En segundo lugar, la disparidad en el desarrollo y la falta de calidad en las políticas de gobierno digital no permiten a las administraciones avanzar hacia verdaderos modelos de Gobierno como Plataforma. Los sistemas siguen careciendo de interoperabilidad y de una arquitectura robusta y segura, que facilite la vida de lxs ciudadanxs y proteja su información personal.

Adicionalmente, la transformación digital del sector público no avanza con la misma celeridad y agilidad con la que lo hace en el sector privado. Esto incrementa la disconformidad de la ciudadanía respecto a los servicios digitales provistos por los gobiernos, y contribuye a acrecer la gran crisis de confianza existente. Ese avance lento, contrastado con el frenético avance de la tecnología, hace que sea incrementalmente más difícil para los gobiernos lograr hacer un *catch-up* con la tecnología necesaria para proveer servicios de calidad y, por ende, alcanzar las expectativas ciudadanas.

La problemática de falta de interoperabilidad y la búsqueda de una construcción de sistemas más seguros ha sido abordada por los gobiernos siempre de una manera similar: anclada en un esquema en línea con la Web2 y con enfoques internos, cerrados y no coordinadados con otras áreas que podrían hacer uso de ese mismo sistema. Cabe destacar que el problema no reside en la digitalización en sí, ya que existe una enorme cantidad de sistemas de gobierno, sino en el enfoque utilizado para la gobernanza de datos.

Esta situación perpetuó la falta de interoperabilidad en dos niveles: backend y frontend. El primero se refiere a la falta de comunicación interna entre los sistemas de gobierno y también con los sistemas de empresas e instituciones privadas. Aquí, la principal problemática son las ineficiencias que se producen, la pérdida de oportunidades de mejora y crecimiento asociadas y el mantenimiento de procesos altamente burocráticos y costosos. El segundo nivel, el de front-end, hace referencia a las consecuencias que enfrentan lxs ciudadanxs por la falta de interoperabilidad, siendo el fenómeno del *ciudadano cadete* el

mayor exponente. Como se ha visto, esto no sólo empeora los niveles de satisfacción y confianza con el gobierno sino es más perjudicial para personas con menores ingresos.

Dentro de las políticas de gobierno digital, la gestión de la identidad es uno de los pilares fundamentales a analizar y mejorar. Esto es así porque actúa como una llave de acceso al mundo digital y a una enorme cantidad de trámites y servicios. Hasta el momento, la identidad digital ha sido abordada con una mirada también muy en línea con el modelo de Web 2. Cada página que requiriera un inicio de sesión, debía realizarse creando una nueva cuenta, ingresando la misma información una y otra vez, y repitiéndola en nuevos servidores que la alojaban.

En los últimos años, algunos servicios incorporaron la posibilidad de iniciar sesión más rápido a través de servicios como Google y Facebook, entre otros. Incluso desde los gobiernos, se permitieron *logins* con credenciales asociadas a aspectos específicos de la identidad, como es el caso de AGIP en Argentina. Si bien estas innovaciones generaron cierta agilidad, surgen dos cuestiones problemáticas al respecto. Por un lado, esto trae aparejado la concentración de información sensible en empresas privadas. Además, estas adquieren un poder cada vez más importante sobre las personas no sólo por poseer sus datos sino por tener la potestad de revocarlos sin previo aviso, inhabilitando el acceso a muchas otras cuentas. Por otro lado, este acercamiento al *single log-in* no se hizo de forma coordinada o unificada, por lo cual no cumple totalmente una función de integración de la identidad -ni está pensado para poder abarcar de forma segura el ingreso a todos los sistemas.

En este sentido, los nuevos modelos de gestión de la identidad digital que llegaron de la mano con el desarrollo de la tecnología blockchain proponen un cambio de paradigma. A través de una mayor autonomía de las personas sobre sus datos y una delegación -aunque coordinada y simplificada- de facilitar la interoperabilidad en gobierno, la información comenzaría a fluir más rápidamente y de forma más estandarizada, sin necesidad de validaciones manuales e inseguras por parte de las instituciones que las requieren. De esta manera, se estaría mejorando indirectamente la calidad de la provisión de servicios, y aumentando asimismo la capacidad de mejora, al poder redirigir recursos hacia estas tareas.

