Gobernanza Digital

Serie Minutas Nº 42-23, 12/04/2023

por Marek Hoehn

Resumen

La presente Minuta busca apoyar la participación de la delegación parlamentaria chilena en el 7o encuentro de la Red de Parlamento Abierto de ParlAmericas "El futuro de la democracia en la era digital" en Santiago, Chile durante los días 20, 21 y 22 de abril de 2023.

En particular, este documento entrega antecedentes para la participación en la Sesión 3: "Acciones parlamentarias para una gobernanza digital íntegra e inclusiva"

Departamento de Estudios, Extensión y Publicaciones - Biblioteca del Congreso Nacional
eMail: mhoehn@bcn.cl, Anexo: 1868

Tabla de contenido

1. Antecedentes generales.....3

2. Tópicos centrales en el debate sobre la gobernanza digital.....4

2.1 interoperabilidad.....4

2.2 eID.....5

2.3 Digital signature.....5

2.4 Self-sovereign identities.....6

2.5 Verifiable credentials.....7

2.6 Zero knowledge proofs.....8

2.7 Privacy by design.....8

2.8 Blockchain.....9

1. Antecedentes generales

La gobernanza digital se refiere a la aplicación de la tecnología de la información y la comunicación (TIC) en la gestión y el gobierno de entidades y organizaciones. Se trata de un enfoque que busca mejorar la eficiencia y transparencia de los procesos gubernamentales a través del uso de herramientas y soluciones digitales, así como establecer estructuras y procesos que aseguren que la estrategia de gobierno digital se alinea con los objetivos públicos. La gobernanza digital también implica la integración de las TIC en la prestación de servicios públicos y en la participación ciudadana en la toma de decisiones.

La gobernanza digital "*es la articulación y concreción de políticas de interés público con los diversos actores involucrados (Estado, Sociedad Civil y Sector Privado), con la finalidad de alcanzar competencias y cooperación para crear valor público y la optimización de los recursos de los involucrados, mediante el uso de tecnologías digitales*". Asimismo define los alcances y contenidos, la política pública, marco normativo, el liderazgo, la infraestructura y soluciones comunes.

La Comisión Económica para América Latina y el Caribe (CEPAL) define los objetivos gobernanza digital como:

- Establecer las estructuras y procesos que aseguren que la estrategia de gobierno digital se alinea con los objetivos estratégicos de gobierno
- Articular y concretar políticas de interés público entre actores involucrados para crear valor público
- Que los riesgos y oportunidades sean adecuadamente administrados
- Optimizar los recursos disponibles a través del uso racional de las tecnologías digitales[1]

La Organización para la Cooperación y el Desarrollo Económicos (OCDE) recomienda aprovechar el valor de las tecnologías digitales para conseguir gobiernos más abiertos, participativos e innovadores:

- Utilización de la tecnología para mejorar la rendición de cuentas, la inclusión social y las asociaciones.
- Crear una cultura de los datos en el sector público.
- Garantizar un uso coherente de las tecnologías digitales en todos los ámbitos políticos y niveles de gobierno.
- Reforzar los vínculos entre el gobierno digital y las agendas de gobernanza pública más amplias.
- Reflejar un enfoque de gestión de riesgos para abordar las cuestiones de seguridad digital y privacidad.
- Desarrollar casos empresariales claros para sostener la financiación y el éxito de los proyectos de tecnologías digitales.
- Reforzar las capacidades institucionales para gestionar y supervisar la ejecución de los proyectos.
- Evaluar los activos existentes para orientar la adquisición de tecnologías

1 https://biblioguias.cepal.org/gobierno-digital/concepto-gobernanza

digitales.

