Escuela Superior de Guerra “General Rafael Reyes Prieto”

Desafíos y tendencias de la identidad digital

MY Javier Hidalgo

MY Leonardo Lagos

CC Pablo Moreno

CC Edgar Zambrano

Habilidades prácticas para el ciberespacio

Prof. Jaider Ospina

Maestría en Ciberseguridad y Ciberdefensa

08 Agosto 2024

Desafíos y tendencias de la identidad digital

La identidad digital es uno de los conceptos más importantes en el ambiente digital moderno. Este abarca identificadores únicos y atributos que representan individuos, organizaciones o dispositivos en ambientes electrónicos y en el mismo ciberespacio. Va más allá de nombres de usuario y contraseñas, al incorporar datos biométricos, llaves criptográficas, e incluso patrones de comportamiento. Es así como se crea una identidad digital con un perfil multifacético que puede ser verificado y autenticado. La identidad digital ha sido definida como “el equivalente electrónico del documento de identidad del mundo real. Es el medio con el que se puede comprobar quien somos para acceder a servicios, derechos y privilegios en el mundo digital” (Tapscott & Tapscott, 2014). La cita anterior muestra como el alcance de la identidad digital hace que sea no solo en extremo importante, sino también útil para la relación ciudadano-gobierno y necesaria de protección.

Como se explicó anteriormente, la identidad digital está compuesta por diversos componentes siguiendo lo establecido por NIST (2017). El primero es el de los *identificadores*, marcadores únicos como direcciones de correo electrónico, nombres de usuario y números de teléfono, con los cuales se puede distinguir con facilidad una identidad digital de otra. En segundo lugar están las *credenciales*, tales como contraseñas, PINs y datos biométricos, usados para autenticar la identidad. En tercer lugar están los *atributos*, porciones de información asociadas con la identidad tales como nombre, edad, género, etc. Finalmente se encuentran los *datos de comportamiento*, tales como patrones y hábitos (ubicación, horas de ingreso y salida), los cuales pueden ayudar a detectar fraudes y a verificar información.

El Estado moderno ha buscado siempre manejar y acceder a la información que requiere de sus ciudadanos para poder cumplir sus funciones. Es por eso por lo que muchos gobiernos en el mundo han adoptado el concepto de la identidad digital en una búsqueda de eficiencia y control. Al adoptar sistemas de identidad digital han logrado mejorar la provisión de servicios, mejorar la seguridad, y agilizar procesos

administrativos de su burocracia. Se pueden categorizar las áreas de aplicación de la siguiente forma: 1) Sistemas nacionales de identificación, 2) servicios electrónicos de gobierno (*e-government*), 3) control de fronteras e inmigración, 4) ciberseguridad y prevención de fraudes, 5) servicios de bienestar social, y 6) ciudades inteligentes e *Internet of Things*.

Se observa como las áreas en donde se puede aplicar la identidad digital por el gobierno son amplias y abarcan aspectos enormes de la vida del ciudadano. Este aspecto de la identidad digital es el que hace que tenga facetas positivas y negativas pues toca la cuestión fundamental de qué tanto control debe ceder el ciudadano a su gobierno ante la búsqueda de la eficiencia. Equilibrar esto es uno de los desafíos que tiene actualmente el concepto de identidad digital, pero existen muchos más. Estos desafíos se relacionan principalmente con preocupaciones sobre la privacidad, la seguridad de datos, la brecha digital que existe entre sectores de gobierno y entre diferentes territorios, problemas de estandarización e interoperabilidad, y acceso equitativo a servicios de comunicaciones.

Una de las tendencias más importantes relacionadas a la identidad digital y el gobierno son los sistemas nacionales de identificación digital. Estos sistemas les permiten a los usuarios acceder de manera segura a servicios electrónicos de gobierno a través de firmas digitales seguras y capacidades de autenticación, reduciendo la necesidad de que los usuarios presenten documentos físicos y, por ende, la probabilidad de sufrir robos de identidad. La aplicación de sistemas como estos por los gobiernos del mundo les ayudará a cumplir el objetivo 16.9 de los Objetivos de Desarrollo Sostenible de la ONU, que reza que la 2030 todos los seres humanos deben tener una identificación legal. Esto representa tanto tendencia como desafío, pues en la actualidad hay alrededor de 1 billón de personas sin siquiera registro de nacimiento, y 3.4 billones tienen dificultades para usar sus identificaciones a través de distintas plataformas digitales (Okunoye, 2022).

La adopción de este tipo de sistemas tiene enormes beneficios, pero para que estos sean aceptados y utilizados por el público en general se requiere un enfoque de ciberseguridad centrada en el humano – *Human Centered Cybersecurity* o HCCS (Hilowle, Yeho, Grobler, Pye, & Jiang, 2023). Los factores principales del HCCS que contribuyen a la adopción de sistemas nacionales de identificación digital son la alfabetización digital y el entrenamiento en aspectos básicos de ciberseguridad. Además, deben existir controles políticos y sociales para evitar que estos sistemas sean usados para afectar derechos humanos y controlar poblaciones. Un ejemplo de esto es el sistema de créditos sociales que utiliza el Partido Comunista Chino sobre su población, una tergiversación de la aplicación de la identidad digital que fue lograda gracias al carácter no democrático de la sociedad china (Beck, 2024). Los gobiernos requieren dedicar recursos a la alfabetización digital con un matiz de diversidad cultural si esperan sacar el máximo provecho a las herramientas que hagan uso de la identidad digital (Hilowle, Yeho, Grobler, Pye, & Jiang, 2023), e incluir dentro de esa diversidad cultural un entendimiento claro de la filosofía política de la sociedad a la que pertenecen y sirven.