En cuanto a la autonomía de los datos, es importante destacar también su relevancia en el contexto de gobiernos totalitarios que busquen revocar credenciales o acceso a la ciudadanía, ya que el registro en blockchain y la propiedad de la credencial una vez emitida

dificulta este accionar y reduce la vulnerabilidad ante posibles situaciones de arbitrariedad estatal. Asimismo, ante fenómenos migratorios -elegidos y forzados- también supone dar mayores herramientas a las personas. Factores como las guerras, el cambio climático o las crisis económicas, entre otros, están generando mayores flujos migratorios, donde es común que las personas pierdan su documentación y puedan llegar a una situación de apatridia.

Por otro lado, dentro de estos nuevos modelos, existe la posibilidad de que un gobierno desarrolle y adopte un protocolo para sí mismo o bien, como se ha analizado con el caso del Gobierno de la Ciudad de Buenos Aires, impulse el desarrollo de protocolos para ser compartidos abiertamente. Este segundo modelo trae una serie de ventajas adicionales. En primera instancia, allana el camino a otros gobiernos y organizaciones que quieran incorporar este tipo de soluciones pero que no tengan los recursos -tanto económicos como humanos- de realizar un desarrollo propio. Teniendo en cuenta el menor desarrollo de soluciones de gobierno digital y de acceso a la identidad digital en países de menores ingresos, este es un gran paso para promover una mayor adopción y no acrecentar las brechas de desigual tecnológica. En este punto es, tal vez, donde más se puede apreciar un cambio de paradigma o cambio cultural, donde los gobiernos buscan ser facilitadores y promotores de un cambio, pero no dueños de este.

Adicionalmente, el enfoque abierto agrega un mayor capa de transparencia a la solución al ser pública tanto la arquitectura como los detalles de funcionalidades para que pueda ser auditado por todo el público. Hoy en día, la mayor parte de los sistemas de gobierno funcionan, para el afuera, como una caja negra donde no está claro qué sucede con la información que se le provee y que se almacena. En el contexto de una crisis generalizada hacia el sector público y de un incremento en la frecuencia y en la calidad de los ciberataques, este enfoque supone también un gran cambio.

Finalmente, el enfoque open-source y colaborativo pareciera promover la participación del sector privado y, de esta manera, dar más confianza de cara a la ciudadanía y entidades con un potencial interés de aplicación. Reducir la presencia de un gobierno concreto de la solución ayudaría a disminuir barreras de tinte ideológico-político o idiosincrático, nuevamente entendiendo la problemática en un contexto de polarización y desconfianza hacia lo público.

Sin embargo, la implementación de modelos descentralizados de gestión de la identidad digital en gobierno tiene grandes desafíos. En primer lugar, cabe mencionar que la mayor

parte de políticas de estas características se encuentran en fases de ideación y/o testeo. Por esta razón, aún existe un gran grado de incertidumbre sobre las problemáticas que puedan surgir una vez implementados.

Por otro lado, existen barreras significativas para que los gobiernos y empresas accedan a, al menos, testear estas soluciones. La barrera educativa es una y aunque existe un gran entusiasmo por conocer sobre ellas también existe un desconocimiento técnico sobre el funcionamiento de blockchain y los esquemas descentralizados. Esto puede demorar o bloquear el avance de estos modelos.

Además, esta barrera educativa se relaciona con la cultural: los gobiernos acostumbran a trabajar de una cierta manera y la gestión del cambio suele ser más lenta que en el sector privado, además de dispar entre áreas. La metodología tradicional de trabajo es, mayormente, interna a la organización, no colaborativa, sin la interoperabilidad como eje de la misma y con un almacenamiento de información en compartimentos estancos. Adoptar protocolos creados con una lógica general para que sean adoptados por una gran variedad de entidades, implica cambiar la lógica de gestión tradicional. Este es, según lxs expertos, uno de los mayores desafíos.