- Revisar los marcos jurídicos y normativos para aprovechar las oportunidades digitales[2]

Asimismo, la OCDE aconseja a los tomadores de decisiones que busquen impulsar gobiernos eficaces y más abiertos, innovadores y participativos:

- Establecer objetivos estratégicos de gobierno digital, tomando medidas para abordar las "brechas digitales" existentes y la necesidad de evitar "nuevas exclusiones digitales"; así como la creación de una cultura impulsada por los datos que permita la apertura de datos para la transparencia, una mejor prestación de servicios y la participación pública.
- Garantizar el uso coherente de la tecnología en todos los ámbitos políticos y niveles de gobierno, estableciendo marcos organizativos y de gobernanza para una coordinación e integración efectivas de los esfuerzos para producir mejores resultados políticos y servicios.
- Reforzar las capacidades para apoyar una mejor aplicación de las estrategias de gobierno digital, adoptando casos empresariales claros para el uso de recursos en objetivos identificados, y deben supervisar los resultados. Deben crearse las capacidades necesarias, incluidos los marcos normativos y jurídicos, no sólo para aprovechar las nuevas oportunidades del gobierno digital, sino también para mitigar los riesgos asociados (como la seguridad y la privacidad).

2. Tópicos centrales en el debate sobre la gobernanza digital

2.1 Interoperabilidad

La interoperabilidad permite que distintos sistemas y dispositivos informáticos se conecten y comuniquen entre sí de forma estandarizada, lo que posibilita el intercambio y la puesta en común de datos e información.

En los sistemas de salud la interoperabilidad es especialmente relevante, ya que los pacientes pueden recibir atención de varios proveedores que trabajan en sistemas de salud diferentes, y tener acceso a información completa y precisa sobre el paciente puede mejorar la calidad de la atención y los resultados de los pacientes.

En otros sectores, la interoperabilidad también puede mejorar la eficiencia, la productividad y la innovación al permitir que los sistemas y procesos funcionen juntos a la perfección.

2 https://www.oecd.org/gov/digital-government/recommendation-on-digital-government-strategies.htm

2.2 eID

Una identificación electrónica ("eID") es una solución digital para autenticar la identidad de ciudadanos u organizaciones. Pueden utilizarse para ver para acceder a prestaciones o servicios proporcionados por las autoridades gubernamentales, bancos u otras empresas, para pagos móviles, etc. Además de la autenticación y el inicio de sesión en línea, muchos servicios de identidad electrónica también ofrecen a los usuarios la posibilidad de firmar documentos electrónicos con una firma digital.

Una forma de identificación electrónica es la tarjeta de identificación electrónica (eIC), que es una tarjeta de identidad física que puede utilizarse para la identificación o autenticación personal en línea y fuera de línea. La eIC es una tarjeta inteligente con el formato ID-1 de una tarjeta bancaria normal, con información de identidad impresa en la superficie (como datos personales y una fotografía) y en un microchip RFID incrustado, similar al de los pasaportes biométricos. El chip almacena la información impresa en la tarjeta (como el nombre y la fecha de nacimiento del titular) y la foto o fotos del titular. Pueden tomarse varias fotos desde distintos ángulos junto con distintas expresiones faciales, lo que permite a los sistemas de reconocimiento facial biométrico medir y analizar la estructura general, la forma y las proporciones del rostro. También puede almacenar las huellas dactilares del titular. La tarjeta puede utilizarse para la autenticación en línea, por ejemplo para verificar la edad o para aplicaciones de administración electrónica. También puede almacenarse en el chip una firma electrónica proporcionada por una empresa privada.

Según el Reglamento de la UE sobre identificación electrónica y servicios de confianza (eIDAS), descrito como un sistema paneuropeo de inicio de sesión, todas las organizaciones que presten servicios digitales públicos en un Estado miembro de la UE deberán aceptar la identificación electrónica de todos los Estados miembros de la UE a partir del 29 de septiembre de 2018.[3]

El documento de identidad estonio también se utiliza para autenticar el sistema de votación por Internet de Estonia. En febrero de 2007, Estonia fue el primer país en permitir el voto electrónico para las elecciones parlamentarias. Más de 30.000 votantes participaron en las elecciones electrónicas del país. A finales de 2014, Estonia amplió el DNI estonio a los no residentes. El objetivo del proyecto es llegar a 10 millones de residentes en 2025, es decir, 8 veces más que la población estonia de 1,3 millones de habitantes.

2.3 Digital signature

Una firma digital es una técnica criptográfica que garantiza la autenticidad e integridad de los mensajes o documentos digitales. Normalmente, las firmas digitales se utilizan para verificar que un mensaje o documento ha sido creado por un remitente conocido, así como para garantizar que no ha sido alterado en tránsito. Las firmas digitales se utilizan ampliamente en conjuntos de protocolos criptográficos, transacciones financieras, distribución de software y gestión de contratos.