Otro gran desafío es el de la vulnerabilidad estatal al aplicar la identidad digital en sus modelos de gobernanza. Los países en desarrollo son particularmente vulnerables cuando se trata de la implementación de herramientas gubernamentales que usen identidad digital, pues la velocidad de implementación exigida los hace pasar por alto los riesgos asociados a ciberseguridad (Okunoye, 2022). Una violación de la ciberseguridad de una herramienta como una base de datos nacional centralizada de identidad digital representa un riesgo enorme.

El debate sobre el rol de la identidad digital sigue siendo álgido y no existe consenso académico. Aunque se reconoce que los programas de identidad digital fomentan el desarrollo nacional (Martin & Taylor, 2021) gracias a que evitan fraudes y facilitan la planeación, otros argumentan que estos programas pueden ser usados en contra de la población a través de una lógica de estado policial con vigilancia excesiva del Estado sobre la ciudadanía (Bennet & Lyon, 2021), facilitando la violación de derechos humanos.

Se recomienda que, para mitigar riesgos cibernéticos, las bases de datos de identidad digital deben ser descentralizadas y el entrenamiento en ciberseguridad básica debe aumentar a través de todos los niveles de empleados gubernamentales que tengan acceso a estas bases de datos (Okunoye, 2022).

Por último, existen también desafíos a los gobiernos por parte del sector privado. Uno en particular es el que López y Castañeda (2024) identifican como “transgresión de esfera”. Este fenómeno ocurre cuando el sector privado intenta forzar su ingreso a una “esfera” tradicionalmente del sector público, como lo es la identificación digital. La empresa multinacional IDEMIA, por ejemplo, ha logrado transgredir esta esfera al adentrarse en los procesos de la Registraduría Nacional del Estado Civil en Colombia desde la década de los 2000. Esto no solo ocurre con empresas contratistas para servicios de gobierno, sino también con empresas de seguridad que aprovechan las necesidades de los países en desarrollo para probar nuevos productos y conceptos (Arora, 2019).

En resumen, la identidad digital se ha convertido en la piedra angular de la gobernanza digital moderna gracias a los beneficios que trae en cuanto a seguridad, eficiencia y facilidad de acceso. Cuando los gobiernos aplican la identidad digital de manera efectiva logran apalancar muchas mejoras en su funcionamiento diario que repercuten positivamente en la ciudadanía. Las mejoras en entrega de servicios y promoción de inclusión social son las mas notorias. Sin embargo, es determinante para que se presenten estos éxitos que la aplicación de identidad digital se amarre a un nivel alto de ciberseguridad transversal a todos los campos de gobierno y de la sociedad en general. La identidad digital tiene enormes retos a la par con sus enormes beneficios, y los Estados deben enfrentar estos retos si quieren aplicar los modelos de gobernanza digital que sus ciudadanos claman. El Estado debe asumir un rol de líder en para enfrentar a estos retos, y debe hacerlo de la mano del sector privado para evitar transgresión de esfera en la que este último se aproveche de los sistemas de identidad digital para beneficio propio a costa del exceso de control sobre los ciudadanos.

Referencias

Arora, P. (2019). *The next billion users: Digital life beyond the West.* Harvard University Press.

Beck, D. (05 de marzo de 2024). *From Digital ID in Democracy to the Social Credit System.* Obtenido de Decentrale: Society, Politics, Technology: https://decentrale.fr/digital-id-in-democracy-to-the-social-credit-system/

Bennet, C., & Lyon, D. (2021). *Playing the Identity Card: Surveillance, Security and Identification in Global Perspective.* New York: Routledge.

Hilowle, M., Yeho, W., Grobler, M., Pye, G., & Jiang, F. (2023). Improving National Digital Identity Systems Usage: Human-Centric Cybersecurity Survey. *Journal of Computer Information Systems*, 1-15. Obtenido de https://doi.org/10.1080/08874417.2023.2251452

López, J., & Castañeda, J. (2024). 'A promising playground': IDEMIA and the digital ID infrastructuring in Colombia. *Information, Communication and Society*. Obtenido de https://doi.org/10.1080/1369118X.2024.2302995

Martin, A., & Taylor, L. (2021). Exclusion and Inclusion in Identification: Regulation, Displacement and Data Justice. *Information Technology and Development, 27*(1), 50-66.

NIST. (2017). *Digital Identity Guidelines - NIST Special Publication 800-63-3.*

Okunoye, B. (2022). Digital identity for development should keep pace with national cybersecurity capacity: Nigeria in focus. *Journal of Cyber Policy, 7*(1), 24-37. Obtenido de https://doi.org/10.1080/23738871.2022.2057865

Tapscott, D., & Tapscott, A. (2014). *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World.* Portfolio.