En cuanto a la implementación en gobierno, también cabe señalar la importancia de tener un cierto nivel en el desarrollo de las políticas de transformación digital así como una arquitectura de software lo suficientemente sólida y robusta como para que la integración con un protocolo descentralizado sea más simple. Si bien no es un requisito *sine qua non*, si puede ser una barrera para una mayor adopción.

Del lado de la adopción externa al gobierno, en particular de la ciudadanía, la cuestión educativa vuelve a surgir como un aspecto clave a trabajar. La comunicación, difusión y capacitación es señalada como esencial para que más gente utilice estas soluciones y aproveche su máximo potencial. En este sentido, los grupos con mayores dificultades de acceso a la tecnología, como los adultos mayores, deberán ser un foco de atención en estas políticas. Nuevamente, la tecnología tiene un gran potencial de incluir pero también de excluir; por ello, es esencial que los gobiernos tengan en cuenta esto a la hora de desarrollar este tipo de políticas.

Asimismo, surge la importancia de diseñar billeteras virtuales y sistemas en general con provean una experiencia de usuarix satisfactoria, sin fricciones ni terminología compleja relacionada con el ecosistema blockchain, de manera de que ser expertx en la temática no

sea un requisito. Esta necesidad no es sólo responsabilidad del gobierno sino también de lxs proveedores de sistemas y/o wallets que operan de cara a la ciudadanía. Actualmente, la mayor parte de aplicaciones disponibles en el mercado apuntan a un uso financiero de blockchain y a un resguardo de criptoactivos pero no de credenciales administrativas, aunque existen empresas que ya están desarrollando soluciones que responden a esta necesidad.

El surgimiento de estas soluciones es una señal importante de que los gobiernos están buscando resolver antiguas problemáticas con nuevas lógicas. Si bien en un comienzo no van a significar una resolución del 100%, sí muestran que el gobierno trata de adoptar un rol de facilitador en pos de una mayor autonomía para sus ciudadanxs.

Finalmente, cabe realizar dos reflexiones acerca de la la adopción de nuevas tecnologías para la resolución de problemáticas públicas. En primer lugar, que la tecnología en general y blockchain en particular deben ser un medio para resolver problemas concretos y no al revés. Es decir, la tecnología que hoy resulta idónea para resolver una problemática puede dejar de serlo conforme evolucionan esas problemáticas y las demás tecnologías disponibles. En segundo lugar, que la seguridad que hoy provee blockchain no exime a los gobiernos a seguir trabajando en estos temas porque el avance de las tecnología sigue siendo exponencial. Avances en la computación cuántica, por ejemplo, podrían poner en jaque los protocolos actuales de encriptación y ciberseguridad.

***

Los modelos descentralizados basados en blockchain demuestran tener un gran potencial para la mejora de la gobernanza de datos de la interoperabilidad en el sector público a través de un esquema radicalmente distinto al tradicional. Los gobiernos parecen tener un alto nivel de interés en probar estos nuevos enfoques para dar una mayor autonomía a las personas sobre sus datos. De cara al futuro, la educación y comunicación sobre este nuevo modelo resultará clave para determinar su impacto y asegurar un uso inclusivo a la vez que productivo del mismo. Asimismo, el foco deberá ponerse más en el cambio cultural que en el tecnológico. No obstante ello, los gobiernos deberán estar atentos a las problemáticas que puedan surgir en las implementaciones y en los avances de la tecnología para asegurarse que la gobernanza de la identidad digital continúe siendo segura y eficiente.