3 https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en

Los esquemas de firma digital suelen constar de tres algoritmos: un algoritmo de generación de claves, un algoritmo de firma y un algoritmo de verificación. El algoritmo de generación de claves selecciona una clave privada al azar de entre un conjunto de posibles claves privadas. El algoritmo de firma utiliza la clave privada para generar la firma de un mensaje o documento determinado. El algoritmo de verificación toma como entrada un mensaje o documento, una firma y la clave pública correspondiente, y emite un resultado verdadero o falso en función de si la firma es válida o no.

Una de las principales ventajas de las firmas digitales es que proporcionan una capa de validación y seguridad a los mensajes enviados a través de un canal no seguro. Las firmas digitales correctamente implementadas dificultan que un tercero pueda falsificar una firma, lo que las hace más seguras que las firmas manuscritas tradicionales. Cuando se utilizan junto con otras medidas de seguridad, como el cifrado y el control de acceso, las firmas digitales pueden proporcionar un alto nivel de confianza en la autenticidad e integridad de las comunicaciones digitales.

Las firmas digitales tienen importancia jurídica en muchos países, como Canadá, Sudáfrica y la Unión Europea. En algunos casos, las firmas electrónicas que utilizan firmas digitales se consideran equivalentes a las firmas de tinta tradicionales. Sin embargo, es importante tener en cuenta que el estatus legal de las firmas electrónicas varía mucho en función de la jurisdicción.

El uso de firmas digitales puede presentar varios inconvenientes. Uno es que requieren un cierto nivel de conocimientos técnicos para aplicarse correctamente, lo que puede suponer un obstáculo para algunas organizaciones. Otro es que pueden ser vulnerables a ataques si la clave privada queda expuesta o si el algoritmo de firma es defectuoso. Por último, el uso de firmas digitales puede plantear problemas de privacidad y protección de datos.

A pesar de estos problemas, las firmas digitales siguen siendo una herramienta importante para garantizar la autenticidad, integridad y validez legal de las comunicaciones digitales. A medida que las organizaciones abandonan los documentos en papel con firmas de tinta, es probable que las firmas digitales adquieran aún más importancia en los próximos años.

2.4 Self-sovereign identities

Las identidades soberanas son un concepto revolucionario en el mundo de la gestión de identidades digitales. Este tipo de identidad permite a los individuos tener pleno control sobre sus propios datos personales, permitiéndoles decidir quién puede acceder a ellos y cómo se utilizan. Mediante el uso de identidades auto-soberanas, los usuarios pueden eliminar a terceros de la gestión de su información, protegiendo la privacidad y la seguridad de los usuarios, a la vez que proporcionan una mayor autonomía a los individuos cuando tratan con servicios en línea.

La tecnología en la que se basan las identidades soberanas se construye sobre la tecnología *blockchain*, que permite el almacenamiento seguro de los datos de los usuarios en libros de contabilidad distribuidos que no pueden ser alterados o manipulados por una sola entidad. Esto garantiza que todas las transacciones relacionadas con los datos personales de un individuo permanezcan privadas y seguras en todo momento, sin necesidad de confiar en ninguna parte en

particular, como gobiernos o corporaciones. Además, este sistema elimina la necesidad de múltiples contraseñas, ya que cada transacción sólo requiere una firma de una fuente de confianza, como una dirección de correo electrónico o un número de teléfono asociado a la cuenta del individuo, lo que simplifica mucho la autenticación frente a métodos tradicionales como las combinaciones de nombre de usuario y contraseña.

En general, las identidades soberanas ofrecen muchas ventajas tanto a las personas que buscan un mayor control sobre su propia información como a las organizaciones que desean mejorar las medidas de seguridad en torno a los procesos de gestión de datos de los clientes.

2.5 Verifiable credentials

Las credenciales verificables son documentos digitales que prueban la identidad y las cualificaciones de una persona. Se utilizan para autenticar la identidad de una persona con el fin de acceder a determinados servicios o productos, como la banca en línea o los historiales médicos. Las credenciales verificables ofrecen a organizaciones y particulares una forma segura de compartir información sin comprometer la privacidad o la seguridad.

El uso de credenciales verificables ha crecido significativamente en la última década debido a la creciente preocupación por la seguridad a la hora de compartir datos entre organizaciones y particulares. Verificar la identidad de una persona es ahora más importante que nunca, ya que ayuda a protegerse contra los estafadores que podrían robar información personal de víctimas desprevenidas. Además, el uso de credenciales verificables puede ayudar a reducir los costos asociados a los procesos de autenticación manual, ya que no requieren documentos físicos como tarjetas de identificación en papel o permisos de conducir a la hora de verificar la identidad de alguien electronicamente.

La tecnología de credenciales verificables también la utilizan muchas empresas hoy en día para la incorporación de empleados; en lugar de hacer que los empleados rellenen manualmente el papeleo en cada nuevo trabajo que aceptan, las empresas pueden verificar simplemente sus identidades a través de este proceso para ponerlos rápidamente en marcha en su primer día de trabajo. Esto ahorra tiempo y dinero, al tiempo que garantiza que se han completado todas las comprobaciones de antecedentes necesarias antes de contratar a alguien nuevo en la organización.

En conclusión, las credenciales verificables ofrecen numerosas ventajas tanto desde el punto de vista de la seguridad como desde la perspectiva de la disminución de costos, lo que las hace cada vez más populares entre las empresas grandes y pequeñas que buscan formas de agilizar las operaciones sin dejar de mantener seguros los datos de los clientes durante las transacciones realizadas en línea, lo que hace que sea más fácil que nunca garantizar la fiabilidad entre las partes implicadas en cualquier transacción que implique el intercambio de información confidencial.

2.6 Zero knowledge proofs

Las pruebas de conocimiento cero son un concepto importante en criptografía y seguridad. Permiten que dos partes interactúen sin que ninguna de ellas tenga que revelar información sensible sobre sí mismas o sus datos. En esencia, una prueba de conocimiento cero permite a una de las partes demostrar que sabe algo sin revelar realmente qué es lo que sabe. Esto puede ser útil para verificar la identidad de alguien en línea o garantizar que sólo los usuarios autorizados tienen acceso a determinados recursos.

Un ejemplo simple es la necesidad de verificar la mayoría de edad a la hora de comprar alcohol. El vendedor no necesita saber todos los datos que están en el carnet de identidad del comprador, ni la edad exacta. Solo debe comprobar que es mayor de edad.

El tipo más común de prueba de conocimiento cero se conoce como versión no interactiva, que no requiere ninguna interacción entre el *prover* y el verificador más allá del envío de mensajes de ida y vuelta a través de algún canal de comunicación como el correo electrónico o servicios de mensajería instantánea. Estos tipos de pruebas se basan en algoritmos matemáticos llamados "esquemas de compromiso" que crean *tokens* criptográficos únicos basados en la información introducida por el usuario, pero no revelan nada más hasta que el *token* ha sido verificado por ambas partes implicadas en el proceso de transacción, asegurándose de que ninguna de las partes pueda saber nada más de lo que se acordó originalmente durante la fase de configuración antes de que se produjera cualquier intercambio real.

En conclusión, las pruebas de conocimiento cero proporcionan una herramienta inestimable para el intercambio seguro de datos entre dos entidades, manteniendo todos los demás detalles privados entre sí - proporcionando fuertes garantías en torno a los procesos de autenticación, incluso cuando puede haber posibles actores maliciosos tratando de obtener acceso no autorizado en cada paso a lo largo del camino. No obstante, cabe señalar que, debido a su complejidad, la implementación de soluciones *zero knowledge proof* puede requerir conocimientos especializados, por lo que las organizaciones deben asegurarse de contar con el apoyo adecuado en caso necesario. Sin embargo, las ventajas generales superan con creces los costes asociados al proceso de implantación, lo que hace que merezca la pena tener en cuenta esta tecnología a la hora de proteger sus activos digitales frente a las ciberamenazas.