Bibliografía

- Allen, Christopher. 2016. “The Path to Self-Sovereign Identity.” Life With Alacrity. http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html.
- Allende López, Marcos. 2020. *Identidad digital auto-gestionada. El futuro de la identidad digital: auto-gestión, billeteras digitales y blockchain*. Banco Interamericano de Desarrollo (BID). http://dx.doi.org/10.18235/0002635.
- Apolitical. 2017. “El intercambio de datos de Estonia le permite pagar sus impuestos en cinco minutos.” Apolitical. https://apolitical.co/solution-articles/es/plataforma-de-intercambio-de-datos-que-convierte-a-estonia-en-lider-de-gobierno-digital.
- Banco Mundial, ed. 2021. *Principios Sobre la Identificacion para el Desarrollo Sostenible : Hacia la Era Digital*. Banco Mundial. https://documentos.bancomundial.org/es/publication/documents-reports/documentdetail/371801496861423208/principles-on-identification-for-sustainable-development-toward-the-digital-age.
- Banco Mundial. “Data | Identification for Development.” ID4D. Accessed Mayo, 2022. https://id4d.worldbank.org/global-dataset.
- Banco Mundial. “Desarrollo digital.” Banco Mundial. Accessed Mayo, 2022. https://www.bancomundial.org/es/topic/digitaldevelopment/overview.
- Banegas, Fernando. 2022. *Estados ágiles en América Latina: la experiencia de Buenos Aires en el uso de canales digitales con ciudadanos.* Caracas: CAF. https://scioteca.caf.com/handle/123456789/1879.
- Berryhill, Jamie, Théo Bourgery, y Angela Hanson. 2018. *Blockchains Unchained: Blockchain Technology and its Use in the Public Sector*. Paris: OECD Publishing. https://doi.org/10.1787/3c32c429-en.
- Cebr. 2022. “The digital trust index: What is the value of digital trust?” Londres. bit.ly/3Wyt5nh.
- Cetina, Camilo. 2022. *DIGIntegridad: La transformación digital de la lucha contra la corrupción*. Edited by Carlos Santiso. CAF. https://scioteca.caf.com/handle/123456789/1901.

- Cheng, Steve, Matthias Daub, Axel Domeyer, y Martin Lundqvist. 2017. “Using blockchain to improve data management in the public sector.” McKinsey. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/using-blockchain-to-improve-data-management-in-the-public-sector.

- Cristia, Julián P., y Razvan Vlaicu. 2022. *Digitalizar los servicios públicos: Oportunidades para América Latina y el Caribe*. Banco Interamericano de Desarrollo (BID). http://dx.doi.org/10.18235/0004543.

- Diofasi, Anna, Jing Lu, y Vyjayanti T. Desai. 2018. “El desafío mundial de la identificación: ¿quiénes son los 1000 millones de personas que no tienen un documento de identidad?” World Bank Blogs. https://blogs.worldbank.org/es/voices/quienes-son-los-1000-millones-de-personas-que-no-tienen-una-identificacion.

- Fernández, Diego. 2022. “Publicación sobre Workshop.” LinkedIn. https://www.linkedin.com/posts/dhfernandez_tangoid-blockchain-identidaddigital-activity-6941042024200441856-D1B7/?utm_source=share&utm_medium=member_desktop
https://www.linkedin.com/posts/dhfernandez_tecnologia-innovacion-identidaddigital-activity-69280578.

- Filer, Tanya, Antonio Weiss, y Juan Cace. 2019. *From City to Nation: Digital government in Argentina, 2015-2018*. Cambridge: Bennett Institute. https://www.bennettinstitute.cam.ac.uk/publications/argentina/.

- Fowler, Geoffrey A., y Geoffrey Fowler. 2021. “Your privacy is the price of Facebook’s monopoly.” *The Washington Post*, August 29, 2021. https://www.washingtonpost.com/technology/2021/08/29/facebook-privacy-monopoly/

- GCBA. 2022. “Boti, el chatbot porteño, superó las 26 millones de conversaciones.” Buenos Aires Ciudad. https://www.buenosaires.gob.ar/jefaturadegabinete/innovacion/noticias/boti-el-chatbot-de-la-ciudad-supero-las-26-millones-de.

- GCBA et al. 2022. “Identidad-digital - Whitepaper.” GitHub. https://github.com/gcba/Identidad-digital/blob/main/Whitepaper%20Tango.md#2-introducci%C3%B3n.

- Gobierno de la Ciudad de Buenos Aires. 2022. “La Ciudad estuvo presente en Labitconf con todos los detalles sobre Quark ID.” Buenos Aires Ciudad. https://www.buenosaires.gob.ar/jefaturadegabinete/innovacion/noticias/la-ciudad-estuvo-presente-en-labitconf-con-todos-los-detalles.

- Hayat, Zia. 2022. “Why digital trust is key to building thriving economies.” The World Economic Forum. https://www.weforum.org/agenda/2022/08/digital-trust-how-to-unleash-the-trillion-dollar-opportunity-for-our-global-economy/.

- Hayat, Zia. 2022. “Why digital trust is key to building thriving economies.” The World Economic Forum. https://www.weforum.org/agenda/2022/08/digital-trust-how-to-unleash-the-trillion-dollar-opportunity-for-our-global-economy/.

- “identidad | Definición | Diccionario de la lengua española | RAE - ASALE.” 2022. Diccionario de la lengua española. https://dle.rae.es/identidad.

- Jolías, Lucas, Ana Castro, y Jesús Cepeda, eds. 2022. *Identidad Digital Descentralizada : una guía de implementación de blockchain en gobierno*. Bahía Blanca: GovTech Hub. https://plus.os.city/publicaciones/identidad-descentralizada.

- Jolías, Lucas, Jesús Cepeda, y Ana Castro. “4 tendencias en el uso de blockchain en el Estado.” OS City. Accessed Octubre, 2022. https://plus.os.city/blog-os-city-plus/posts/4-tendencias-en-el-uso-de-blockchain-en-el-estado.

- LABITCONF. 2022. “Bases de las Identidades Digitales Auto Soberanas - Presentación de los ganadores del Hackathon.” YouTube. https://www.youtube.com/watch?v=qQf_o8Mj4XU.

- LABITCONF. 2022. “QuarkID - La construcción de una Identidad Digital Auto Soberana para Argentina.” YouTube. https://www.youtube.com/watch?v=nz9O3Rn-tN0.

- Lau, Edwin. 2006. “E-Government and the Drive for Growth and Equity.” *Paper, Belfer Center for Science and International Affairs, Harvard Kennedy School*. https://www.belfercenter.org/publication/e-government-and-drive-growth-and-equity.

- Lindman, Juho, et Al. 2020. “The uncertain promise of blockchain for government.” In *OECD Working Papers on Public Governance, No. 43,*. OECD-ilibrary.

https://www.oecd-ilibrary.org/governance/the-uncertain-promise-of-blockchain-for-government_d031cd67-en.

- Magee, Tamlin. 2014. “Social ID Raises Questions On Data Ownership, Privacy, Monopoly.” Forbes. https://www.forbes.com/sites/tamlinmagee/2014/01/31/social-id-raises-questions-on-data-ownership-privacy-monopoly/?sh=7668d2ec39a4.

- Mckinsey. 2019. *Digital identification: A key to inclusive growth*. https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/digital%20identification%20a%20key%20to%20inclusive%20growth/mgi-digital-identification-report.pdf.

- Naciones Unidas. 2020. *United Nations E-Government Survey 2020*. Nueva York: Naciones Unidas. https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2020-Survey/2020%20UN%20E-Government%20Survey%20(Spanish%20Edition).pdf.

- Naciones Unidas. “Objetivo 16: Promover sociedades justas, pacíficas e inclusivas.” UN.org. Accessed December 27, 2022. https://www.un.org/sustainabledevelopment/es/peace-justice/.

- Naser, Alejandra (coord), ed. 2021. *Gobernanza digital e interoperabilidad gubernamental: una guía para su implementación*. Santiago de Chile: Comisión Económica para América Latina y el Caribe (CEPAL). https://repositorio.cepal.org/bitstream/handle/11362/47018/1/S2100258_es.pdf.

- Navarro, Juan Carlos. 2018. “El imperativo de la transformación digital: Una agenda del BID para la ciencia y la innovación empresarial en la nueva revolución industrial.” https://publications.iadb.org/publications/spanish/viewer/El-imperativo-de-la-transformaci%C3%B3n-digital-Una-agenda-del-BID-para-la-ciencia-y-la-innovaci%C3%B3n-empresarial-en-la-nueva-revoluci%C3%B3n-industrial.pdf.

- Neri, Antonio. 2022. “Public sector risks losing trust as digital transformation lags.” The World Economic Forum. https://www.weforum.org/agenda/2022/05/the-public-sector-must-accelerate-digital-transformation-or-risk-losing-sovereignty-and-trust/.