2.7 Privacy by design

La privacidad desde el diseño es un concepto que ha adquirido cada vez más importancia en la era de la tecnología digital. Se refiere a la idea de que, al desarrollar nuevos productos o servicios, la privacidad debe tenerse en cuenta desde el principio e integrarse en todas las fases de desarrollo. El objetivo es garantizar que la recopilación y el uso de datos sean transparentes y seguros, y respeten los derechos de los usuarios sobre su propia información personal. Este enfoque puede ayudar a proteger la privacidad de los usuarios y, al mismo tiempo, mejorar la confianza entre empresas y clientes, así como promover la innovación en las industrias impulsadas por la tecnología.

Un componente clave de la aplicación de la privacidad desde el diseño es asegurarse de que existan políticas claras sobre cómo se utilizarán los datos de los clientes antes incluso de recopilarlos, lo que incluye especificar qué tipo de datos se necesitarán para un servicio o producto concreto, de modo que los usuarios sepan exactamente a qué se comprometen cuando aceptan proporcionarlos.

Las empresas también deben esforzarse por reducir al mínimo la recopilación o retención innecesaria de información personal; recopilar sólo lo estrictamente necesario ayuda a reducir los riesgos potenciales asociados al almacenamiento de este tipo de material sensible en los servidores de la empresa (por ejemplo, la piratería informática). Además, las empresas deben adoptar medidas de seguridad adecuadas para evitar el acceso no autorizado; las tecnologías de encriptación también pueden ayudar en este sentido.

Por último, la comunicación efectiva sobre estas políticas debe ser periódica, tanto a nivel interno (para que los empleados lo entiendan) como externo (a través de la página web, los términos y condiciones, etc.). Los usuarios deben estar seguros de que no se hace un mal uso de su información privada si las empresas quieren que vuelvan una y otra vez. Tomando medidas proactivas como éstas, las empresas pueden construir relaciones sólidas con sus clientes basadas en la confianza mutua, lo que en última instancia conduce al éxito.

2.8 Blockchain

La tecnología blockchain tiene el potencial de revolucionar la administración pública. Aprovechando esta innovadora tecnología, los organismos gubernamentales pueden mejorar la eficiencia y la transparencia al tiempo que reducen costos. Blockchain es un sistema de contabilidad distribuida que registra las transacciones de forma inmutable, lo que permite una mayor rendición de cuentas en todos los niveles de la administración. Esto proporciona a los ciudadanos una mayor confianza en sus funcionarios electos y les permite exigir más fácilmente a esos líderes que rindan cuentas de sus acciones.

Un caso clave de uso de la tecnología blockchain en la administración pública es su capacidad para realizar un seguimiento seguro de los activos digitales a lo largo del tiempo sin necesidad de intermediarios ni bases de datos centralizadas. Por ejemplo, los gobiernos podrían utilizar la tecnología blockchain como parte de un sistema de registro de la propiedad que permitiría la transferencia segura de la propiedad entre las partes sin depender de documentos en papel u otros procesos manuales que son propensos a errores y fraudes debido al riesgo de corrupción asociado a la participación humana en cada paso a lo largo de la cadena del proceso. Además, permite un seguimiento más fácil al proporcionar actualizaciones en tiempo real sobre las transferencias de activos entre las personas u organizaciones involucradas en la transacción, lo que dificulta que cualquiera de las partes involucradas intente manipular los datos relacionados con estas transacciones.

Por último, blockchain también tiene aplicaciones en los sistemas de votación, donde los votos pueden seguirse de forma transparente en cada etapa, desde el registro hasta la presentación del voto en el proceso de recuento final. Los gobiernos ya han empezado a explorar formas de implementar este tipo de soluciones utilizando herramientas como los contratos inteligentes para que las identidades de los votantes permanezcan en el anonimato, pero puedan ser

verificadas por las autoridades si es necesario durante las auditorías posteriores para garantizar que no se produzcan actividades fraudulentas durante los ciclos electorales. Todas estas características hacen de blockchain la herramienta ideal para los gobiernos que quieren aumentar la transparencia, la precisión y la seguridad cuando se trata de información sensible relacionada con los asuntos públicos en general y ayuda a prevenir el mal uso de los fondos asignados a diversos proyectos bajo diferentes departamentos dentro de los órganos administrativos que operan a nivel local y estatal.