- OCDE. 2019. *OECD Digital Government Studies Digital Government Review of Argentina: Accelerating the Digitalisation of the Public Sector*. París: OECD Publishing. https://doi.org/10.1787/354732cc-en.
- OCDE. 2019. *The Path to Becoming a Data-Driven Public Sector*. París: OECD Publishing. https://doi.org/10.1787/059814a7-en.
- Proyecto DIDI. 2021. “Identidad y blockchain: presentan nuevos proyectos de gobierno digital e inclusión financiera en….” Proyecto DIDI. https://proyectodidi.medium.com/identidad-y-blockchain-presentan-nuevos-proyectos-de-gobierno-digital-e-inclusi%C3%B3n-financiera-en-d9a134f569c8.
- Puliti, Riccardo. 2022. “La inclusión digital hace posible una recuperación más resiliente para todos.” World Bank Blogs. https://blogs.worldbank.org/es/voces/la-inclusion-digital-hace-posible-una-recuperacion-mas-resiliente.
- PwC. “Estonia – the Digital Republic Secured by Blockchain.” PwC. Accessed Junio, 2022. https://www.pwc.com/gx/en/services/legal/tech/assets/estonia-the-digital-republic-secured-by-blockchain.pdf.
- Ramírez Alujas, Álvaro, Jesús Cepeda, y Jolías Lucas. 2021. *GovTech en Iberoamérica : ecosistema, actores y tecnología para reinventar el sector público*. Bahía Blanca: GovTech Hub. https://www.trustfortheamericas.org/media/projects/attachments/en/Libro-Govtech-Iberoamerica-2021.pdf.
- Roseth, Benjamin. 2021. “Gobierno Digital: 5 pilares para tener servicios públicos sin salir de casa.” Blogs iadb. https://blogs.iadb.org/administracion-publica/es/gobierno-digital-5-pilares-que-permiten-al-gobierno-ofrecer-servicios-sin-salir-de-casa/.
- Roseth, Benjamin, Angela Reyes, y Carlos Santiso, eds. 2018. *El fin del trámite eterno: Ciudadanos, burocracia y gobierno digital*. Banco Interamericano de Desarrollo (BID). http://dx.doi.org/10.18235/0001150.
- Santiso, Carlos, y Idoia Ortiz de Artiñano. 2020. *Govtech y el futuro del gobierno 2020*. CAF y PublicTechLab de IE University de España. https://docs.ie.edu/publicteclab/GOVTECH_Y_EL_FUTURO_DEL_GOBIERNO.pdf.

- Semenzin, Silvia, David Rozas, y Samer Hassan. 2022. “Blockchain-based application at a governmental level: disruption or illusion? The case of Estonia.” research gate. https://www.researchgate.net/publication/359908026_Blockchain-based_application_at_a_governmental_level_disruption_or_illusion_The_case_of_Estonia/citation/download.

- Semenzin, Silvia, David Rozas, y Hssan Samer. 2022. “Blockchain-based application at a governmental level: disruption or illusion? The case of Estonia.” *Policy and Society* 41, no. 10 (Abril). 1093/polsoc/puac014.

- Sherlock communications. 2021. *INFORME BLOCKCHAIN LATAM 2021*. Sherlock communications. https://mcusercontent.com/4b2c98cfb207cdaae9e24e227/files/c62efd21-e66a-9942-8f50-2353d4c27e89/Sherlock_Communications_Ebook_Blockchain_LATAM_ES.pdf.

- UNICEF. “CryptoFund.” CryptoFund UNICEF. Accessed Julio, 2022. https://cryptofund.unicef.io/home/.

- United Nations. 2001-2022. *UN E-Government Survey*. https://publicadministration.un.org/egovkb/en-us/Overview.

Fuentes

- Entrevista a Fabio Moto, Project Manager de Quark ID en el Gobierno de la Ciudad de Buenos Aires. Realizada de forma virtual durante Noviembre del 2022.

- Entrevista a Pablo Mosquella, COO de Extrimian. Realizada de forma virtual durante Diciembre del 2022.

Anexo

Listado de tablas y gráficos: