Guía de Identidad Digital para la Administración Tributaria

MINISTERIO DE ASUNTOS EXTERIORES, UNIÓN EUROPEA Y COOPERACIÓN
aecid
cooperación española

Guía de Identidad Digital para la Administración Tributaria

Guía de Identidad Digital para la Administración Tributaria

ISBN: 978-9962-722-96-0 (PDF)
ISBN: 978-9962-722-97-7 (ePub)

Citar así:
Centro Interamericano de Administraciones Tributarias (CIAT). (2026). *Guía de identidad digital para la administración tributaria.*

Autores

- Alejandra Carratú
- Jimena Hernández
- Juan Pablo García

Revisado por

Raul Zambrano
Fransheska López
Elizabeth Rodríguez

Contenido

Agradecimiento

Este trabajo ha sido posible gracias al valioso aporte de personas clave en diversas administraciones tributarias de la región. Expresamos nuestro especial agradecimiento a los equipos técnicos, directivos y corresponsales institucionales de las administraciones tributarias de Brasil, Chile, Costa Rica, Ecuador, España, Guatemala, Honduras, México, Panamá, Perú y Uruguay.

Agradecemos especialmente al equipo técnico del CIAT por su constante apoyo, acompañamiento metodológico y visión estratégica para guiarnos en esta investigación.

Introducción

En el marco del acuerdo de cooperación internacional entre la Agencia Española de Cooperación para el Desarrollo (AECID) y el Centro Interamericano de Administraciones Tributarias (CIAT), se busca proporcionar a los profesionales de las administraciones tributarias de América Latina capacitación especializada en la incorporación de la digitalización y nuevas tecnologías. En ese sentido, la elaboración de esta Guía tiene como propósito servir de referencia para las administraciones tributarias, especialmente las de América Latina, en la implementación y gestión de mecanismos de identidad digital, considerando las particularidades y necesidades específicas del sector tributario, tanto de la administración como de los contribuyentes.

La transformación digital de las administraciones tributarias requiere contar con marcos tecnológicos, normativos y operacionales que garanticen la eficiencia, transparencia y accesibilidad a los servicios digitales brindados. En este contexto, la identidad digital surge como un componente esencial para habilitar interacciones confiables y fluidas entre contribuyentes, organismos públicos y sistemas automatizados. Su relevancia radica en que permite identificar de forma **segura, única y remota** a ciudadanos, empresas y terceros que interactúan con la administración.

La identidad digital no es solamente un recurso tecnológico: es una **capacidad institucional habilitante.** Su adopción tiene carácter estratégico, dado que su correcta implementación permite transformar el vínculo con el contribuyente, mejorar la gestión tributaria y avanzar hacia modelos más inteligentes y centrados en las personas.

A continuación, se presentan algunos de sus beneficios más relevantes, que explican por qué constituye un componente estratégico en los procesos de modernización de las administraciones tributarias:

- **Facilita el acceso a servicios digitales tributarios:** la identidad digital es la puerta de entrada a trámites, declaraciones, pagos y consultas sin necesidad de presencia física.
- **Reduce costos y tiempos operativos:** al automatizar la verificación de identidad, disminuye la carga administrativa tanto para la administración tributaria como para el contribuyente.
- **Aumenta la certeza jurídica y la seguridad:** asegura que las interacciones digitales estén protegidas frente a suplantaciones y/o fraudes.

- **Mejora las condiciones para facilitar el cumplimiento de las obligaciones tributarias:** una experiencia digital más ágil y confiable promueve una relación más transparente entre el contribuyente y la administración.
- **Permite la interoperabilidad entre sistemas públicos:** una identidad digital estandarizada favorece el intercambio de datos con otras instituciones, mejora la trazabilidad, la integración de los servicios del Estado y el valor público ofrecido al ciudadano.

En relación con las recomendaciones internacionales, tanto la Organización para la Cooperación y el Desarrollo Económicos (OCDE) como el Banco Interamericano de Desarrollo (BID) reconocen la identidad digital como un componente clave en sus respectivos marcos estratégicos. El modelo de administración tributaria 3.0 (OCDE, 2020) incluye la identidad digital como uno de sus “componentes básicos”, al permitir la identificación segura, única e integrada de los contribuyentes. Por otro lado, en el modelo de madurez digital del BID (Banco Interamericano de Desarrollo, 2023), se la considera una capacidad transversal crítica que habilita servicios digitales centrados en el usuario.

Sin embargo, según el informe de la OCDE (2024), si bien se destaca que la mayoría de las administraciones tributarias ya ofrecen acceso digital autenticado, también se reconoce que el grado de avance varía significativamente entre jurisdicciones, lo que refleja asimetrías regionales en cuanto a capacidades tecnológicas, infraestructura y nivel de digitalización.

Dada la diversidad de realidades de los diferentes países de América Latina, esta Guía tiene como objetivo brindar un enfoque práctico sobre los aspectos estratégicos, técnicos y jurídicos vinculados a la identidad digital en contextos tributarios, utilizando un lenguaje sencillo y accesible.

En el Capítulo 1 se verán conceptos clave vinculados a la identidad e identificación digital, como su evolución hacia modelos más confiables, interoperables y alineados con buenas prácticas. Se identifican también los desafíos técnicos y normativos que deben abordarse para consolidar un ecosistema digital inclusivo, seguro y regionalmente integrado. Se abordan experiencias concretas que ilustran los avances en identificación transfronteriza y se reflexiona sobre el rol estratégico de las administraciones tributarias en impulsar esta transformación.

El Capítulo 2 contiene un relevamiento de la situación actual de la identidad digital en las administraciones tributarias en América Latina, teniendo en cuenta los aspectos normativos, tecnológicos y el grado de implementación y desarrollo en cada jurisdicción. Este relevamiento se realizó mediante una encuesta estructurada y una investigación complementaria en portales de gobierno digital, con el objetivo de comprender los desafíos y problemas que limitan el despliegue efectivo de servicios digitales en las diferentes administraciones y su relación con la identidad digital.

En el Capítulo 3, se analizan las tendencias de vanguardia y se realizan recomendaciones estratégicas para la evolución de la identificación digital en las administraciones tributarias, teniendo en cuenta los enfoques emergentes y las dinámicas actuales, pero reconociendo los diferentes puntos de partida existentes en los países. Asimismo, se profundiza en componentes clave como la autorización y la auditoría, pilares del modelo de Triple A, cuya implementación resulta esencial para garantizar trazabilidad, control y confianza en los esquemas de identidad digital.

La aspiración es que esta Guía sea una herramienta orientada a acompañar a las organizaciones que estén iniciando este proceso, al tiempo que apoye la consolidación de modelos ya existentes. Asimismo, pretende promover buenas prácticas y facilitar la toma de decisiones informadas en materia de política pública vinculada al tema, contribuyendo a fortalecer la transformación digital de las administraciones tributarias en la región.

1. Evolución y tendencias en la identificación digital

1.1. Identidad e identificación digital

Identidad digital

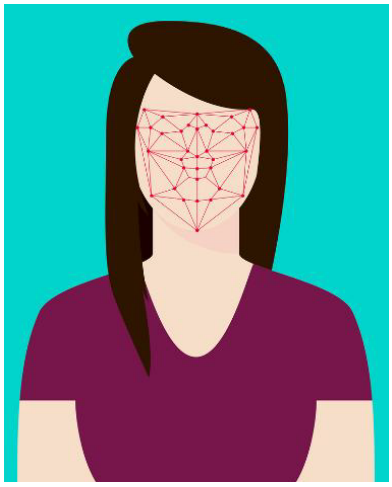
La **identidad digital** es la Información de una persona que existe en el mundo digital. Esa información se compone de datos de diversos tipos; pueden ser datos estructurados como nombres y apellidos, números identificatorios, pero también puede ser información relativa a sus costumbres o imágenes y videos, entre otros. Estos datos son generados por cada persona en base a información específica que se ingresa en diferentes sistemas, pero también información que algunas aplicaciones y dispositivos deducen sobre nosotros, como comportamientos, gustos, opiniones o formas de pensar, preferencias, lugares que visitamos, videos, incluso cada uno de los "me gusta" que registramos a través de **nuestras** interacciones en redes sociales. Mucha de esta información se genera sin que sepamos o, al menos, sin que seamos conscientes.

Todo este rastro de información sobre cada persona que va quedando en Internet se conoce como huella digital. No es el objetivo de esta publicación ahondar en este tema, pero es importante tenerlo en cuenta: la huella digital representa quiénes somos, qué nos gusta y qué no nos gusta, qué pensamos, nuestras costumbres, nuestras relaciones, nuestros intereses y valores. Es importante ser conscientes de este tema y conocer técnicas y herramientas para protegerla. La huella digital activa es la que vamos creando con nuestras acciones conscientes como publicar en redes sociales o llenar formularios electrónicos, entre otros. La pasiva es la que se va creando sin que seamos del todo conscientes, como las direcciones IPs que utilizamos, datos de geolocalización, tiempos de visita en páginas web, artículos o noticias que leemos, entre otros.

La identidad se compone de muchos y variados tipos de datos que son parte de nuestra huella y pueden ser utilizados para diferentes fines, por su propio dueño (persona) o por un tercero (algoritmo, software, persona u organización). Algunos buscadores la utilizan para personalizar las búsquedas del usuario o para ofrecer

publicidad en forma personalizada. Entre la información que compone la identidad digital de una persona, están los datos personales como nombres, números de documentos, fecha de nacimiento, dirección, correo electrónico, credenciales, documentos personales, etc.

Por otro lado, haciendo un abordaje del tema desde un punto de vista más filosófico, se puede concluir que, en el mundo digital, nuestra identidad ya no depende solo de nuestra corporalidad o de estar presentes físicamente. Como se ha visto, se va formando a partir de la información que compartimos en internet, cómo interactuamos en redes y los perfiles que armamos. Cada acción, cada preferencia manifestada, cada vínculo generado contribuye a delinear una versión de nosotros mismos que existe y evoluciona en el ecosistema informático. Con esa perspectiva, la identidad digital no es tan sólo un montón de datos: es una forma de mostrar quiénes somos en esta era marcada por la información.



Identificación digital (Autenticación)

La identificación digital es el proceso mediante el cual una persona, entidad, software u objeto es reconocido y validado por otro (persona, entidad, software u objeto) en un entorno digital. En el mundo físico, para que nos reconozcan, nos presentamos mostrando un documento de identificación (DNI, cédula de identidad, pasaporte, etc.) y la verificación de nuestra identidad se produce en forma implícita, ya que estamos presentes. En cambio, en el mundo digital, una persona se debe identificar utilizando datos vinculados a su identidad digital -como nombre de usuario, número de documento o credenciales- y además debe brindar pruebas que demuestren que la persona es efectivamente quien dice ser, ya que no hay presencia física para poder verificarlo. Ese proceso que permite identificarse y verificar la identificación, en términos técnicos, se conoce como el proceso de autenticación.

A su vez, en el mundo digital, cuando dos sistemas informáticos interoperan, es necesario que también se identifiquen digitalmente para asegurar el correcto tratamiento de los datos y reducir riesgos relativos a la filtración de información o al acceso no debido a información.

Fundamentos operativos de la identidad digital

Tras revisar distintas aproximaciones al concepto de identidad digital e identificación digital, es importante establecer que, en el contexto de esta publicación, se adoptará una definición de identidad digital centrada en su rol como mecanismo de identificación y en forma equivalente. En este sentido, se entiende la *Identidad*

Digital como el conjunto de atributos y credenciales que permiten reconocer de forma segura y única a los ciudadanos en su interacción con servicios digitales, funcionando como una herramienta para validar que quien accede a un servicio en línea es efectivamente quien afirma ser.

La identidad es utilizada para validar, utilizando diferentes técnicas o tecnologías, a una persona o entidad durante el proceso de identificación digital.

La triple A (Autenticación, Autorización, Auditoría)

En el contexto de la ciberseguridad, la Autenticación, Autorización y Auditoría son conocidas con el acrónimo de la triple A y son conceptos importantes que están asociados y determinados por la identificación digital. Es crucial la importancia y confianza en la identificación para determinar la autorización y luego realizar en forma correcta la auditoría.

Dependiendo de cómo sea implementada, la autenticación y autorización, sobre todo en sistemas informáticos bajo estándares y modelos obsoletos, muchas veces son vistas como un único tema, pero en la actualidad no es así. Tal como se comentará más adelante, cada vez hay más separación entre la Autenticación y la Autorización, dado que, a partir del surgimiento de sistemas o ecosistemas de identificación digital, donde las personas utilizan una identificación digital en múltiples servicios digitales, es necesario que cada servicio se concentre en desarrollar un correcto esquema de autorización y gestión de roles.

A su vez, en un mundo donde las amenazas cibernéticas se han disparado exponencialmente, la auditoría pasa a ser un elemento clave para la confianza en los sistemas informáticos. Una correcta implementación de auditoría, sobre un sistema que gestiona información permite determinar qué sucedió, en qué momento sucedió, quiénes fueron los actores involucrados (qué hizo cada actor) y desde dónde actuaron, entre otros. Todos estos elementos permiten reconstruir los hechos y, con esto, la integridad de la información, y también permiten contar con información confiable como evidencia ante actos delictivos.

Si bien el foco de este trabajo está en la identificación digital (Autenticación) en las administraciones tributarias, a continuación, se define Autorización y Auditoría:

- **Autorización:** una vez que la persona es autenticada por el sistema, el mismo le autoriza a acceder a determinada información y realizar determinadas acciones. Este proceso depende del perfil del usuario, así como de la confianza en los métodos de autenticación que utilizó, pero también de las reglas específicas del sistema. No es parte del alcance de esta Guía introducir este tema en detalle, pero es importante tenerlo en cuenta dado que la autorización depende, antes que nada, de la

identificación digital. Tal como se comentará más adelante, en sistemas donde la autenticación se resuelve en otro ámbito, es necesario que el proceso de autorización siga siendo resuelto por el propio sistema.

- **Auditoría:** es el seguimiento y registro de todas las acciones que cada usuario realiza sobre un sistema. Es un aspecto importante en la actualidad por múltiples factores, como la posibilidad de poder determinar qué sucedió ante un incidente y contestar preguntas como cuáles usuarios accedieron y/o modificaron qué información, entre otros.

En el capítulo 3 se profundizará en estos dos temas dado que, según las tendencias actuales, son aspectos que van a ser cada vez más relevantes en las administraciones tributarias.

1.2. Evolución de la identificación digital

Los inicios de la identificación digital

Durante la década de los 70, con el surgimiento de los primeros sistemas informáticos, la identificación digital se reducía a un código único que el usuario ingresaba en un sistema para identificarse y así acceder a su información y a las operaciones que el sistema le disponía en función de su perfil. Este código cumplía ambas funciones: identificaba a la persona y a la vez validaba su identificación, por lo que era considerado un secreto entre el sistema y la persona. Generalmente se creaba en el sistema y se le informaba al usuario, en un mundo totalmente diferente al actual.

Identificación digital clásica

Poco tiempo después, se fueron desarrollando sistemas que separaban a la entidad “usuario” (identificador) de la verificación y con esto surgió el concepto de **autenticación**. El acto de autenticarse, también conocido como “*login*” (por su nombre en inglés, log-in), es el proceso de identificarse y verificar la identificación.
En este escenario, una persona ingresa un dato que lo identifica unívocamente en el sistema, por ejemplo, el número de identificación nacional, un “usuario” único o un correo electrónico, y a continuación debe verificar su identificación, de modo que la otra parte (el sistema informático) compruebe que la persona es efectivamente quien se identificó. Para validar la identificación, debe utilizar algún factor predefinido entre el sistema y el usuario. Estos factores pueden ser de tres tipos:

- Algo que sé: algo que solo el sistema informático y la persona saben, es decir, un secreto compartido como una contraseña o un pin.

- Algo que tengo: algo que tiene el usuario y el sistema informático sabe que solamente esa persona lo tiene. Esto puede ser, por ejemplo, una coordenada, un número único o código de un solo uso (One Time Password -OTP-, por sus siglas en inglés).
- Algo que soy: en este punto entran en juego las tecnologías biométricas que obtienen información como la huella dactilar, el iris o el reconocimiento facial.

Hace unas décadas, muchos sistemas daban a elegir al usuario identificador, por lo que la persona debía ingresar una palabra que lo identificara, siempre y cuando esa palabra no hubiese sido elegida por otra persona previamente. Esa palabra era única en ese sistema, de modo que permitía identificar unívocamente a la persona en el sistema. Desde principios de este siglo, esto comenzó a evolucionar hacia identificadores más universales, como, por ejemplo, direcciones de correo. Una dirección de correo, según su estándar RFC 5322 (Resnick, 2008), se compone de un nombre de usuario, el símbolo especial arroba (@), subdominio (opcional), dominio y extensión del servidor de correo (ejemplo: juan.perez@gmail.com, juan_perez@correo.universidad.edu.pa, etc.).

Nótese que una dirección de correo electrónico es un identificador universal. También es universal un identificador compuesto por un código de país, un tipo de documento y un número de documento (ejemplo: Uruguay – Cédula de Identidad – Número de cédula de identidad). Esta tendencia a utilizar identificadores universales, o al menos más amplios, se profundizó a partir de los primeros años del presente siglo. Este enfoque se desarrollará en profundidad más adelante.

Este sistema de autenticación basado en un identificador y un método para validar la identificación ha debido evolucionar fortaleciendo diversos aspectos, dada la evolución de la tecnología, la masificación de Internet, el incremento de la capacidad de cómputo y los riesgos que todos estos avances implican desde el punto de vista de la ciberseguridad y, en particular, de la suplantación de identidad.

Una de las primeras acciones para fortalecerlo fue el surgimiento de “políticas de contraseña” que, mediante una correcta implementación en los diferentes sistemas, aseguran que las personas elijan contraseñas fuertes. Esto es una combinación de caracteres lo suficientemente larga y compleja de modo que, desde una perspectiva estadística, a un sistema le tomaría décadas descifrarla mediante técnicas de fuerza bruta o utilizando diccionarios de posibles combinaciones de textos.

Las políticas también se fueron haciendo más complejas debido al nivel de riesgo creciente con respecto a la ciberseguridad, exigiendo que las contraseñas sean cambiadas periódicamente y no permitiendo utilizar contraseñas anteriores. Además, las buenas prácticas y recomendaciones aconsejan que se elijan contraseñas diferentes para todos los sistemas que se utilizan.

También se comenzaron a tomar otras precauciones a nivel de seguridad y, en particular, sobre cómo guardar las contraseñas de los usuarios en las bases de datos. Desde hace muchos años las buenas prácticas indican que las contraseñas no se deben guardar en texto plano, porque si un tercero no autorizado accede a esa base de datos podría acceder a las credenciales de los usuarios en forma muy simple. La práctica más recomendada y utilizada se basa en el uso de criptografía, específicamente funciones matemáticas *hash* que transforman la contraseña en una secuencia irreconocible e irreversible.

No es el objetivo de esta Guía profundizar en este tema, pero sí destacar que, desde hace décadas, el almacenamiento de las contraseñas en texto plano se considera una vulnerabilidad importante. Si un atacante logra extraer una base de datos con credenciales de usuarios, por más que estén cifradas, existe el riesgo de un ataque de fuerza bruta que intente descifrar las contraseñas. Este es uno de los motivos para que las políticas de contraseña exijan *contraseñas fuertes* y la necesidad de cambiarlas periódicamente.

Sin embargo, ese escenario —con contraseñas cifradas y fuertes— ya no es suficiente por sí solo. En los últimos años, se han intensificado y sofisticado los métodos de ataque, como el *phishing* o el uso de *malware* diseñado para interceptar la actividad del usuario. Por ejemplo, los *keyloggers*, capaces de registrar cada pulsación del teclado, permiten capturar contraseñas aún antes de que lleguen al sistema y sean cifradas. Ante este panorama, la fortaleza de la contraseña sigue siendo necesaria, pero no suficiente y se requieren mecanismos adicionales.

Sistemas con Múltiples Factores de Autenticación (MFA)

La implementación de Múltiples Factores de Autenticación se convirtió en una de las estrategias más efectivas para reducir riesgos, especialmente en entornos donde la información sensible, como la financiera o tributaria, requiere altos niveles de protección. Fue así como comenzaron a surgir sistemas que utilizan dos factores de autenticación (2FA).

Estos mecanismos funcionan de la siguiente manera: una vez identificada la persona (usuario), hay que utilizar “algo que sé” y a continuación “algo que tengo” o “algo que soy”. Una combinación muy adoptada es una contraseña fuerte (algo que sé) y un código de un único uso OTP (*one time password,* algo que tengo). Un OTP es un código, generalmente de 6 números, que se genera con un algoritmo matemático que tiene la propiedad de ser impredecible. Esto hace que no sea posible saber cuál será el siguiente código, de modo que, si el usuario ingresa el código correcto, se valida la identificación.

Un OTP se puede gestionar de tres formas:

- Luego que el usuario ingresa la contraseña, en caso de ser correcta, el sistema genera el código y se lo envía al usuario por otro medio previamente acordado, por ejemplo, a través de SMS o WhatsApp al dispositivo móvil o al correo electrónico del usuario. Para esto es necesario contar con un dispositivo con carga, conectividad y/o acceso al correo electrónico.
- El usuario se descarga una aplicación móvil para este fin como Google *Authenticator* o Microsoft *Authenticator* y lo sincroniza previamente con el sistema. Esto hace que ambos utilicen el mismo algoritmo matemático, los mismos tiempos y comiencen a generar números a partir de la misma semilla, por lo que, en todo momento, ambos deberían tener válidos los mismos OTPs. Para esto es necesario contar con el dispositivo móvil a la hora de identificarse digitalmente.
- La organización responsable del sistema le entrega un token físico al usuario. Esto es un hardware que posee el algoritmo matemático configurado, tal cual sucede con el caso de la aplicación móvil y además una pequeña pantalla donde le va mostrando al usuario el número generado. En este caso es necesario entregarle el dispositivo presencialmente al usuario (o de una forma segura), además el usuario debe contar con el dispositivo cuando desee Identificarse digitalmente.

Para los últimos dos casos, existe un estándar internacional muy utilizado llamado *Time-based One-Time Password* (TOTP) que es una contraseña de un solo uso basado en el tiempo, definido por *Internet Engineering Task Force* (IETF). Para que funcione correctamente, además de definir una semilla en común, es necesario que los relojes de los dos dispositivos -teléfono o token y servidor- estén sincronizados (M'Raihi, Machani, Pei, & Rydell, 2011).

Hay algunas diferencias significativas en materia de seguridad a la hora de implementar un mecanismo de OTP. Un envío de OTP mediante SMS es más vulnerable que mediante WhatsApp ya que el canal utilizado por mensajes SMS es más inseguro. A su vez, la generación sincronizada de OTP mediante una aplicación de autenticación o un token, especialmente si no está vinculado al teléfono móvil, es más seguro que cualquier envío (aunque sea por WhatsApp o correo). En este caso, el código no se transmite por ningún canal, sino que se genera en forma simultánea en el dispositivo del usuario y en el sistema de verificación, reduciendo el riesgo de interceptación.

Según las buenas prácticas y recomendaciones, cada OTP debería durar entre 30 y 60 segundos, pero para sistemas críticos con información muy sensible se podría reducir a 20 segundos esa duración, para mayor seguridad. También generalmente se permite una cantidad de intentos limitados, luego de cierto número de intentos fallidos, el mecanismo de OTP deja de ser válido o el sistema directamente bloquea al usuario. Para

aplicaciones móviles o web, donde es necesario conectarse mediante Internet, generalmente se permiten tiempos un poco más extensos debido a la posible latencia en las conexiones.

En todos los casos, existen algunas desventajas y limitaciones. Para el envío del código al dispositivo móvil, existen costos asociados a mensajería que en servicios masivos representan gastos considerables. El OTP generado en una aplicación móvil muchas veces no es una herramienta simple de utilizar para usuarios poco experimentados y en el caso del OTP por hardware es necesario entregarle el dispositivo al usuario personalmente (o de una forma segura), lo cual genera costos logísticos y operativos, y el usuario debe tenerlo consigo siempre que precise identificarse digitalmente.

También es posible utilizar factores biométricos, es decir, “algo que soy”. Hoy en día todos los dispositivos móviles tienen cámaras y posibilidades de tomarle una foto al usuario, algunos además cuentan con lectores de huella. En el caso de las fotos, es necesario que el sistema también implemente una herramienta conocida como prueba de vida. Se trata de un software que toma un video o secuencia de imágenes, para luego analizarla con Inteligencia Artificial y así asegurarse que la imagen obtenida pertenece a una persona viva y no a un mero registro fotográfico previo. En caso de que esta condición se cumpla, se debe comparar biométricamente la fotografía tomada a la persona con otra fotografía disponible en el sistema, previamente cargada. Si bien existen variantes en este tema, se trata de una forma útil pero que genera importantes costos para todo el sistema y exige que el usuario posea dispositivos con cámaras y un lugar adecuado en términos de iluminación, posición, saturación, etc. para tomar las imágenes.

En la actualidad, el uso de identificaciones digitales con contraseñas robustas y mecanismos de autenticación multifactor se ha vuelto imprescindible, no obstante, estos métodos presentan vulnerabilidades. Lamentablemente, en la última década, la evolución de las amenazas cibernéticas ha sido vertiginosa. Actualmente existen múltiples variantes de métodos de *phishing* – como *smishing* (mediante SMS), *vishing* (por voz), *quishing* (a través de QR fraudulentos) – que, combinados con herramientas de Inteligencia Artificial, ingeniería social avanzada, algunas técnicas de ataques sofisticados o algunos tipos de *malwares*, han debilitado la confiabilidad del esquema de autenticación de dos factores (2FA).

En los últimos años se comenzó a hablar de Múltiples Factores de Autenticación (MFA). Esto significa agregar más factores, combinando “algo que sé” con “algo que tengo” y “algo que soy”. La siguiente imagen muestra el concepto de 2FA y MFA:

Figura 1. 2FA y MFA.

***Fuente**:* elaboración propia

Si bien esta tendencia en MFA ayuda a proteger las identificaciones digitales, continúan siendo acciones para fortalecer un mecanismo diseñado hace varias décadas atrás, en una realidad totalmente diferente. Utilizar múltiples factores generan grandes costos, dificultan la usabilidad en forma considerable y no aseguran la suplantación de identidad.

Bajo este modelo de identificación digital tradicional, las recomendaciones sugieren que se tengan diferentes y complejas contraseñas en cada uno de los sistemas, que se cambien periódicamente y además se utilicen en todos los casos otros métodos de autenticación que requieren contar con un dispositivo físico específico y/o con un teléfono móvil y una aplicación previamente configurada. Aunque bien intencionadas, todas estas recomendaciones, no son infalibles, y, además, hacen que sea extremadamente complejo para las personas gestionar sus identificaciones digitales, lo que de por sí, introduce posibles vulnerabilidades (muchas veces "humanas"), que termina implicando un aumento de riesgos. Además de costos considerables.

Estos métodos, basados históricamente en el binomio usuario – contraseña y luego reforzados con diversas acciones adicionales están llegando al fin de su vida útil. Con el objetivo de cubrir esta necesidad, desde hace unos años, se comenzó a promover nuevos métodos y tecnologías de identificación digital, así como el concepto de "Autenticación Continua", que busca repensar la seguridad digital.

Passwordless

Otro concepto claro en la evolución y principales recomendaciones en la identificación digital es el de *passwordless* (autenticación sin contraseña). Se trata de un enfoque de seguridad en que un usuario puede identificarse digitalmente (autenticarse) sin necesidad de recordar, ingresar o gestionar contraseñas. Tal como se vio anteriormente, los métodos basados en contraseña para verificar una identidad fueron diseñados en un mundo totalmente diferente al actual. Tener que administrar a diario múltiples contraseñas seguras y distintas para cada sistema, además de actualizarlas periódicamente, representa una tarea compleja y poco trivial para la mayoría de las personas. Esta situación ya de por sí, trae riesgos y dificultades.

En lugar de usar "algo que sé", como se describió anteriormente, este enfoque promueve utilizar factores más seguros y fáciles como:

- Algo que tengo: un dispositivo (celular, token criptográfico, llave física también conocida como *passkeys*) o llaves criptográficas también conocidas como FIDO2 (*Fast IDentity Online*).
- Algo que soy: biometría facial, huella o iris.

En este caso, las credenciales para verificar la identidad están en poder del usuario, pero, además, en el caso de un dispositivo o llaves criptográficas, utilizan la firma digital como medio para la verificación de la identificación y la clave privada reside en un dispositivo criptográfico en forma protegida y segura. Se profundizará en estos métodos basados en firma digital en el punto "*3.1 Tendencias en Identificación Digital*" en el capítulo 3. En este mismo capítulo, también se presentan en modo resumido los modelos más relevantes en identificación digital en el mundo y en todos los casos, se destaca este tema como los métodos más fuertes y confiables de identificación digital.

Autenticación continua

La autenticación continua es un enfoque de seguridad en el cual se verifica continuamente la identidad del usuario de forma dinámica y transparente, mientras el usuario interactúa con el sistema, en lugar de hacerlo únicamente al iniciar la sesión.

Para esto, se implementan una serie de acciones y controles que revisan constantemente la actividad del usuario para poder detectar posibles anomalías o intentos de fraude. Es decir, el sistema ajusta el nivel de autenticación requerido dependiendo del perfil de riesgo de cada acción realizada. Además, puede tomar acciones como solicitar nuevamente la identificación digital, o enviarle un OTP a algún dispositivo o correo electrónico.

Algunos de los tipos de controles que se implementan bajo este enfoque son:

- **Datos biométricos:** incluyen elementos como el patrón de movimiento del *mouse* o el ritmo de tipeo en el teclado. Las personas tienden a tener patrones que el sistema va aprendiendo a medida que se utiliza y de esta forma puede detectar comportamientos anómalos. Otro factor biométrico utilizado, siempre que esté explicitado en los "términos de uso" y aceptado por el usuario, es el acceso a la cámara del dispositivo en forma continua o intermitente, para llevar a cabo un reconocimiento facial, buscando reforzar la validación de la identidad en tiempo real.
- **Datos del comportamiento**: de forma similar al mecanismo de control anterior, pero referido a patrones de uso, navegación, velocidad de lectura, tiempo de uso, horarios, días en la semana, etc.
- **Datos del entorno:** incluye datos relativos a la ubicación geográfica (obtenida a través de GPS y/o dirección IP), las redes utilizadas, el tipo de dispositivo utilizado, etc. Con respecto al dispositivo, las personas tienden a utilizar generalmente siempre los mismos equipos, como notebook, teléfonos móviles o tabletas. El sistema puede registrar una huella que los identifique y asociarlos a su usuario, de modo que, cada vez que el usuario utilice sus dispositivos frecuentes, el nivel de riesgo puede ser considerado menor.

Una correcta gestión de riesgos debe ser la base para abordar mecanismos de autenticación continua. Todos los controles que se implementan van generando un nivel de riesgo dinámico en cada sesión de trabajo que debe ser considerada por la criticidad de la información y las acciones que el usuario está realizando. Además, este enfoque requiere una etapa de aprendizaje y entrenamiento ya que mucha información es generada con el uso histórico del propio usuario. Las herramientas basadas en el uso de Inteligencia Artificial son muy útiles para sacar mejor provecho de la información e ir mejorando la eficiencia en la autenticación continua.

La autenticación continua representa una línea estratégica de evolución para los sistemas informáticos hoy en día y su adopción debe enmarcarse bajo una filosofía de mejora continua.

Principales referencias y niveles de seguridad en la identificación digital

En la actualidad, existen tres grandes marcos en identificación digital que se utilizan como referencia en lo que tiene que ver con los niveles de seguridad:

- **ISO/IEC 29115, Marco de Aseguramiento de Autenticación de Entidades:** norma internacional que establece cuatro niveles de aseguramiento para la autenticación (*International Organization for Standardization*, 2013).
- **eIDAS, Identificación Electrónica y Servicios de Confianza:** marco normativo de la Unión Europea donde la identificación digital está enmarcada dentro de un grupo de servicios de confianza con fuerte foco en la interoperabilidad. eIDAS incorpora conceptos de la ISO/IEC 29115, pero no se basa formalmente en esta norma (Unión Europea, 2014).
- **Directrices del Instituto Nacional de Estándares y Tecnología de los Estados Unidos (NIST):** pautas y recomendaciones emitidos por el NIST, agencia del Departamento de Comercio de los Estados Unidos, que definen los requerimientos que deben cumplir las agencias federales estadounidenses en sus sistemas de identificación digital (*National Institute of Standards and Technology*, 2017).

La siguiente tabla muestra una comparación en alto nivel con los principales temas referente a la identificación digital de cada estándar:

ISO/IEC 29115	eIDAS	NIST SP 800-63-3
Nivel 1 – IAL1: Baja o confianza nula sobre la identidad. Métodos de autenticación sencillos como nombre de usuario/contraseña. **Nivel 2 – IAL2:** Poca confianza sobre la identidad basado en documentos oficiales y controles básicos. Dos factores de autenticación (contraseña fuerte y OTP o app). **Nivel 3 – IAL3:** Alta confianza sobre la identidad, verificación basada en documentos oficiales y biometría fuerte. Métodos de autenticación multifactorial (contraseña + token físico, criptografía o FIDO2). **Nivel 4 – IAL4:** Muy alta confianza sobre la identidad, verificada presencialmente con múltiples elementos. Métodos de autenticación multifactorial robustos con dispositivos criptográficos (hardware) con controles cruzados con fuentes fiables.	**Nivel 1 _ Bajo:** Mínima confianza sobre la identidad. Datos autodeclarados con verificaciones simples. Autenticación simple (usuario / contraseña) con segundo factor opcional. **Nivel 2 – Sustancial:** Confianza elevada, verificación mediante documentos oficiales y/o biometría. Al menos un segundo factor de autenticación. Procedimientos formales de revocación, auditorías, monitoreo, etc. **Nivel 3 – Alto:** Confianza muy alta, verificación presencial o biométrica con pruebas de vida. Autenticación con chips criptográficos según FIDO2.	**Verificación de la ID:** **IAL1:** Autodeclarada, no hay verificación de la identidad. **IAL2:** Remota o presencial en base a documentos oficiales y controles automáticos con biometría. **IAL3:** Verificación presencial con controles físicos y biometría fuerte. **Autenticación:** **AAL1:** Factor único. **AAL2:** Dos factores de autenticación distintos y fuertes. **AAL3:** Autenticación con hardware criptográfico, protección y múltiples factores.

Los tres casos presentan leves diferencias, pero coinciden en los temas más críticos como son la necesidad de uso de biometría fuerte y documentos oficiales para la verificación de la identidad y métodos de autenticación basados en hardware criptográfico (firma digital) descentralizados.

Equivalencias normativas

En el mismo sentido que se crean marcos técnicos para la estandarización de la identificación digital y sus niveles de seguridad, también se han incorporado marcos normativos que buscan brindar seguridad jurídica a las transacciones que se realizan en el mundo digital y parten de un proceso de identificación.

La seguridad jurídica en entornos digitales comprende todo aquello que contribuye al logro de la seguridad, como las herramientas o instrumentos específicamente tecnológicos o digitales sumados factores o elementos normativos e institucionales que las respalden.

Cuando se habla de estos instrumentos hay dos conceptos sumamente relevantes que constituyen la base para la construcción del marco normativo antes mencionado como lo son el principio de equivalencia funcional y el reconocimiento de la validez legal y la admisibilidad probatoria de los instrumentos de identificación digital.

Respecto al principio de **equivalencia funcional**, refiere a que se necesitan en el mundo electrónico, en el ciberespacio, elementos que presten la misma función que en el mundo material, en el mundo tangible. El ejemplo por excelencia ha sido la consagración del documento electrónico como equivalente funcional del documento papel y la firma electrónica frente a la firma hológrafa. No se trata de la misma cosa, sino de “algo” que tiene la misma funcionalidad. Este mismo criterio se puede tomar para realizar la equivalencia entre la identificación presencial y la digital.

En la misma línea de lo mencionado en el apartado anterior, y tomando como base el principio de equivalencia funcional se deben introducir algunas ideas respecto a la **admisibilidad** y **valor probatorio** de los soportes digitales. En este caso, para hacer referencia a la necesidad de establecer la validez de las identificaciones digitales como elemento esencial para reconocer la validez de los actos que derivarán de esos procesos.

Un marco normativo sobre identificación digital debe establecer las bases legales, técnicas y operativas para garantizar que los sistemas de identificación electrónica sean seguros, interoperables, confiables y respetuosos de los derechos de las personas.

Algunos aspectos clave que deberían contener estos marcos normativos son:

- **Definiciones clave:** muchas veces cuando se dictan normas en temas tecnológicos es necesario establecer el alcance de algunos de los términos técnicos que se utilizan para facilitar su aplicación e interpretación. Es importante definir, por ejemplo: identidad digital, niveles de registro y autenticación, firma electrónica, proveedor de servicios de identificación digital.
- **Alcance del marco normativo o ámbito de aplicación subjetivo**: personas físicas o naturales, jurídicas, nacionales o extranjeras, sector público y/o privado.
- **Principios rectores**: la equivalencia funcional, la seguridad, la confidencialidad y protección de datos personales, interoperabilidad, compatibilidad internacional, neutralidad o no discriminación tecnológica, entre otros.
- **Niveles de seguridad de la identificación:** basado en estándares y según el riesgo asociado a la transacción. Asimismo, podrían incluirse los requisitos técnicos mínimos por nivel (por ejemplo, autenticación de doble factor para nivel alto), así como los tipos de medios de identificación aceptados (por ejemplo, biometría, certificados digitales, credenciales móviles).
- **Interoperabilidad y estándares técnicos:** adopción de estándares nacionales e internacionales.
- **Marco institucional y roles:** autoridad supervisora y reguladora. Responsabilidades de los proveedores de servicios de identificación y autenticación. Obligaciones de los organismos públicos y privados que implementan o consumen servicios de identificación digital. Régimen de infracciones por mal uso, negligencia, filtraciones, fraude, suplantación de identidad.
- Mecanismos de **auditoría, control y supervisión** de los datos usados para identificación.
- **Reconocimiento legal de medios de identificación digital:** equivalencia jurídica con la identidad física. En caso de corresponder se puede definir expresamente la validez de la identidad digital en procesos administrativos, notariales, financieros, etc.
- Mecanismos de reconocimiento **transfronterizo** de sistemas de identidad digital.

La construcción de estos marcos normativos resulta fundamental para cualquier servicio de confianza digital ya que no solo representan una solución tecnológica, sino una transformación profunda de cómo se construye la seguridad jurídica, la autenticidad y la prueba en el entorno digital. Su construcción y consolidación requiere un enfoque multidimensional: jurídico, técnico e institucional.

Actualidad de la identificación digital

En el presente, se está en una etapa de transición, donde métodos que fueron utilizados y reforzados durante décadas están llegando al final de su vida, más allá de que los tipos de factores de autenticación (algo que sé, algo que soy, algo que tengo) siguen vigentes. Las amenazas y las tecnologías evolucionan muy rápido, por lo que la identificación digital debe evolucionar para que los métodos sigan siendo seguros y fáciles de utilizar.

La transformación digital y el amplio y masivo uso de las TIC introdujo múltiples oportunidades, pero, a la vez, nuevos y desafiantes riesgos. Las amenazas relativas a la seguridad de la información han experimentado un aumento drástico durante la última década y, seguramente esta tendencia no se va a detener en el futuro.

Existen múltiples estudios de organizaciones reconocidas al respecto, a modo de ejemplo, el Foro Económico Mundial en su Reporte de Riesgos Globales 2025, destaca a la ciberseguridad como un componente imprescindible de la resiliencia nacional y corporativa. Específicamente, el *Global Cybersecurity Outlook* 2025, del Foro Económico Mundial, estima una proyección de entre 10.5 y 12,000,000.00 millones de dólares de costo global de la ciberseguridad para 2025. Esta cifra es equivalente a la tercera economía mundial, luego de Estados Unidos y China. (*World Economic Forum*, 2025).

La identificación digital es un componente crítico en el mundo digital, ya que la identificación protege nuestra información privada del mundo público y eso delimita una frontera fundamental. Muchos de los ciberataques, fraudes o delitos comienzan vulnerando alguna identificación digital. Actualmente, con el avance en herramientas de Inteligencia Artificial, técnicas sofisticadas de ingeniería social y la alta dependencia que se tiene de las TIC, hacen que las amenazas sean realmente complejas.

En los últimos años han surgido métodos de identificación digital innovadores, más seguros y fáciles de utilizar, incluso algunos de ellos se comportan de manera similar a como se comportan las identificaciones tradicionales presenciales.

1.3. Sistemas y ecosistemas de identificación digital

Sistema de identificación digital nacional

En el entorno digital se utiliza una identificación específica para cada uno de los sistemas, portales o servicios digitales; generalmente mediante la combinación de un usuario y una contraseña. Sin embargo, desde hace un tiempo, existe una tendencia a que las identificaciones digitales se comporten en forma semejante a los modelos presenciales tradicionales.

Los ciudadanos suelen obtener la identificación nacional en forma presencial (DNI, cédula, pasaporte, etc.) en una organización reconocida y competente y se utiliza en muchos lugares públicos y privados. Lo mismo sucede con el pasaporte que se usa en todas las fronteras. De esta forma, se cuenta con un conjunto reducido de identificaciones (estandarizadas) emitidas por organizaciones reconocidas, en las cuales confía todo un ecosistema compuesto por múltiples organizaciones públicas y privadas según sea el caso.

En el mundo digital, diversos sistemas informáticos y servicios digitales comenzaron a integrar proveedores de identificación y, de forma análoga, grandes concentradores de credenciales de usuarios comenzaron a posicionarse como proveedores de identificaciones digitales. Hoy en día es posible ingresar a Spotify, Booking y muchos portales y servicios digitales utilizando una cuenta (identificación) de Google, Apple, LinkedIn o Facebook, entre otras.

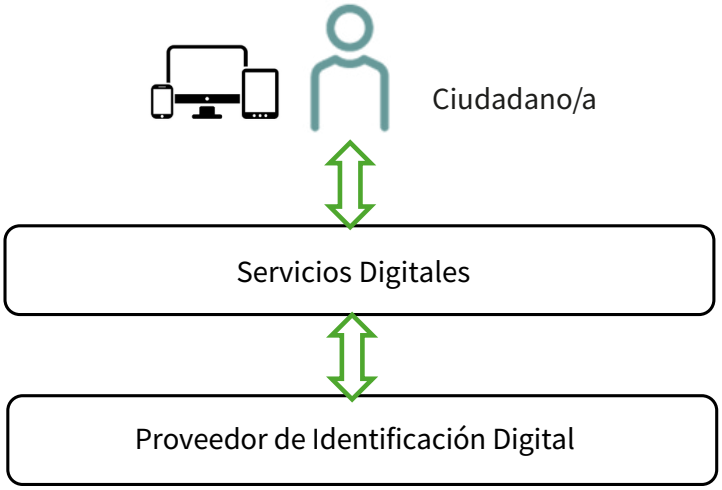
Esta tendencia, donde las identificaciones digitales se están acercando al comportamiento de las identificaciones tradicionales, simplifica y reduce riesgos en el entorno digital. Se puede contar con un número reducido de identificaciones más seguras y utilizarlas en múltiples servicios digitales.

No todos los proveedores de identificación digital poseen las características necesarias para ser utilizados en sectores que gestionan información de carácter sensible como la Salud, el sector Financiero o el Estado. Algunos países, fundamentalmente en el sector público, desde hace unos años vienen construyendo un sistema nacional de identificación digital. De esta forma se desarrolla un proveedor único de identificación digital, donde las personas se registran y obtienen sus credenciales, que se integra a los servicios digitales públicos. Como resultado, cada persona posee una identidad digital que la utiliza en todo el sector público, o al menos en gran parte. En algunos casos, esto también se extiende al sector privado, es decir, la misma identificación digital que se usa para acceder a servicios digitales públicos, también se puede utilizar para servicios digitales del sector privado.

El sistema de identificación digital nacional centralizado, no es solamente una solución de software que gestiona identidades digitales, debe desarrollar estrategias, marcos regulatorios, estándares y requerimientos que aseguren que las identificaciones digitales estarán aptas para los servicios digitales integrados, tal como sucede con los proveedores de identificaciones tradicionales o físicas (DNI, Cédula de Identidad, Pasaporte, etc.).

El siguiente esquema muestra esta situación en forma simplificada:

Figura 2. Esquema de sistema de identificación digital nacional centralizado.



Fuente: elaboración propia

Ecosistema de identificación digital nacional

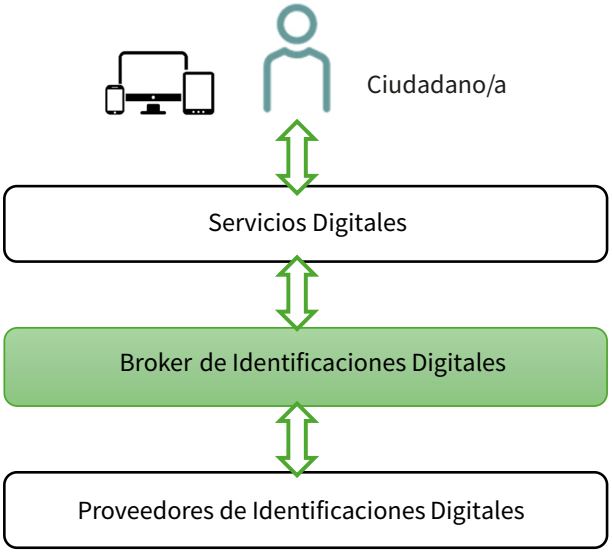
Algunos países están avanzando hacia un esquema federado de identificaciones digitales. Esto implica contar con un grupo regulado y estandarizado de proveedores de identificaciones digitales integrados a múltiples servicios digitales, generalmente en el sector público, pero se podría extender también al privado.

Las personas poseen una única identidad digital, cada proveedor de identificación en un ecosistema posee diferentes métodos para identificarse, pero utilizan la misma identidad. Esto implica que la persona siempre es la misma, pero dispone de diferentes métodos para identificarse digitalmente, lo que facilita enormemente el acceso.

En este tipo de esquemas, es sumamente importante (pero no excluyente), incluir una pieza extra de software, un intermediario, llamado *broker* de identificaciones digitales para facilitar las integraciones y la evolución. Un *broker* de identificaciones digitales **es una plataforma** que se posiciona entre sistemas digitales y proveedores de identificaciones digitales. Por un lado, integra proveedores de identificaciones digitales aptos para su ecosistema, públicos o privados. Por otro lado, se integra a servicios digitales (trámites

en línea, portales, sistemas de gestión del Estado, etc.) que, de esta forma, heredan todo el ecosistema de identificaciones digitales. El siguiente esquema ilustra esta situación en forma simplificada:

Figura 3. Esquema de Ecosistema de Identificación Digital Nacional.



Fuente: elaboración propia

Un ciudadano que necesita acceder a un servicio digital del ecosistema, a través del *broker* elige un proveedor de identificación, se identifica digitalmente en su proveedor y regresa al servicio accediendo a su información personal. Los servicios, delegan en los proveedores integrados al *broker*, la identificación digital (o autenticación) de las personas. De esta forma, la identificación digital de las personas es única para todo el ecosistema, en forma similar a lo que sucede con las identificaciones tradicionales presenciales.

El control de acceso (autorización) lo define en forma específica cada servicio digital en función del perfil o rol de la persona que se identificó y el nivel de confianza de la identificación que utilizó.

Al igual que un sistema de identificación digital nacional centralizado, este esquema también debe desarrollar y evolucionar estrategias, marco normativo, estándares y requerimientos, pero, a su vez, posee algunas ventajas:

- **Diversidad de proveedores:** incluir más de un proveedor de identidad digital (públicos y privados) puede ser importante para lograr mayor alcance y, por lo tanto, facilita la posibilidad de que las personas accedan a alguna identificación digital dentro del ecosistema.

- **Integración de nuevos métodos:** si aparecen nuevos proveedores y, sobre todo, nuevos métodos de identificación digital, basta con integrarlos una vez al *broker* para que queden disponibles en todo el ecosistema y los usuarios lo puedan utilizar en todos los servicios integrados, sin necesidad de reconfigurar cada uno de ellos. Esto maximiza la eficiencia y la economía de escala del sistema nacional, ya que todos los servicios integrados, incluida la administración tributaria, se benefician automáticamente de los avances sin reconfigurar individualmente cada uno de ellos.
- **Autenticación continua mediante IA:** incorporar servicios inteligentes de ciberseguridad al *broker*, utilizando herramientas de inteligencia artificial, permite fortalecer todas las identificaciones digitales de todo el ecosistema, reduciendo riesgos y aumentando la eficiencia.
- **Estadística y transparencia**: al centralizar en un único punto de articulación, se produce un gran volumen de datos estadísticos confiables, que puede ser utilizado para la toma de decisiones estratégicas y para la generación de datos abiertos (apertura de datos públicos).
- **Identificación transfronteriza:** el *broker* actúa como intermediario entre el ecosistema nacional del internacional, realizando las transformaciones y validaciones necesarias para facilitar la interoperabilidad.

En un sistema nacional de identificación digital centralizado y especialmente dentro de un ecosistema articulado mediante un *broker* de identificaciones, se requieren abordar ciertos temas estratégicos que son clave y que se desarrollaran a continuación:

Gobernanza: es necesario definir la gobernanza a nivel nacional, quién se encargará de definir estándares, protocolos, reglamentos, etc. En el caso de un ecosistema, la gobernanza también debe contemplar el desarrollo, evolución y operación del *broker*. Esto implica definir un regulador a nivel país, que lleve adelante las iniciativas para el reconocimiento transfronterizo de identificaciones digitales.

Normativa: se debe formular la normativa asociada a la identidad e identificación digital, dotándola de un marco legal robusto y alineado con los estándares internacionales. Se deben contemplar aspectos como la validez jurídica de las identificaciones digitales, los principios rectores y la protección de los datos personales. Una normativa clara no solo brinda seguridad jurídica a las operaciones digitales, sino que también facilita la adopción por parte de organismos públicos, privados y ciudadanos.

Niveles de seguridad: una identificación digital puede tener diferentes grados de confianza. Este grado de confianza generalmente depende de dos variables: la forma en cómo la persona obtuvo su identificación (en línea sin verificación de la identidad, presencialmente con verificación biométrica, etc.) y qué formas de verificación de la identificación utilizó al autenticarse en un sistema (contraseña débil, contraseña fuerte, MFA

o firma digital, entre otras). Es importante que a nivel nacional estén claramente definidos estos parámetros y, con esto, los niveles de seguridad.

Algunas experiencias de la región definen tres niveles posibles:

- **Bajo:** Un usuario que se registró en línea, validó la cuenta desde su correo y el sistema realizó algunos chequeos simples, pero no hay garantías de que la persona sea quien dice ser ya que no fue validada su identidad. Cuando se identifica digitalmente utiliza su usuario y una contraseña fuerte.
- **Medio:** Un usuario que inicialmente era básico y validó su identificación por algún medio habilitado (presencialmente, biometría, firma digital, etc.). Cuando se identifica digitalmente utiliza su usuario, una contraseña considerada fuerte y un segundo factor de autenticación.
- **Alto:** Un usuario que se registró en un proveedor en forma presencial y se realizó una validación biométrica de su huella digital con el registro público. El registro tiene vencimiento por lo que es necesario renovarlo periódicamente. Cuando se identifica digitalmente, lo hace a partir de un certificado digital reconocido por la Infraestructura Nacional de Claves Públicas, utilizando la firma electrónica avanzada para identificarse digitalmente.

Datos de identificación: es necesario definir, en primer lugar, un identificador universal a nivel nacional. Las personas van a obtener sus identidades digitales en un proveedor de identificación digital ya sea con un único proveedor, en el caso de un sistema nacional, o en alguno de los proveedores del ecosistema, en un modelo federado. Para eso, es importante tener en cuenta que el usuario debe ser unívocamente identificado en cada sistema, independientemente del proveedor que utilice, ya que en todos los casos se trata de la misma persona. Algunos ecosistemas de la región utilizan tres campos para identificar a un usuario:

- Código de país según la norma ISO 3166-1 alpha-2, estándar que define los códigos de países utilizados en los dominios de nivel superior geográfico (ar, br, pe, pa, uy, etc.).
- Código de documento: código del documento físico con el que se registró el usuario (CI -cédula de identidad-, DNI -documento nacional de identificación-, PSP -pasaporte-, etc.).
- Número de documento utilizado para registrarse, es decir, el número del documento correspondiente al código anterior, emitido por el país según el código de la ISO 3166-1.

Esta combinación con los tres elementos hace que la identificación sea universal, no solo a nivel nacional. Este es un punto importante para la identificación digital transfronteriza que se abordará en el siguiente apartado dentro de este capítulo.

Otros datos del usuario: es necesario que esté normado qué datos se va a gestionar (intercambiar) de los usuarios, además del identificador, como, por ejemplo: nombres, apellidos, correo electrónico, teléfono y/o fecha de nacimiento. En este sentido, utilizar un conjunto suficiente pero mínimo de datos puede ser una buena práctica para proteger la información personal. Si luego los servicios a los que los usuarios ingresan necesitan más información, deberán interoperar con fuentes de datos externas en forma específica, siempre con el debido permiso del usuario.

Fuentes oficiales para validar identidades: en muchos países, los gobiernos, a través de sus registros oficiales de población civil desarrollaron servicios digitales que son consumidos por proveedores de identificación digital entre otros. Este servicio, se formaliza mediante un convenio entre las partes y permite que un tercero valide datos de la identidad del usuario, inclusive en muchos casos datos biométricos, principalmente imagen facial y huella dactilar. Si bien se deben tomar las precauciones necesarias para proteger la privacidad de la información del usuario, es una herramienta importante para fortalecer la confianza en la identificación digital en todo el país, ya que puede ser usada por el sector público y privado.

Protocolos y estándares técnicos: es necesario incorporar protocolos, así como estándares de seguridad. En el caso de protocolos existe una serie de protocolos comprobados para este fin, los más reconocidos son *Security Assertion Markup Language* (SAML), *Open ID Connect* (OIDC basado en OAuth2.0) y más recientemente *OpenID Connect for Verifiable Credentials* (OIDC4VC) para integrar métodos basados en el uso de credenciales verificables. En el capítulo tres se abordará con mayor detalle este tema.

***Single Sign-On* (SSO) o inicio de sesión único:** la implementación de un mecanismo de autenticación centralizado, como el SSO, es fundamental para garantizar una experiencia de usuario fluida y segura dentro de un ecosistema digital nacional. Se trata de un mecanismo que, bajo una autenticación centralizada como puede ser un sistema o ecosistema permite que un usuario se identifique una sola vez y mantenga su identificación activa durante toda la sesión de trabajo en todos los sistemas integrados. Esta propiedad ampliamente utilizada y cómoda para el usuario, en términos simplificados, se implementa de la siguiente forma:

1. El usuario elige un proveedor de identificación e introduce sus credenciales (independientemente del método).
2. Si las credenciales son válidas el proveedor de identificación genera un token de autenticación (*assertion* SAML o ID Token en OIDC).
3. Cuando el usuario intenta acceder a un servicio que confía en el proveedor de identificación utilizado, en lugar de volver a solicitar las credenciales, el servicio valida el token emitido en forma transparente al usuario.

Un token de autenticación es una cadena de texto firmada por el proveedor de identificación, emitida en forma personalizada a un usuario, dispositivo o entidad una vez que su identidad haya sido verificada. Este token representa la sesión autenticada, vinculada tanto al usuario como a su proveedor de identificación, considerado de confianza para el ecosistema.

Cuando el usuario accede a un nuevo sistema informático integrado, dicho sistema simplemente verifica la firma del token y si la firma es válida, asume que la información incluida en él, sobre la autenticación del usuario es correcta. Por cuestiones de seguridad, los tokens de autenticación tienen una vigencia limitada, al crearse se define una duración específica, tras la cual, el usuario deberá volver a autenticarse.

En muchos casos, el SSO se combina con una adecuada autenticación continua. A modo de ejemplo, un usuario puede navegar por diferentes sistemas del ecosistema manteniendo la sesión activa, pero si realiza una operación sensible o accede a información confidencial, el sistema le solicita al proveedor de identificación que vuelva a validar la identidad del usuario.

Hacia la identificación digital transfronteriza

A medida que los países avanzan en el desarrollo de sistemas o ecosistemas de identificaciones digitales nacionales, es necesario abordar el desafío de la interoperabilidad a nivel transfronterizo. Una forma sencilla de empezar a pensar ese camino, una vez más, es mirar cómo se ha resuelto ese problema en el mundo físico y aplicar la misma lógica en el mundo digital.

Desde hace muchas décadas se obtienen las identificaciones físicas en organizaciones acreditadas y reconocidas para este fin en los países de origen. Los documentos de identificación nacional, la licencia de conducir, entre otros, son tramitados en forma presencial con determinados protocolos estrictos de verificación de la identidad, como el uso de tecnología biométrica (por ejemplo, huella dactilar), entre otros. Estos documentos se utilizan para identificarse en oficinas públicas, pero también en organizaciones privadas.

A su vez, estos documentos también son utilizados fuera de frontera para identificarse y son confiables por muchas organizaciones en todo el mundo. Es importante tener en cuenta que estos documentos identifican a las personas, pero no hay que olvidarse que, además, en algunos casos puede ser necesario contar con permisos adicionales como por ejemplo visas. Estos permisos no son parte de la identificación de la persona, eso ya está resuelto con el pasaporte, son parte del control de acceso o autorización según la normativa aplicable.

Este modelo tiene su equivalente en el entorno digital: una vez que una persona ha sido identificada correctamente, cada sistema puede requerir mecanismos adicionales de autorización para permitir el acceso a funcionalidades específicas, conforme a las políticas y/o al nivel de sensibilidad de la información. Es por eso, que en el mundo digital se debe avanzar en esta línea, es decir, que las personas utilicen las

identificaciones digitales confiables de sus países, no solo para identificarse dentro, sino fuera de fronteras, en servicios digitales de otros países.

Esto, además de resultar más natural y fácil de utilizar, ya que se haría de la misma manera que se realiza desde hace muchas décadas con las identificaciones físicas, sería más accesible para las personas y de mayor confianza para todas las partes. Para los ciudadanos es mucho más sencillo obtener una identificación digital verificada en su país -por ejemplo, de forma presencial y con control biométrico de huella-, que, en el extranjero, donde en la mayoría de los casos es inviable. Además, resultaría más seguro porque en su país se pueden realizar mejores controles de la identidad y, por lo tanto, lograr identificaciones digitales con mucho más nivel de confianza, tal cual sucede con las identificaciones tradicionales.

Existen algunas iniciativas para avanzar en la identificación digital transfronteriza, logrando que las personas utilicen identificaciones digitales confiables de sus países de origen para ingresar a servicios digitales de otros países.

En Europa, eID es un sistema federado de identificación digital electrónica reconocido a nivel europeo. Este ecosistema está regulado por eIDAS (*Electronic Identification, Authentication and Trust Services*) (Unión Europea, 2014). Su objetivo es permitir que ciudadanos, empresas y administraciones públicas se identifiquen y accedan a servicios digitales de forma segura y transfronteriza en la Unión Europea (UE), utilizando identificaciones confiables de cada país. Permite a un ciudadano utilizar su identidad digital confiable de su país para acceder a servicios públicos o privados en otro país de la UE.

Este ecosistema incluye identificaciones digitales basadas en el uso de tarjetas inteligentes que utilizan una firma digital para identificarse, aplicaciones móviles de identificación o identificadores combinados con sistemas de autenticación considerados fuertes. La primera versión del marco normativo eIDAS fue publicada en 2016 y estableció un esquema común para el reconocimiento mutuo de identificaciones digitales, reglamentos para servicios de confianza basado en firmas digitales, sellos, entre otros.

A finales de 2024 se lanzó eIDAS 2.0 donde, si bien aún resta definir numerosos reglamentos técnicos, se introduce y se le da mucha relevancia al uso de credenciales verificables en billeteras electrónicas como método para identificarse digitalmente (Comisión Europea, s.f.), también utilizando la firma digital. Tal como se comentará en el capítulo 3, el marco normativo europeo está avanzando en favorecer identificaciones sin uso de contraseña, donde las credenciales están en poder del usuario – por ejemplo, mediante tarjetas inteligentes o credenciales verificables en su dispositivo móvil-, y la identificación se realiza en base al uso de la firma digital.

Actualmente, cada país posee y gestiona su sistema de identificación digital, y para interoperar en el ámbito europeo existe un “*hub* de identidades digitales” (Comisión Europea s.f), donde los ciudadanos pueden seleccionar su país de origen, identificarse a través del sistema nacional correspondiente y navegar en los distintos sistemas integrados a este ecosistema digital europeo.

En América Latina y el Caribe, con el apoyo de la Red de Gobierno Electrónico en América Latina y el Caribe (Red Gealc) (s.f) comenzaron a desarrollarse las primeras experiencias piloto de integración de identificaciones digitales en la región.

En 2023 se logró la primera integración entre Uruguay y Argentina a nivel de prueba de concepto, en fase de prueba. Uruguay posee un ecosistema de identificación digital activo desde 2018 con un *broker* de identificaciones llamado ID Uruguay que articula cuatro proveedores de identificación, tres de ellos utilizando la firma digital como método para identificarse digitalmente. Argentina, por su parte, posee el *broker* de identificaciones digitales llamado Autenticar.

En octubre de 2024 se alcanzó un nuevo hito, cuando se puso en producción la primera integración transfronteriza en América Latina y el Caribe entre Uruguay y Brasil. En esta oportunidad, ID Uruguay se integró con Gov.br, *broker* de identificaciones digitales brasilero. Ambos *broker*, en uso desde hace varios años, fueron diseñados bajo los mismos estándares y buenas prácticas, inspirados en eIDAS y las buenas prácticas de NIST, por lo que la integración fue muy simple. Como resultado, los ciudadanos brasileños pueden acceder a más de 360 servicios digitales del Estado en Uruguay utilizando sus identificaciones digitales brasileñas confiables incluyendo todos los trámites vinculados al Comercio Exterior en Uruguay.

Las experiencias entre los tres países han demostrado que el *broker* de identificaciones digitales es una pieza fundamental para habilitar la identificación digital transfronteriza dentro del esquema "*building blocks*" de gobierno digital de cada país, asegurando de esta manera la estandarización de la identificación digital transfronteriza.

Este proceso de co-creación entre los países mencionados permitió no solo lograr el primer caso de identificación digital transfronteriza, sino diseñar y validar el estándar para impulsar la identificación digital transfronteriza en toda la región. En el contexto transfronterizo, contar con un *broker* ofrece ventajas estratégicas al desarrollar un ecosistema nacional interoperable:

- **Separación:** permite distinguir de forma clara el ecosistema nacional del internacional, facilitando las transformaciones y validaciones de datos que sean necesarias entre países.
- **Filtrado**: permite aplicar criterios de confianza centralizados, de modo que a nivel transfronterizo solamente se utilicen identificaciones consideradas confiables por los países involucrados.
- **Gradualidad:** permite habilitar las identificaciones digitales transfronterizas en forma progresiva y controlada, permitiendo que cada país active esta funcionalidad según el nivel de madurez de sus servicios y normativas.

Ante esta experiencia tan positiva, durante el primer semestre 2025, la Red Gealc, con el apoyo del Banco Interamericano de Desarrollo (BID), la Organización de Estados Americanos (OEA), el Banco Mundial y Co-Develop asignaron financiamiento para el desarrollo de un *broker* de identificaciones digitales modelo para toda la región. El objetivo es que este *broker* sea un bien público digital, para que los países lo puedan implementar, generando un ecosistema de identificaciones digitales a nivel nacional, pero, adicionalmente, creando las condiciones para avanzar en la identificación digital transfronteriza en América Latina y el Caribe.

El *broker* de identificaciones digitales modelo, alineado a los últimos estándares y buenas prácticas reconocidas a nivel mundial en identificación digital será una pieza clave para la estandarización de la identificación digital a nivel continental, lo que acelerará las integraciones y el uso. Se espera lograr un importante impacto a nivel continental en sectores como el turismo, la educación, la salud, el comercio exterior, las administraciones tributarias y migraciones, entre otros.

Desafíos para las administraciones tributarias

Es de prever que, en el futuro, América Latina y el Caribe deberán afrontar desafíos que tienen que ver con la definición de la gobernanza y la construcción de un *hub* de *brokers* de identificaciones digitales, de modo que cada *broker* de cada país se integre una sola vez al *hub* y ya sea parte de todo el ecosistema regional. Utilizar las identificaciones digitales de sus propios países para acceder en forma simple a servicios digitales de otros países implica un ahorro de tiempos y costos considerables en diversos sectores, a la vez de fortalecer la confianza y facilitar en el uso de herramientas digitales.

Las administraciones tributarias tienen un rol clave en la integración digital regional. En este sentido, tienen mucho que aportar ya que existen casos de uso concretos en el ámbito de las identificaciones digitales transfronterizas, facilitando el acceso a servicios digitales para personas y empresas de otros países.

Este tipo de implementación puede simplificar significativamente la relación entre la administración tributaria y sus contribuyentes donde sea que se encuentren, extendiendo su alcance más allá de las fronteras, de manera segura, sencilla y confiable. Al mismo tiempo, permite aprovechar todo el potencial del entorno digital y contribuir activamente al fortalecimiento de la integración y el desarrollo regional.

Más allá de ser beneficiarias directas de estas soluciones, las administraciones tributarias pueden ser agentes facilitadores, impulsando la cooperación entre países y ayudando a construir experiencias exitosas, creando puentes digitales seguros para que otros puedan transitar y que respondan a las necesidades de integración de la región. Se abordará con mayor detalle este tema en el capítulo 3.

2. Situación actual en las administraciones tributarias de América Latina y el Caribe

Este capítulo desarrolla un análisis de la situación actual de la identificación digital en las administraciones tributarias de la región. Para recabar información, uno de los principales métodos fue realizar una encuesta mediante un formulario estructurado (disponible en el Anexo I) a cada administración tributaria. Los países que enviaron información fueron:

- Brasil
- Chile
- Costa Rica
- Ecuador
- España
- Guatemala
- Honduras
- México
- Panamá
- Perú
- Uruguay

Complementando la información recabada por la encuesta, se realizó una investigación en los portales de gobierno digital y administraciones tributarias para obtener más información de interés. En el primer punto de este capítulo se presenta un resumen sobre los principales casos de sistemas o ecosistemas de identificación digital a nivel nacional y su relación con la administración tributaria. Se realiza un análisis sobre diferentes dimensiones: sistemas o ecosistemas a nivel nacional, métodos de identificación digital y la relación con las administraciones tributarias.

En el siguiente punto, se analizan los principales desafíos y dificultades para la digitalización en las administraciones tributarias y el uso de canales digitales y su relación con la identificación digital desde la

óptica de los principales servicios de la administración. Finalmente, al cierre del presente capítulo se presenta un resumen de la situación actual, agrupada en diferentes niveles o categorías con respecto a la identificación digital.

2.1. Administraciones tributarias e identificación digital

La siguiente tabla muestra un resumen de las principales iniciativas de identificación digital nacional y su relación con la administración tributaria en algunos países de la región.

País	Iniciativas de sistemas o ecosistemas de identificación digital nacional y su relación con la administración tributaria
Argentina	La Secretaría de Innovación, Ciencia y Tecnología gestiona la plataforma Autenticar, que actúa como un *broker* de identificaciones digitales por lo que habilita un ecosistema federado con proveedores de identificaciones digitales oficiales utilizando el protocolo *Open ID Connect*. Autenticar se integra a servicios digitales para que las personas a través de esta plataforma seleccionen y utilicen uno de sus proveedores de identificación para todos los sistemas integrados. Este *broker* tiene 6 proveedores oficiales de identificación digital integrados y algunos en desarrollo (basados en el uso de firma digital), entre los que se destaca: • RENAPER: Registro Nacional de las Personas de Argentina, organismo estatal que identifica y documenta a las personas y tiene la responsabilidad exclusiva de emitir el DNI y el Pasaporte. Las personas se identifican en línea mediante su número de DNI y número de trámite (impreso en la tarjeta). Posee validación biométrica mediante una selfie y prueba de vida. Desde este organismo también se está avanzando en un documento físico con chip, con posibilidades de firmar e identificarse digitalmente. • **AFIP / ARCA: La administración tributaria Argentina es un proveedor de identificación digital en el ecosistema nacional. El usuario se identifica con su clave fiscal (CUIT) y valida su identidad con una clave fuerte.** • Mi Argentina: El usuario se identifica con su número de CUIL y una contraseña fuerte. Puede validar su registro desde la aplicación de Mi Argentina mediante una *selfie* y prueba de vida. La aplicación móvil también posee una cartera digital con el documento de identificación nacional y licencia de conducir, según el estándar ISO18013-5. En fase experimental, el ecosistema de identificación digital de Argentina está avanzando en identificaciones digitales autosoberanas sobre *blockchain*. Argentina también está avanzando en la implementación de un documento de identidad con chip, con capacidades de firmar e identificarse digitalmente.

País	Iniciativas de sistemas o ecosistemas de identificación digital nacional y su relación con la administración tributaria
Bolivia	La Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación (AGETIC) desarrolló un sistema de identificación digital nacional que consiste en el Registro en Ciudadanía Digital y la identificación mediante el uso de dicho registro. Las personas se identifican mediante Ciudadanía Digital ingresando su número de cédula de identidad y validándola con una contraseña fuerte. El sistema presenta la opción de identificarse desde la App de Ciudadanía Digital mediante un código QR con las mismas credenciales. **El sistema Integrado de Administración Tributaria (SIAT) posee su propio sistema de identificación (no está integrado a Ciudadanía Digital) donde los usuarios se identifican mediante un NTI, CUR o Cédula de Identidad y un correo electrónico y validan su identidad utilizando una contraseña fuerte.**
Brasil	Brasil posee un ecosistema de identificación digital con Gov.br como *broker* de identificaciones digitales federadas. Este ecosistema funciona desde hace varios años con más de 4.500 servicios digitales integrados y más de 20 proveedores de identificación con tres niveles de seguridad (bronce, plata y oro). Además del volumen, se destacan varias características. Hay 17 bancos públicos y privados que son proveedores de identificación en Gov.br, por lo que, una persona que tenga una identificación digital en alguno de estos bancos la puede utilizar para acceder a los servicios públicos integrados. Además, posee proveedores de identificación que brindan la identificación en base al uso de la firma digital. Este ecosistema también incluye una aplicación móvil que posee herramientas para validar identidades en forma biométrica, utilizando pruebas de vida y se puede utilizar para autenticarse mediante códigos QR en sistemas web. Además, es posible utilizar métodos basados en la firma cualificada para identificarse digitalmente en el ecosistema de Gov.br a nivel “oro”. Brasil está realizando pilotos a nivel estadual para el uso de identificaciones digitales descentralizadas, autosoberanas sobre *blockchain*. **La administración tributaria brasileña (Receita Federal), está integrada a Gov.br, por lo que es posible utilizar cualquiera de las identificaciones digitales del ecosistema Gov.br para ingresar a los servicios digitales de la administración tributaria.**
Chile	El Ministerio de Hacienda, a través de la División de Gobierno Digital administra la Clave Única chilena. Se trata de un único proveedor de identificación digital para el sector público y empresas privadas que estén habilitadas bajo convenio y cumplan los estándares necesarios. Las personas se identifican con RUN (Rol Único Nacional), obtenido a partir de la Cédula de Identidad y verifican su identificación con una contraseña fuerte. A finales de 2024, a través de un proyecto para modernizar el Registro Civil, Chile comenzó a emitir una cédula de identidad que incorpora características biométricas que se complementa con una aplicación que permite portar el documento digitalmente, obteniéndose mediante código QR. **El Servicio de Impuestos Internos (SII) posee un sistema de identificación digital propio donde los contribuyentes se identifican con RUT y validan su identificación con una contraseña fuerte. Adicionalmente, el SII está integrado a Clave Única por lo que es posible utilizarla para ingresar a la administración tributaria.**

País	Iniciativas de sistemas o ecosistemas de identificación digital nacional y su relación con la administración tributaria
Colombia	La Agencia Nacional Digital desarrolló la plataforma de Autenticación Digital, la cual es un proveedor único de identificación digital para los servicios públicos digitales. Las personas se identifican usando su número de cédula y luego verifican su identificación con una contraseña fuerte. La Registraduría Nacional del Estado Civil a partir de este año comenzó a emitir cédulas digitales, alojadas en porta documentos móviles. Esta cédula tiene posibilidades de ser utilizada para Identificarse en forma digital, pero no está integrada a la plataforma de Autenticación Digital aún. **La Dirección de Impuestos y Aduanas Nacionales (DIAN) posee su propio sistema de identificación digital (no integrado a Autenticación Digital) donde los usuarios se pueden identificar con diferentes números de documentos (tarjeta de identidad, registro civil de nacimiento, cédula de ciudadanía, etc.) y verifican su identidad con una contraseña fuerte.**
Costa Rica	El Tribunal Supremo de elecciones recientemente lanzó la Identidad Digital Costarricense que se obtiene en base a la cédula de identidad y se gestiona en una aplicación móvil (IDC-Ciudadano) que, entre otros controles, verifica la identidad de la persona mediante una prueba biométrica facial. Esta iniciativa es sumamente reciente, por lo que el Banco Central de Costa Rica está desarrollando un proveedor que habilite este método de identificación para los servicios públicos digitales. **La Dirección General de Tributación no está integrada al sistema nacional de identificación digital y en principio no tiene planes de hacerlo (el sistema es incipiente aún). La Dirección General de Tributación posee su propio sistema de identificación digital, los usuarios se identifican con el número identificador de contribuyente y validan su identificación con una contraseña fuerte. Este sistema, además, posee un segundo factor de autenticación de uso obligatorio para todos los usuarios.**
Ecuador	El Registro Civil de Ecuador emite una cédula de identidad desde 2021 con un chip que contiene datos biométricos del ciudadano y capacidades de firmar digitalmente. Desde 2023 el Registro Civil comenzó a otorgar una cédula de identidad digital en forma opcional que se porta en la aplicación Gob.ec y es equivalente a la física. Adicionalmente, el portal Gob.ec y su aplicación poseen una cuenta única para Identificarse digitalmente en portales y trámites en línea. Esta cuenta se propone como un punto único para identificarse en portales y servicios en línea del Estado, donde las personas se identifican con un usuario y validan su identificación con una contraseña fuerte. **El Servicio de Rentas Internas (SRI) posee su propio sistema de identificación digital y en el corto plazo no hay planes para integrarse a Gob.ec. Los contribuyentes se identifican con el RUC, CI o pasaporte, adicionalmente pueden ingresar un número de cédula adicional (utilizado para gestionar perfiles) y validan su identificación con una contraseña fuerte.**

País	Iniciativas de sistemas o ecosistemas de identificación digital nacional y su relación con la administración tributaria
El Salvador	El Salvador posee un sistema llamado Identidad Digital que se constituye como un único proveedor de identificación digital para servicios digitales públicos y actúa como *Single Sign-On* en todo su ecosistema. Las personas se pueden identificar con su número de DUI (Documento Único de Identidad), pasaporte o carné de residente. Validan su identidad con una contraseña fuerte. El Registro Nacional de Personas Naturales tiene planes para desarrollar un DUI digital. **La Dirección General de Impuestos Internos (DGII) posee un sistema de identificación digital propio, las personas se identifican con su número NIT o DUI y validan su identidad con una contraseña fuerte.**
España	España posee un proveedor centralizado para identificarse en todos los servicios digitales públicos llamado Cl@ve Móvil. Las personas pueden hacerse de una identificación en este sistema mediante una videollamada, en forma presencial o utilizando un certificado electrónico (firma cualificada). Este sistema posee una aplicación móvil (opcional pero sugerida) para facilitar la identificación mediante un código QR en todos los servicios públicos del país. En caso de no contar con la aplicación, es posible identificarse mediante el número de DNI o NIE y validar la identificación con una contraseña fuerte y un segundo factor de autenticación. España posee un DNI electrónico, el carné de identificación físico con un chip criptográfico que permite firmar e identificarse digitalmente. Además, hay 6 prestadores de servicios electrónicos de confianza cualificados que otorgan certificados para identificarse en servicios digitales públicos. **La Agencia Tributaria española está integrada a Cl@ave Móvil, los contribuyentes se pueden identificar leyendo el código QR con la aplicación o directamente ingresar su número de DNI o NIE en el portal. La administración tributaria también tiene el rol de proveedor de identificación digital ya que permite crear y validar identificaciones en este sistema. Adicionalmente, la Agencia Tributaria permite utilizar el DNI electrónico o certificados digitales otorgados por prestadores de servicios electrónicos de confianza cualificados para identificarse digitalmente.**
Guatemala	Guatemala no posee un sistema o ecosistema de identificación digital en el sector público. Cada portal y servicio digital posee un sistema independiente de identificación digital. **La Superintendencia de Administraciones Tributarias (SAT) posee su propio sistema de identificación digital. Las personas se identifican con número de NIT o CUI y validan su identificación con una contraseña fuerte.**
Honduras	Honduras no posee un sistema o ecosistema de identificación digital en el sector público. Cada portal y servicio digital posee un sistema independiente de identificación digital. **El Servicio de Administración de Rentas (SAR) posee su propio sistema de identificación digital. Los usuarios se identifican con número RTN y validan su identificación con una contraseña fuerte.**

País	Iniciativas de sistemas o ecosistemas de identificación digital nacional y su relación con la administración tributaria
Jamaica	Jamaica está desarrollando el NIDS (*National Identification System*) que asigna un NIN (*National Identification Number*), registra datos biométricos y biográficos de la persona y emite una tarjeta de identificación nacional que posee un chip sin contacto con los datos de la persona gestionada por la NIRA (*National Identification and Registration Authority*). Este sistema dispondrá de un servicio en línea para la verificación de la identidad para organismos públicos y, mediante cobro, organizaciones privadas para validar datos contra el registro nacional. **La administración tributaria (*Tax Administration*), posee un sistema independiente de identificación digital. Los contribuyentes se identifican mediante un usuario y validan su identidad con una contraseña fuerte.**
México	La Llave MX es un proveedor de identificación digital único para ingresar a servicios públicos digitales. Actúa como un *Single Sign On* entre todos los sistemas integrados y utiliza *Open ID Connect* como protocolo de identificación digital. Las personas se identifican con un correo o número de teléfono móvil y validan su identidad con una contraseña fuerte. Actualmente, RENAPO (Registro Nacional de Población e Identidad) está en desarrollo un proyecto para evolucionar el documento de identificación nacional (CURP, Clave Única de Registro de Población) a una versión física y digital, su despliegue está planificado para 2026. La Credencial para Votar del INE (Instituto Nacional Electoral) es un documento físico muy utilizado como identificación presencial. Dispone de un servicio web para validar la identidad de una persona previa firma de convenio y cumplimiento de requerimientos de seguridad. **El SAT (Servicio de Administración tributaria) posee un sistema de identificación digital propio que funciona en dos modalidades (no integrado a Llave MX). Acceso por contraseña, el usuario se identifica con un número de RFC (Registro Federal de Contribuyente) y valida su identidad con una contraseña fuerte, teniendo la posibilidad opcional de un segundo factor de autenticación. El otro método es utilizando una firma digital del SAT (firma electrónica avanzada en México), presentando el certificado emitido por la Autoridad Certificadora del SAT, la clave privada y su contraseña.**
Nicaragua	Nicaragua no posee un sistema o ecosistema de identificación digital en el sector público. Cada portal y servicio digital posee un sistema independiente de identificación digital. El Servicio de Registro Civil e Identificación (SRCEI) posee una aplicación llamada Identificación Digital para portar una identificación en el dispositivo móvil y un validador que funciona mediante código QR, pero su uso no está destinado a identificarse en servicios digitales. La **Dirección General de Ingresos (DGI) posee su propio sistema de identificación digital. Los usuarios se identifican con un usuario y validan su identificación con una contraseña fuerte.**

País	Iniciativas de sistemas o ecosistemas de identificación digital nacional y su relación con la administración tributaria
Panamá	La Autoridad Nacional para la Innovación Gubernamental (AIG) desarrolló el portal Panamá Digital que en 2025 evolucionó a Panamá Conecta. Como parte de esta solución, hay un sistema de Identidad Digital Única con el que se puede acceder a algunos servicios públicos digitales. Actualmente las personas se identifican con un correo, número de cédula o pasaporte y validan su identidad con una contraseña fuerte. Posee un segundo factor como opcional. El Tribunal Electoral es quién gestiona la cédula de identidad y anunció intenciones de avanzar en la cédula digital, como una credencial en el dispositivo móvil. Recientemente se lanzó la licencia de conducir digital. **La Dirección General de Ingresos posee un sistema propio de identificación digital. El contribuyente se identifica con un usuario o RUC y utiliza una contraseña fuerte (NIT) para validar su identidad.**
Paraguay	El Ministerio de Tecnologías de la Información y Comunicación (MITIC) desarrolló un sistema de Identidad Electrónica para identificarse digitalmente en los servicios públicos digitales. El usuario se identifica con el número de cédula y valida su identidad con una contraseña fuerte. El Departamento de Identificaciones desde 2023 comenzó a entregar cédulas de identidad con chip, con registros biométricos, biográficos y capacidades para firmar digitalmente. Con la cédula con chip, puede crear y validar su identidad digital en el sistema de Identidad Electrónica del MITIC. **La Dirección Nacional de Ingresos Tributarios (DNIT) posee algunos sistemas accesibles desde la Identidad Electrónica y otros con sistemas de identificación digital independientes. Algunos sistemas permiten validar la identidad mediante una fotografía de la cédula de identidad y algunos casos utilizan la firma digital cualificada para validar la identidad.**
Perú	RENIEC (Registro Nacional de Identificación y Estado Civil) está desarrollando ID Perú con el objetivo de lograr un único proveedor de identificación digital para los servicios públicos digitales. Adicionalmente hay planes para desarrollar un documento de identidad electrónico que interactúe con ID Perú. **La Superintendencia Nacional de Aduanas y de Administración Tributaria (SUNAT) posee su propio sistema de identificación digital. Las personas se identifican con su número de DNI y las empresas con su número de RUC. En ambos casos, validan su identificación con una contraseña fuerte. En el caso de las empresas, además de RUC se solicita un usuario para distinguir roles dentro de cada contribuyente.**

País	Iniciativas de sistemas o ecosistemas de identificación digital nacional y su relación con la administración tributaria
República Dominicana	Desde el Portal Único de servicios del Gobierno Dominicano se está llevando a cabo una iniciativa para lograr un proveedor unificado de identificación digital en los servicios digitales públicos llamado Cuenta Única. Las personas se registran con el número de DNI, entre otros datos y el sistema provee una solución de prueba de vida para validar la identidad de su cuenta. Se identifican con el número de DNI y validan su identificación con una contraseña fuerte. En el ámbito de la Junta Central Electoral que es la responsable de emitir la Cédula de Identidad y Electoral se está avanzando en un documento de identidad con chip, con registro biométrico, biográfico y capacidades para firmar e identificarse digitalmente. **La Dirección General de Impuestos Internos (DGII) posee su propio sistema de identificación digital. Las personas se identifican con su número de cédula y las empresas con su número de RNC para luego validar su identidad con una contraseña fuerte y código de transacción a partir de un token digital otorgado por la DGII.**
Uruguay	La Agencia de Gobierno Electrónico y Sociedad de la información y del Conocimiento (AGESIC) gestiona el ecosistema de identificación digital del Estado. Esta plataforma se compone de un *broker* de identificaciones digitales llamado ID Uruguay que posee 4 proveedores de identificación digital que pueden ser utilizados para identificarse digitalmente en la mayoría de los trámites y servicios públicos digitales. Un proveedor de usuario.gub.uy, gestionado por AGESIC, donde las personas se identifican con su número de documento (cédula o pasaporte extranjero) y validan su identidad con una contraseña fuerte. Este sistema posee un segundo factor como opcional y brinda niveles de seguridad básicos (identidad sin validar) e intermedio (identidad validada). Los otros tres proveedores brindan identificación de nivel avanzado (equivalente jurídicamente a la presencialidad), basadas en el uso de la firma electrónica avanzada, en el contexto de la Infraestructura Nacional de Claves Públicas. Uno proveedor es una empresa privada y otro es una empresa pública de telecomunicaciones, ambas proveen la identificación digital en base a la firma en la nube. El cuarto proveedor es la Dirección Nacional de Identificación Civil que desde 2015 entrega una cédula de identidad con chip con capacidades para firmar e identificarse digitalmente. **La Dirección General de Impositiva (DGI) está integrada a la plataforma ID Uruguay, por lo que es posible identificarse digitalmente a través de cualquiera de los cuatro proveedores de identificación digital del ecosistema ID Uruguay. La DGI tenía un sistema de identificación digital propio, donde las empresas se identificaban con su número de RUT, pero desde hace unos años tomó la decisión de integrarse completamente a ID Uruguay e ir deshabilitando su sistema de identificación digital. Para esto desarrolló un sistema de autorización, para que las personas, una vez se identifiquen puedan cumplir determinados roles sobre las diferentes empresas.**

País	Iniciativas de sistemas o ecosistemas de identificación digital nacional y su relación con la administración tributaria
Venezuela	El Servicio Administrativo de Identificación, Migración y Extranjería (SAIME) posee una iniciativa de identificación digital centralizada para algunos trámites principalmente de su contexto. Si bien algunos servicios digitales de otros ministerios y entes lo integraron como sistema de identificación digital, no hay una amplia expansión aún. Las personas se identifican con número de cédula o correo electrónico y validan su identidad con una contraseña fuerte. Adicionalmente, SAIME posee servicios web para validar la identidad de una persona principalmente basado en datos biométricos. Si bien no ha habido aún un despliegue masivo, Venezuela ha implementado la cédula de identidad con chip, con información biométrica y capacidades para firmar e identificarse digitalmente. **El Servicio Nacional Integrado de Administración Aduanera y Tributaria (SENIAT) posee su propio sistema de identificación digital. Las personas se identifican con un usuario y validan su identificación con una contraseña fuerte.**

2.2 Principales hallazgos

A continuación, se presenta un resumen de los hallazgos relacionados con la temática, estructurados según las distintas perspectivas pertinentes al análisis.

Sistemas o ecosistemas de identificaciones digitales

En lo que respecta a sistemas o ecosistemas de identificaciones digitales nacionales y su relación con la administración tributaria, se observa lo siguiente:

- **Ecosistemas de identificación digital**: Existen algunos países que están consolidando un ecosistema de identificación digital a nivel nacional. Una plataforma que posee más de un proveedor de identificación digital estandarizado y se integra a servicios de públicos digitales, con el fin de que las personas utilicen cualquiera de sus proveedores de identificación para identificarse en el sector público: Argentina, Brasil, España y Uruguay.

  En estos casos, generalmente un *broker* de identificaciones digitales es un componente crítico para estandarizar y facilitar la integración entre más de un proveedor de identificación digital y los servicios públicos digitales.

Las Autoridades Tributarias actúan como un grupo de servicios públicos digitales integrados, por lo que es posible ingresar a la administración tributaria utilizando alguno de los proveedores de identificaciones digitales del ecosistema. En algunos casos, como por ejemplo en Uruguay, la DGI optó por deshabilitar gradualmente su sistema propio de identificación digital, sustituyéndolo por el ecosistema ID Uruguay. En otros casos, la administración tributaria habilitó el ecosistema, pero también mantiene funcionando su sistema de identificación digital original.

En el caso de Argentina, la administración tributaria, además, cumple el rol de proveedor de identificación digital, por lo que es posible utilizar la identificación digital de la administración tributaria para identificarse en otros servicios públicos digitales.

- **Sistemas de identificación digital**: Algunos países están desarrollando un sistema de identificación digital centralizado; esto es, un único proveedor que se integra a los diferentes servicios públicos digitales. Algunas administraciones tributarias (por ejemplo, el caso chileno) se integraron y ofrecen a sus contribuyentes la posibilidad de utilizar la identificación propia de la administración tributaria o el proveedor único de identificación digital (Cuenta Única). En otros casos, la administración tributaria todavía no se integra, por lo que sigue utilizando 100% su sistema de identificación digital.
- **Identificaciones digitales individuales** para cada servicio público digital o para cada organización pública. Estos casos no poseen sistemas o ecosistemas nacionales, sino que cada organismo (o servicio digital) posee su propio sistema de identificación digital. En estos casos, la administración tributaria posee su propio sistema de identificación digital.

Métodos de identificación

Con referencia a los métodos de identificación, se detallan a continuación:

- En la mayoría de los casos todavía se utilizan usuarios para identificarse y contraseñas para validar la identificación. En pocos casos se ha desarrollado en forma opcional el uso de un segundo factor de autenticación para fortalecer las identificaciones.
- En algunos casos existen sistemas de biometría para validar la identidad de la persona. Estos sistemas generalmente se basan en una imagen facial, tomada por el dispositivo móvil al usuario y comparada con un registro público (en el mejor de los casos) o con una foto de su documento de identidad proporcionado por el usuario. Esta útil herramienta se utiliza algunas veces como medio para validar la identificación del registro de un usuario, no tanto a la hora de identificarse. Algo a tener presente es que muy pocos

países poseen leyes de protección de datos personales, pero, sobre todo, herramientas para asegurar que las imágenes sean debidamente tratadas y no almacenadas por terceros. En muchos países de la región existen carencias normativas que podrían ocasionar que muchos sistemas tomen imágenes de personas sin control ni seguramente de un debido tratamiento de esos datos.

- Algunos países utilizan métodos más avanzados y seguros, como identificaciones descentralizadas basadas en el uso de la firma digital en el contexto de una Infraestructura Nacional de Claves Públicas. En este sentido, hay diferentes formas:
    - Documentos de identidad nacional con chip, utilizados como dispositivos criptográficos, donde el chip tiene datos biográficos y biométricos, pero además claves y certificado digital para firmar, otorgado por el ente responsable de identificación civil, que además es prestador de firma e identificación digital. El mismo documento de identidad físico se puede utilizar en el mundo digital, con total confianza. Si bien estos métodos ofrecen mayores niveles de seguridad, presentan ciertas fricciones en términos de usabilidad. El usuario debe contar con un lector de tarjeta inteligente, es decir, un dispositivo que permite insertar la tarjeta y conectarla a la computadora. Además, se requiere la instalación de controladores y aplicaciones específicas en el equipo, lo que puede generar dificultades relacionadas con los privilegios del usuario, el sistema operativo, los navegadores u otros componentes técnicos. Otro punto crítico es la limitada compatibilidad con dispositivos móviles. Aunque es técnicamente posible desarrollar soluciones móviles, aún no se registran implementaciones en la región.
    - Prestadores acreditados de firma e identificación digital otorgan dispositivos criptográficos -tarjetas inteligentes o tokens- que, si bien no son el documento de identidad nacional, poseen las mismas características que el caso descrito en el punto anterior y se utilizan para firmar o identificarse digitalmente.

La mirada desde las administraciones tributarias a la identificación digital nacional

- En los países que se está avanzado en un ecosistema o sistema de identificación digital nacional, muchas veces la administración tributaria está integrada como un grupo de servicios digitales, por lo que las identificaciones digitales disponibles en el ecosistema o sistema están habilitadas para ingresar a la administración tributaria. A medida que los sistemas o ecosistemas se vayan expandiendo, naturalmente las administraciones se van a ir integrando y es probable que a mediano plazo la identificación digital específica de la administración tributaria vaya dejando de utilizarse.

- En algunos países, la administración tributaria también se ha convertido en un proveedor de identificación digital en el sistema o ecosistema nacional. Las administraciones tributarias son organizaciones que poseen una gran base de datos con usuarios verificados y esto puede ser de mucho valor para un ecosistema o sistema nacional, por lo que es un escenario válido que la administración tributaria también sea un proveedor de identificación digital a nivel nacional.
- En otros casos, no hay relación aún entre la administración tributaria y el sistema o ecosistema de identificación digital. Esto puede deberse a la ausencia de una iniciativa nacional en materia de identidad digital, o a que dicha iniciativa se encuentra en una etapa incipiente, lo que ha llevado a que la administración tributaria no haya tomado aún la decisión de integrarse. Se espera que, a medida que estos sistemas se consoliden y se expandan, las administraciones tributarias se incorporen progresivamente. Esta incorporación puede darse, como mínimo, en calidad de consumidor de servicios digitales, accediendo mediante las credenciales del ecosistema; pero también como proveedor de identidad digital a nivel nacional, contribuyendo activamente al fortalecimiento del modelo.

2.3. Digitalización e identificación digital en las administraciones tributarias

En el entendido de que la identidad digital constituye un componente habilitante fundamental para el desarrollo de los procesos de digitalización en las administraciones tributarias, se exploró en la encuesta cuáles son los principales desafíos y problemas que enfrentan dichas instituciones en la implementación de servicios digitales.

En este marco, se procuró identificar las barreras técnicas, normativas y operativas que limitan el despliegue efectivo de servicios digitales en las administraciones tributarias, con el propósito de generar evidencia comparativa que permita orientar recomendaciones en materia de identificación digital, así como hojas de ruta diferenciadas, ajustadas a los distintos niveles de madurez digital.

Principales desafíos: síntesis basada en encuesta

La consigna planteada en la encuesta solicitaba ordenar los siguientes desafíos en función de su importancia, según la percepción de cada país participante:

- Los contribuyentes prefieren concurrir presencialmente a las oficinas

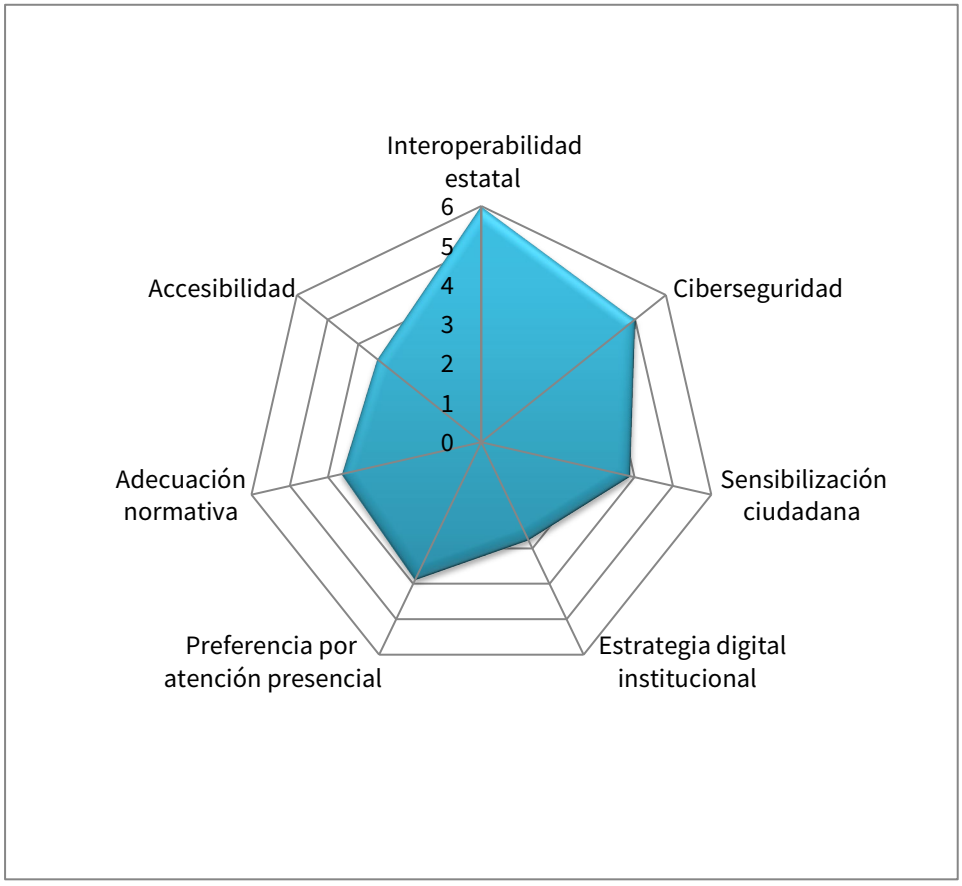
- Falta de una estrategia sólida de transformación digital
- Adaptación de normativas legales para regular trámites digitales
- Necesidad de sensibilizar a la población sobre las ventajas de los servicios digitales
- Garantizar accesibilidad para personas con discapacidades o barreras tecnológicas
- Incorporar ciberseguridad robusta para proteger los datos de los contribuyentes
- Implementar la interoperabilidad entre sistemas gubernamentales
- Otro

Fueron ocho los países que respondieron de manera estructurada a esta parte de la encuesta, habilitando su análisis sistemático. En la mayoría de los países, *la interoperabilidad entre sistemas gubernamentales* aparece como uno de los tres principales desafíos. Esto sugiere que la integración tecnológica estatal sigue siendo uno de los principales desafíos para avanzar en servicios digitales a la ciudadanía. Por otro lado, *la ciberseguridad* también se posiciona como prioridad alta en más de la mitad de los países, reflejando una creciente preocupación por la protección de datos personales y la confianza institucional. En lo que tiene que ver con la resistencia cultural —manifestada en la preferencia por la atención presencial y la necesidad de sensibilización ciudadana— se mantiene como un obstáculo relevante.

En cinco países, la ciberseguridad fue ubicada como el desafío número uno o dos, lo que indica que, en ciertos contextos, la protección de datos se percibe como el principal riesgo operativo. En estos mismos países, los desafíos culturales como la atención presencial fueron relegados a posiciones bajas, lo que podría reflejar una ciudadanía más familiarizada con los canales digitales.

Para concluir el análisis, en la mayoría de los países la estrategia de transformación digital aparece sistemáticamente en los últimos puestos del ranking; esto podría indicar que, aunque reconocida como importante, no se percibe como un obstáculo inmediato para la implementación operativa. La accesibilidad para personas con discapacidades o barreras tecnológicas también tiende a ocupar posiciones bajas, lo que representa una oportunidad para fortalecer el enfoque inclusivo en el diseño de servicios.

Figura 4. Mapa radar de desafíos para la implementación de servicios digitales – promedio.



Fuente: elaboración propia en base a una encuesta de 8 países.

Principales problemas: síntesis basada en encuesta

La consigna planteada en la encuesta solicitaba ordenar los siguientes problemas en función de su importancia, según la percepción de cada país participante:

- Problemas de conectividad en el país
- Poco acceso a dispositivos digitales por parte de los contribuyentes
- Falta de habilidades digitales en la población
- Servicios que cuentan con una mala experiencia de usuario

- Falta de personal de TI
- Falta de presupuesto adecuado
- Problemas legales por no tener certeza que sea el contribuyente quien realiza el trámite
- Otro

Fueron ocho los países que respondieron de manera estructurada a esta parte de la encuesta, habilitando su análisis sistemático. En la mayoría de los países, la falta de presupuesto adecuado aparece como una barrera prioritaria, posicionándose en el primer lugar del ranking. Esta situación refleja que, en varios contextos, la transformación digital aún compite con otras prioridades institucionales, lo que limita la inversión en soluciones escalables y seguras.

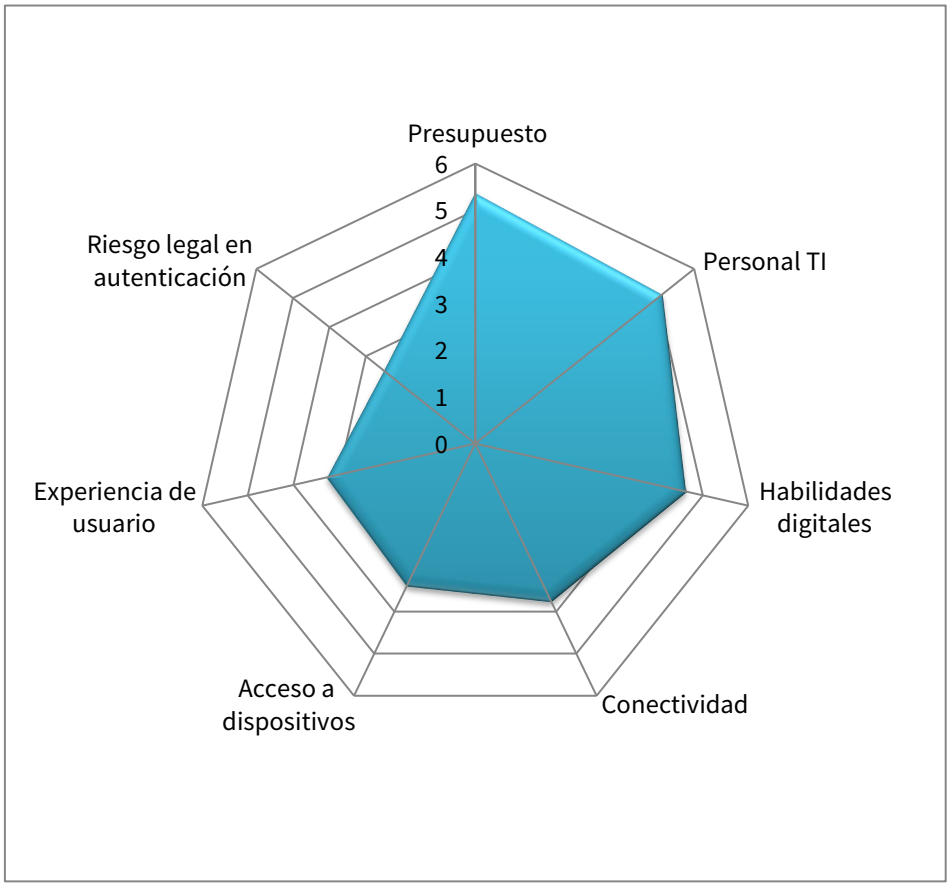
Asimismo, la falta de personal técnico especializado en TI se ubica entre los tres principales desafíos para seis países. Esto sugiere que, más allá de la infraestructura tecnológica, las capacidades humanas constituyen una limitante crítica para el despliegue de servicios digitales tributarios. La escasez de perfiles técnicos puede afectar la sostenibilidad operativa, la seguridad de los sistemas y la capacidad de adaptación normativa.

Por el contrario, las barreras vinculadas a la experiencia de usuario y la conectividad tienden a ocupar posiciones menores, lo que sugiere que, si bien relevantes, no se perciben como los principales obstáculos inmediatos. Esto podría indicar que en varios países ya se han realizado avances en infraestructura y diseño de servicios, aunque aún persisten desafíos en inclusión digital.

Aunque los problemas legales vinculados a la autenticación del contribuyente no aparecen como el principal desafío en ningún país, sí se posicionan como una barrera moderada en algunos contextos. En la mayoría de los casos, esta temática ocupa posiciones bajas en el ranking, lo que sugiere que no se percibe como un obstáculo inmediato. Esta percepción podría estar vinculada, por un lado, a la existencia de marcos normativos que reconocen la equivalencia jurídica entre la identidad digital y la presencial; por otro, a una menor priorización institucional del riesgo normativo asociado a la autenticación.

Finalmente, el acceso limitado a dispositivos y las habilidades digitales de la población presentan una distribución mixta: en algunos países son prioritarios, mientras que en otros se relegan. Esta variabilidad sugiere que las hojas de ruta deben contemplar enfoques diferenciados, combinando estrategias de sensibilización ciudadana, provisión de medios de acceso y fortalecimiento de capacidades digitales.

Figura 5. Mapa radar de problemas para la implementación de servicios digitales – promedio.



***Fuente*:** elaboración propia en base a una encuesta de 8 países.

Identificación digital en las administraciones tributarias

La siguiente tabla presenta un resumen de los métodos de identificación digital que utiliza cada administración tributaria de cada país basada en la encuesta.

Referencias:

- País
- Id Nacional:
  - No: la administración tributaria no está integrada a una identificación nacional.

  - Opcional: La administración tributaria está integrada a una identificación nacional. Los contribuyentes pueden utilizar la de la administración tributaria o la nacional, opcionalmente.
  - Obligatoria: La administración tributaria está integrada a una identificación nacional y su uso es obligatorio.
  - Administración tributaria es IdP: en estos casos, la administración tributaria también es un proveedor de identificación digital en el sistema o ecosistema nacional.

- Usuario:
  - PF: Persona física o natural
  - NIF: Número de identificación fiscal
  - Ambos
- Contraseña fuerte: existe una política que garantice el uso de contraseñas fuertes.
- Segundo factor de autenticación (2FA):
  - No: no existe la posibilidad de utilizar un segundo factor de autenticación.
  - Opcional: existe la posibilidad y es opcional.
  - Obligatorio: todos los accesos utilizan un segundo factor de autenticación.

País	Id Nacional	Usuario	Contraseña fuerte	Segundo factor de autenticación
Brasil	Obligatoria	PF	Si, para todos	Si, obligatorio para algunos sectores
Chile	Opcional	Ambos	Si, para todos	No
Costa Rica	No	NIF	Si, para todos	Si, obligatorio para todos
Ecuador	No	NIF	Si, para todos	Si, obligatorio para algunos sectores
España	Obligatoria AT es IdP	Ambos	Si, para todos	Si, obligatorio para todos
Guatemala	No	NIF	Si, para todos	Opcional para todos
Honduras	No	NIF	Si, para todos	No
México	No	PF	Si, para todos	Opcional para todos
Panamá	No	NIF	Si, para todos	No
Perú	No	NIF	Si, para todos	Si, obligatorio para el registro
Uruguay	Obligatoria para PF	Ambos	Si, para PF	Si, obligatorio para PF

Principales servicios de la administración tributaria: sus usos a través de canales digitales y relaciones con la identificación digital.

La siguiente tabla presenta los servicios analizados.

Servicio	Descripción
Registro en el sistema tributario	Incorporación formal del contribuyente (persona natural o jurídica) al sistema tributario mediante la asignación de un número de identificación fiscal y la definición de sus obligaciones.
Presentación de declaraciones	Remisión de información fiscal por parte del contribuyente, detallando ingresos, gastos, tributos calculados y otros datos requeridos por la normativa vigente.
Declaraciones precargadas	Formularios tributarios que incluyen información previamente completada por la administración, basada en datos disponibles, para facilitar la presentación por parte del contribuyente.
Pago de obligaciones	Cumplimiento de los compromisos fiscales mediante el abono de tributos, multas o recargos, a través de medios habilitados por la administración tributaria.
Tramitación de constancias y/o certificados	Solicitud de emisión de documentos oficiales que acreditan situaciones fiscales específicas, como inscripción, cumplimiento de obligaciones o inexistencia de deuda.
Tramitación de Acuerdos de pago	Gestión de convenios entre el contribuyente y la administración para el pago fraccionado o diferido de obligaciones tributarias.
Solicitudes de Crédito o beneficios fiscales	Presentación de requerimientos para acceder a deducciones, exoneraciones, devoluciones u otros incentivos previstos en la normativa tributaria.
Presentación de descargos y/o peticiones	Canal formal para que el contribuyente ejerza su derecho de defensa, formule observaciones o solicite actuaciones específicas ante la administración.
Comunicaciones y/o notificaciones	Envío y recepción de actos administrativos, avisos, requerimientos u otras comunicaciones oficiales entre la administración y el contribuyente.
Envío o carga de información	Transmisión de datos o documentación requerida por la administración.
Consulta de cuenta corriente/ estado de situación	Acceso al detalle actualizado de obligaciones tributarias, pagos realizados, saldos pendientes y otros movimientos registrados en la cuenta fiscal del contribuyente.
Consultas vinculantes	Solicitudes formales de interpretación de la normativa tributaria, cuya respuesta por parte de la administración genera efectos jurídicos para el solicitante.
Consultas generales	Requerimientos informativos no vinculantes sobre procedimientos, normativa o servicios ofrecidos por la administración tributaria.
Agendamiento para una cita presencial en oficina	Solicitud de turno para atención personalizada en dependencias de la administración.
Solución de controversias	Mecanismos administrativos o jurisdiccionales disponibles para resolver desacuerdos entre el contribuyente y la administración en materia tributaria.

Los canales digitales contemplados fueron:

- Web: portal web de la administración tributaria, acceso mediante explorador o *browser*.
- Móvil: aplicación móvil de la administración tributaria.
- API: Interoperabilidad entre los sistemas de la administración tributaria y otro sistema donde el contribuyente realiza el servicio (por ejemplo, otro organismo público, bancos, etc.).
- Correo electrónico: el contribuyente interactúa con la administración tributaria mediante el envío y la recepción de correos electrónicos.
- Mensajería (SMS, WhatsApp o similar): el contribuyente interactúa con la administración tributaria mediante el envío y recepción de este tipo de mensajes.
- Redes sociales: el contribuyente interactúa con la administración tributaria mediante redes sociales.

En todos los casos, se asume que también podrían existir canales presenciales. El canal Web es el más utilizado y está disponible para todos los servicios con algunas excepciones. En segundo lugar, se destaca el canal móvil, pero disponible para servicios que requieren menos información y son más simples, a través de aplicaciones móviles de la administración tributaria. A diferencia del canal web, no todos los servicios se pueden realizar a través del canal móvil y la mayoría de las administraciones tributarias carecen de aplicaciones móviles.

En tercer lugar, se distinguen dos canales: **API**, más popular en pagos de obligaciones, envío o carga de información o presentación de declaraciones, y **correo electrónico,** más orientado a comunicaciones, servicios como tramitación de constancias, comunicación y notificaciones.

En algunas administraciones tributarias todavía hay algunos servicios que carecen de canales digitales; solamente pueden ser realizados en forma presencial. Muy pocos casos utilizan para algunos servicios canales digitales novedosos como **chats** y **videollamadas**, donde un funcionario asiste al contribuyente. Casi nulo es el uso de **redes sociales** como medios para que el contribuyente interactúe con la administración tributaria.

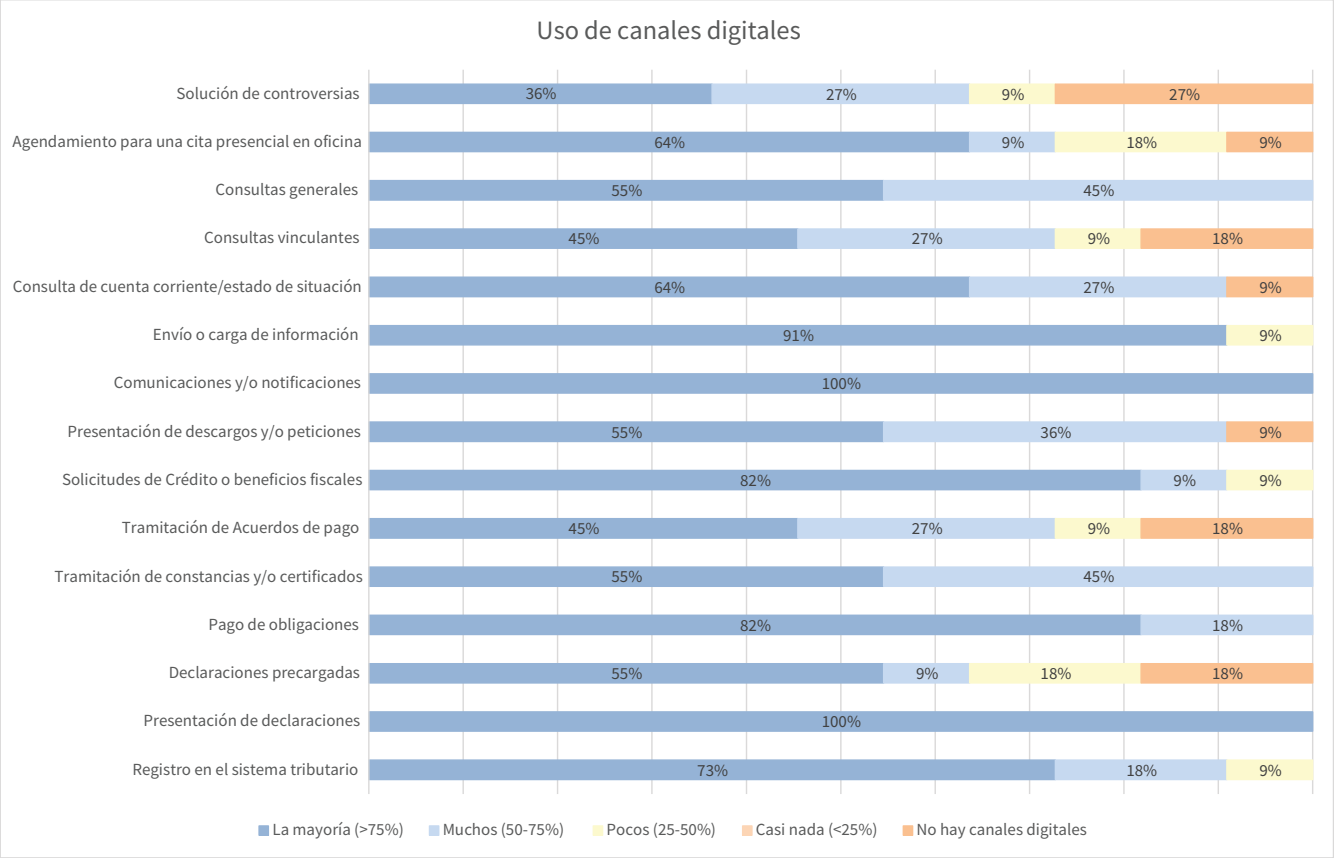
Un único país mencionó contar con un modelo multicanal desarrollado. En este caso se cuenta con una estrategia que contempla la interacción con contribuyentes a través de canales web, móviles, teléfono, videoasistencia y presencial en forma coherente, buscando ofrecer una experiencia consistente independientemente del canal.

Con respecto al uso de canales digitales, se tomó la siguiente escala:

1. No hay canales digitales disponibles.
2. Casi nada se hace por canales digitales – menos del 25%
3. Pocos se hacen por canales digitales – entre el 25% y 50%
4. Muchos se hacen por canales digitales – entre el 50% y 75%
5. La mayoría se hacen por canales digitales – más del 75%

La siguiente imagen muestra en promedio cuánto se utilizan los canales digitales por cada servicio:

Figura 6. Uso de canales digitales.



Fuente: elaboración propia en base a la encuesta de 8 países.

Si bien en todos los servicios, en promedio, predomina la opción “La mayoría (>75%)” en formato digital, todavía quedan casos en que no hay canales o se usa muy poco. Analizando estos últimos, dentro de los principales factores, tenemos que los sistemas informáticos no lo permiten o poseen limitaciones considerables. Las razones de mayor peso señaladas por los países con menor uso de canales digitales fueron la falta de presupuesto, y la falta de capacidades y la adaptación normativa que habilite y brinde confianza en los canales digitales.

En forma general, asumiendo que “la mayoría” o “muchos” representa un alto uso de canales digitales y “pocos”, “casi nada” o “no hay canales digitales”, representa un bajo uso, se puede apreciar que los servicios más digitalizados son: Consultas generales, Consulta de cuenta corriente/estado de situación, Envío o carga de información, Comunicaciones y/o notificaciones, Presentación de descargos y/o peticiones, Solicitudes de Crédito o beneficios fiscales, Tramitación de constancias y/o certificados, Registro en el sistema tributario, Pago de obligaciones y Presentación de declaraciones. En estos dos últimos casos, se destaca que la mayoría se realiza por canal digital, lo que evidencia un alto nivel de adopción tecnológica en el cumplimiento de estas dos obligaciones tributarias fundamentales.

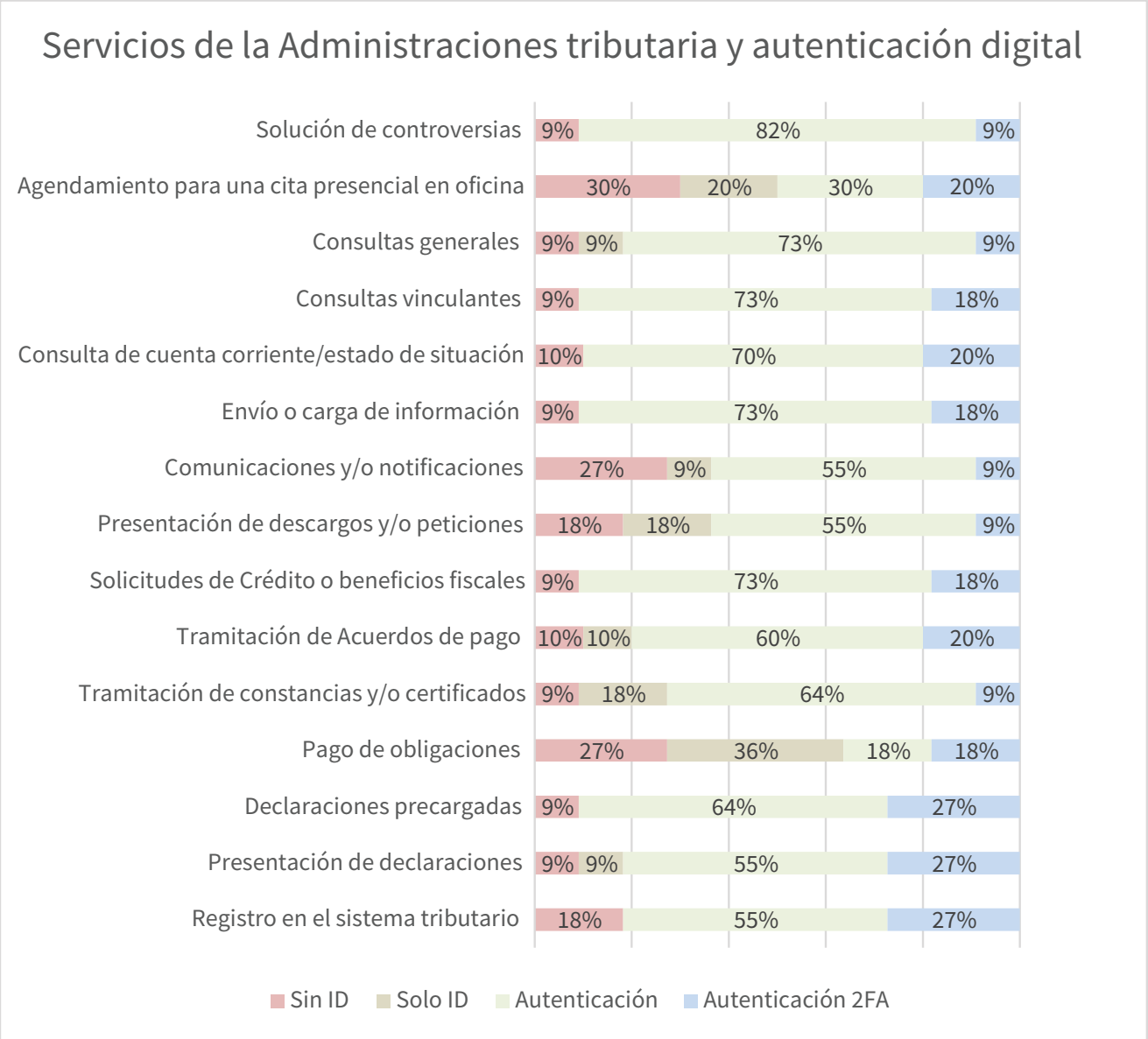
Por otro lado, los servicios menos digitalizados son: solución de controversias, tramitación de acuerdos de pago y declaraciones precargadas. La baja digitalización de los dos primeros probablemente se deba a que el canal digital aún no ofrece la fluidez ni la confiabilidad necesarias para abordar situaciones complejas vinculadas a incumplimientos tributarios, en donde se puede requerir interacción personalizada, análisis de documentación y discusiones de interpretaciones normativas. En cuanto a las declaraciones precargadas, la ausencia de un canal digital podría indicar que el servicio aún no ha sido implementado, ya que una propuesta precargada de declaración jurada es intrínsecamente digital.

Para analizar la relación entre cada servicio y la identificación se relevó si el servicio requiere o no identificación digital para poder realizarlo, con la siguiente escala:

1. No hay necesidad de identificación digital
2. Solamente se ingresa el número de identificación del contribuyente
3. Se exige autenticación
4. Además de autenticación se exige un segundo factor de autenticación

La siguiente imagen muestra para cada servicio el porcentaje en promedio del tipo de identificación digital (sin id, solo id, autenticación y 2FA).

Figura 7. Tipo de identificación digital para diferentes servicios – promedio.



Fuente: elaboración propia en base a la encuesta de 11 países.

En primer lugar, se puede concluir que hay un uso variado de la identificación digital, más allá de que sea una identificación digital o propia de la administración tributaria. Esto es porque no todos los servicios requieren necesariamente identificación digital; solamente hay una sola administración tributaria dentro de las encuestadas que utiliza identificación digital para todos los servicios. Tal como se definió en el capítulo

1, cuando se habla de identificación digital se refiere a la autenticación, es decir, el usuario se identifica y luego valida su identificación, ambos pasos son necesarios en el mundo digital. Es importante esta salvedad porque en casi todas las administraciones tributarias, muchos servicios solo requieren un identificador de contribuyente (número de contribuyente), sin verificación de la identidad. Si bien en muchos casos esto puede no ser un problema, puede ser utilizado por cibercriminales para tareas de inteligencia social, es decir, descubrir información de personas o contribuyentes, en principio "inofensiva", que pueda ser aprovechada para un fraude o ciberataque.

Con respecto a la fortaleza de la identificación digital, son pocos los casos que utilizan métodos más seguros basados en firma digital (se abordará este tema con mayor detalle en el capítulo 3), pero a su vez, estos métodos no son excluyentes, por lo que los usuarios pueden ingresar con métodos clásicos basados en el binomio usuario-contraseña. Solo hay una administración tributaria que exige un segundo factor de autenticación para todos los servicios y hay cuatro administraciones tributarias que en algunos servicios exigen un segundo factor de autenticación.

Las dos gráficas anteriores demuestran que, si bien hay un alto grado de uso de canales digitales en promedio, también hay usos heterogéneos. Esto pone de manifiesto ciertas debilidades respecto a la adopción de una visión "digital por defecto", que debería incorporar estrategias orientadas a:

- **Omnicanalidad:** fortalecer la relación entre la administración tributaria y los contribuyentes bajo un enfoque de omnicanalidad. Esto significa que todos los canales estén integrados entre sí, donde el contribuyente experimente la misma experiencia y calidad de servicio, independientemente del canal que utilice. Y en donde sea posible iniciar un proceso en un canal y continuarlo desde el mismo punto en otro canal.
- **Identificación digital:** en la mayoría de los casos, se exigen diferentes criterios para los servicios de la administración tributaria. Algunos servicios no incluyen ni siquiera un identificador; otros solicitan solo un identificador; otros exigen identificación digital y, en algunos casos, identificaciones digitales más fuertes.

2.4. Actualidad de la identificación digital en la administración tributaria de la región

El diagnóstico regional permitió identificar con mayor precisión los obstáculos que enfrentan las administraciones tributarias en la adopción de servicios digitales, particularmente en lo que respecta al

diseño, implementación y gestión de sistemas de identidad digital. Los resultados evidencian una diversidad de niveles de madurez institucional, capacidades técnicas y marcos normativos, lo que plantea desafíos concretos en términos de interoperabilidad, seguridad, inclusión y gobernanza.

Este análisis comparativo constituye una base para orientar recomendaciones diferenciadas y promover una adopción más coherente y sostenible de la identidad digital en la región durante el próximo capítulo, sentando las condiciones habilitantes para una futura integración regional.

Si bien existen diferentes realidades, la administración tributaria con respecto al desarrollo digital se encuentra inmersa en la realidad de cada país. Si bien en algunos países la administración tributaria es uno de los organismos más maduros digitalmente, en todos los casos tiene una amplia dependencia de todo el contexto nacional. La brecha digital a nivel de país impacta en el uso y aprovechamiento de los canales digitales de la administración tributaria.

Para que la administración tributaria se integre a un sistema o ecosistema de identificación digital a nivel de país, es necesario que este sistema o ecosistema exista. Para esto se necesitan políticas públicas con continuidad en el tiempo, un marco jurídico sólido, una adecuada gobernanza y articulación entre los diferentes actores involucrados – donde la administración tributaria desempeña un rol estratégico-. Además, se necesita un ecosistema digital pujante que busque sinergias entre el sector público, privado, la academia y la sociedad civil.

En definitiva, el desarrollo digital del país influye directamente en forma positiva o negativa en el desarrollo digital de la administración tributaria y, por lo tanto, sus servicios digitales se ven influenciados positiva o negativamente en función de todo el contexto.

Con respecto a la “Autorización”, también existen diferentes grados de madurez. Las administraciones tributarias que son parte de un ecosistema o sistema de identificación digital nacional han desarrollado diferentes soluciones para el control de acceso o autorización, adaptándose a un entorno donde los usuarios —ya identificados digitalmente— interactúan con múltiples servicios en línea. Esta evolución ha exigido a las administraciones tributarias abordar la gestión de roles, dado que deben vincular a personas con empresas o contribuyentes y asignarles distintos perfiles según sus funciones, responsabilidades o relaciones jurídicas. En este sentido, existen diferentes grados de avance y criterios en los casos analizados; algunos poseen una gestión de roles superficial y otros un poco más profunda, pero en casi ningún caso una gestión de roles en profundidad, alineada con una adecuada gobernanza de datos.

Las administraciones tributarias que todavía no están integradas a un sistema o ecosistema de identificación digital nacional todavía siguen gestionando la Autenticación y Autorización en forma casi unitaria, es decir, los

contribuyentes se identifican con un identificador tributario y en la mayoría de los casos poseen muy pocos roles o hasta un único rol que no distingue proceso, funcionalidad o datos.

En un mundo donde, una clara tendencia es avanzar hacia identificaciones digitales nacionales o universales, las administraciones tributarias dependen de las políticas públicas y del desarrollo del gobierno digital en cada país, pero sí está claro que deben repensar y estandarizar la Autorización bajo una moderna gestión de roles teniendo en cuenta al menos tres niveles: funcionalidades, objetos y datos, y de esa manera para prepararse para ser parte de un sistema universal de identificación digital. Se abordará este tema en mayor detalle en el siguiente capítulo.

Entre otras fuentes relevantes, el informe *Tax Administration Digitalization and Digital Transformation Initiatives* publicado por la OCDE en junio de 2025 (OCDE, 2025) ofrece estadísticas actualizadas sobre el estado de la identificación digital en las administraciones tributarias.

3. Guía de implementación y hoja de ruta

3.1. Tendencias en identificación digital

Buenas prácticas en identificación digital

Antes de desarrollar las tendencias, se resaltan algunas características de los estándares y buenas prácticas que comenzaron a surgir hace unos años en identificación digital:

- **Evitar el uso de contraseñas:** si bien las políticas de contraseñas son necesarias, su aplicación suele ser difícil de gestionar por los usuarios. Algunos métodos modernos de identificación evitan el uso de contraseñas, ya que entienden que ya no son confiables y dificultan mucho el uso de las identificaciones digitales. Existen diferentes técnicas y *malwares* en la actualidad que hacen que las contraseñas sean vulnerables, por más que se cumplan las políticas.
- **Biometría:** la alta adopción de los dispositivos móviles, así como las grandes capacidades que poseen, permite explotar de manera eficiente algunas funcionalidades al servicio del fortalecimiento de las identificaciones digitales. El uso de la cámara, el lector de huellas, la ubicación geográfica son características que el dispositivo puede aportar para fortalecer la identificación digital.
- **Custodia de credenciales por parte del usuario:** tener una base de datos centralizada con millones de credenciales de usuarios, por más que estén cifradas, representa un riesgo considerable. Los nuevos modelos están orientados a que las credenciales ya no se almacenen en los sistemas informáticos centralizados, sino en poder del usuario, en dispositivos criptográficos (tarjetas inteligentes, *token*, dispositivos móviles, etc.). Al estar distribuidas, se reducen considerablemente los riesgos asociados al robo masivo de credenciales.
- **Utilización de métodos de criptografía de clave pública:** se promueve el uso de mecanismos criptográficos robustos, especialmente aquellos basados en clave pública, en particular, la firma digital. En la publicación del CIAT, “Las TIC como Herramienta Estratégica para Potenciar la Eficiencia de las Administraciones Tributarias” (CIAT, 2020), en el capítulo 10 se abordan con mayor detalle los temas de cifrado asimétrico, firma digital y certificados de identidad digital. El desafío en estos casos es la usabilidad: lograr reducir barreras para que sean fáciles de usar por todas las personas.

- **Mayor protección de la privacidad:** con identificaciones enteramente bajo la custodia del usuario, no es fácil rastrear dónde el usuario las utiliza, o al menos no es fácil desde los sistemas de identificación; algunos exploradores y rastreadores Web pueden tener este objetivo.
- **Escalabilidad y facilidad de uso:** estos nuevos métodos están diseñados para escalar y, a su vez, ofrecer una experiencia de uso más simple y accesible para los usuarios y ciudadanos.

Muchos de los conceptos anteriores se han impulsado desde la *Fast IDentity Online* (FIDO) Alliance, junto con el *World Wide Consortium* (W3C), a través del desarrollo de un nuevo estándar abierto de autenticación fuerte sin contraseñas, llamado FIDO2. FIDO2 combina un estándar de W3C de autenticación basada en criptografía de clave pública (firma digital) con dispositivos externos, como USB, dispositivos móviles, lectores biométricos, etc., que se comunican con un explorador (*browser*) sin necesidad de ingresar contraseñas. Esto permite que un usuario utilice un dispositivo externo, bajo su custodia, para presentar sus credenciales, basadas en el uso de la firma digital para identificarse digitalmente en un sistema informático.

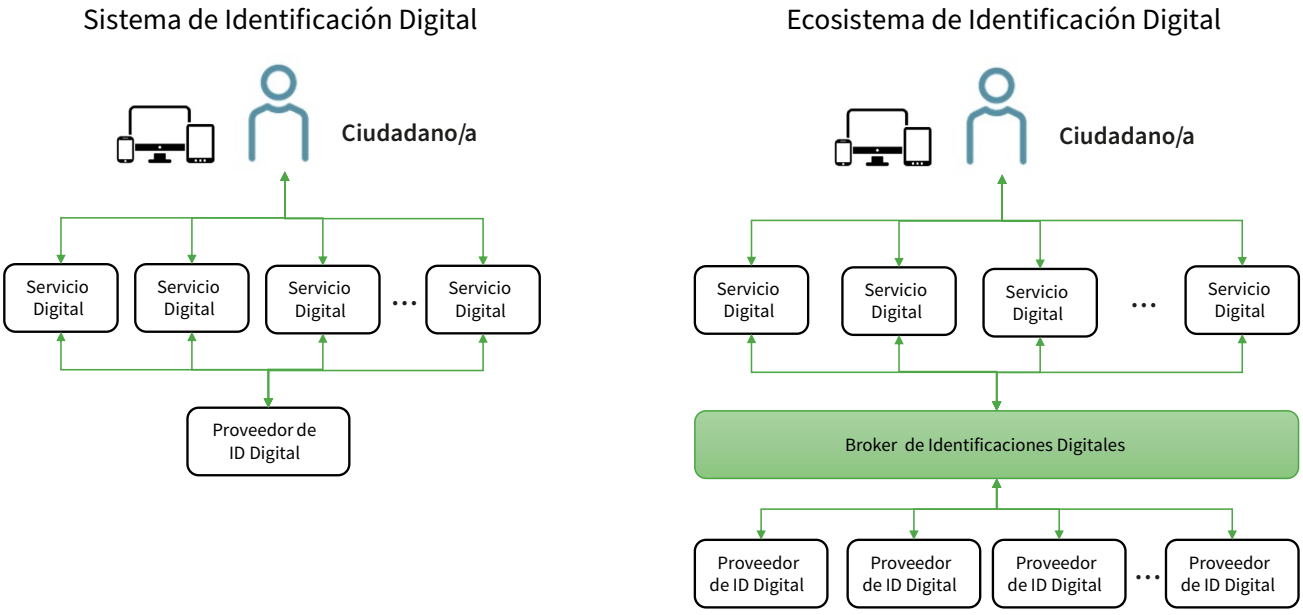
A continuación, se desarrollan las principales tendencias en cuatro dimensiones de interés.

Uso de las identificaciones digitales

El uso de la identificación digital, desde hace unos años, se está comportando tal como se comportan las identificaciones físicas desde hace muchas décadas. Las personas obtienen una identificación en una organización acreditada y confiable y la utilizan en múltiples lugares, tal como se comentó en el capítulo 1.

Esta situación lleva a la necesidad de desarrollar sistemas o ecosistemas a nivel de país, para que los proveedores de identificación digital acreditados estén disponibles para ser utilizados en los diferentes servicios digitales. La siguiente imagen compara un esquema simplificado entre un sistema (un proveedor) y un ecosistema (varios proveedores con el *broker* de identificaciones digitales como intermediario):

Figura 8. Esquema comparativo entre un sistema (un proveedor) y un ecosistema.



Fuente: Elaboración propia

En el capítulo 1 se resaltan algunas ventajas del ecosistema y el *broker* como pieza clave, a continuación, se resaltan algunos desafíos que deben ser abordados para la implementación de un sistema o ecosistema a nivel nacional:

- **Protección de la privacidad de la información**: asegurando, como mínimo, el cumplimiento de la normativa. Considerar un conjunto minimalista de información a intercambiar de cada persona (proveedor de identificación – *broker* – servicio digital). Si el sistema informático integrado luego necesita más información, deberá resolver esta situación -previo consentimiento del usuario-, interoperando con otros sistemas.

- **Regulación del *broker*:** la regulación de la existencia y funcionamiento del *broker* no solo permitiría su validación y formalización, sino que también podría constituir una estrategia clave para consolidar un ecosistema nacional de identificación digital, con participación tanto del sector público como del privado. Un *broker* en el sector público podría ser una solución para que todas las personas se identifiquen con algún proveedor en todo el sector público. Sin embargo, integrar a todo el sector privado al mismo *broker* que al sector público generaría considerables sobrecostos al sector público y un alto nivel de riesgo al centralizar toda la identificación digital del país en una sola pieza de software. Regular el *broker* puede ser una estrategia para habilitar el desarrollo de nuevos *broker* con los mismos estándares, criterios y

proveedores de identificación en el país. Esto traería la ventaja a las personas de que podrían utilizar las mismas identificaciones en todo el país, reduciendo costos y riesgos. En algunos países, luego de algunos años de discusión, se está llegando a esta conclusión.

- **Intermediación técnica:** en un ecosistema de identificaciones digitales a nivel nacional, el *broker* puede ser comparable a cómo funciona una pasarela de pagos. Una pasarela de pagos (*payment Gateway*) es una pieza de software que actúa como intermediaria entre una tienda en línea y medios de pago electrónicos. La pasarela incorpora varios métodos de pago (bancos, tarjetas de crédito, billeteras electrónicas, etc.) y se integra como servicio una sola vez a cada tienda. De esta manera, cada tienda realiza una sola integración y les ofrece a sus usuarios los métodos de pago incorporados en la pasarela. Al igual que el *broker*, la pasarela debe cumplir con determinada normativa, implementar ciertos estándares y controles de seguridad, entre otros requerimientos específicos.

Principales protocolos para sistemas y ecosistemas federados

Con el surgimiento de sistemas federados de identificación digital, grandes concentradores de credenciales -como Google, Microsoft o Apple, entre otros- comenzaron a posicionarse como proveedores de identificación. En paralelo, se desarrollaron diferentes protocolos específicos para este tipo de uso, que a continuación se describen:

- **SAML 2.0 (*Security Assertion Markup Language*):** se trata de un estándar abierto de autenticación y autorización basado en XML que permite implementar un sistema de *Single Sign-On* entre diferentes sistemas y proveedores de identificación en forma segura. Se basa en el intercambio de mensajes llamados "*assertions*" (afirmaciones), que son documentos XML firmados digitalmente que contienen información sobre la identidad del usuario. Al validar la firma de los documentos XML, todos los sistemas pueden confiar en la información que incluyen, es decir, en la identidad del usuario. Utiliza firmas sobre archivos XML y certificados X.509.

- ***Open ID Connect* (OIDC):** es un protocolo de autenticación que se desarrolló a partir de OAuth 2.0 (protocolo de autorización), extendiéndose para la autenticación. Similar a SAML, pero utilizan tokens JSON (JWT) que son formatos más livianos. Este protocolo se considera más simple y moderno que SAML; en la actualidad, es el más utilizado para estos fines.

- ***Open ID Connect for Verifiable Credentials* (OIDC4VC):** es una extensión del estándar *OpenID Connect*, diseñado para llevar la autenticación federada tradicional al mundo de la identidad digital descentralizada o credenciales verificables (se desarrolla este tema en el punto 3.2). OIDC4VC permite

utilizar una credencial en un dispositivo móvil -por ejemplo, un DNI o cédula de identidad digital en una billetera- para identificarse digitalmente en un servicio digital (web o móvil). Este estándar posee dos especificaciones complementarias:

- *Open ID Connect for Verifiable Credential Issuance* (OIDC4VCI): establece el protocolo mediante el cual un emisor —como la autoridad nacional de identificación— puede emitir una credencial verificable (por ejemplo, el documento de identidad o cédula) y transferirla directamente a la billetera electrónica de la persona en su dispositivo móvil.
- *Open ID Connect for Verifiable Presentations* (OIDC4VP): define cómo el propietario (persona) presenta una credencial (por ejemplo, DNI o cédula de identidad en su billetera digital) a un proveedor de identificación en un sistema o ecosistema de identificaciones digitales utilizado OIDC.

JSON (*JavaScript Object Notation*), al igual que XML (*eXtensible Markup Language*), definido por el *World Wide Web Consortium* (W3C), es un formato de texto diseñado para almacenar e intercambiar datos estructurados, pero mucho más liviano. Se utiliza ampliamente en aplicaciones web, móviles y APIs porque es fácil de leer por humanos y fácil de procesar por las máquinas. XML utiliza etiquetas para definir la estructura de datos (similar a HTML) y es más “descriptivo”; JSON posee una sintaxis mucho más compacta y legible.

Seguridad y confianza basada en la firma digital

El modelo basado en un binomio identificador/validador, que ha sido reforzado de diferentes formas durante las últimas décadas ya no es sostenible. Por más contraseña fuerte y factores que se posean, lo que lo hace cada vez más complejo y costoso, sigue siendo vulnerable. Si bien con una contraseña fuerte y al menos dos factores correctamente implementados, en la actualidad se sigue considerando fuerte, es inminente su obsolescencia.

Este modelo implica contar con una base de datos centralizada donde las contraseñas sean cifradas, más específicamente utilizando funciones matemáticas *hash*. Sin embargo, existen técnicas de ataque que permiten comprometer estas credenciales sin necesidad de vulnerar directamente el algoritmo de *hash*. Ejemplos de ello son los ataques por *rainbow tables*, que utilizan diccionarios precomputados de *hashes* para realizar comparaciones masivas, o los *malwares* que capturan las contraseñas antes de ser cifradas. A esto se suman vectores como la ingeniería social, que explotan el factor humano. Contar con una base de datos de millones de credenciales centralizadas, de por sí, implica un importante riesgo.

Las tendencias indican que cada vez se utilizarán más métodos de identificación digital basados en firma digital donde las claves y el certificado están descentralizados, en poder del titular. Esto daría mucha más confianza a las partes a la hora de identificarse digitalmente.

Otra forma de verlo sería la siguiente: La firma digital (dependiendo del país, podría llamarse electrónica avanzada, cualificada, certificada, etc.) posee dos propiedades:

1. Chequeo matemático de la integridad del documento firmado.
2. No repudio, es decir, quien firmó el documento no puede negarlo, lo que también se puede considerar como una identificación fehaciente de la identidad del firmante.

Estas dos propiedades basadas en el uso de criptografía asimétrica y funciones *hash* en el contexto de una infraestructura de claves públicas permiten utilizar la firma digital como un método de identificación digital totalmente confiable. Cuando un usuario firma un documento, el documento es enviado al servidor y el servidor valida la firma digital. Este proceso garantiza la integridad del contenido, asegurando que no haya sido alterado durante la transmisión, y el principio de no repudio, que confirma la identidad del firmante e impide que éste niegue su participación en la operación. Esta situación, implementada de forma que sea fácil de utilizar por el usuario, con la normativa correcta, genera diversas formas de utilizar la firma digital para identificarse digitalmente. Al finalizar este punto, con la consolidación de las tendencias, se verán algunos métodos modernos de identificación digital basados en el uso de la firma digital.

La firma digital de una persona sobre un documento se realiza en dos pasos:

1. Se calcula el *hash* del documento: esta función genera un código único de un documento (llamado *hash*) y tiene dos propiedades:
    a. Es irreversible: dado el *hash,* no existe una función inversa que genere el documento que lo originó.
    b. Es único: si se le cambia un solo carácter al documento, el nuevo *hash* va a ser diferente al anterior.
2. El *hash* del documento se encripta con la clave privada de quien firma. En este caso se utiliza criptografía asimétrica o de clave pública. En la criptografía asimétrica cada entidad posee una clave pública, que puede ser conocida por todo el mundo, y una privada (confidencial), las cuales están asociadas matemáticamente. Lo que se cifra con una se descifra únicamente con la otra. Cuando un documento se cifra con la clave privada y un tercero, utilizando su “par público”, lo descifra, puede afirmar que el cifrado se produjo con el “par privado” correspondiente a la clave pública utilizada.

    La firma digital se obtiene al encriptar el *hash* de un documento usando la clave privada de la persona. Esto permite vincular de forma segura a esa persona con el documento que generó el *hash*.

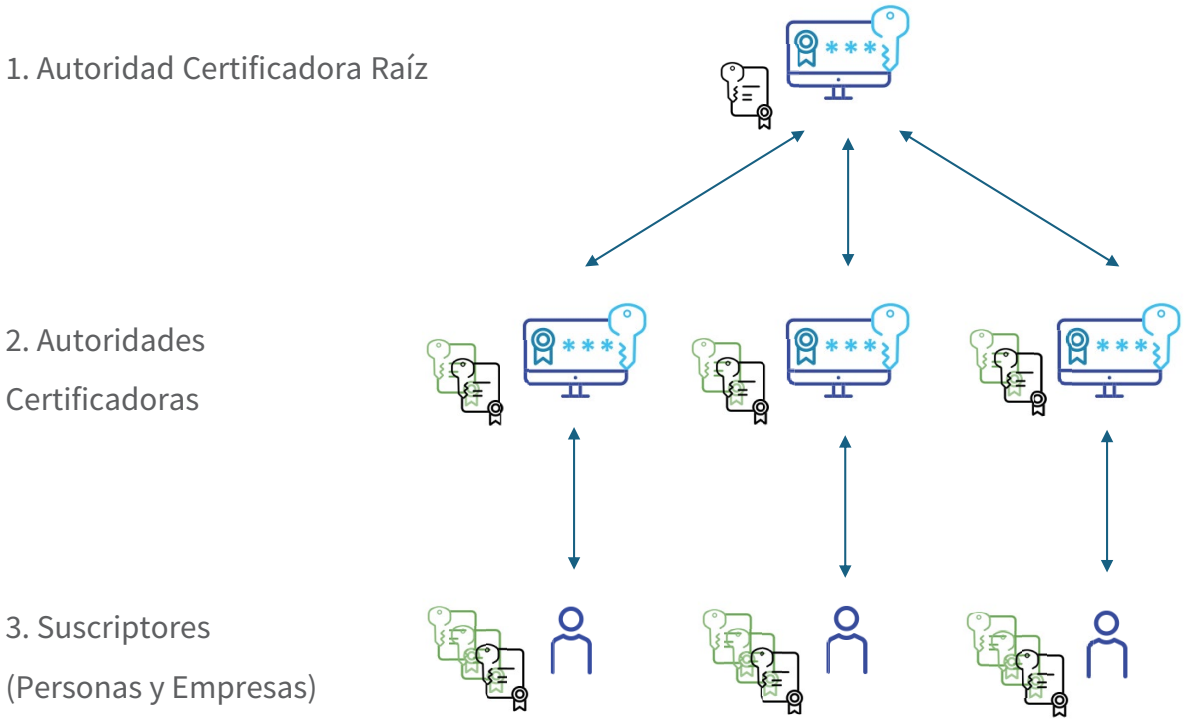
Cuando una firma es electrónica avanzada, cualificada o certificada (dependiendo del país), quiere decir que se realizó un proceso de verificación de la identidad del firmante por parte de una autoridad certificadora. La normativa moderna, la de la mayoría de los países de la región, exige dos características relevantes con respecto a las claves otorgadas a la persona:

- **Clave privada:** debe residir en un dispositivo criptográfico y nunca salir de él; además, el mismo debe estar protegido con un *pin* o contraseña como mínimo. Un dispositivo criptográfico puede ser un token, una tarjeta inteligente (muchas veces además utilizada como documento de identificación nacional), un dispositivo móvil o un HSM (*Hardware Security Module*), que es un dispositivo físico diseñado específicamente para proteger, gestionar y ejecutar operaciones criptográficas.
- **Clave pública:** debe estar en un certificado digital en formato X.509. Este es un documento electrónico estandarizado que sirve para vincular de forma segura una identidad (persona, empresa o servidor) con una clave pública. Este certificado es otorgado y firmado por la autoridad certificadora, por lo que la firma de la autoridad certificadora protege la integridad del certificado y a la vez le da validez, ya que demuestra que fue otorgado por una autoridad certificadora habilitada.

Los dos puntos anteriores son críticos ya que se puede asegurar ante un documento firmado que la clave privada utilizada nunca salió de un dispositivo criptográfico y, en caso de validar la firma, la clave pública utilizada está vinculada a determinada persona, especificada en el certificado digital correspondiente. La Autoridad Certificadora que emitió y firmó el certificado da garantías de esto.

Una infraestructura de claves públicas (PKI, *Public Key Infrastructure*) es un conjunto de tecnologías, políticas, entidades y procedimientos que permiten emitir, gestionar, distribuir y revocar certificados digitales y claves criptográficas de manera segura y confiable. Se trata de una estructura jerárquica en forma de árbol que puede tener varios niveles. Muchas veces hay una raíz, pero no es absolutamente necesaria. El siguiente esquema ilustra un ejemplo de PKI de tres niveles:

Figura 9. Esquema PKI de tres niveles.



Fuente: Elaboración propia

Las Autoridades Certificadoras “padres” firman los certificados de las Autoridades Certificadoras “hijas” una vez estas sean reconocidas por la normativa y así sucesivamente. Las personas obtienen sus claves y certificados en una Autoridad Certificadora habilitada, conservando en su poder la clave privada, que suele almacenarse de forma segura en un dispositivo criptográfico.

Cada nivel superior firma el certificado del nivel siguiente inferior y, de esta manera, se crea lo que se conoce como cadena de confianza. El certificado con la identidad y la clave pública de una persona es el último eslabón de una cadena de confianza que asegura la integridad e identidad de cada eslabón, al validar las firmas de forma matemática.

La lista de confianza de un país, en el caso de la firma electrónica avanzada (cualificada o certificada) es la lista de todos los certificados de todas sus Autoridades Certificadoras habilitadas por la normativa del país. La lista de confianza es un elemento clave para validar la firma de una persona sobre un documento y permite determinar cuándo es avanzada y, por lo tanto, hay garantías de la identidad del firmante.

Los certificados se pueden revocar ante la pérdida de confianza de una clave privada, por ejemplo, cuando una persona pierde su dispositivo criptográfico. Cada Autoridad Certificadora posee una lista de revocación con los certificados que ha revocado. Este es otro elemento clave para validar una firma: una firma es válida si el certificado que se utilizó para verificarla no está revocado o si la firma fue realizada antes de su fecha de revocación.

El capítulo 10 de la publicación del CIAT *"Las TIC como Herramienta Estratégica para Potenciar la Eficiencia de las Administraciones tributarias"* (CIAT, 2020) profundiza en los aspectos vinculados a la confianza en la firma digital y el rol de las infraestructuras de claves públicas (PKI).

En resumen, la firma digital puede utilizarse como forma de identificación digital y es un método sumamente confiable; la confianza está dada por la infraestructura de claves públicas que sostiene la firma digital.

Tecnologías

Métodos biométricos

En el primer capítulo se desarrollaron métodos biométricos, principalmente faciales y dactilares. Estos métodos están siendo ampliamente utilizados dada la amplia adopción de los dispositivos móviles inteligentes y la facilidad de uso. Si bien las herramientas biométricas para validar identidades han logrado un muy buen nivel de madurez, hay dos temas a considerar, en lo relativo a la biometría facial, para que sean confiables:

1. Previo a la foto, debe utilizarse un sistema de prueba de vida reconocido, para asegurarse de que la fotografía tomada por el usuario sea tomada a una persona viva – y no a la fotografía de una persona, por ejemplo-. Existen varios reconocidos en el mercado y muy buenas tasas de efectividad. También hay estándares y certificaciones que aseguran determinados niveles de confianza, pero generan costos importantes. Esto asegura que la fotografía sea tomada a una persona viva; sin esta herramienta, estos sistemas no son tan seguros.
2. La imagen facial tomada a la persona debería ser comparada con el registro público y no depender del documento que suba la persona a la aplicación ya que eso implicaría menos seguridad. Para esto es necesario que el registro público posea esta capacidad desarrollada. En este caso, resulta fundamental que la imagen sea recibida directamente por el registro público y que la comparación biométrica se realice en sus propios sistemas. Este enfoque garantiza que la imagen no sea transferida a terceros, preservando

así la privacidad del titular. En muchos casos, esta comparación se realiza con un documento que el usuario proporciona y no contra el registro público, y en otros casos, la comparación se realiza fuera del registro, por lo que no es la mejor situación desde el punto de vista de la privacidad de la información. Bajo estas condiciones, no puede garantizarse que las imágenes provenientes del registro público no sean almacenadas ni procesadas fuera de sus sistemas, lo que incrementa los riesgos asociados a la protección de datos personales.

Otros métodos biométricos, como el escaneo del iris, si bien son muy confiables y precisos, es utilizado en casos puntuales dada la forma de uso que resulta invasiva y genera fuertes fricciones para el uso masivo.

La biometría también presenta desafíos importantes. A diferencia de las contraseñas, los datos biométricos utilizados para validar la identidad —como el rostro o la huella digital— no pueden ser modificados fácilmente por la persona. En caso de sufrir un accidente, una alteración física o envejecimiento, estos datos podrían no ser reconocidos correctamente, dificultando el acceso.

En la actualidad, los avances en Inteligencia Artificial y en particular el *deepfake* (video, audio o imagen en el que la IA hace que parezca que una persona dijo o hizo algo que en realidad nunca ocurrió) representan una verdadera amenaza para la biometría, dado que es probable que en poco tiempo ya no sea confiable una prueba de vida o una comparación biométrica facial, al menos bajo las tecnologías y técnicas actuales.

Chip RFID

Actualmente hay muchos documentos de identificación nacional, así como pasaportes que poseen un chip RFID sin contacto, según el estándar ICAO (*International Civil Aviation* Organization, Organización Internacional de Aviación Civil). ICAO estableció estándares para pasaportes electrónicos donde el chip debe contener información estructurada y estandarizada sobre la identidad de la persona (los mismos datos impresos, por ejemplo, en el pasaporte), la clave pública del país emisor y la firma de la autoridad de dicho país. Esto forma parte de una Infraestructura de Claves Públicas global, y la clave pública del país es parte de la lista de confianza de esta PKI, en ICAO llamada *Public Key Directory* (PKD). La firma en el certificado asegura la integridad y la identidad de la autoridad emisora del país.

El chip RFID puede leerse por NFC (*Near Field Communication*), una tecnología de comunicación inalámbrica de corto alcance que permite intercambiar datos entre dos dispositivos simplemente acercándolos, normalmente a menos de 10 cm de distancia. Actualmente, no solo los lectores de aeropuertos tienen esta tecnología, sino que también múltiples dispositivos, entre ellos muchos teléfonos móviles.

Según *ICT indicators for the SDGs* del *International Telecommunication Union (ITU)*, Naciones Unidas, en 2024 el 80% de la población mayor o igual a 10 años posee al menos un teléfono celular en el mundo. Un reporte no tan reconocido, *NFC-enabled handsets market* de *Verified Market Reports,* señaló que cerca del 80% de los celulares inteligentes vendidos en 2023 contaban con tecnología NFC. Si bien estas cifras son estimadas y varían por región (América Latina y el Caribe están por encima de la media mundial en personas con teléfonos móviles, según ITU), de todas formas, hay una gran cantidad de personas con dispositivos móviles con NFC. Es una tecnología ampliamente extendida, confiable y simple que se utiliza muy poco para las posibilidades que brinda. Estos sistemas están ampliamente utilizados en fronteras, como aeropuertos, pero no tanto para la autenticación en el mundo web o en dispositivos móviles.

Los países que tienen cédulas de identidad con chip podrían implementar una aplicación móvil que permita a los usuarios que poseen teléfonos móviles con NFC aproximar sus documentos físicos al dispositivo e identificarse digitalmente en un servicio digital utilizando la aplicación móvil como medio entre el documento de identidad físico y el servicio digital. Se trata de un método seguro, basado en el uso de la firma digital (no de la firma de persona física o natural, pero sí de una PKI reconocida), con credenciales distribuidas y protegidas por dispositivos criptográficos (tarjetas inteligentes).

Todos estos estándares son abiertos y conocidos, por lo que podría ser de interés y alto impacto para los países de la región, sobre todo los que poseen documentos de identidad con chip, al menos en parte de la población, desarrollar métodos utilizando estas formas de identificación digital y beneficiar a todo el ecosistema, a las administraciones tributarias y a otros interesados.

3.2. Nuevos modelos de identificación digital

Basados en las tendencias del punto anterior, teniendo en cuenta los principales estándares y buenas prácticas promovidas por las organizaciones más reconocidas en la temática, a continuación, se presentan los nuevos métodos de identificación digital.

Firma digital en la nube para la identificación digital

Los certificados y claves en dispositivos criptográficos en poder del usuario poseen algunas fricciones en su uso. Las tarjetas inteligentes (documentos de identificación) necesitan un lector, es decir, un dispositivo físico en el que se introducen y se conectan a la computadora mediante USB. Para utilizar tarjetas y tokens es necesario instalar *drivers* del fabricante, lo que genera costos y alta dependencia del país con el fabricante, así

como programas específicos que pueden generar diversos problemas: permisos del usuario para instalarlos, conflictos con el sistema operativo o componentes, conflictos con los exploradores o, inclusive, si no son descargados del lugar incorrecto podrían hasta incluir *malwares* como troyanos, entre otros.

Esto genera barreras para que sean utilizados de forma masiva, llegando a todos los públicos. Además, no es posible -o sumamente complejo- utilizarlos en teléfonos móviles; sus interfaces físicas generalmente son USB y los controladores no están desarrollados para Android o iOS.

Desde hace varios años, comenzaron a popularizarse los servicios de firma digital de custodia centralizada. En este caso, un prestador de firma, en lugar de otorgar las credenciales y el certificado a una persona en un dispositivo criptográfico externo (token o tarjeta inteligente), lo genera y lo almacena en una zona exclusiva del titular en un HSM (*Hardware Security Module*). Eso es un almacenamiento mucho más grande en capacidad, y además con controles criptográficos sumamente fuertes, donde cada usuario posee sus claves y certificado en forma exclusiva y el proveedor lo custodia.

Esta firma digital “en la nube” también puede utilizarse para la identificación digital, tal como la firma en un dispositivo criptográfico en poder del usuario, pero con menores fricciones. No se necesita un lector, no se necesitan controladores y se puede utilizar desde el dispositivo móvil. El proveedor de firma también actúa como proveedor de identificación digital. En este caso, si bien las claves y certificados están centralizados -en la nube del proveedor-, las características y fortalezas de los HSM garantizan la independencia de las claves y otorgan un nivel de seguridad superior al de una base de datos con usuarios y contraseñas cifradas.

Un estándar muy utilizado en dispositivos criptográficos es el *Federal Information Processing Standard* (FIPS), actualmente en la versión 3 desde 2020, emitido por el NIST (*National Institute of Standards and Technology*, Estados Unidos). El objetivo de FIPS es garantizar que cualquier hardware o software que realice operaciones criptográficas cumpla con un nivel verificable de protección frente a ataques físicos y lógicos. Las Autoridades Certificadoras que gestionan claves en la nube generalmente utilizan, como mínimo, *Hardware Security Modules* (HSM) FIPS 2 y FIPS 3. Los FIPS 3 garantizan, entre otras cosas, que las claves privadas nunca puedan ser extraídas en texto plano y poseen un diseño físico con sellos, sensores anti-intrusión, blindaje electromagnético que ante una intromisión no autorizada destruye, automáticamente la información.

Los métodos de identificación digital basados en firmas en la nube ya están operativos en varios países de la región. Dado que la clave privada del usuario permanece resguardada en el módulo de seguridad hardware (HSM) del proveedor y nunca se expone, resulta indispensable establecer conexiones seguras entre los servicios digitales del ecosistema y dicho proveedor. En este contexto, **la incorporación de un *broker* de identificaciones digitales como componente central de un ecosistema nacional es clave** ya que permite

realizar una única integración con el proveedor de identidad, habilitando así el uso transversal de este mecanismo en múltiples servicios públicos digitales, sin necesidad de desarrollar integraciones individuales para cada uno.

Identidad digital autogestionada, credenciales verificables y billeteras digitales

En los últimos años se ha venido desarrollando un conjunto de estándares, protocolos y tecnologías que buscan ofrecer un nuevo concepto de identidad digital en el cual se otorga al individuo un control total sobre su persona digital. Este nuevo modelo de identidad se conoce como identidad digital autogestionada o autosoberana e incorpora dos elementos tecnológicos innovadores: las billeteras digitales y los registros descentralizados de información.

Estos son modelos en los cuales la identidad no está en posesión de un tercero, o en un prestador de servicios de identificación, sino que se reconoce que un individuo debe poseer y controlar su identidad sin la intervención de las autoridades administrativas

En 2016, Christopher Allen estableció los 10 principios de la identidad autogestionada. Dichos principios son:

- Acceso: los usuarios deben tener acceso a sus propios datos.
- Consentimiento: los usuarios deben aceptar previamente el uso de su identidad por parte de terceros.
- Control: los usuarios deben poder controlar sus identidades.
- Existencia: los usuarios deben tener una existencia independiente.
- Interoperabilidad: las identidades deben poder utilizarse ampliamente.
- Minimización: la divulgación de reclamaciones debe reducirse.
- Persistencia: las identidades deben ser duraderas.
- Protección: los derechos de los usuarios deben ser protegidos.
- Portabilidad: la información y los servicios de identidad deben ser portables.
- Transparencia: los sistemas y algoritmos deben ser transparentes.

Una de las formas de materializar este concepto es a través de las billeteras digitales, repositorios privados, por ejemplo, en una aplicación móvil, que permitan a las personas manejar todos sus activos digitales con

completa autonomía y privacidad. Se podría tener acceso rápido a versiones digitales de documentos de identidad, diplomas universitarios, libretas de conducir, etc.

Esta modalidad ya ha sido habilitada en la Unión Europea con la aprobación del eIDAS 2.0 y la regulación de la denominada Cartera de Identidad Digital Europea (EUDI *Wallet*).

Conceptos y fundamentos de las credenciales verificables

Las credenciales verificables son una forma digital, segura y estandarizada de representar información sobre una persona, organización o entidad, de manera que pueda ser verificada por un tercero criptográficamente, sin depender de una autoridad central en cada verificación. En el mundo físico desde hace varias décadas existe la costumbre de gestionar diversos tipos de credenciales físicas, como, por ejemplo:

- Identidad: credenciales que prueban quiénes somos, como el documento nacional de identificación, la cédula de identidad, el pasaporte y la licencia de conducir (en algunos casos).
- Académicas y profesionales: diplomas universitarios, certificados internacionales, certificados de idiomas, constancias de empleos, etc.
- De salud: carné de vacunación, certificado médico, resultado de pruebas de laboratorio, etc.
- Financieras o de cumplimiento: prueba de identidad, verificación de solvencia o de afiliación bancaria, historial o certificado de cumplimiento tributario, entre otras.
- De membresía o acceso: acreditaciones para ingresar a un club, edificio o evento; credencial de oficial de policía o de inspector de tránsito; o de miembro de alguna organización.

Existen muchos tipos de credenciales, pero también diferentes niveles de alcance. Por ejemplo, un pasaporte es una credencial de identidad de nivel global, pero el carné de membresía del gimnasio solamente es reconocido en el gimnasio.

También se pueden abordar desde el punto de vista del nivel de confianza, en este sentido se pueden catalogar en tres niveles:

- Bajo: información autodeclarada por el titular, por ejemplo, una cuenta en una red social.
- Medio: información verificada por una entidad, por ejemplo, un número de teléfono o un documento.

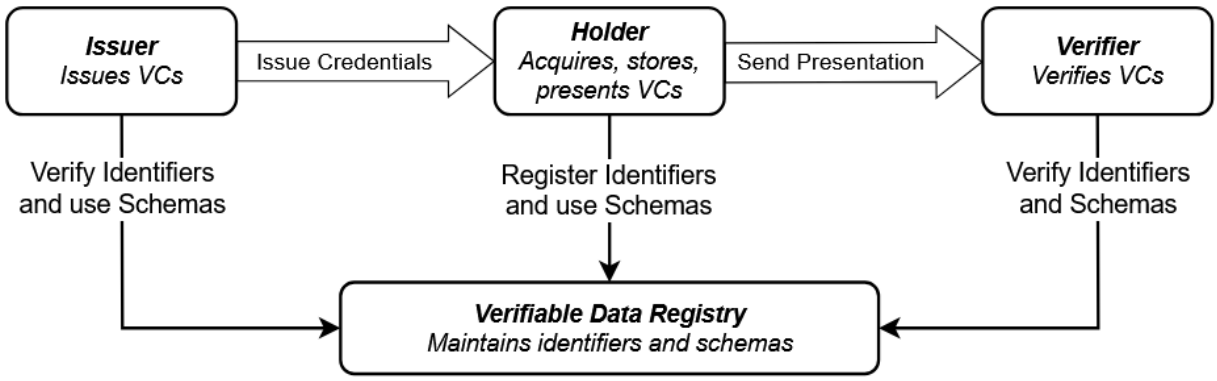
- Alto: credencial verificada presencialmente o mediante tecnologías acordes (firma digital, chip NFC, biometría que cumple determinados requerimientos). En esta categoría están las credenciales, como los documentos de identidad nacional, pasaportes, licencias de conducir, etc.

Estándares y protocolos relevantes

Si bien las credenciales verificables es un tema que se viene desarrollando desde hace unos años, en la actualidad hay algunos estándares que aparentemente están prevaleciendo dado que son los que poseen una comunidad más amplia para su desarrollo y evolución, están patrocinados por organizaciones relevantes y son los que se están adoptando en un número cada más más grande de países.

W3C Verifiable Credentials Data Model 2.0 (VCDM 2.0) es el estándar internacional más importante para representar identidades digitales y credenciales verificables en la web. Es desarrollado por el *World Wide Web Consortium* (W3C), el mismo organismo que define los estándares de Internet (como HTML, CSS, etc.). El siguiente esquema ilustra este estándar:

Figura 10. Diagrama del estándar W3C VCDM 2.



Nota: Adaptado de *Verifiable Credentials Data Model v2.0*, por Sporny, Longley y Lindström (2023). Recuperado de [URL].

Este estándar se focaliza en definir los actores involucrados en este ecosistema para crear, emitir, compartir y verificar credenciales de forma segura e interoperable y protegiendo la privacidad de la información y una gran nomenclatura.

Está basado en los siguientes principios:

- Descentralización: no depende de una autoridad centralizada o base de datos única;
- Verificabilidad: cualquiera puede comprobar la autenticidad de una credencial sin contactar al emisor;
- Portabilidad: el usuario guarda las credenciales en su propio dispositivo (billetera);
- Privacidad selectiva: el titular puede elegir qué datos compartir;
- Interoperabilidad: compatible con otros estándares reconocidos como DID, JSON-LD, JWT y OIDC4VC.

Se trata de un estándar que está prevaleciendo para definir todo el ecosistema a nivel de país de credenciales verificables. La Unión Europea y la mayoría de sus países lo están adoptando; Estados Unidos y Canadá, Australia, Japón y Corea del Sur y en América Latina y el Caribe, los países que poseen iniciativas al respecto han definido este estándar como base para su ecosistema. Dentro de estos países, el grado de madurez y avance es variable; algunos países han tomado la decisión, otros están comenzando con el desarrollo y otros ya poseen algunas credenciales sobre la versión 1.0, por lo que están en transición. La versión actual, 2.0 es de mayo de 2025.

Otro grupo de estándares que está predominando es *OpenID Foundation*, que se focaliza mayoritariamente en protocolos para el intercambio, como *OpenID Connect for Verifiable Credentials* (extensión de *OpenID Connect*) en sus dos posibilidades: OIDC4VCI para que el emisor transfiera la credencial al titular y OIDC4VP para que el titular la presente para identificarse presencial o digitalmente.

La otra gran familia es la ISO/IEC 18013-5, que define específicamente algunas credenciales de identificación, como la de identificación nacional y la licencia de conducir. Este estándar está siendo adoptado por la Unión Europea, Estados Unidos, Australia y algunos países de América Latina y el Caribe han manifestado interés.

Adicionalmente hay estándares específicos como DID (*Decentralized Identifiers*) de *World Wide Web Consortium* (W3C) que define identificadores globales, verificables y descentralizados y la especificación *DID Resolution & DID Document* que describe cómo resolver un DID para obtener las claves públicas y metadatos, así como otros específicos que definen los detalles de las firmas digitales sobre las credenciales y otros temas relevantes de seguridad.

Ecosistema operativo – Actores y flujo de credenciales verificables

Estas credenciales físicas, que se utilizan naturalmente desde hace décadas, es el mismo concepto que las credenciales verificables actuales del mundo digital. Independientemente de su tipo o nivel de confianza, los

actores involucrados en un ecosistema de credenciales verificables son los siguientes (también aplica para las credenciales físicas):

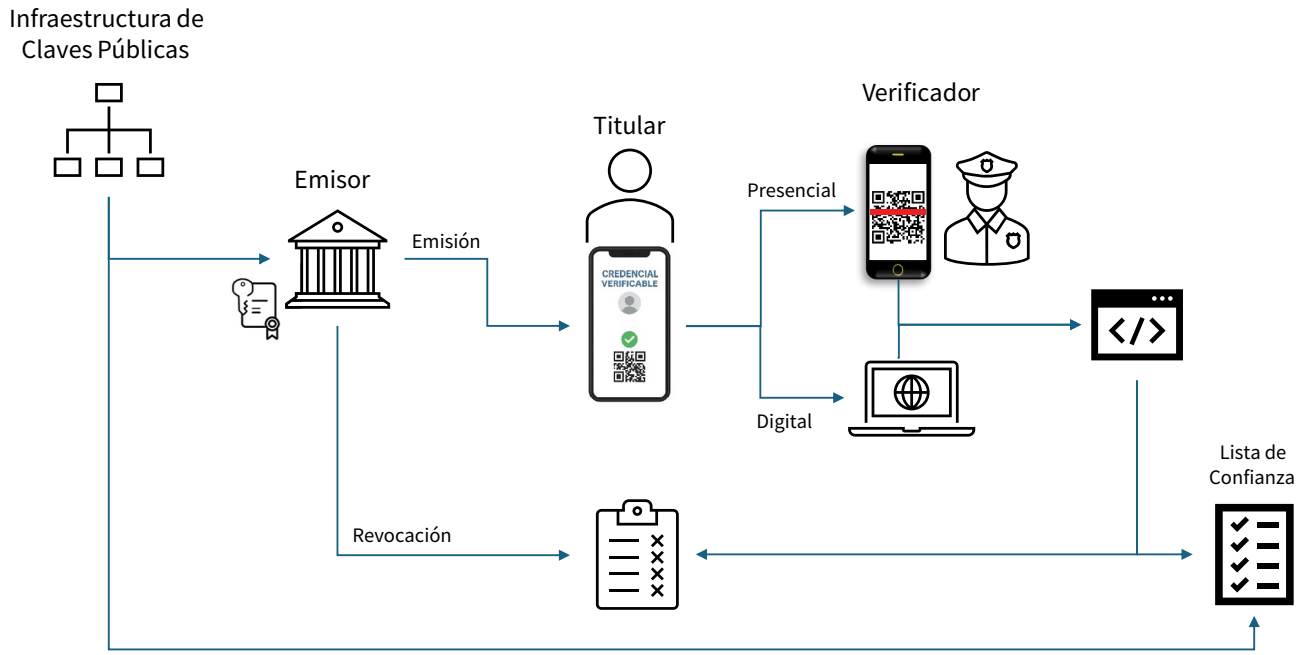
- Emisor (*Issuer*): entidad competente por normativa que emite credenciales de determinado tipo. Esta entidad es reconocida como de confianza para el ecosistema para determinada credencial, independientemente del alcance (organismo de identificación civil tiene un alcance país o global en el caso del pasaporte, club deportivo se limita a sus instalaciones). El emisor firma la credencial, lo que da garantías al verificador de que toda la información que contiene la credencial es confiable. La firma puede variar en función de la credencial, su ecosistema y su criticidad. Una credencial de identidad debe estar firmada con la firma digital (avanzada, cualificada o certificada) de la autoridad competente, como parte de una Infraestructura Nacional de Claves Públicas. Una credencial de acceso a un gimnasio puede estar firmada con una firma simple del gimnasio, pero reconocida como de confianza en las instalaciones del gimnasio. Los emisores, además, pueden revocar credenciales en función de la normativa aplicable a cada credencial (algunas pueden no ser revocables).

- Titular (*holder*): Persona que posee la credencial en su billetera electrónica, generalmente en su teléfono móvil, y decide cuándo y con quién compartirla. El titular puede mostrarla presencialmente en su dispositivo, en formato gráfico (legible para el ser humano, pero de menor confianza), en formato QR (legible para un validador, donde, además, el QR está firmado por lo que garantiza su contenido) o utilizarla para identificarse digitalmente (autenticarse) en un servicio digital web o móvil mediante el protocolo OIDC4VP.

- Verificador (*verifier*): quien recibe y valida la credencial. Esto depende del alcance de la credencial, puede ser un oficial de policía ante una credencial de identidad o un portero en un edificio ante una credencial de acceso. Esto puede hacerse más o menos automatizado y la información que presenta el titular puede ser mínima o más ampliada. El verificador, entre otros, debe contar con la lista de confianza (certificados de Emisores) del ecosistema para poder validar las firmas de las credenciales verificables y, de esta forma, confiar en la información de su contenido. Otro tema que debe revisar el validador es la revocación.

El siguiente esquema muestra en forma simplificada un ecosistema de credenciales verificables:

Figura 11. Ecosistema de credenciales verificables.



Fuente: Elaboración propia

Los pasos para el funcionamiento del ecosistema son los siguientes:

1. El emisor (por ejemplo, el registro civil para el documento de identidad nacional) obtiene un par de claves y un certificado de la Infraestructura Nacional de Claves Públicas para firmar las credenciales que emita. Esta firma es similar a la firma o sello de persona jurídica o empresa que se utiliza para la facturación electrónica. En el caso de la facturación electrónica, la empresa que va a emitir facturas obtiene las claves y el certificado para firmar las facturas. Cuando emite una factura, la misma es firmada por la empresa y esto garantiza la integridad del documento (factura) y la identificación del firmante, el certificado otorgado por el prestador vincula el número o identificador tributario de la empresa con su clave pública.
2. El certificado otorgado al emisor es dado de alta en la lista de confianza de emisores habilitados.
3. Una persona (titular) que desea obtener su credencial acude al emisor (o lo realiza en forma remota con las debidas comprobaciones, en función de la criticidad de la credencial), el emisor emite y firma la credencial y se la transfiere a la billetera electrónica en el dispositivo móvil de la persona. Para transferirla, utiliza el protocolo OIDC4VCI.

4. El titular gestiona su credencial en la billetera en el teléfono móvil. Para esto, cada credencial puede contar con diferentes requerimientos con respecto a la autenticación en la billetera, las características del dispositivo móvil, entre otros. El titular decide identificarse utilizando la credencial en forma presencial o digital:

    a. Presencial legible por máquina: una persona (por ejemplo, agente) solicita al titular que se identifique utilizando su credencial verificable:

        i. El Agente, utilizando un validador compatible y reconocido en su dispositivo móvil, despliega un código QR dinámico firmado por el validador.

        ii. El titular aproxima su dispositivo móvil, lee el código QR con la billetera y la misma solicita permiso para compartir determinada credencial con el validador. En algunos casos, además, estas credenciales pueden ser minimalistas, protegiendo la privacidad de la información (por ejemplo, si tiene que demostrar que es mayor de edad, solo alcanza con transferir esta información y no la fecha de nacimiento, nacionalidad, nombres, apellidos, etc.).

        iii. El titular aprueba y la billetera le envía la credencial al validador. Esta transmisión se puede realizar con diferentes tecnologías inalámbricas de aproximación como NFC o *Bluetooth.*

        iv. El validador recibe la credencial y valida la firma de quien emitió la credencial (emisor). Para esto utiliza la lista de confianza del ecosistema y la lista de revocación. Ambas listas pueden estar cargadas localmente en el validador y actualizarse cada vez que el mismo cuente con conexión.

        v. En caso de que el formato sea correcto y la firma también, despliega en pantalla la información de la credencial. La validación se puede realizar de forma 100% local y sin conexión, con total confianza, basada en la firma del emisor en el contexto de la Infraestructura Nacional de Claves Públicas. Una variante, aunque requiere conexión, es que el QR del validador posea un *Uniform Resource Identifier* (URI, *endpoint*) dinámica a donde sea enviada la credencial por parte de la billetera.

    b. Presencial legible por humano: el titular despliega la credencial en forma gráfica en la pantalla del dispositivo móvil, tal como sucede hoy en día al mostrar el plástico en el caso del DNI o cédula de identidad.

    c. Digital: el titular desea ingresar a un portal o servicio web o móvil (por ejemplo, a la administración tributaria) y selecciona la opción para Identificarse con una credencial verificable en el sistema de autenticación. El sistema de identificación digital posee implementado el protocolo OIDC4VP:

i. Al seleccionar esta opción, el sistema web genera un código QR dinámico donde está la información de un *endpoint* (URI) en el servidor a donde la billetera debe enviar la presentación verificable.

ii. La billetera lee el código QR del portal (por ejemplo, de la administración tributaria) y solicita permiso al titular para enviarle credenciales. En este caso, además, el titular puede personalizar la información que desea compartir con el portal, que debe ser necesaria y suficiente para Identificarse.

iii. La billetera arma una verificación presentable; esto es, un conjunto de credenciales verificables bajo una única presentación armada para este caso firma la presentación y la envía junto a su clave pública (de la billetera) al *endpoint* del portal.

iv. El *endpoint* del portal recibe la verificación presentable y, con la clave pública válida, la firma para garantizar la integridad. A continuación, valida cada credencial verificable incluida en la verificación presentable. Cada credencial está firmada por su correspondiente emisor (reconocido por la lista de confianza). También valida la revocación y, en caso de que todo sea correcto, utiliza la información de las credenciales transferidas para identificar al usuario (titular).

5. Dependiendo de la normativa asociada a cada credencial, el emisor puede revocar una credencial dándola de alta en la lista de revocación. Generalmente, esto puede ocurrir por decisión del emisor, solicitud del titular o de un tercero, como, por ejemplo, de un juez.

Ventajas de las credenciales verificables e implicancias para la administración tributaria

Esta forma de identificarse presencial y digitalmente ha tomado mucha relevancia en los últimos años por múltiples razones y se está convirtiendo en el nuevo método de identificación presencial y digital a nivel mundial ya que posee múltiples ventajas:

- La misma credencial utilizada en el mundo digital y presencial, simple y natural de usar para las personas, de la misma forma en que se obtienen y utilizan las físicas desde hace muchas décadas.
- En algunos casos, las credenciales de identificación son equivalentes jurídicamente a sus pares físicos (DNI, cédula de identidad, pasaporte, licencia de conducir, etc.), lo que les otorga total confianza a las credenciales verificables.
- Alta adopción de dispositivos móviles inteligentes en todo el mundo, por lo que no hay grandes barreras para portarlos y utilizarlos.

- Alto nivel de confianza, las firmas digitales involucradas, si se cumplen los estándares reconocidos actuales y la normativa asociada a la Infraestructura Nacional de Claves Públicas no son posibles de falsificar o adulterar. Inclusive más confiables que sus pares físicos.

Con respecto al uso para la identificación digital (autenticación), este novedoso sistema posee múltiples ventajas:

- Credenciales distribuidas y claves privadas permanecen protegidas en dispositivos criptográficos; nunca salen de ellos. Las credenciales y, especialmente, la clave pública, están distribuidas y en total control de su titular. Esto evita contar con bases de datos con millones de credenciales centralizadas, que por más que estén cifradas (*hash* de contraseña), el hecho de que estén centralizadas ya de por sí es un riesgo considerable.
- Credenciales basadas en el uso de firma digital y sin contraseñas, tal como sugieren las tendencias en la materia, pero reduciendo considerablemente la fricción (barreras) que poseen los métodos de identificación digital basadas en firmas digitales en otros dispositivos criptográficos (tarjetas inteligentes o tokens). Inclusive reducen más aún las barreras generadas por los casos de uso de firma en la nube para la identificación.
- Fáciles de utilizar. La alta penetración de dispositivos móviles ha logrado que sea muy simple e intuitivo para las personas instalar y utilizar aplicaciones móviles, utilizar métodos de transferencia de información por proximidad (NFC o *Bluetooth*) y leer códigos QR, entre otros.
- No es necesario contar con actores de tarjetas inteligentes, programas específicos ni controladores que puedan generar problemas de permisos o compatibilidades con sistemas operativos, otros componentes o exploradores.
- Estándares abiertos, lo cual conlleva una baja dependencia de softwares propietarios. Si las credenciales utilizan determinado estándar, es posible utilizar cualquier billetera compatible con el estándar lo que amplía considerablemente la posibilidad de acceder a billeteras y genera baja dependencia entre algunos pocos fabricantes y los sistemas de identificación digital a nivel de país.
- Bajos requerimientos tecnológicos, ya que sólo se necesita un dispositivo móvil con NFC o *Bluetooth*.

Un aspecto relevante es la visión del uso de credenciales verificables para identificarse digitalmente fuera de fronteras. En este caso, pueden ocurrir diferentes escenarios:

- Identificación presencial fuera de fronteras, por ejemplo, presentarse en la administración tributaria de otro país. Lo que se necesita para poder utilizar una credencial fuera de fronteras es lo siguiente:

  - La credencial de identificación que el prestador posee debe tener un formato compatible con el validador. Para esto es necesario utilizar estándares reconocidos entre los diferentes países.
  - La lista de confianza de firma del país origen debe ser accedida por el validador del otro país.

- Identificación digital fuera de fronteras, por ejemplo, ingresar al portal web de la administración tributaria de otro país. En esta situación podría haber dos escenarios:
  - No hay integración transfronteriza de identificación digital entre los países: el usuario accede al portal de la administración tributaria del otro país; el cual tiene desarrollado un método de identificación utilizando OIDC4VP. Para que el portal pueda validar la credencial, debe conocer el estándar que utiliza la credencial y contar con la lista de confianza del país de origen. Esta situación, si bien es viable, no es la más recomendada; lo ideal sería lograr escenarios donde los sistemas o ecosistemas de identificaciones digitales a nivel de cada país se integren con sus pares de otros países.
  - Existe una integración transfronteriza entre los sistemas o ecosistemas de ambos países. Este sería el escenario ideal, dado que la credencial se valida en su país de origen y la persona vuelve al portal de la administración tributaria del país extranjero validado. Tal como se comentó en el capítulo 1, la persona accede al portal de la administración tributaria, cuando se va a identificar elige su país de origen y es redirigido al sistema o ecosistema (*broker*) de identificación digital de su país. En este momento elige presentar la credencial, el sistema o ecosistema debe solicitar la credencial utilizando *OpenID Connect for Verifiable Presentations*. Una vez que el usuario se identifica, el sistema lo redirige al portal de la administración tributaria.

En un sistema o ecosistema de identificación digital a nivel país, donde la administración tributaria es un actor relevante e integrada, de modo que sus usuarios se identifican digitalmente en su portal y aplicaciones (web y móviles) utilizando las identificaciones digitales nacionales, este novedoso método puede ser de mucho interés.

Si el país posee un ecosistema articulado por un *broker* de identificaciones digitales, la implementación de este nuevo método como proveedor de identificación se facilita considerablemente. El *broker* deberá implementar el protocolo *OpenID Connect for Verifiable Presentations* (extensión del protocolo *OpenID Connect* que seguramente ya posee) y simplemente este nuevo método queda habilitado para todos los sistemas integrados, la administración tributaria entre ellos.

Como parte de la gobernanza del *broker* y el ecosistema de identificación digital del país, además de implementar este protocolo que habilite utilizar las credenciales verificables de identidad para identificarse digitalmente, es necesario tomar algunas decisiones que tienen que ver con los estándares. Estas decisiones son importantes por varias razones:

- Facilitan la interoperabilidad no solo a nivel nacional, sino también transfronteriza. Que las personas cuenten con credenciales verificables de identidad en sus billeteras, con los estándares adecuados, es crítico para que puedan utilizarlas en todo el país y fuera de fronteras.
- Facilitan la evolución y la vida útil. Los estándares adecuados perduran en el tiempo; con esto, toda la vida útil de las credenciales.
- Facilitan el uso. Los estándares que prevalezcan van a contar con mayores ofertas de billeteras y utilidades, en más plataformas y con mejores condiciones de evolución.

Resumen y hoja de ruta

A modo de resumen, en lo que respecta a la identificación digital en las administraciones tributarias, utilizar las credenciales verificables como método de identificación será seguramente el método dominante en el futuro dada su simplicidad y alto nivel de confianza, donde se destacan los siguientes puntos:

- Definir a nivel de país los estándares adecuados es un gran y crítico desafío. En particular, para credenciales verificables de identificación, basarse en el *World Wide Web Consortium* (W3C) *Verifiable Credentials Data Model 2.0* para definir su ecosistema (actores y roles), utilizar OIDC4VC para la transferencia y la ISO/IEC 18013-5 para la especificación detallada parece ser una combinación ganadora actual y probablemente sea la que perdure en los próximos años para este caso de uso.
- Desarrollar la gobernanza y la normativa adecuada, logrando que las credenciales verificables sean equivalentes a sus pares físicos.
- Contar con un ecosistema articulado por un *broker* de identificaciones digitales, donde se implemente el protocolo OIDC4VP, para que sea posible identificarse digitalmente en todos los servicios digitales y móviles utilizando una credencial verificable, es importante para facilitar y viabilizar este método seguro y simple de usar, logrando un impacto a nivel de país. Si la administración tributaria está integrada, no es necesario que realice ningún desarrollo ni modificación en sus sistemas.
- Además de adoptar los estándares correctos, integrar sistemas o ecosistemas de identificación digital a nivel transfronterizo para habilitar en forma sencilla y segura el uso de credenciales verificables de identificación para autenticarse digitalmente en servicios de otros países, así como abrir la puerta de los servicios propios del país a personas de otros países. Las administraciones tributarias podrían verse sumamente favorecidas en este escenario.

3.3. Evolución de la identificación digital en las administraciones tributarias

Las administraciones tributarias deberían pasar a formar parte de un ecosistema o sistema nacional de identificación digital. Claramente esto no depende únicamente de la administración tributaria, pero lo que sí depende son los siguientes temas:

- **Promover la identidad digital nacional:** como actor relevante dentro de la administración pública, en caso de que exista, o al menos, haya una iniciativa, apoyar el desarrollo de una solución de carácter nacional o en un ecosistema articulado dado que esto representa una significativa economía de escala para el Estado. Al delegar la verificación de identidad en un proveedor o sistema unificado, se logra reducir costos operativos, ya que se evita la duplicación de inversiones en seguridad por parte de cada organismo y se reaprovecha la inversión que el país pueda realizar en nuevos métodos de autenticación. Todo ello contribuye, además, a ofrecer una experiencia más unificada, cómoda y segura para el ciudadano a la hora de identificarse para acceder a todos los servicios digitales del Estado.

- **Integrarse a la identidad digital nacional:** en caso de que exista un sistema o ecosistema nacional, integrarse como consumidor de sus identificaciones digitales, es decir, delegar la autenticación.

- **Ofrecer su identificación digital (en caso de que sea conveniente):** junto con los actores del ecosistema, analizar la posibilidad de ser un proveedor más de identificación digital. Para esto la administración tributaria debe poseer las condiciones necesarias e invertir en desarrollos informáticos e infraestructura. Como condiciones, en términos generales, se debe contar con una base de personas físicas y naturales cuyas identidades estén validadas (para la identificación nacional solamente cuentan las personas, no las empresas) y los datos que utiliza para identificar a una persona deben ser compatibles con los datos definidos por el ecosistema nacional, o al menos, simples de transformar y adecuar. Debe ser capaz de aislar su sistema de identificación digital e implementar un protocolo conocido para integrarse al *broker* nacional, como los mencionados anteriormente. Asimismo, deberá tener en cuenta la carga operativa que el uso de su sistema de identificación para ingresar a otros sistemas públicos pueda ocasionar. En consecuencia, será necesario realizar inversiones en infraestructura, revisiones de seguridad y calidad y establecer un acuerdo de nivel de servicio que garantice la disponibilidad y confiabilidad del sistema. En países donde la identificación digital nacional sea una iniciativa incipiente, utilizar a nivel nacional la identificación de la administración tributaria puede ser conveniente para acelerar el desarrollo del ecosistema.

- **Autorización:** proveer una solución integral para la Autorización, una vez que la persona física o natural se identifica mediante el ecosistema o el sistema nacional. Este punto se abordará en detalle a continuación.

- **Auditoría:** diseñar en forma detallada un sistema de auditoría (trazabilidad de la actividad del sistema), dado que van a empezar a ingresar diferentes personas que tendrán diversos roles en las empresas y contribuyentes. La auditoría es esencial para reconstruir información en caso de pérdida de integridad, reconstruir los hechos con precisión y confianza y también como evidencia ante delitos o fraudes.
- I**dentificaciones digitales nacionales más fáciles de usar y más seguras para mayor confianza:** apoyar y, a la vez, exigir a los sistemas o ecosistemas nacionales para que se fortalezcan los métodos de identificación disponibles donde se implementen en forma obligatoria el uso de segundos factores o, mejor aún, evolucionar hacia métodos *passwordless*, descentralizados, basados en el uso de firma digital.
- **Identificaciones más confiables en la administración tributaria:** si no se cuenta con un sistema o ecosistema nacional, la administración tributaria deberá fortalecer sus identificaciones digitales exigiendo como mínimo un segundo factor de autenticación y, de ser posible, evolucionar hacia métodos *passwordless*, descentralizados, basados en el uso de firma digital.
- **Más allá de fronteras:** apoyar a los sistemas o ecosistemas nacionales para que se integren con sus pares fuera de fronteras y de esta forma facilitar el acceso en forma simple y confiable a contribuyentes extranjeros.

En suma, las administraciones tributarias deberían apoyar el desarrollo de los sistemas o ecosistemas nacionales de identificación, cuando sea posible, delegando en ellos la identificación de sus usuarios y concentrándose en desarrollar en profundidad sistemas de **autorización y auditoría**.

3.4. Autorización en las administraciones tributarias

El concepto de “autorización” adquiere un papel central —tal como se abordó en el capítulo 1 de esta publicación— al constituirse como un fundamento operativo esencial dentro de los sistemas de identidad digital. En el ámbito de las administraciones tributarias, la autorización trasciende su dimensión técnica como mecanismo de control de acceso: se configura como un instrumento de garantía institucional, asegurando que cada interacción digital se lleve a cabo bajo criterios explícitos de legitimidad, en concordancia con la normativa vigente en materia de representatividad y evitando situaciones de repudio.

Acceso delegado y gestión de roles

La autorización no puede entenderse de manera aislada, ya que esta requiere de una base sólida de autenticación confiable y contextualizada. Una vez que la persona ha sido autenticada (identificada) por el

sistema, este procede a autorizarla para acceder a determinada información y ejecutar acciones específicas. Este proceso está condicionado por el perfil del usuario, el nivel de confianza asociado al método de identificación utilizado y las reglas particulares definidas por el sistema. Si bien esta Guía no aborda en profundidad el diseño e implementación de mecanismos de autorización, es fundamental reconocer su estrecha dependencia de la identificación digital y tratar sus aspectos fundamentales.

En el ámbito de la administración tributaria, la delegación de funciones constituye el mecanismo jurídico mediante el cual un contribuyente o su representante legal transfiere determinadas facultades a un tercero autorizado, garantizando la validez y la trazabilidad de dicha representación. Esta delegación debería verse reflejada en la **gestión de roles** dentro de los sistemas digitales, donde se asignan perfiles específicos que determinan los permisos y responsabilidades de cada usuario.

Principios de asignación de accesos

La seguridad en los sistemas de identificación digital tributaria debe sustentarse en un pilar fundamental: la asignación de accesos debe ser a personas físicas, incluso cuando actúan en representación de entidades. Las administraciones tributarias deben evitar otorgar credenciales directamente a entidades jurídicas o asociaciones sin personería.

En su lugar, se recomienda asignar accesos a personas físicas que actúen en representación de dichas entidades, bajo un esquema de roles o de delegación de permisos claramente definidos en donde cada usuario debe declarar, al momento de autenticarse, si actúa en nombre propio o en nombre de otro contribuyente – ya sea persona física o una entidad – para lo cual debe haber recibido previamente una autorización formal que habilita un rol y le permite operar en su nombre.

Esta habilitación debe contar con respaldo jurídico adecuado. En el caso de las personas físicas, el titular puede otorgar directamente el rol. En el caso de las personas jurídicas, la asignación de roles deberá ser realizada por sus representantes legales o por quienes éstos autoricen formalmente. Cuando exista representación conjunta, será necesario asegurar el consentimiento expreso de todos los involucrados para validar la asignación.

Niveles de autorización

Los roles por delegar que debe manejar el sistema de autorización podrían llegar a tener estos tres niveles, yendo de los más generales a los más específicos:

- **Por función o rol profesional**: El contribuyente puede asignar funciones específicas a personas físicas, como: gestor, asesor contador, abogado, etc. La Administración podría ofrecer una suite de servicios digitales vinculados a cada rol: por ejemplo, el contador accedería a todos los servicios tributarios, mientras que el abogado solo a los relacionados con aspectos jurídicos. Estos roles podrían ser predeterminados por la Administración, con posibilidad de personalización por parte del contribuyente. Además, se podría habilitar la "subdelegación de roles", como en el caso de un gestor que delega funciones a empleados de su gestoría. En este esquema, es fundamental que, al revocar el rol original, se eliminen automáticamente todas las subdelegaciones asociadas.
- **Por objetos:** El contribuyente puede asignar permisos sobre objetos concretos ofrecidos por la administración tributaria dentro de las funcionalidades de los sistemas. Para facilitar esta gestión, se recomienda el uso de matrices de asignación de roles, que permitan visualizar y administrar los permisos otorgados de forma clara y estructurada.
- **Por dato o conjunto de datos:** Este nivel permite otorgar o revocar permisos sobre datos específicos asociados a la empresa o a la persona física o natural, dentro de los objetos de las diversas funcionalidades. Su implementación debe alinearse con las políticas de Gobernanza de Datos de la administración tributaria, considerando la clasificación de la criticidad de los datos según los lineamientos de seguridad de la información institucional.

La visión de implementar la autorización en estos tres niveles – por función, por objeto, por dato- puede brindar una buena combinación de simplicidad para el contribuyente, pero con la potencialidad suficiente para gestionar hasta el nivel del dato si considera oportuno. En cada uno de estos niveles, la administración tributaria podría establecer el grado de seguridad requerido, en función del tipo de acción a realizar. Por ejemplo, para el envío de la declaración jurada se puede solicitar un nivel avanzado de identificación, mientras que para realizar la solicitud de una constancia bastaría con un nivel intermedio.

El sistema de control de acceso debe estar acompañado de guías y herramientas de apoyo, así como de reportes, consultas y alertas dirigidas a roles clave (como titulares o representantes), para que puedan monitorear la asignación de permisos sobre la empresa, así como el uso que están haciendo del mismo.

Ciclo de vida de identidades y permisos

Las autorizaciones deben poder otorgarse de forma general o específica, con vigencia temporal y posibilidad de revocación inmediata. El sistema de roles y delegación debe contemplar el ciclo de vida de las identidades y permisos en el ámbito tributario, incluyendo eventos críticos que impactan en la validez de los accesos:

- **Alta**: incorporación de nuevos representantes o mandatarios.

- **Modificación:** cambios de rol, reasignación de funciones o actualización de niveles de acceso.
- **Baja:** situaciones como la jubilación, el fallecimiento, la desvinculación laboral, las fusiones o las escisiones institucionales. En caso de que la subdelegación de roles esté presente, la baja debe revocar en cascada los roles subdelegados.

Cada una de estas transiciones debe ser **r**egistrada y sujeta a auditoría, a fin de garantizar la integridad, la trazabilidad y la confiabilidad del sistema de identidad digital. Desde el punto de vista de la seguridad, es importante resaltar el **principio de mínimo privilegio**. Esto significa que un usuario debe contar con el mínimo privilegio posible que le permita realizar su trabajo. La razón de tener en cuenta este principio es simplemente limitar el impacto que pueda tener un mal comportamiento del usuario (adrede o por equivocación), así como una suplantación de identidad, entre otros riesgos relativos a la seguridad de la información.

Herramientas y tecnologías para fortalecer la gestión de roles

La gestión de roles es un aspecto importante para la gestión tributaria, contribuye directamente a su transparencia, eficiencia, disminución de riesgos de cumplimiento y de seguridad de la información. A lo largo de esta Guía se han desarrollado los aspectos vinculados con la identificación digital, en donde estos sistemas identifican personas físicas o naturales y estas personas poseen relaciones modeladas bajo roles con los contribuyentes en la administración tributaria.

Estas relaciones necesitan ser comprobadas, por lo que es necesario que cada persona demuestre que posee determinada potestad para actuar frente a la administración tributaria por determinado contribuyente. Actualmente existen diversas formas de implementar el registro de estas relaciones. Se presenta la documentación necesaria ante la administración tributaria para acreditar determinada relación o vínculo de una persona física con determinada persona física o jurídica y, a partir de ahí, cuando esa persona física o natural ingresa a la administración tributaria el sistema lo reconoce con determinado rol y le habilita las operaciones definidas a nivel de funcionalidades, objetos y datos para dicho rol.

Dependiendo de cada caso, la criticidad de las operaciones e información, la normativa y las posibilidades que brindan los sistemas de la administración tributaria, esta asignación de roles puede resolverse en forma remota y simple o deberá ser necesario realizarlo en forma presencial y más compleja (presentando documentación certificada que avale dichas potestades). En este último escenario, dada la criticidad de las funciones y sensibilidad de la información, puede ser engorroso y costoso para un contribuyente mantener actualizados estos registros, dado que ante cualquier movimiento deberá elaborar la documentación pertinente y acudir presencialmente a la administración tributaria.

Para estos casos, más complejos, sensibles y riesgosos, actualmente existen herramientas y tecnologías que, correctamente habilitadas (con normativa habilitante mediante), podrían resolver la gestión de roles en forma 100% remota y digital con muy altos niveles de confianza. Esto reduciría considerablemente los tiempos y costos, pero, a la vez, los riesgos asociados, ya que sería mucho más fácil para un contribuyente mantener actualizado su registro en la administración tributaria.

A continuación, se presentan tres herramientas y tecnologías que se basan en el uso de la firma digital y toda la confianza que implica una infraestructura de claves públicas reconocida para resolver esta temática en forma 100% remota y digital:

1. **Firmas digitales con atributos:** Se trata de una firma electrónica avanzada que posee atributos que determinan los roles o competencias del titular. Esta firma es otorgada por un prestador de servicios de certificación acreditado, que, no sólo valida la identidad de su titular, sino que además valida competencias de la persona y las especifica en el certificado digital emitido. El titular se presenta ante el prestador de servicios de certificación (firma digital) y solicita una firma que, además, especifique determinada competencia (por ejemplo, abogado, médico, representante de una empresa, socio de una empresa, etc.). Dependiendo de la competencia solicitada, deberá presentar información que avale dicha competencia ante el prestador. El prestador verifica la competencia (en base a la información presentada y/o interactuando con la organización que posee la rectoría de la competencia solicitada). En caso de que posea la competencia solicitada, se explicita en atributos incorporados en el certificado emitido por el prestador. Los atributos son datos adicionales a la firma, por lo que cuando una persona interviene un documento con este tipo de firma, no solo está firmando como persona física o natural, sino que, además está cumpliendo determinado rol, potestad o competencia, según esté especificado en los atributos del certificado. Los atributos podrían ser relativos a profesiones (médicos, arquitectos, abogados, etc.), cargos (gerente, director, titular, representante de determinada empresa), roles (auditor, administrador, funcionario público, etc.), certificados, matrículas o cualquier otra potestad, atributo o competencia que una autoridad competente (regulada para tal caso) pueda acreditar sobre la persona. Este modelo asegura la confianza en las potestades atribuidas, del mismo modo que la firma electrónica avanzada garantiza la identidad del suscriptor y, una vez implementado, no es complejo de utilizar, dado que se firma un documento una sola vez con los atributos que correspondan. Algunas dificultades de este modelo son:

- En los casos en que se requiera, los prestadores de firma deben interactuar de forma segura con las organizaciones rectoras para determinar si la persona posee determinada competencia y emitir el certificado de firma correspondiente. Idealmente, esto debería resolverse interoperando entre ambos sistemas para mayor automatización, pero en un caso con menor desarrollo digital el titular podría presentar toda la documentación comprobatoria al prestador de firma. Si bien esto genera dificultades,

también simplifica, ya que centraliza la emisión de todas las firmas en los prestadores acreditados de firma (que ya poseen las capacidades correspondientes).

- El usuario debe contar con un conjunto de firmas y tener claro cuál utilizar en cada momento según la normativa del caso de uso y gestionar todas ellas. Debería contar con una firma de persona física o natural, pero, además, una firma con cada uno de los atributos que posee, lo que podría llevar a un conjunto amplio de firmas a gestionar.

  Revocación: ante la solicitud de quien corresponda (en caso de una empresa, el titular), del prestador o de un tercero (dependiendo del caso), el prestador deberá revocar toda la firma, por lo que todo lo que se firme después de la revocación no será válido. El prestador acreditado debe mantener actualizada y accesible la lista de revocación.

2. **Sellos de competencia:** Si bien en el caso anterior en algunos países también se consideran sellos (en la Unión Europea no existe más el concepto de firma de persona jurídica, sino que se cambió por el de sellos), este sería un modelo más simple para las personas (usuarios finales) y complejo para las autoridades de competencia. En este escenario, cada persona posee su firma de persona física o natural y cada autoridad de competencia posee un sistema para sellar documentos. Cuando una persona necesita firmar un documento y demostrar una competencia, firma el documento con una firma de persona física o natural y, utilizando un servicio de la autoridad competente, solicita que se selle el documento. La autoridad competente, a partir de la firma, utilizando su registro, determina si la persona en ese momento posee o no la competencia y, en caso de poseerla, sella el documento. El sello, técnicamente, es igual a la firma electrónica avanzada de persona jurídica y es lo que da certeza de que la persona que firmó en ese momento poseía determinada competencia. Este modelo tiene ventajas y desventajas. Como ventaja, es más simple la gestión para cada persona, ya que solo debe contar con su firma electrónica avanzada de persona física o natural y no es necesario contar con revocación. El documento se sella en un momento dado, lo que garantiza que, en ese momento, la persona contaba con esa competencia. Es recomendable que esto se acompañe de un sello de tiempo acreditado, a fin de garantizar el momento del sello. Una barrera o dificultad de este modelo es que todas las autoridades de competencia deben contar con un sistema para sellar. Dependerá de cada normativa: darle determinado período de validez al documento sellado o mantenerlo hasta que el contribuyente indique lo contrario.

   Revocación: en este escenario es más simple, dado que la autoridad, cuando va a sellar, debe validar si la competencia sigue vigente y, en tal caso, realizar el sello. La confianza en este caso se apoya en el momento que se realiza el sello, no es necesario contar con una lista de revocación.

3. **Credenciales verificables para competencias:** Anteriormente, en este capítulo se desarrolló el concepto de credenciales verificables orientadas a la identificación, equivalentes a lo que podría ser un documento de identidad a nivel nacional. De la misma forma, existen credenciales verificables

que acreditan competencias, roles o potestades. En este caso, el interesado acude a la autoridad de competencia correspondiente, solicita una credencial, la autoridad la genera y se la envía a la billetera electrónica del titular. Este proceso puede realizarse remoto o presencial, dependiendo de la normativa y las soluciones que provea la autoridad de competencia. En este escenario, la administración tributaria deberá desarrollar un servicio en su sistema de autorización para que el usuario, una vez identificado, envíe su credencial. Estas credenciales no son de identificación, por lo que el usuario deberá identificarse digitalmente para luego, cuando solicita determinado rol, enviarle la credencial utilizando algún protocolo como *Open ID Connect for Verifiable Presentations* visto anteriormente. El usuario gestionaría sus competencias en su billetera electrónica y las podría utilizar presencial y digitalmente, tal como se vio en el caso de las credenciales verificables para la identificación. En un escenario donde las credenciales verificables se popularicen, tal como lo indican las tendencias, esta posibilidad tendría menos barreras; el usuario podría utilizar su credencial de identificación para solicitar las credenciales de competencias en forma remota y segura y gestionar todas sus credenciales en forma simple y cómoda en su billetera electrónica. Las autoridades de competencia deberían estar en la lista de confianza a nivel de país y contar con un sistema de revocación, de la misma forma que se realiza con las credenciales verificables para la identificación.

Revocación: en forma similar a las firmas digitales con atributos, las autoridades que emitan credenciales verificables deben mantener una lista de revocación que será consumida por los validadores. Dependiendo del modelo, la lista de revocación podrá ser centralizada (para todas las credenciales), tal como sugiere el modelo *World Wide Web Consortium* (W3C), o distribuida, es decir, una lista en cada autoridad, de forma similar a la firma digital.

La siguiente tabla presenta un resumen comparativo de los tres modelos. Es importante resaltar que, desde el punto de vista de la confianza, los tres son equivalentes y totalmente confiables.

Firmas digitales con atributos	Sellos de competencia	Credenciales verificables para competencias
Autoridades de competencia		
Interactúan con los prestadores de firma para validar competencias y solicitar revocaciones. Desarrollo tecnológico bajo o moderado. La autoridad de competencia deberá solicitar al prestador de firma las revocaciones que considere en función de su normativa.	Deben desarrollar un servicio para sellar documentos utilizando un certificado en el contexto de una Infraestructura de Claves Públicas reconocida. Desarrollo tecnológico alto. La revocación se simplifica dado que se comprueba al momento de sellar.	Deben desarrollar un servicio para emitir y revocar credenciales verificables utilizando un certificado en el contexto de una Infraestructura de Claves Públicas reconocida. Desarrollo tecnológico alto. Cada Autoridad deberá mantener una lista de revocación.
Usuarios		
Interactúan con los prestadores de firma. Deben poseer múltiples firmas con sus competencias y utilizar un sistema para firmar. Gestión compleja.	Deben contar con una única firma de persona física o natural y utilizar un servicio de la autoridad para sellar documentos. Gestión simple.	Deben contar con una billetera electrónica para gestionar sus credenciales. Gestión media.
Administración tributaria		
Debe desarrollar funcionalidades para que los usuarios envíen documentos firmados y validadores más complejos para cada tipo de firma o realizar revisiones manuales.	Debe desarrollar funcionalidades para que los usuarios envíen documentos firmados y sellados y el validador debe contar con la capacidad de validar la firma del usuario y el sello de competencias o realizar revisiones manuales.	Debe desarrollar capacidades para que el usuario presente su credencial verificable de competencia desde su billetera electrónica en el sistema de Autorización luego de identificarse digitalmente. Asimismo, debe desarrollar la capacidad de validar la credencial presentada por el usuario.

Dependiendo de las capacidades a nivel nacional, para todo lo que implica validaciones (en los tres casos), la administración tributaria podría integrarse a un servicio que sea desarrollado y mantenido por un sistema centralizado a cargo de la autoridad competente en Gobierno Digital.

En el último punto de este capítulo, “3.8 Hoja de Ruta”, se presentan sugerencias de cómo la administración tributaria podría avanzar en el desarrollo de estas herramientas y tecnologías para fortalecer y hacer más eficiente la gestión de roles o de delegación como parte del sistema de Autorización.

Modelos de control de acceso

La gestión de accesos en sistemas de identidad digital requiere enfoques estructurados que permitan asignar, modificar y revocar permisos de manera segura, trazable y adaptable al contexto operativo. En este sentido, se presentan dos modelos ampliamente reconocidos por los estándares internacionales que ofrecen marcos conceptuales sólidos para el diseño de políticas de autorización en entornos tributarios.

Por un lado, el modelo RBAC *(Role-Based Access Control)*, formalizado por el estándar ANSI INCITS 359-2004, permite asignar permisos en función de roles predefinidos, facilitando la administración centralizada y coherente de accesos en organizaciones con estructuras jerárquicas claras. Por otro lado, el modelo ABAC (*Attribute-Based Access Control)*, descrito en el marco NIST SP 800-162, introduce una lógica más dinámica, basada en atributos del usuario, del recurso y del entorno, lo que habilita decisiones de acceso más granulares y contextuales.

A continuación, se describen sus características principales, aplicaciones sugeridas y consideraciones para su implementación, así como otros dos modelos no tan utilizados o ideales para una administración tributaria:

Modelo	Descripción	Aplicación
RBAC (*Role-Based Access Control*)	Asigna permisos en función de roles predefinidos dentro de la organización. Cada rol agrupa un conjunto de permisos que reflejan responsabilidades específicas, lo que facilita la administración centralizada y coherente de accesos.	Ideal para perfiles estables como mandatarios, asesores tributarios y contadores, donde las funciones están claramente delimitadas.
ABAC (*Attribute-Based Access Control*)	Define accesos según atributos dinámicos del usuario, del recurso o del entorno. Estos atributos pueden incluir tipo de entidad, nivel de riesgo, horario de acceso, entre otros. Este enfoque permite decisiones más granulares y adaptativas.	Recomendado para escenarios donde el contexto influye en la autorización, por ej: accesos solo en determinado horario desde una jurisdicción específica.
DAC (Control de Acceso Discrecional)	El propietario del recurso define quién puede acceder y con qué permisos directamente.	Algunos sistemas operativos basados en UNIX lo implementan. Es simple y flexible pero difícil de escalar y controlar en grandes entornos
MAC (Control de Acceso Mandatorio)	El sistema define las políticas según los niveles de seguridad y clasificación de la información. Los recursos se clasifican en niveles (ejemplo, público, restringido y confidencial) y se asocian a grupos de usuarios en base al diseño de políticas.	Es una forma centralizada con poca flexibilidad, complejo de implementar, pero fácil para escalar. RBAC es una alternativa menos rígida y más fácil de administrar.

Ambos enfoques (RBAC y ABAC) ofrecen ventajas complementarias y pueden combinarse estratégicamente para responder a los desafíos de seguridad, representatividad y flexibilidad que enfrentan las administraciones tributarias en sus procesos digitales. La combinación de ambos modelos permite una gestión flexible, segura y escalable de los accesos, teniendo en cuenta los tres niveles propuestos.

3.5. Auditoría en las administraciones tributarias

Como parte de la Triple A, presentada en el capítulo 1, en un escenario donde la Autenticación (Identificación Digital) es resuelta a nivel país y delegada en un sistema o ecosistema por parte de la administración tributaria, la misma debe concentrarse en desarrollar en forma adecuada la Autorización y la Auditoría.

Con respecto a la auditoría, en este contexto, se refiere a la trazabilidad de toda la actividad de todos los usuarios en el sistema de la administración tributaria. Esto implica registrar una traza de cada movimiento que debe incluir como mínimo:

- Usuario: identificador del usuario que realizó el movimiento;
- *Timestamping*: fecha y hora con precisión, obtenidas desde un servidor de tiempo confiable del momento de la acción;
- Origen: información acerca del origen, desde donde estuvo trabajando el usuario. Esto no solo puede ser la IP utilizada por el usuario, sino también una huella (*fingerprint*) del equipo que el usuario utilizó para trabajar);
- Información acerca del movimiento: descripción de qué realizó el usuario, pero también información estructurada sobre un catálogo de posibles acciones (nuevo, modificación, eliminación, visualización, etc.) sobre el dato;
- Estado anterior del dato a ser modificado y demás información de interés.

Si bien la auditoría se utiliza para múltiples fines, cada uno de los sistemas que integran la plataforma de la Autoridad Tributaria puede contar con diferentes herramientas y, a su vez, hay herramientas específicas para gestión de *logs*, aunque generalmente estas son destinadas a eventos de interés desde el punto de vista de la ciberseguridad y no tanto de la trazabilidad del dato.

Las fuentes de información generadas para auditoría deben ser tratadas con los mismos cuidados que las fuentes de datos de los sistemas, dado que poseen información sensible e incluso mayor detalle porque conservan su historial completo.

El objetivo final es poder determinar con precisión y confianza qué realizó cada usuario, desde dónde y cuándo, en cada momento en el sistema, manteniendo un histórico completo y detallado de la trazabilidad de todas las acciones de cada usuario interno y externo.

El sistema de auditoría debería contar con, al menos, los siguientes componentes:

- **Captura de eventos:** módulo que captura automáticamente cada movimiento o acción de un usuario (inicio o cierre de sesión, creación, modificación, eliminación, consulta, exportación, cambios en permisos, etc.). Es importante que el dato del momento exacto del día sea obtenido de un servidor central en la administración tributaria para mayores garantías. En un caso más sofisticado podría utilizarse un sellado de tiempo o *timestamping* con NTP. Identificar inequívocamente al usuario, la autorización cuando aplique y la acción sobre el recurso exacto que está realizando también es clave para la calidad y confiabilidad de la información de la auditoría. Es importante que la información, en este caso, sea lo más estructurada posible con el fin de facilitar el almacenamiento y las búsquedas, así como comprobaciones de calidad o búsqueda de anomalías o inconsistencias.
- **Persistencia de la traza**: estos sistemas generan grandes volúmenes de información, por lo que elegir la solución es un desafío considerable, así como los recursos que se les asignen y sus políticas de respaldo, protección de la confidencialidad, etc. La trazabilidad debería contar con herramientas para proteger su integridad; no debería ser posible modificarla y esto debería ser verificable matemáticamente. El uso de funciones *hash* para proteger y verificar su integridad con el paso del tiempo puede ser una herramienta importante.
- **Sistemas de correlación o análisis:** Puede haber sistemas que revisen en tiempo real (o muy próximo) así como a posterior los diferentes movimientos en búsqueda de anomalías, intentos de fraude, accesos a información no permitidos, etc. Integrar la auditoría a un *Security Operation Center* (SOC) puede ser una muy buena estrategia para detectar posibles fraudes o accesos no autorizados en la administración tributaria. El SOC podría utilizar una herramienta SIEM (*Security Information and Event Manager*) para correlacionar o analizar eventos, inclusive, cruzándolos con fuentes externas (otros servidores y tráfico de red).
- **Retención y borrado:** La retención y conservación deberían estar alineadas a la gobernanza de los datos de la administración tributaria. Es importante contar con un sistema de respaldo (*backup*) adecuado.

Los principales estándares en la materia son:

- ISO/IEC 27001, que establece el funcionamiento de un Sistema de Gestión de Seguridad de la Información posee dos controles al respecto: A.12.4 “Logeo y Monitoreo” y A.12.7 “Consideraciones de la Auditoría de Sistemas”.
- ISO/IEC 27002, guía de buenas prácticas complementarias: cómo implementar y proteger registros de auditoría.
- NIST SP 800-92, guía sobre almacenamiento y análisis de *logs*.
- NIST SP 800-137, marco de monitoreo continuo de la seguridad de la información, lo que incluye el monitoreo de la actividad del usuario.

Construcción de evidencia válida

La necesidad de construir buenas trazas de auditorías de actividad en los diferentes sistemas y accesos a datos está directamente relacionada con la necesidad de poder construir evidencia válida para la administración tributaria. La evidencia digital es fundamental en los procesos de identificación digital porque garantiza la autenticidad, la integridad y la trazabilidad de las acciones y de los datos utilizados para verificar la identidad de una persona.

La evidencia digital respalda cada paso de estos procesos, permitiendo demostrar la legitimidad de una identidad o transacción digital.

De acuerdo con la Norma ISO/IEC 27037:2012, la evidencia digital se define como “*información o datos almacenados o transmitidos en forma digital que pueden ser utilizados como prueba*”. Su adecuada gestión fortalece la confianza en los sistemas de autenticación, protege contra fraudes y facilita la trazabilidad de las operaciones.

Su relevancia puede expresarse en varios niveles:

- **Prueba de autenticidad:** La evidencia digital (como registros de acceso, firmas electrónicas, metadatos o biometría) permite demostrar que una persona efectivamente participó en un proceso de identificación o autenticación. Permite vincular de manera fiable a una persona con una acción o un evento específico.

- **Integridad de la información**: Garantiza que los datos de identidad (documentos, imágenes, registros biométricos, etc.) no han sido alterados desde el momento de su captura.
- **Trazabilidad y auditoría:** La evidencia digital documenta quién, cuándo y cómo se realizó el proceso de identificación. Es vital para auditorías e investigaciones forenses, ya que la evidencia digital tiene valor probatorio ante controversias, fraudes, accesos no autorizados o suplantaciones de identidad.

La correcta recolección, preservación y validación de evidencia digital refuerzan la confianza del usuario y de las instituciones en los sistemas de identificación digital. La evidencia digital es el soporte verificable que respalda cada paso de un proceso de identificación digital, garantizando seguridad, legalidad y confiabilidad en la gestión de identidades electrónicas.

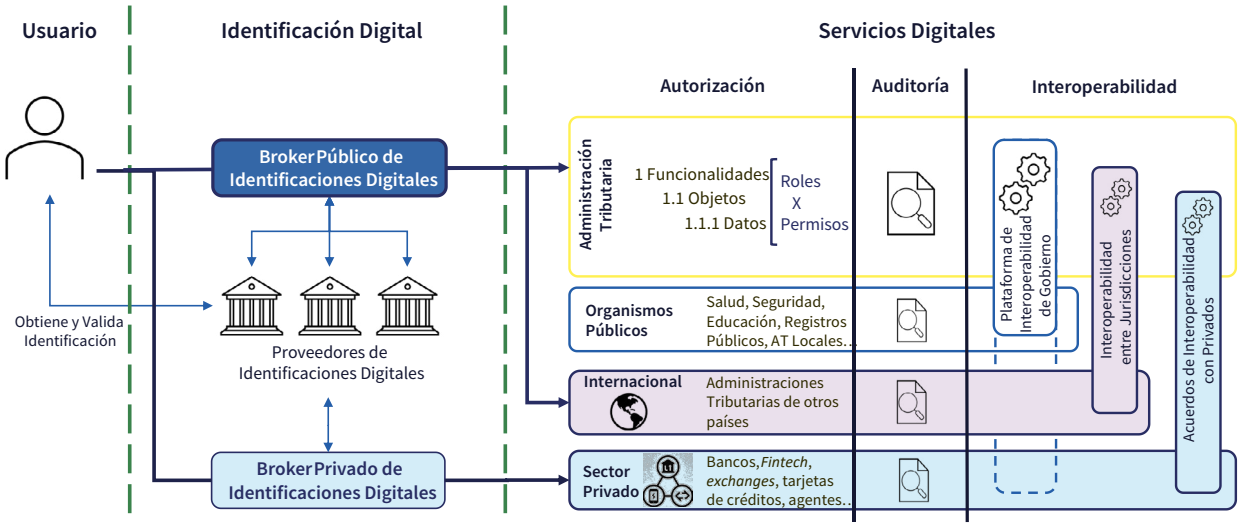
3.6. Diagrama integrador modelo

En la publicación del CIAT, “Las TIC como Herramienta Estratégica para Potenciar la Eficiencia de las Administraciones Tributarias” (CIAT, 2020), en el capítulo 10, en el punto “10.1.7 “Seguridad interna en los sistemas de información y sus aplicaciones” se definen tres niveles de seguridad basado en roles:

- Funcional: permisos para brindar acceso a las partes funcionales del sistema dentro de cada proceso.
- Objetos: gestionar los permisos para el acceso a objetos, por ejemplo, dentro de un contribuyente, se podrán definir permisos específicos para acceder a las declaraciones juradas.
- Campos (datos): Son el permiso más granular y se trata de permitir el acceso a un campo o dato necesario en forma específica.

En la publicación anteriormente mencionada se presenta un diagrama muy completo, modelado con base en casos de uso que poseen roles mediante los cuales se definen diversos permisos sobre funcionalidades, objetos y/o campos, presentando de esta forma un esquema completo de gestión del acceso o autorización. A continuación, el siguiente diagrama muestra la relación entre la identificación digital y un sistema de control de acceso o autorización basado en el esquema de la publicación mencionada, continuando con la auditoría y luego la interoperabilidad:

Figura 12. Esquema de relación entre la identificación digital, el acceso, la auditoría e interoperabilidad.



Fuente: Elaboración propia

En el diagrama anterior pueden distinguirse las siguientes secciones la relación entre un usuario y la administración tributaria:

- **Proveedores de identificación digital:** un usuario obtiene y valida su identificación digital en un proveedor acreditado o regulado por el ecosistema.
- **Identificación digital:** un usuario se identifica digitalmente ante un servicio digital, en este caso podrían existir varios escenarios:
  - ***Broker* público de identificaciones digitales:** se trata de un ecosistema nacional articulado por un *broker* tal como se detalló anteriormente. En este caso, el usuario podría utilizar uno de los métodos de identificación integrados para acceder a la administración tributaria su otro organismo público.
  - **Identificación digital transfronteriza:** se trata del escenario detallado en el capítulo 1.3, donde es posible ingresar a servicios digitales de otro país utilizando identificaciones digitales confiables de su país. De esta forma, el usuario ingresa a una administración tributaria de otro país. En el esquema anterior, no se visualiza el *broker* del otro país para hacerlo más simple, se asume que es parte del ecosistema de identificación digital.
  - ***Broker* privado de identificaciones digitales:** si bien este concepto es reciente, en algunos países la estrategia nacional de identificación digital para lograr un mejor alcance a nivel de país, habilita en forma regulada la creación de *brokers* en el sector privado, que incluyan los proveedores de

identificación reconocidos (al menos en niveles altos de confianza) y ofrezcan su integración al sector privado. Si bien esto podría resolverse con un solo *broker* a nivel país, separar el mundo público del privado podría generar menos riesgo (no todo el país dependería de una única pieza de software para resolver la identificación digital) y podrían coexistir diferentes modelos de negocio que hagan más sustentable el ecosistema. Desde el punto de vista del usuario, esta situación mantendría la idea de utilizar una o pocas identificaciones digitales para identificarse en todo el país (y más allá) porque los proveedores de identificación acreditados estarían presentes en todos los *brokers*.

- **Autorización:** al ingresar identificado a los servicios de la administración tributaria, el sistema de Autorización de la administración tributaria define a qué funcionalidades, objetos y datos el usuario tendrá permisos, en función de los roles que tiene asociado. A su vez, a partir de los permisos asignados a dichos roles, el sistema determinará qué podrá hacer el usuario sobre las funcionalidades, objetos y datos asociados (crear, borrar, modificar, ver, eliminar, ejecutar, aprobar, etc.). Es necesario que haya un correcto y actualizado mapeo entre todas las funcionalidades, sus objetos asociados y los campos (datos) involucrados en cada caso con cada rol y, a su vez, qué operaciones (permisos) permite cada caso. Se trata de un sistema de autorización complejo, pero sumamente potente y flexible, de modo de facilitar la operativa de cada usuario, reduciendo riesgos con respecto a la seguridad de la información. Las herramientas de reportes, alertas y chequeos que la administración tributaria desarrolle para el servicio del sistema de autorización son fundamentales para facilitar la configuración y el mantenimiento a cada contribuyente. Es fundamental que cada contribuyente mantenga coherencia entre los roles asignados en el sistema y las funciones reales que desempeñan sus usuarios. En consecuencia, el ingreso de nuevos funcionarios (ya sean propios o tercerizados), los cambios de cargo o la desvinculación de personal deben reflejarse de manera inmediata en el Sistema de Autorización de la administración tributaria. Mantener el sistema de Autorización actualizado para cada contribuyente es crítico para proteger su información. En la publicación del CIAT, “Las TIC como Herramienta Estratégica para Potenciar la Eficiencia de las Administraciones Tributarias” (CIAT, 2020), en el capítulo 10, en el punto “10.1.7, “Seguridad interna en los sistemas de información y sus aplicaciones”, se desarrolla con mucho más detalle este tema. En el punto 3.6 “Identificación Digital e Inteligencia Tributaria”, se abordan en forma resumida algunas ventajas que la identificación nacional, la correcta gestión de Autorizaciones y Auditoría, así como la interoperabilidad pueden ocasionar para la inteligencia tributaria.

- **Auditoría:** en este punto se modela la importancia de la auditoría en una administración tributaria, sobre todo contemplando las tendencias actuales de contar con identificaciones digitales de personas a nivel de país que ingresan a la administración tributaria con diversos roles en múltiples contribuyentes. Si bien existen estándares y buenas prácticas, la auditoría es un tema específico de cada organización.

- **Interoperabilidad:** es importante aclarar que este tema es sumamente complejo y amplio, en este documento se desarrolla de forma superficial, dado que la identificación digital es un elemento que

favorece una interoperabilidad más eficiente o precisa. El esquema anterior muestra la siguiente configuración desde las administraciones tributarias:

- **Plataforma de interoperabilidad de gobierno:** es una plataforma transversal al Estado que resuelve la interoperabilidad entre organizaciones públicas. Esta plataforma también puede contemplar al sector privado (gráfico en punteo), por lo que, desde esa plataforma, también puede resolverse la interoperabilidad a nivel de país.
- **Interoperabilidad entre jurisdicciones:** la interoperabilidad entre las administraciones tributarias resulta esencial para fortalecer la cooperación internacional y el control fiscal. El intercambio de información tributaria a través de acuerdos internacionales permite que las administraciones compartan datos sobre contribuyentes, operaciones financieras y estructuras empresariales. Este intercambio puede materializarse a través de distintos mecanismos; sin embargo, la existencia de ecosistemas nacionales de identificación digital, integrados bajo estándares comunes, será clave para alcanzar una interoperabilidad transfronteriza entre las administraciones cada vez más eficiente y segura. Esta interoperabilidad técnica entre países es clave para que estos acuerdos se traduzcan en capacidades operativas efectivas y jurídicamente válidas.
- **Acuerdos de interoperabilidad con privados:** Si bien siempre deben existir acuerdos entre la administración tributaria y los diferentes actores privados (bancos, *Fintech*, *exchanges*, tarjetas de créditos, *hubs* de pagos, etc.), es importante que estos acuerdos se terminen materializando mediante interoperabilidad. Esto puede resolverse de diferentes formas con respecto a la solución tecnológica: utilizando la misma plataforma de interoperabilidad de gobierno (mostrado en punteado en el esquema), o desarrollando una plataforma de interoperabilidad entre la administración tributaria y el sector privado (mostrado en el esquema) o resolviendo la interoperabilidad punto a punto entre la administración tributaria y cada uno de los actores relevantes.

Desde la perspectiva del esquema anterior, que representa el flujo de trabajo de un usuario, realizando alguna función sobre un contribuyente en la administración tributaria, la estandarización de la identificación digital a nivel nacional es determinante. Ésta influye sustancialmente en los procesos posteriores y repercute directamente en la coherencia de los distintos procedimientos de la administración tributaria.

Es fundamental que el esquema de identificación digital nacional se pueda complementar con un correcto sistema de autorización y de auditoría en la administración tributaria.

3.7. Identificación digital e inteligencia tributaria

La inteligencia tributaria se puede definir como la inteligencia fiscal aplicada al ámbito tributario. En (CIAT, 2020) se conceptualiza como una función fundamental que una administración tributaria moderna debe crear, con autonomía, para transformar los datos en información útil destinada a la toma de decisiones. Su objetivo principal es que la administración tributaria conozca a sus contribuyentes y sea lo más predictiva posible respecto de sus conductas presentes y futuras, buscando mejorar la eficiencia, la justicia y minimizar los riesgos de evasión y elusión

Los datos son un activo crítico hoy en día para todas las organizaciones. Las administraciones tributarias no son ajenas a esta realidad y deben explotarlos para mejorar la eficiencia y efectividad en todos los procesos. Para esto es necesario definir una correcta gobernanza de datos, pero además desarrollar otros factores importantes que pueden ser abordados en base al flujo de trabajo que un usuario, en nombre de un contribuyente, realiza frente a la administración tributaria.

Analizando el Diagrama integrador modelo presentado en la figura 12 de esta publicación, se pueden identificar varias etapas a lo largo del flujo de trabajo de cada usuario en los sistemas de la administración tributaria. A continuación, se describen algunos factores que contribuyen a una mejor inteligencia tributaria en cada una de las etapas:

1. **Identificación digital:** contar con un ecosistema a nivel nacional, inclusive con interoperabilidad transfronteriza (mejor aún), estandarizado y articulado por un *broker* de identificaciones digitales aporta diversas oportunidades. Que todos los servicios digitales, identifiquen con los mismos datos a cada usuario y esto sea mapeado con cada persona física, implica que será mucho más fácil obtener e intercambiar información. Asimismo, los métodos de identificación robustos contribuyen a generar mayor confianza en la veracidad de los datos que se interoperan, dado que reducen considerablemente los riesgos vinculados a la suplantación de identidad.

   Por otro lado, la identificación digital no solo facilita la verificación técnica de quién está detrás de una operación digital, sino que también podría permitir a las administraciones tributarias mapear estructuras societarias y reducir el uso de intermediarios ficticios, obviamente, sin ser infalible. Se podrían vincular de forma confiable datos como nombre legal, fecha de nacimiento, nacionalidad y residencia con registros societarios en las diferentes jurisdicciones, reduciendo la posibilidad de usar testaferros o identidades falsas. Al exigir métodos de autenticación robustos (ej. biometría, MFA, certificados digitales) en la constitución de sociedades o apertura de cuentas, se aseguraría que la persona que figura como accionista o directivo sea efectivamente quien dice ser o por lo menos, se dificulta que alguien actúe -sin conocimiento- como “pantalla” para ocultar al verdadero *Ultimate Beneficial Owner* (UBO) o Beneficiario

Final. A su vez, si los sistemas de identificación digital pudieran interactuar con registros mercantiles, notariales y bancarios, se facilitaría el cruce de información para detectar quién controla realmente una empresa. El *Legal Entity Identifier* (LEI), impulsado por el G20 y promovido por la OCDE, puede ser muy potente en combinación con la identidad digital, al funcionar como un identificador único y estandarizado de personas jurídicas. Vincularlos, permitirían a las administraciones tributarias mapear con mayor precisión las relaciones comerciales y societarias e identificar beneficiarios. Por ejemplo, una empresa está registrada con un LEI único, y una persona con identidad digital nacional abre una cuenta bancaria para esa empresa, al cruzar ambos datos, la administración tributaria podría identificar al presunto UBO, verificar la legitimidad de la operación y detectar vínculos con otras entidades en diferentes jurisdicciones.

2. **Autorización:** un sistema de autorización correctamente diseñado, desarrollado y actualizado, basado en la gestión de roles y permisos en tres niveles (funcionalidad – objetos – datos), potencia aún más la riqueza de los datos que posee la administración tributaria. Además, la información vinculada a las autorizaciones (es decir, quién accede, modifica o consulta determinados objetos o datos dentro de los sistemas tributarios) es un insumo valioso para descubrir relaciones funcionales, operativas y jurídicas entre actores. Estos registros permiten identificar patrones de interacción, jerarquías internas, delegaciones de responsabilidad y vínculos indirectos que no siempre se evidencian en los datos tributarios tradicionales. En este sentido, los "metadatos" del sistema de autorización se convierten en elementos de interés para la inteligencia tributaria, especialmente cuando se integran en programas de análisis relacional de visualización de redes, completando el multígrafo de relaciones comerciales y jurídicas. Al incorporar estos datos, es posible enriquecer los modelos de riesgo y detectar estructuras de evasión más complejas. Utilizando métodos más confiables y robustos para gestionar la autorización, como los mencionados anteriormente (firmas digitales con atributos y sellos de competencia), se fortalece aún más la confianza en las relaciones entre los contribuyentes y los usuarios que actúan en su nombre frente a la administración tributaria.

3. **Auditoría:** a partir de la identificación nacional y la gestión de la autorización, la auditoría permite trazar y determinar con precisión la actividad de cada usuario en cada contribuyente en la administración tributaria a lo largo del tiempo. No solo garantiza la integridad operativa, sino que también aporta insumos valiosos para la inteligencia tributaria, en particular, la información derivada de los registros de auditoría contribuye a detectar patrones no tradicionales de conducta, como accesos en horarios inusuales, direcciones IP provenientes de jurisdicciones atípicas, correlaciones temporales entre eventos críticos y acciones específicas, o anomalías en la secuencia lógica de operaciones. Estos elementos, cuando se integran en modelos analíticos, permiten identificar comportamientos atípicos y fortalecer la capacidad de detectar operaciones sospechosas dentro y fuera de la organización.

4. **Interoperabilidad:** los sistemas maduros de interoperabilidad de datos, generalmente desarrollados y gestionados por las organizaciones rectoras en Gobierno Digital en cada país, son un elemento clave en

el desarrollo digital en el país. Deberían ser abordados como una plataforma transversal a todo el Estado, orientada a interoperar datos, cumpliendo los lineamientos de seguridad y privacidad de la información. Es necesario que exista normativa al respecto, no solo una posible Ley de Privacidad de la Información, sino de intercambio de datos ante determinadas situaciones, bajo determinadas garantías y consentimiento de sus dueños, así como una gobernanza clara de datos a nivel país. Cada organización se integra a la plataforma de interoperabilidad y expone sus datos en forma segura, controlada y confiable, así como puede acceder a obtener datos de otras organizaciones. No es el objetivo de esta Guía analizar en detalle la interoperabilidad, pero sí es un tema relevante para los intereses de la administración tributaria ya que la interoperabilidad permite que la administración tributaria acceda a información de registros civiles, aduanas, seguridad social, catastros, registros productivos y más. Esto enriquece la experiencia del usuario al interactuar con la administración en forma más fluida, pero también, con los consentimientos del caso, puede enriquecer el perfil del contribuyente y permitir detectar inconsistencias o riesgos.

El desarrollo de una inteligencia tributaria robusta exige bases sólidas y articuladas. Entre ellas, se destacan la identificación digital estandarizada a nivel nacional (preferentemente con capacidad transfronteriza), los sistemas de autorización y auditoría, la gobernanza y la calidad de los datos y la interoperabilidad transversal en el país.

La correcta gestión y aseguramiento de la calidad de los datos generados por los distintos procesos de la administración tributaria es esencial para cumplir con sus objetivos institucionales. Estos datos, cuando son confiables, permiten potenciar las capacidades analíticas, operativas y estratégicas del organismo.

En este marco, en la actualidad, las herramientas de Inteligencia Artificial ofrecen oportunidades disruptivas y únicas para mejorar la gestión de cumplimiento, la detección de riesgos y la toma de decisiones. Sin embargo, su efectividad depende directamente de la solidez de los pilares mencionados: sin identificación digital confiable, sin sistemas de autorización bien diseñados, sin auditoría adecuada ni gobernanza de datos, los beneficios de la IA no podrán maximizarse ni sostenerse en el tiempo.

3.8. Conclusiones

En un mundo donde las actividades cotidianas dependen cada vez más de las Tecnologías de la Información y la Comunicación (TIC) y, a su vez, las amenazas cibernéticas han crecido exponencialmente, cuidar nuestra identidad digital y contar con métodos de identificación robustos, simples y seguros resulta crítico.

Los métodos tradicionales de identificación digital están quedando obsoletos por más factores que se les incluyan, que además son costosos y dificultan la usabilidad. Una de las principales vulnerabilidades es que

estos métodos, basados en el binomio identificador / verificación (generalmente como usuario y contraseña), utilizan una base de datos centralizada con millones de credenciales de usuarios y otra es que la gestión de contraseñas fuertes es incómoda para los usuarios.

Las herramientas biométricas han mejorado mucho su precisión y, con el uso extendido de dispositivos móviles inteligentes, se han hecho muy populares para validar identidades o identificarse digitalmente. De todas formas, estos métodos generan algunas fricciones; para ser más confiables, deberían interactuar con el registro público y generan costos considerables. Adicionalmente, actualmente se encuentran amenazadas por la Inteligencia Artificial, si bien no es posible saber con exactitud qué sucederá en el futuro cercano, la IA es posible que logre engañar a herramientas biométricas y pruebas de vida.

Se necesita evolucionar rápidamente hacia métodos de identificación basados en firma digital, con toda la confianza que implica una infraestructura de claves públicas, donde, además, sus claves están distribuidas, en poder del titular. Las claves están en un dispositivo criptográfico y nunca salen de él, de modo que no existe una base de datos centralizada con millones de credenciales de usuarios.

La firma en la nube utilizada para la identificación digital es una muy buena solución que aprovecha las ventajas de la firma digital y simplifica su uso, pero, sin duda, las Credenciales Verificables seguramente sean el método que definitivamente logre escalar en métodos basados en firma en la identificación digital en forma masiva. Las credenciales verificables poseen varias ventajas: identificación basada en firma digital, credenciales distribuidas, infraestructura de claves públicas para la confianza y protección de la privacidad. Además, son muy fáciles e intuitivas de utilizar y también se pueden utilizar para identificarse en forma presencial con total facilidad y confianza. Es una identificación confiable y robusta utilizada tanto en forma presencial como digital.

Otra tendencia desde hace años es que las identificaciones digitales se empiezan a comportar como las físicas, es decir, las personas físicas o naturales obtienen una identificación digital de un proveedor de confianza y la utilizan en múltiples sistemas. Esto facilita enormemente la gestión de las identificaciones por parte de las personas. Se está atravesando una etapa de transición, donde van desapareciendo identificaciones individuales en cada uno de los servicios digitales por sistemas o ecosistemas a nivel de país. Inclusive, en la Unión Europea ya es un hecho la identificación digital transfronteriza y en América Latina y el Caribe hay una iniciativa que ya abarca a 13 países en el ámbito de la Red Interamericana de Gobierno Digital.

Este nuevo escenario va a lograr que los sistemas o ecosistemas nacionales interoperen, de modo que las personas no solo utilicen su identificación digital confiable para identificarse en servicios digitales de su país, sino también en otros países, reduciendo costos y tiempos, simplificando el uso, aumentando la inclusión y generando mayor confianza.

Las administraciones tributarias desempeñan un rol estratégico dentro del ecosistema digital de un país, por lo que es importante que apoyen y se integren a los sistemas o ecosistemas nacionales de identificación digital. Tal como se expone en el capítulo 2, la relación entre los contribuyentes y la administración tributaria se configura, en la práctica, como predominantemente digital. Algunos países han avanzado hacia modelos multicanal, lo que no sólo consolida su carácter de administración tributaria Digital, sino que también optimiza la experiencia del contribuyente.

Integrar los servicios de la administración tributaria a los sistemas o ecosistemas nacionales de identificaciones digitales tiene varias ventajas. Entre ellas, la posibilidad de que los contribuyentes accedan a los servicios tributarios, así como lo hacen a los demás servicios públicos. Además, se beneficiarán de todo lo que el país invierta en seguridad (como la autenticación continua gestionada por el *broker* de identificación digital) y en la medida en que se vayan agregando nuevos métodos de identificación digital, como el uso de credenciales verificables, sin tener que preocuparse por realizar inversiones propias.

En algunos casos, las administraciones tributarias también pueden analizar la posibilidad de desacoplar su sistema de identificación digital e integrarlo al ecosistema nacional como proveedor bajo determinadas condiciones, de modo que los contribuyentes puedan utilizar la identificación de la administración tributaria para ingresar a otros servicios públicos digitales.

En este contexto, donde las administraciones tributarias delegan la identificación digital en otro proveedor de confianza, es necesario repensar y diseñar un sistema de Autorización basado en roles y permisos en tres niveles: funciones, objetos y datos. Las personas se van a identificar como una persona física o natural frente a la administración tributaria y tendrán roles que los asocien a contribuyentes y les brinden determinados permisos en estos tres niveles.

Otro tema crítico es la auditoría. Con muchos usuarios actuando bajo roles asociados a contribuyentes, es relevante contar con un sistema de auditoría que permita determinar con precisión quién, desde dónde y cuándo se realizó cada acción a lo largo del tiempo. Esto es importante para preservar o restaurar la integridad de la información, contar con evidencia confiable ante fraudes o en casos judiciales y contribuir con datos de calidad a los sistemas de inteligencia tributaria.

Finalmente, dado que la relación entre el contribuyente y la administración tributaria es digital, los procesos de la administración deberían ser pensados en “digital por defecto”, bajo una estrategia omnicanal que facilite y simplifique la interacción con el contribuyente de manera uniforme y estandarizada, independientemente del canal que se use, logrando altos niveles de satisfacción, confianza y transparencia.

3.9. Hoja de ruta

El objetivo de esta sección es presentar una hoja de ruta evolutiva desde la óptica de la identificación digital, pero contemplando otros factores relevantes y asociados, como la autorización, la auditoría y la interoperabilidad en las administraciones tributarias.

En base a la situación actual de las administraciones tributarias analizadas en el capítulo 2, se especifican en forma general dos alternativas diferenciadas en la hoja de ruta, una para un escenario donde no existe un sistema o ecosistema nacional de identificación digital y otra para los países que poseen iniciativas en marcha de identificación digital, esté o no integrada la administración tributaria.

<table>
<tr><th colspan="2">Identificación digital</th></tr>
<tr><th>Escenario sin identificación nacional</th><th>Escenario con identificación nacional</th></tr>
<tr><td>Rediseñar el sistema de identificación digital para que se identifiquen personas físicas o naturales (no empresas) que van a actuar con diferentes roles en cada empresa.

Elegir un set de datos minimalista y universal para identificar personas:

• Minimalista para proteger la privacidad de la información.

• Universal porque en un futuro va a ser relevante poder identificar una persona más allá del contexto de la administración tributaria y el país. Ejemplo: código país – código documento – número de documento.

Realizar los desarrollos tecnológicos y adaptaciones necesarias para que los sistemas se basen en identificación de personas. Es importante que este sistema conviva con el actual y lo vaya sustituyendo gradualmente.

El nuevo sistema de identificación deberá ser único para todos los sistemas y todos los contribuyentes, actuando como un Single Sign On en todas las soluciones de la administración tributaria.</td><td>Rediseñar el sistema de identificación delegando la identificación en el sistema o ecosistema nacional, asumiendo que se identificarán personas físicas o naturales. Se podrá incorporar la identificación nacional en forma alternativa a la de la administración tributaria en forma gradual ir obligando los ingresos al sistema o ecosistema nacional hasta alcanzar el 100%.

Realizar las adecuaciones necesarias para adaptarse a la identificación digital nacional (por ejemplo, en los datos de identidad) y los desarrollos tecnológicos necesarios.</td></tr>
</table>

Identificación digital	
Escenario sin identificación nacional	**Escenario con identificación nacional**
Fortalecer la identificación digital (corto plazo): • Todas las funcionalidades de la administración tributaria deberían exigir identificación digital en todos los canales. • Todas las identificaciones digitales deberían asegurar el uso de una contraseña fuerte y un segundo factor. Se recomienda como mínimo habilitar una aplicación de autenticación y la posibilidad de recibirlo por correo (otras opciones se describen en el capítulo 1.3). • Desarrollar funcionalidades de Autenticación Continua (capítulo 1.2) basada en gestión de riesgos como gestión de dispositivos de confianza, integración a *Security Operation Center* (análisis de eventos de seguridad vinculados a la identificación digital), etc.	Fortalecer la identificación digital (corto plazo): • Todos los accesos a funcionalidades de la administración tributaria deberían exigir identificación digital en todos los canales. • Apoyar a la organización responsable del sistema o ecosistema de identificación digital nacional para fortalecer la identificación digital: o Como mínimo una contraseña fuerte y un segundo factor de autenticación. o Que el sistema o ecosistema nacional desarrolle funcionalidades de Autenticación Continua (capítulo 1.2) basada en gestión de riesgos como la gestión de dispositivos de confianza, integración a *Security Operation Center (*análisis de eventos de seguridad vinculados a la identificación digital), etc. Si el sistema o ecosistema de identificación digital nacional no avanza según los requerimientos de la administración tributaria, la misma podría desarrollar algunas acciones complementarias, como un segundo factor obligatorio luego de ingresar a la administración tributaria y requerimientos vinculados al concepto de Autenticación Continua.
Resiliencia en la identificación digital: • Implementar métodos de identificación digital basados en firma digital. Esto implica implementar una Infraestructura de Claves Públicas (o realizar un convenio con organizaciones especializadas públicas o privadas) para otorgar a cada usuario un método basado en firma digital, en un *token* o *smart card* tal como se comenta en el capítulo 3.1. • Desarrollar estándares y requerimientos para métodos de identificación digital confiables basados en firma digital.	Administración tributaria como Proveedor de Identificación Digital en el ecosistema de identificación digital nacional: Si se considera conveniente (por la administración tributaria y el ente rector del ecosistema nacional), la administración tributaria puede ser un proveedor de identificación digital. Esto implica la realización de desarrollos y eventualmente fortalecer capacidades, para que el sistema de identificación digital de la administración tributaria se integre al ecosistema nacional utilizando uno de los protocolos definidos por el ecosistema nacional (como, por ejemplo, *Open ID Connect* o SAML).

Identificación digital	
Escenario sin identificación nacional	**Escenario con identificación nacional**
• A largo plazo: implementar algoritmos de cifrado resistente a la computación cuántica para la infraestructura de claves públicas de la administración tributaria y distribuir nuevos certificados y claves de firma post-cuánticos para los contribuyentes. En la publicación del NIST, "*Post-Quantum Cryptography*" (NIST, actualizada el 19/11/2025), se detallan los algoritmos.	
Control de acceso	
Rediseñar el sistema de control de acceso para que las personas que ingresen con su identidad digital puedan actuar con diferentes roles sobre las empresas: • Definir roles, por ejemplo: Titular, responsable, contador, abogado, gestor, etc. • Definir operaciones (alta, baja, modificación, edición, lectura, ejecución, etc.). • Definir funcionalidades para cada uno de los procesos de la administración tributaria y para el ciclo de cumplimiento de obligaciones del contribuyente. • Asociar Roles – Operaciones – Funcionalidades En esta primera etapa el sistema de roles podría focalizarse a nivel de funcionalidades.	
Ampliar y potenciar el Control de Acceso gestionado a nivel de objetos y datos: • Identificar los objetos para cada función definiendo las operaciones posibles en cada caso. • Teniendo en cuenta la gobernanza de datos, asociar datos con objetos y roles. Realizar los desarrollos necesarios para implementar el control de acceso en los tres niveles.	
Desarrollar reportes y sistemas de alertas para facilitar el control de acceso a los usuarios, en particular a los responsables de las empresas. En un escenario complejo, donde muchos usuarios ingresarán a la administración tributaria a realizar diversas operaciones en diferentes niveles (funciones, objetos y datos) en nombre de los diferentes contribuyentes ya sean personas físicas o jurídicas, es necesario desarrollar funcionalidades para que los responsables o titulares en cada caso, puedan gestionar en forma simple los accesos, roles y usuarios. Un sistema inteligente de aprobaciones, comprobaciones y alertas puede ser útil para evitar errores y/o fraudes.	

<table>
<tr><th colspan="2">Identificación digital</th></tr>
<tr><th>Auditoría</th><th>Interoperabilidad</th></tr>
<tr><td>Rediseñar un sistema de auditoría integral y detallado que permita registrar todos los movimientos de los usuarios tal como se detalló en el punto 3.5.

Se podrá contemplar la posibilidad de desarrollar un sistema completo de auditoría y, a partir de él, alimentar una fuente de información anonimizada para objetivos estadísticos.

La información de auditoría debería ser considerada como información sensible por lo que deberá contar con herramientas y técnicas para proteger la confidencialidad.</td><td>Si bien la interoperabilidad no depende solamente de la administración tributaria, asumiendo que las demás organizaciones poseen capacidades que habiliten la interoperabilidad con la administración tributaria, se sugiere avanzar en tres líneas (según el diagrama de la figura 12 del capítulo 3.6):

• Interoperabilidad en el Sector Público: Integrarse a la plataforma de interoperabilidad del sector público, participar activamente de su evolución definiendo requerimientos y accesos a datos junto al órgano rector en Gobierno Digital.

• Interoperabilidad entre jurisdicciones: En el marco de acuerdos de intercambio de información tributaria, tanto bilaterales como multilaterales, trabajar en la generación de capacidades operativas efectivas, de modo que la fiscalización internacional se sustente en evidencia confiable, trazable y jurídicamente válida.

• Interoperabilidad con el sector privado: Realizar acuerdos y desarrollar la interoperabilidad con operadores privados de interés como bancos, Fintech, exchanges, tarjetas de crédito, etc.

• Social: Si bien no se especifica en el diagrama de la figura 12 del capítulo 3.6, puede ser importante interactuar con las redes sociales para obtener información de interés.</td></tr>
<tr><th colspan="2">Inteligencia tributaria</th></tr>
<tr><td colspan="2">A medida que avanzan los puntos anteriores, junto a otros factores se podrá sofisticar y potenciar la inteligencia tributaria y lo que impactará positivamente en ahorro de costos y tiempos, transparencia, justicia y recaudación, entre otros.

En términos generales, para lograr un escenario maduro y sofisticado en inteligencia tributaria, es necesario contemplar los siguientes puntos:

• Infraestructura.

• Información: incorporar fuentes de información como la identificación digital, el control de acceso, la auditoría, otras fuentes internas y las fuentes que se puedan acceder según lo comentado anteriormente en interoperabilidad.</td></tr>
</table>

Identificación digital
• *Data lakes* (repositorios centralizados de datos) estructurados para realizar diferentes tipos de análisis. • Gobernanza y calidad de datos: asociado a lo anterior, es importante que esté claramente definida la gobernanza de datos y se cuente con políticas, herramientas y técnicas que aseguren un nivel alto en la calidad de datos. • Herramientas de análisis de datos, en algunos casos utilizando Inteligencia Artificial, como, por ejemplo: o Herramientas que analicen datos en tiempo real y en forma automatizada. o Herramientas que permitan generar modelos analíticos de riesgos y segmentación de contribuyentes. o Modelos de cumplimiento y predictivos. o Herramientas para desarrollar controles, alertas o detección de anomalías. o Se podrían utilizar herramientas RPA (*Robotic Process Automation* o Automatización Robótica de Procesos) con decisiones no determinísticas, sino mediante aprendizaje. o Herramientas geoespaciales, por ejemplo, para tributos que tienen que ver con reconocimiento de bienes suntuosos en terrenos.

La tabla anterior no determina precedencias ni dependencias; es decir, no es requisito alcanzar un nivel “resiliente” en identificación digital para comenzar a avanzar en ámbitos como la auditoría, la interoperabilidad o la inteligencia tributaria. El foco principal de este documento es la identificación digital en las administraciones tributarias; otros aspectos relevantes se presentan de manera general y, por ello, puede que no se incluyan todos los elementos necesarios para un abordaje integral.

Glosario y abreviaciones

Término	Definición
AAL	Del inglés *Authenticator Assurance Level*, nivel de Fortaleza de la autenticación. Utilizado en ISO/IEC 29115 y en NIST para definir los niveles de seguridad en la autenticación.
ABAC	Del inglés *Attribute-Based Access Control* (Control de Acceso Basado en Atributos). Es un modelo de control de acceso donde las decisiones (permitir o denegar) se toman según atributos del usuario, del recurso, del entorno y de la acción, en lugar de depender solo de roles fijos.
AECID	Agencia Española de Cooperación para el Desarrollo.
ANSI	*American National Standards Institute*. Es una organización estadounidense que coordina el desarrollo de estándares nacionales para múltiples industrias: tecnología, seguridad, telecomunicaciones, ingeniería, salud, manufactura, etc.
API	Del inglés *Application Programming Interface*. Una API es una interfaz que permite que dos programas o sistemas se comuniquen entre sí de forma sencilla y segura.
Autenticación	Proceso mediante el cual se verifica la identidad de una persona, sistema o dispositivo. En otras palabras, sirve para asegurarse de que alguien es quien dice ser. Se puede realizar mediante una contraseña, una huella dactilar, una comparación biométrica de una imagen facial, entre otros factores.
BID	Banco Interamericano de Desarrollo.
Blockchain	Es una tecnología de registro distribuido que permite almacenar información de forma segura, inmutable, transparente y sin necesidad de un intermediario central.
Bluetooth	Estándar de comunicación inalámbrica de corto alcance que permite la transmisión de datos entre dispositivos electrónicos mediante ondas de radio en la banda de 2,4 GHz. Su objetivo principal es facilitar la conectividad sin necesidad de cables, garantizando interoperabilidad entre equipos de diferentes fabricantes.
Broker de identificaciones digitales	Sistema informático que se posiciona entre servicios digitales y proveedores de identificación reconocidos para su ecosistema. De esta forma, uno o más proveedores se integran al *broker* y muchos servicios digitales utilizan el *broker* para ofrecer a sus usuarios diferentes métodos de identificación digital.
Canales digitales	Son todos los medios o plataformas en línea que se usan para comunicarse, interactuar o hacer negocios a través de internet tales como portales web, correo electrónico, redes sociales, WhatsApp, entre otros.
Chatbots	Es un programa o sistema que puede simular una conversación con personas, ya sea por texto o voz. Su objetivo es responder preguntas, ayudar con tareas o brindar información, todo de forma automática, generalmente basado en el uso de inteligencia artificial.

Término	Definición
Comparación biométrica de imagen facial	Se trata de algoritmos especializados para comparar dos imágenes. Aplicado a la identificación digital, en caso de que el sistema tenga acceso a una foto de la cara de la persona, previamente registrada u obtenida desde el registro público se le puede tomar una imagen facial a la persona y comparar esta imagen con la del registro previo. Es una técnica que se puede utilizar para validar la identificación de una persona, similar a lo que podría ser la comparación de una huella dactilar.
Control de acceso	Un sistema informático, luego que una persona se identifica digitalmente, posee un sistema para determinar a qué información y funcionalidades puede acceder, en función del nivel de confianza de la identificación digital que utilizó y sus roles en la organización.
Cuenta única	Equivalente a "Identificación Digital Nacional", en algunos países suele llamarse cuenta única a una única identificación digital (posiblemente usuario / contraseña) para ingresar a muchos servicios digitales del sector público.
CIAT	Centro Interamericano de Administraciones Tributarias.
DAT	Del inglés *Discretionary Access Control*, es modelo de control de acceso donde el propietario del recurso (archivo, registro, base de datos, documento) tiene la capacidad de delegar permisos a otros usuarios.
Data lakes	Repositorio centralizado que almacena grandes volúmenes de datos en su forma cruda (sin procesar), tal como llegan desde múltiples fuentes: bases de datos, aplicaciones, logs, sensores, APIs, dispositivos IoT, etc.
Deepfake	Es un contenido audiovisual manipulado mediante inteligencia artificial, generalmente redes neuronales profundas, para alterar la apariencia, voz o acciones de una persona, haciéndolo parecer real, aunque sea falso.
DID	Del inglés Decentralized Identifiers, son un nuevo tipo de identificadores digitales diseñados para permitir identidad soberana, descentralizada e interoperable, sin depender de un proveedor central (gobierno, empresa, plataforma).
Dispositivos de confianza	En el contexto de la identificación digital, muchos sistemas informáticos tienen desarrollada una funcionalidad para que un usuario gestione sus dispositivos de confianza. Cuando un usuario ingresa al sistema con su computadora o dispositivo móvil, el sistema obtiene una huella del dispositivo (información que lo identifica) y le permite al usuario guardarlo asociado a su identificación digital como de confianza. Esto implica que cada vez que el usuario ingrese con un dispositivo de confianza el sistema podría no exigirle un segundo factor, asumiendo que hay menos riesgo ya que el dispositivo que el usuario utiliza comúnmente para ingresar al sistema.
eIDAS	Reglamento Europeo de Identidad Digital, Servicios de Confianza y Transacciones Electrónicas. Define cómo deben funcionar las identidades digitales, firmas electrónicas, sellos, certificados y servicios de confianza en la Unión Europea.
FAL	Del inglés *Federation Assurance Level*. Nivel de confianza en el *token* en un sistema federado de autenticación. Utilizado en ISO/IEC 29115 y en NIST para definir los niveles de confianza entre los proveedores de identificación en un sistema federado de autenticación.
FIDO	Del inglés *Fast IDentity Online*, es un estándar internacional de autenticación fuerte sin contraseñas, diseñado para reemplazar claves tradicionales por métodos más seguros, más rápidos y resistentes al phishing.

Término	Definición
FIPS	Del inglés *Federal Information Processing Standards*. Son estándares técnicos y de seguridad publicados por el NIST (*National Institute of Standards and Technology*) de Estados Unidos.
G20	Foro internacional que reúne a las 20 economías más importantes del mundo para coordinar políticas económicas, financieras y estratégicas a nivel global.
Gobierno Digital	El gobierno digital es el uso de tecnologías digitales (como internet, aplicaciones, plataformas en línea, inteligencia artificial, etc.) para que los gobiernos presten servicios, se comuniquen con los ciudadanos y gestionen procesos de forma más eficiente, transparente y accesible.
Google *Authenticator*	Es una aplicación móvil gratuita de Google que se utiliza para generar OTPs. Esta aplicación se configura con el sistema informático, sincronizando algoritmos para la generación de códigos de un solo uso de modo que el usuario cuando va a ingresar el segundo factor de autenticación ingresa el código otorgado por Google *Authenticator*, que debería coincidir con el código que espera el sistema informático para validar su identificación.
GPS	Del inglés *Global Positioning System.* Sistema mundial de navegación por satélite que permite determinar la posición geográfica de un objeto o persona en cualquier lugar del planeta con alta precisión.
Hash	Es el resultado de aplicar una función hash, es decir, un algoritmo criptográfico que convierte cualquier dato (texto, archivo, contraseña, transacción, etc.) en una cadena fija de caracteres.
HSM	Del inglés *Hardware Security Module*. Dispositivo físico especializado que ha sido diseñado para proteger y gestionar claves criptográficas de manera segura. Se utiliza para realizar operaciones críticas como el cifrado, descifrado, generación y almacenamiento de claves, garantizando altos niveles de seguridad frente a accesos no autorizados.
HTML	Del inglés *HyperText Markup Language*. Es el lenguaje estándar que define la estructura de todas las páginas web en Internet.
IAL	Del inglés *Identity Assurance Level*. Nivel de verificación de la identidad. Utilizado en ISO/IEC 29115 y en NIST para definir los niveles de seguridad en identificaciones digitales.
ICAO	*International Civil Aviation Organization* (Organización de Aviación Civil Internacional). Es un organismo especializado de las Naciones Unidas encargado de regular, coordinar y estandarizar la aviación civil internacional, incluyendo temas de seguridad aérea, documentación de viaje y pasaportes electrónicos.
Identificación Digital en la administración tributaria	Sistema para identificarse digitalmente en los sistemas informáticos de la administración tributaria (posiblemente usuario / contraseña).
Identificación Digital Nacional	Se refiere a un sistema unificado de identificación digital, donde los usuarios utilicen una única identificación (posiblemente usuario / contraseña) para identificarse en muchos sistemas informáticos en el sector público.
IdLAC	Modelo de Identificación Digital para América Latina y el Caribe.
IETF	*Internet Engineering Task Force*. Es la organización internacional encargada de desarrollar y estandarizar los protocolos técnicos que hacen funcionar Internet.

Término	Definición
Infraestructura de Claves Públicas	La Infraestructura de Claves Públicas (PKI, por sus siglas en inglés) es el conjunto de tecnologías, procesos y entidades que permiten usar criptografía de clave pública para: • autenticar identidad, • firmar digitalmente, • cifrar y descifrar información, • garantizar integridad y no repudio. Es la base técnica de firmas digitales, certificados electrónicos, pasaportes electrónicos, eID, HTTPS, banca, gobiernos digitales, etc.
ISO	*International Organization for Standardization* (Organización Internacional de Normalización). Es el organismo mundial que desarrolla y publica estándares internacionales para casi todas las industrias: tecnología, calidad, salud, seguridad, medio ambiente, energía, producción, logística, etc.
ITU	Del inglés *International Telecommunication Union.* Es un repertorio oficial de términos técnicos en telecomunicaciones y tecnologías de la información, disponible en varios idiomas y actualizado de forma constante.
JSON	Del inglés *JavaScript Object Notation.* Formato ligero de intercambio de datos basado en texto, fácil de leer y escribir para las personas, y sencillo de procesar por las máquinas. Se utiliza ampliamente para estructurar información en pares clave–valor y listas ordenadas, facilitando la comunicación entre sistemas y aplicaciones.
keyloggers	Programa malicioso o dispositivo físico diseñado para registrar todas las teclas que una persona escribe en un teclado (computadora, tablet o celular), normalmente sin que la víctima lo note.
LEI	Del inglés *Legal Entity Identifier* es un identificador global único de 20 caracteres usado para identificar entidades legales que participan en transacciones financieras en cualquier parte del mundo.
MAC	Del inglés *Mandatory Access Control* (Control de Acceso Mandatorio). Es uno de los modelos de control de acceso más estrictos, usado cuando la seguridad debe ser centralizada, rígida y no delegable.
Malware	Malware es un término que engloba cualquier tipo de software malicioso diseñado para dañar, interrumpir o robar información de un sistema informático o dispositivo. La palabra proviene de "*malicious software*" (software malicioso) y se refiere a programas creados con fines perjudiciales o criminales.
MFA	Del inglés *Multi-Factor Authentication* (Autenticación Multifactor). Es un método de autenticación que requiere dos o más factores independientes para verificar la identidad de un usuario antes de permitir el acceso.
NFC	Del inglés *Near Field Communication*. Es una tecnología de comunicación inalámbrica de corto alcance que permite que dos dispositivos se comuniquen entre sí simplemente acercándolos (a unos pocos centímetros).

Término	Definición
NIST	*National Institute of Standards and Technology* (Instituto Nacional de Estándares y Tecnología de Estados Unidos).
Niveles de seguridad	En el contexto de la identificación digital se refiere a que puede haber diferentes grados de seguridad o confianza en el uso de las identificaciones digitales. Un nivel bajo podría ser cuando alguien utiliza una identificación que no ha sido validada, un nivel más alto en confianza es cuando alguien utiliza una identificación que fue validada por un tercero y utiliza un segundo factor de autenticación de modo que el sistema informático al cual la persona está ingresando tiene un alto grado de confianza en esa identificación digital.
NTP	Del inglés *Network Time Protocol*. Es un protocolo que permite sincronizar la hora exacta entre computadoras, servidores y dispositivos a través de una red.
OCDE	Organización para la Cooperación y el Desarrollo Económico.
OEA	Organización de los Estados Americanos.
OIDC	Del inglés *OpenID Connect*, es un estándar moderno de autenticación que permite que un usuario inicie sesión en una aplicación usando la identidad gestionada por otro proveedor.
OIDC4VC	Del inglés *OpenID Connect for Verifiable Credentials*. Es una extensión de OIDC que permite emitir y enviar Credenciales Verificables a una billetera electrónica en el teléfono móvil del usuario.
OIDC4VP	Del inglés *OpenID Connect for Verifiable Presentations*. Es una extensión del estándar OIDC que permite presentar Credenciales Verificables desde billeteras electrónicas como método para identificarse digitalmente.
OTP	Del inglés *one time password* o código de un solo uso. Se utiliza como segundo factor de autenticación, el sistema informático genera un código de un solo uso y se lo envía al usuario a través de un medio conocido por ambos (correo, SMS, WhatsApp, etc.). El usuario lo recibe por otro medio y lo ingresa al sistema, si ingresa el código correcto se verifica el usuario.
Passkeys	Nombre comercial de la tecnología de autenticación sin contraseñas basada en estándares FIDO2 + WebAuthn, creada para reemplazar definitivamente las contraseñas tradicionales.
Passwordless	Modelo de autenticación sin contraseñas, donde los usuarios acceden a sistemas usando métodos más seguros y simples como biometría, llaves criptográficas o enlaces de verificación, en lugar de memorizar y escribir contraseñas.
Phishing	Es una técnica de engaño usada por ciberdelincuentes para robar información personal como contraseñas, datos bancarios, tarjetas de crédito, o incluso acceso a redes sociales o correos electrónicos u otra información sensible.
PKI	Del inglés *Public Key Infrastructure.* Es un conjunto de tecnologías, políticas, entidades y procedimientos que permiten emitir, gestionar, distribuir y revocar certificados digitales y claves criptográficas de manera segura y confiable.
Proveedores de identificación	Organización que cumple con determinada normativa y entrega identificaciones digitales a usuarios. De esta forma, las personas concurren a esta organización reconocida para obtener y validar su usuario y crear su contraseña, así como registrar sus datos de contacto. Utilizan esta identificación para ingresar a sistemas informáticos.

Término	Definición
QR	Del inglés *Quick Response code*, es un tipo de código de barras bidimensional que puede almacenar información en un patrón de puntos negros y blancos.
Quishing	Es una forma de phishing que usa códigos QR para engañar a las personas y llevarlas a sitios maliciosos, robar credenciales o infectar dispositivos.
RBAC	Del inglés *Role-Based Access Control* (Control de Acceso Basado en Roles). Es uno de los modelos de control de acceso más usados en empresas, gobiernos y sistemas informáticos donde los accesos a objetos son definidos a partir de roles y los usuarios son asociados a roles.
Red Gealc	Red de Gobierno Electrónico en América Latina y el Caribe. Red para impulsar la cooperación entre países para el desarrollo del Gobierno Digital.
RFID	Del inglés *Radio Frequency Identification*. Tecnología de identificación automática que utiliza ondas de radio para transmitir datos entre un lector y una etiqueta o dispositivo electrónico. Permite reconocer, rastrear y gestionar objetos o personas sin necesidad de contacto físico ni línea de visión directa.
RPA	Del inglés *Robotic Process Automation.* Tecnología para Automatización Robótica de Procesos.
Segundo factor de autenticación (2FA)	El usuario se identifica digitalmente con su identificador (número de documento, correo, etc.), luego ingresa un primer factor de autenticación (como una contraseña, por ejemplo) y a continuación, el sistema le exige un segundo factor. Generalmente se implementa mediante el envío de un código de un solo uso a su dispositivo móvil (SMS, WhatsApp o similar) o a su correo electrónico, pero puede haber otros medios. En la actualidad se considera importante contar con un 2FA para fortalecer la identificación digital.
SAML	Del inglés *Security Assertion Markup Language*. Es un estándar de autenticación y federación de identidad que permite que un usuario inicie sesión en un sistema usando la identidad gestionada por otro proveedor.
SIEM	*Security Information and Event Management*, es una plataforma de seguridad informática que centraliza, correlaciona y analiza eventos provenientes de múltiples sistemas para detectar amenazas, responder incidentes y cumplir normas de auditoría.
Single Sign-On (SSO)	Inicio de sesión única. Mecanismo de autenticación que permite a un usuario acceder a múltiples aplicaciones, sistemas o servicios con una sola credencial (usuario y contraseña, certificado, token, etc.). Una vez validada la identidad en el sistema principal, el usuario no necesita volver a autenticarse en cada aplicación vinculada.
Smishing	Es un tipo de phishing por SMS. El atacante envía un mensaje de texto falso para engañar a la víctima.
SMS	*Short Message Service*. Es el servicio estándar de mensajería de texto que permite enviar y recibir mensajes cortos entre teléfonos móviles.
SOC	*Security Operations Center*, es el centro de operaciones de seguridad de una organización. Es un equipo especializado —con personal, procesos y tecnología— encargado de monitorear, detectar, analizar y responder a incidentes de ciberseguridad en tiempo real.

Término	Definición
Técnicas de fuerza bruta	Método de ataque utilizado en seguridad informática que consiste en probar sistemáticamente todas las combinaciones posibles de credenciales (como contraseñas o claves criptográficas) hasta encontrar la correcta.
Texto plano	Formato de representación de datos que contiene únicamente caracteres legibles por humanos, sin ningún tipo de formato, estilo, codificación especial ni elementos multimedia.
Timestamping	**Timestamping** (o **sellado de tiempo**) es un **mecanismo criptográfico** que permite demostrar **cuándo** ocurrió un evento digital, **sin posibilidad de alteración**. Sirve para probar que un documento, archivo, transacción o dato **existía en un momento exacto** y **no fue modificado después** y consiste en sellar un documento estampando a partir de una autoridad de tiempo habilitada.
Token físico	Es un dispositivo físico que genera OTPs. Se configura sincronizándose con el sistema informático, de modo que los dos generen el mismo código de un solo uso en un período de tiempo determinado, por lo que el usuario cuando va a ingresar el segundo factor de autenticación ingresa el que le indica el token físico, que debería ser el mismo que espera la aplicación. En ese caso se valida la identificación del usuario.
TOTP	*Time-based One-Time Password*, Contraseña de un solo uso basada en tiempo y es un método de autenticación de dos factores (2FA) o multifactor (MFA).
UBO	*Ultimate Beneficial Owner*, Beneficiario Final. Es la persona física que, en última instancia, posee, controla o se beneficia de una empresa, cuenta bancaria, trust, fundación o estructura jurídica.
UE	Unión Europea.
URI	*Uniform Resource Identifier*, es un identificador estándar que se usa en Internet para nombrar, localizar o identificar un recurso, ya sea una página web, un archivo, un servicio, un usuario, un DID, etc.
Usabilidad	Facilidad de uso de un sistema informático.
USB	Del inglés *Universal Serial Bus*. Es un estándar de conexión física y comunicación usado para conectar dispositivos (computadoras, teléfonos, teclados, cámaras, pendrives, etc.) y transferir energía y datos de forma sencilla y universal.
Vishing	Es un tipo de *phishing* por voz, donde el atacante usa llamadas telefónicas (tradicionales o VoIP) para engañar a una persona y lograr que entregue datos personales, credenciales, códigos MFA, información bancaria o realice pagos.
W3C	Del inglés, *World Wide Web Consortium*, es el organismo internacional que define los estándares técnicos de la Web.
XML	Del inglés *eXtensible Markup Language*. Es un lenguaje de marcas diseñado para almacenar, estructurar y transportar datos de manera organizada, legible y estandarizada.

Referencias

Agencia de Gobierno Electrónico, Sociedad de la Información y del Conocimiento. (n.d.). *ID Uruguay*. https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/id-uruguay

Banco Interamericano de Desarrollo. (2023). *Índice de madurez digital: Cómo medir el avance de la transformación digital en las administraciones tributarias*. https://blogs.iadb.org/gestion-fiscal/es/indice-de-madurez-digital-como-medir-el-avance-de-la-transformacion-digital-en-las-administraciones-tributarias/

Bray, T. (2017). *The JavaScript Object Notation (JSON) data interchange format (RFC 8259)*. RFC Editor. https://www.rfc-editor.org/rfc/rfc8259

CIAT. (2020). *Las TIC como herramienta estratégica para potenciar la eficiencia de las administraciones tributarias*. https://biblioteca.ciat.org/opac/book/5731

CIAT. (2025). *Cómo los datos de las empresas pueden "hablar" entre sí: El Identificador de Personas Jurídicas (IPF)* (Nuria Vegas). https://ciat.org/ciatblog-how-companies-data-can-talk-to-each-other-the-legal-entity-identifier-lei-a-g20-initiative-for-transparency-and-efficiency-in-international-transactions/

Comisión Europea. (n.d.). *eID – Identificación electrónica*. https://ec.europa.eu/digital-building-blocks/sites/display/DIGITAL/eID

Comisión Europea. (n.d.). *Identidad digital europea*. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_es

Comisión Europea. (n.d.). *EU Login: Iniciar sesión con su eID*. https://ecas.ec.europa.eu/cas/login?loginRequestId

FIDO Alliance. (n.d.). *FIDO Alliance*. https://fidoalliance.org/

FIDO Alliance. (n.d.). *FIDO authentication: A passwordless vision*. https://fidoalliance.org/fido2/

Fusillo, M. (2021, mayo 12). *Los 10 principios de la self-sovereign identity*. Self Sovereign Identity. https://www.selfsovereignidentity.it/los-10-principios-de-la-self-soveregn-identity/

Gobierno Federal de Brasil. (n.d.). *Gov.br – Portal único del gobierno federal*. https://www.gov.br/pt-br

International Civil Aviation Organization. (n.d.). *Document 9303 – Machine readable travel documents*. https://www.icao.int/publications/doc-series/doc-9303

International Organization for Standardization. (2012). *Guidelines for identification, collection, acquisition and preservation of digital evidence (ISO/IEC 27037:2012)*. https://www.iso.org/standard/44381.html

International Organization for Standardization. (2013). *Information technology — Security techniques — Entity authentication assurance framework (ISO/IEC 29115:2013, revised 2020)*. https://www.iso.org/es/contents/data/standard/04/51/45138.html

International Telecommunication Union. (n.d.). *ICT indicators for the SDGs*. https://www.itu.int/en/ITU-D/Statistics/Pages/SDGs-ITU-ICT-indicators.aspx

Lodderstedt, T., Yasuda, K., Looker, T., & Bastian, P. (2023, July 13). *OpenID for verifiable presentations 1.0*. OpenID Foundation. https://openid.net/specs/openid-4-verifiable-presentations-1_0.html

Lodderstedt, T., Yasuda, K., Looker, T., & Bastian, P. (2025, September 16). *OpenID for verifiable credential issuance 1.0*. OpenID Foundation. https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html

M'Raihi, D., Machani, S., Pei, M., & Rydell, J. (2011). *TOTP: Time-based one-time password algorithm (RFC 6238)*. Internet Engineering Task Force. https://doi.org/10.17487/RFC6238

Ministerio de Salud Pública de Uruguay. (n.d.). *Solicitud de constancias para transporte de yerba mate*. https://www.gub.uy/tramites/solicitud-constancias-transporte-yerba-mate

National Institute of Standards and Technology. (2017). *Digital identity guidelines (NIST Special Publication 800-63)*. https://www.nist.gov/itl/applied-cybersecurity/special-publication-800-63

National Institute of Standards and Technology. (n.d.). *Federal Information Processing Standards (FIPS) publications*.

National Institute of Standards and Technology. (n.d.). *Digital identity guidelines (NIST SP 800-63-4)*. https://pages.nist.gov/800-63-4/

National Institute of Standards and Technology. (2025). *Post-quantum cryptography* (Actualizado al 19/11/2025). https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-3-submissions

OCDE. (2020). *Administración tributaria 3.0: La transformación digital de la administración tributaria*. http://www.oecd.org/tax/forum-on-tax-administration/publications-and-products/taxadministration-3-0-the-digital-transformation-of-tax-administration.htm

OCDE. (2024). *Administración tributaria: Información comparativa sobre los países de la OCDE y otras economías avanzadas y emergentes*. https://www.oecd.org/es/publications/administracion-tributaria-2024_ac2f5866-es.html

OCDE. (2025). *Tax administration digitalization and digital transformation initiatives*. https://www.oecd.org/en/publications/tax-administration-digitalisation-and-digital-transformation-initiatives_c076d776-en/full-report.html

OpenID Foundation. (2014). *OpenID Connect core specification*. https://openid.net/

OpenID Foundation. (2023). *OpenID for verifiable credentials (OpenID4VC)*. https://openid.net/sg/openid4vc/

Organization for the Advancement of Structured Information Standards. (2005). *Security assertion markup language (SAML) V2.0*. https://www.oasis-open.org/standard/saml/

Presidencia de la Nación Argentina. (n.d.). *Autenticar*. https://www.argentina.gob.ar/jefatura/innovacion/autenticar

Red de Gobierno Electrónico de América Latina y el Caribe. (n.d.). *Sitio oficial de la Red GEALC*. https://www.redgealc.org/

Resnick, P. (2008). *Internet message format (RFC 5322)*. Internet Engineering Task Force. https://doi.org/10.17487/RFC5322

Sporny, M., Longley, D., & Lindström, N. (2023, October 3). *Verifiable credentials data model v2.0*. World Wide Web Consortium (W3C). https://www.w3.org/TR/vc-data-model-2.0/

Unidad de Certificación Electrónica. (2023). *Primer caso de uso de identificación digital transfronteriza entre Brasil y Uruguay*. https://www.gub.uy/unidad-certificacion-electronica/comunicacion/noticias/primer-caso-uso-identificacion-digital-transfronteriza-entre-brasil-uruguay

Unidad Reguladora de Servicios de Energía y Agua. (n.d.). *Trámites y servicios disponibles para identificaciones brasileñas*. https://www.gub.uy/unidad-reguladora-servicios-energia-agua/tramites-y-servicios/tramites

Unión Europea. (2014). *Reglamento (UE) n.º 910/2014 sobre identificación electrónica y servicios de confianza para las transacciones electrónicas en el mercado interior (Reglamento eIDAS)*. Diario Oficial de la Unión Europea. https://eur-lex.europa.eu/eli/reg/2014/910/oj

Unión Europea. (2014). *Reglamento eIDAS sobre identificación electrónica y servicios de confianza para las transacciones electrónicas en el mercado interior*. https://digital-strategy.ec.europa.eu/es/policies/eidas-regulation

Unión Europea. (2024). *Reglamento (UE) 2024/1183 sobre la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (Reglamento eIDAS 2.0)*. Diario Oficial de la Unión Europea. https://eur-lex.europa.eu/eli/reg/2024/1183/oj

Unión Europea. (2024). *Marco europeo de identidad digital*. https://eur-lex.europa.eu/eli/reg/2024/1183/oj

Unión Europea. (n.d.). *Identidad digital europea (eID)*. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_es

Ventanilla Única de Comercio Exterior (VUCE) de Uruguay. (n.d.). *Ventanilla Única de Comercio Exterior*. https://vuce.gub.uy

Verified Market Reports. (n.d.). *NFC-enabled handsets market*. https://www.verifiedmarketreports.com/product/nfc-enabled-handsets-market/

World Economic Forum. (2025). *The global risks report 2025*. https://www.weforum.org/publications/global-risks-report-2025/

World Economic Forum. (2025). *Global cybersecurity outlook 2025*. https://www.weforum.org/publications/global-cybersecurity-outlook-2025/

World Wide Web Consortium. (2008). *Extensible markup language (XML) 1.0 (Fifth edition)*. https://www.w3.org/TR/REC-xml/

World Wide Web Consortium. (n.d.). *World Wide Web Consortium (W3C)*. https://www.w3.org/

Anexo I. Encuesta de relevamiento

En este anexo se presenta el formulario utilizado para la encuesta de relevamiento de información a las administraciones tributarias.

Datos de la administración tributaria

Por favor complete la siguiente tabla:

Sobre la administración tributaria
Nombre
País
Portal Web
Responsable en la administración tributaria por el cuestionario
Nombre
Cargo
Teléfono
Correo Electrónico
Referente en informática
Nombre
Cargo
Teléfono
Correo Electrónico

Sección A. Identificación digital nacional

En esta sección se espera relevar información sobre la identificación digital a nivel nacional, si en su país no existe una iniciativa (independientemente de su grado de desarrollo) al respecto, por favor continue con la sección B.

¿Qué organización posee la rectoría de la identificación digital nacional?	
¿Qué organización posee la rectoría de la identificación digital nacional?	
Por favor ingrese el enlace (link) al portal de la organización:	
¿Qué organización implementa la id digital nacional? (si es la misma que la rectoría, puede saltear esta pregunta)	
Por favor ingrese el enlace (link) al sistema de identificación digital nacional.	
Por favor ingrese un enlace (link) a la normativa de la identificación digital nacional.	

Uso y características de la identificación digital nacional	
Situación actual de la identificación digital nacional con respecto a la integración de servicios digitales públicos (por favor marque en negrita o bold la opción correcta).	1. Existe una iniciativa que no ha comenzado a implementarse 2. Existe una iniciativa en proceso, integrada a muy pocos servicios digitales 3. Existe una iniciativa en proceso, integrada a muchos servicios digitales, pero menos del 50% 4. Existe una iniciativa en proceso, integrada a la mayoría de los servicios digitales. 5. La identificación digital está integrada a todos los servicios digitales públicos.
Proveedores de identificaciones digitales disponibles en la identificación digital nacional (por favor marque en negrita o bold la opción correcta).	1. Existe un único proveedor “cuenta única” y no hay planes de integrar nuevos proveedores. 2. Existe un único proveedor “cuenta única” y hay planes de integrar nuevos proveedores. 3. Existe más de un proveedor de identificación digital disponibles en el sistema de identificaciones digitales nacionales.

Uso y características de la identificación digital nacional	
Relación con el sector privado (por favor marque con negrita o bold las opciones correctas)	1. El sistema de identificación digital no tiene ninguna relación con el sector privado. 2. Si bien no hay ninguna relación, está previsto incluir al sector privado en el sistema de identificación digital nacional. 3. Existen sistemas informáticos privados integrados a la identificación digital nacional por lo que un usuario puede usar su ID para acceder al sector público y a algunos privados. 4. Existen proveedores de identificación digital disponibles en el sistema de identificación digital nacional.
El sistema de identificación digital nacional distingue diferentes tipos de usuarios. Por favor selecciones con negrita o bold las opciones correctas.	1. El sistema identifica personas (naturales o físicas), no hay distinción de sus roles o relaciones. 2. El sistema gestiona además personas jurídicas. 3. Entre las personas naturales, se distingue a funcionarios públicos. 4. Entre las personas naturales, se distingue a extranjeros. 5. Se distinguen los siguientes tipos de usuarios [COMPLETAR]:
¿Qué información de cada usuario gestiona el sistema de identificación digital nacional? Por favor seleccione con negrita	1. Número de identificación nacional 2. Número de identificación estatal o de provincia 3. Nombres y apellidos o razón social 4. Residencia o domicilio 5. Sexo 6. Fecha de nacimiento 7. País 8. Correo electrónico 9. Número de teléfono celular 10. Fotografía (facial). 11. Firma (hológrafa escaneada). 12. Contiene otros atributos o datos relevantes para administraciones tributarias (por ejemplo, funcionario público, representante de empresa, etc.). Por favor detallar:
El sistema gestiona más de un nivel de seguridad en las identificaciones digitales. Por favor marque con negrita o bold las opciones correctas. **Aclaración**: si esta información existe en un portal, sugerimos que solamente ingrese el enlace (link), no es necesario contestar la pregunta.	1. Confianza baja: usuario registrado en línea cuyos controles no aseguran su identidad. 2. Confianza media: usuario validado por diferentes medios (presencial, con biometría, biometría + prueba de vida, etc.). 3. Confianza muy alta: usuario validado con autenticación fuerte (más de un factor de autenticación, uso de biometría o firma digital, etc.)

Relación entre la identificación digital nacional y la administración tributaria	
¿La administración tributaria está integrada al sistema de identificación digital nacional? Por favor seleccione con negrita o bold las opciones correctas.	1. No está y no hay planes de hacerlo. 2. No está, pero está planificado integrarse. 3. La administración tributaria es un proveedor de identificación digital en el sistema nacional. 4. La administración tributaria está integrada, los contribuyentes pueden usar la identificación de la administración tributaria o la identificación nacional. En este caso: a. Muy pocos contribuyentes ingresan a la administración tributaria con identificación digital nacional. b. El uso entre la identificación digital nacional y la de la administración tributaria es similar por parte de los contribuyentes. c. La mayoría de los contribuyentes utiliza la identificación digital nacional para ingresar a la administración tributaria. 5. Además de la opción 4, el objetivo de la administración tributaria es ir utilizando cada vez más la identificación digital nacional e ir “apagando” la identificación digital de la administración tributaria 6. La administración tributaria está integrada y solamente se puede utilizar la identificación digital nacional para ingresar a la administración tributaria.
Teniendo en cuenta los niveles de seguridad de la identificación digital nacional, ¿qué niveles acepta la administración tributaria? Por favor seleccione con negrita o bold las opciones correctas.	1. Confianza baja 2. Confianza media 3. Confianza muy alta
Es posible obtener o validar una identificación digital nacional en las oficinas de la administración tributaria. Por favor seleccione con negrita o bold la opción correcta.	1. No 2. Si
¿Cuáles cree son los principales desafíos y oportunidades de mejora a futuro en la identificación digital nacional?	Respuesta:
¿Cuáles cree son los principales beneficios para los usuarios y los sistemas informáticos de integrarse al sistema de identificación digital nacional?	Respuesta:

Sección B. Identificación digital en la administración tributaria

En esta sección se espera relevar información sobre la identificación digital de la administración tributaria, independientemente de que exista o no un sistema nacional de identificación digital. Si la administración tributaria está totalmente integrada a la identificación digital nacional y solamente utiliza la identificación digital nacional por favor continúe con la sección C.

Características de la identificación digital de la administración tributaria	
Cuando un contribuyente va a ingresar a la administración tributaria, usualmente se le solicita un identificador (código de usuario).	1. El número identificador del contribuyente. En el caso de personas jurídicas, todos los usuarios vinculados con la empresa comparten un usuario-contraseña. 2. El número identificador del contribuyente. Si bien hay un único número de contribuyente por persona jurídica hay un método para distinguir qué persona natural está operando en nombre de la persona jurídica. El método funciona de la siguiente forma: 3. Un identificador de usuario y el sistema de la administración tributaria ya previamente conoce a qué personas jurídicas está relacionado el usuario. 4. Otro [Especificar]:
Con respecto a los métodos de autenticación habilitados, una vez el usuario ingresa, por favor marque con negrita o bold las opciones correctas.	1. Se utiliza una contraseña y no existe una política de contraseñas fuertes. 2. Existe una política de contraseñas que asegura (y obliga) a los usuarios a mantener contraseñas fuertes. 3. Con respecto a la posibilidad de utilizar un segundo factor de autenticación (seleccione con negrita o bold la opción correcta): a. Obligatorio para todos los usuarios. b. Obligatorio para algunos sectores de usuarios. c. Opcional para todos los usuarios. d. No existe la posibilidad de utilizar un segundo factor de autenticación. 4. En caso de existir un segundo factor (obligatorio o no), por favor seleccione los métodos disponibles para los usuarios (seleccione con negrita o bold las opciones correctas): a. OTP (one time password o código de un solo uso) al correo o celular (SMS, WhatsApp o similar). b. Aplicación de autenticación como Google Authenticator o similar. c. Token físico otorgado por la administración tributaria. d. Comparación biométrica de imagen facial con una imagen guardada en el sistema de una persona asociada a la empresa. e. Comparación biométrica de imagen facial con una imagen guardada en el sistema previa prueba de vida de una persona asociada a la empresa. f. Otro (detallar): [COMPLETAR]

Características de la identificación digital de la administración tributaria	
Con respecto al control de acceso y roles de la identificación digital de la administración tributaria. Por favor marque con negrita o bold las opciones correctas.	1. El sistema determina si el usuario es un contribuyente, funcionario de la administración tributaria, administrador del sistema, una persona natural o persona jurídica, etc. 2. En caso de ser una persona natural, el sistema determina a qué empresas está asociado, pero no distingue roles de actuación dentro de las empresas. 3. En caso de ser una persona natural, el sistema determina a qué empresas está asociado y además con qué roles puede actuar en cada empresa (titular, gestor, representante, contador, etc.) 4. Otro [COMPLETAR]:
Con respecto a la delegación de permisos desde un titular hacia terceros, por favor seleccione con negrita o bold las opciones correctas.	1. No existe la posibilidad de delegar funciones, por lo que el usuario y sus gestores utilizan la misma identificación digital. 2. El usuario tiene la posibilidad de seleccionar, desde un catálogo, a otros usuarios que pueden operar en su empresa con diferentes roles (contador, gestor, etc.). 3. Existe la posibilidad de delegar roles, pero en forma presencial, el/los titulares/titulares tiene/n que concurrir a la administración tributaria para indicar qué usuarios pueden operar con qué roles sobre su empresa. 4. Otro [COMPLETAR]:
Con respecto a los métodos para obtener la identificación digital de la administración tributaria, ¿cuáles se utilizan? Por favor marque con negrita o bold las opciones correctas.	1. El usuario se registra en línea y no hay ningún chequeo de la identidad, ni de duplicidad de registro. 2. El usuario se registra en línea y el sistema chequea que el usuario no esté previamente registrado (su identificador, número de documento, correo electrónico, etc.). 3. El usuario se registra en línea, el sistema además de chequear duplicidad también realiza algunos chequeos de consistencia de la información interoperando con otros servicios públicos. (Por ejemplo, consume un servicio web para obtener sus datos de registro en el organismo público pertinente). 4. El usuario se registra en línea, el sistema realiza una comparación biométrica de una foto tomada al rostro del usuario con una foto del registro público. 5. El usuario se registra en línea, el sistema realiza una comparación biométrica de una foto tomada al rostro del usuario con una foto del registro público, pero previamente aplica una prueba de vida automática. 6. El usuario se registra presencialmente solamente en la administración tributaria. 7. El usuario se registra presencialmente en la administración tributaria y/o en otros organismos públicos en los cuales la administración tributaria delega esta función. 8. El usuario se registra presencialmente en la administración tributaria y/o en empresas privadas en los cuales la administración tributaria delega esta función. 9. Otro [COMPLETAR]:

Características de la identificación digital de la administración tributaria	
¿La identificación digital de la administración tributaria fue desarrollada en base a algún marco de referencia conocido? Por favor marque con negrita o bold la opción correcta.	1. No, se realizó en base a los requerimientos de la administración tributaria. 2. Se utilizaron los siguientes marcos en forma parcial, en algunos servicios [COMPLETAR] 3. Se utilizaron los siguientes marcos en forma completa [COMPLETAR]:
¿Es posible que las personas naturales sin documento de identidad o certificado de nacimiento reciban una identificación digital para fines tributarios? (seleccione con negrita o bold las opciones correctas):	1. No. 2. Aún no, pero se está considerando la necesidad de implementarlo. 3. Si, a través de la identificación digital nacional que está integrada a la administración tributaria. 4. Si, mediante el uso de medios privados de identificación, por ejemplo, tarjetas bancarias. 5. Si, mediante el uso de identificaciones físicas extranjeras (por ejemplo, pasaporte). 6. Otro [COMPLETAR]:
La identificación digital del contribuyente, que utiliza para hacer uso de servicios digitales brindados por la administración tributaria, ¿es utilizada para interoperar con otras organizaciones públicas? (seleccione con negrita o bold las opciones correctas):	1. No 2. Aún no, pero se está considerando la necesidad de implementarlo. 3. Si, para obtener o verificar información relativa a posibles beneficios fiscales según la actividad del contribuyente, el tipo de contribuyente, etc. 4. Si, para obtener u otorgar constancias necesarias para completar trámites digitales. 5. Si, para iniciar un trámite o servicio en la administración tributaria y continuar en otro organismo (o viceversa). 6. Si, para obtener información acerca del perfil del usuario como por ejemplo si pertenece a algún colegio (abogados, contadores, fiscales, etc.).
Con respecto a la protección de la Identificación Digital de la administración tributaria (seleccione con negrita o bold las opciones correctas):	1. Se realizan campañas en forma periódica para sensibilizar a los usuarios (solamente funcionarios de la administración tributaria) con respecto a los cuidados asociados a la identificación digital. 2. Se realizan campañas en forma periódica para sensibilizar a todos los usuarios con respecto a los cuidados asociados a la identificación digital. 3. Se realizan campañas para sensibilizar en temas como phishing. 4. Existe un sistema que permite a los usuarios gestionar los dispositivos de confianza con los que ingresa a la administración tributaria.

Características de la identificación digital de la administración tributaria	
	5. El sistema de identificación digital está integrado a un servicio que analiza información en tiempo real en búsqueda de posibles anomalías o fraudes relacionados al uso de la identificación digital. 6. El sistema de la pregunta anterior, en algunos casos toma acciones automáticas como bloquear usuarios. 7. La identificación digital de la administración tributaria está integrada a un servicio de registro de defunciones con el fin de bloquear usuarios fallecidos. 8. Existen controles y acciones para evitar que los usuarios compartan identificaciones digitales.

El futuro de la identificación digital en la administración tributaria	
¿Considera que es importante que se desarrolle un ecosistema de identificación digital nacional, donde la administración tributaria se integre de modo que los usuarios utilicen una única identificación nacional para acceder a diversos servicios digitales públicos y privados?	Comentarios:
¿Considera que es importante integrar identificaciones digitales a nivel regional para facilitar el acceso a los servicios de la administración tributaria de extranjeros, inclusive utilizando identificaciones digitales confiables de otros países? ¿Qué beneficios podría traer esta iniciativa para las administraciones tributarias y para los contribuyentes?	Comentarios:

Sección C. Desarrollo digital

Para los diferentes servicios de la administración tributaria, por favor seleccione las opciones de canales digitales que están disponibles y la cobertura a través de los canales digitales disponibles (marque con negrita o bold las opciones correctas en la columna “Canales digitales habilitados” y la opción correcta en “Cobertura Digital”).

Teniendo en cuenta la siguiente escala aproximada:

1. La mayoría se hacen por canales digitales – más del 75%
5. Muchos se hacen por canales digitales – entre el 50% y 75%
6. Pocos se hacen por canales digitales – entre el 25% y 50%
7. Casi nada se hace por canales digitales – menos del 25%
8. No hay canales digitales disponibles.

Servicio	Canales digitales habilitados	Cobertura digital
Registro en el sistema tributario	• Web • Móvil • API • Correo electrónico • Otros:	1. La mayoría se hacen por canales digitales. 2. Muchos se hacen por canales digitales. 3. Pocos se hacen por canales digitales. 4. Casi nada se hace por canales digitales. 5. No hay canales digitales disponibles.
Presentación de declaraciones	• Web • Móvil • API • Correo electrónico • Otros:	1. La mayoría se hacen por canales digitales. 2. Muchos se hacen por canales digitales. 3. Pocos se hacen por canales digitales. 4. Casi nada se hace por canales digitales. 5. No hay canales digitales disponibles.
Declaraciones precargadas	• Web • Móvil • API • Correo electrónico • Otros:	1. La mayoría se hacen por canales digitales. 2. Muchos se hacen por canales digitales. 3. Pocos se hacen por canales digitales. 4. Casi nada se hace por canales digitales. 5. No hay canales digitales disponibles.

Servicio	Canales digitales habilitados	Cobertura digital
Pago de obligaciones	• Web • Móvil • API • Correo electrónico • Otros:	1. La mayoría se hacen por canales digitales. 2. Muchos se hacen por canales digitales. 3. Pocos se hacen por canales digitales. 4. Casi nada se hace por canales digitales. 5. No hay canales digitales disponibles.
Tramitación de constancias y/o certificados	• Web • Móvil • API • Correo electrónico • Otros:	1. La mayoría se hacen por canales digitales. 2. Muchos se hacen por canales digitales. 3. Pocos se hacen por canales digitales. 4. Casi nada se hace por canales digitales. 5. No hay canales digitales disponibles.
Tramitación de Acuerdos de pago	• Web • Móvil • API • Correo electrónico • Otros:	1. La mayoría se hacen por canales digitales. 2. Muchos se hacen por canales digitales. 3. Pocos se hacen por canales digitales. 4. Casi nada se hace por canales digitales. 5. No hay canales digitales disponibles.
Solicitudes de Crédito o beneficios fiscales	• Web • Móvil • API • Correo electrónico • Otros:	1. La mayoría se hacen por canales digitales. 2. Muchos se hacen por canales digitales. 3. Pocos se hacen por canales digitales. 4. Casi nada se hace por canales digitales. 5. No hay canales digitales disponibles.
Presentación de descargos y/o peticiones	• Web • Móvil • API • Correo electrónico • Otros:	1. La mayoría se hacen por canales digitales. 2. Muchos se hacen por canales digitales. 3. Pocos se hacen por canales digitales. 4. Casi nada se hace por canales digitales. 5. No hay canales digitales disponibles.
Comunicaciones y/o notificaciones	• Web • Móvil • API • Correo electrónico • Otros:	1. La mayoría se hacen por canales digitales. 2. Muchos se hacen por canales digitales. 3. Pocos se hacen por canales digitales. 4. Casi nada se hace por canales digitales. 5. No hay canales digitales disponibles.

Servicio	Canales digitales habilitados	Cobertura digital
Envío o carga de información	• Web • Móvil • API • Correo electrónico • Otros:	1. La mayoría se hacen por canales digitales. 2. Muchos se hacen por canales digitales. 3. Pocos se hacen por canales digitales. 4. Casi nada se hace por canales digitales. 5. No hay canales digitales disponibles.
Consulta de cuenta corriente/estado de situación	• Web • Móvil • API • Correo electrónico • Otros:	1. La mayoría se hacen por canales digitales. 2. Muchos se hacen por canales digitales. 3. Pocos se hacen por canales digitales. 4. Casi nada se hace por canales digitales. 5. No hay canales digitales disponibles.
Consultas vinculantes	• Web • Móvil • API • Correo electrónico • Otros:	1. La mayoría se hacen por canales digitales. 2. Muchos se hacen por canales digitales. 3. Pocos se hacen por canales digitales. 4. Casi nada se hace por canales digitales. 5. No hay canales digitales disponibles.
Consultas generales	• Web • Móvil • API • Correo electrónico • Otros:	1. La mayoría se hacen por canales digitales. 2. Muchos se hacen por canales digitales. 3. Pocos se hacen por canales digitales. 4. Casi nada se hace por canales digitales. 5. No hay canales digitales disponibles.
Agendamiento para una cita presencial en oficina	• Web • Móvil • API • Correo electrónico • Otros:	1. La mayoría se hacen por canales digitales. 2. Muchos se hacen por canales digitales. 3. Pocos se hacen por canales digitales. 4. Casi nada se hace por canales digitales. 5. No hay canales digitales disponibles.
Solución de controversias	• Web • Móvil • API • Correo electrónico • Otros:	1. La mayoría se hacen por canales digitales. 2. Muchos se hacen por canales digitales. 3. Pocos se hacen por canales digitales. 4. Casi nada se hace por canales digitales. 5. No hay canales digitales disponibles.

Para cada uno de los servicios y trámites (si existen), por favor indique su relación con la identificación digital (marque con negrita o bold las opciones correctas).

Servicio	Relación con la identificación digital
Registro en el sistema tributario	1. No hay identificación digital. 2. Solamente se ingresa el número de identificación del contribuyente. 3. Se exige autenticación. 4. Además de autenticación se exige un segundo factor de autenticación.
Presentación de declaraciones	1. No hay identificación digital. 2. Solamente se ingresa el número de identificación del contribuyente. 3. Se exige autenticación. 4. Además de autenticación se exige un segundo factor de autenticación.
Declaraciones precargadas	1. No hay identificación digital. 2. Solamente se ingresa el número de identificación del contribuyente. 3. Se exige autenticación. 4. Además de autenticación se exige un segundo factor de autenticación.
Pago de obligaciones	1. No hay identificación digital. 2. Solamente se ingresa el número de identificación del contribuyente. 3. Se exige autenticación. 4. Además de autenticación se exige un segundo factor de autenticación.
Tramitación de constancias y/o certificados	1. No hay identificación digital. 2. Solamente se ingresa el número de identificación del contribuyente. 3. Se exige autenticación. 4. Además de autenticación se exige un segundo factor de autenticación.
Tramitación de Acuerdos de pago	1. No hay identificación digital. 2. Solamente se ingresa el número de identificación del contribuyente. 3. Se exige autenticación. 4. Además de autenticación se exige un segundo factor de autenticación.
Solicitudes de Crédito o beneficios fiscales	1. No hay identificación digital. 2. Solamente se ingresa el número de identificación del contribuyente. 3. Se exige autenticación. 4. Además de autenticación se exige un segundo factor de autenticación.

Servicio	Relación con la identificación digital
Presentación de descargos y/o peticiones	1. No hay identificación digital. 2. Solamente se ingresa el número de identificación del contribuyente. 3. Se exige autenticación. 4. Además de autenticación se exige un segundo factor de autenticación.
Comunicaciones y/o notificaciones	1. No hay identificación digital. 2. Solamente se ingresa el número de identificación del contribuyente. 3. Se exige autenticación. 4. Además de autenticación se exige un segundo factor de autenticación.
Envío o carga de información	1. No hay identificación digital 2. Solamente se ingresa el número de identificación del contribuyente. 3. Se exige autenticación. 4. Además de autenticación se exige un segundo factor de autenticación.
Consulta de cuenta corriente/estado de situación	1. No hay identificación digital. 2. Solamente se ingresa el número de identificación del contribuyente. 3. Se exige autenticación. 4. Además de autenticación se exige un segundo factor de autenticación.
Consultas vinculantes	1. No hay identificación digital. 2. Solamente se ingresa el número de identificación del contribuyente. 3. Se exige autenticación. 4. Además de autenticación se exige un segundo factor de autenticación.
Consultas generales	1. No hay identificación digital. 2. Solamente se ingresa el número de identificación del contribuyente. 3. Se exige autenticación. 4. Además de autenticación se exige un segundo factor de autenticación.
Agendamiento para una cita presencial en oficina	1. No hay identificación digital. 2. Solamente se ingresa el número de identificación del contribuyente. 3. Se exige autenticación. 4. Además de autenticación se exige un segundo factor de autenticación.
Solución de controversias	1. No hay identificación digital. 2. Solamente se ingresa el número de identificación del contribuyente. 3. Se exige autenticación. 4. Además de autenticación se exige un segundo factor de autenticación.

Anexo II: Modelo de Identificación Digital para América Latina y el Caribe (IdLAC)

En los capítulos anteriores se comentaron algunos modelos de identificación digital reconocidos y ampliamente utilizados, como el de NIST, ISO y eIDAS en la Unión Europea. En América Latina y el Caribe se está desarrollando un modelo de identificación digital llamado IdLAC.

La Red Interamericana de Gobierno Digital (Red GEALC), creada en 2003 se compone de las agencias o ministerios responsables por el desarrollo del Gobierno Digital de cada país miembro de la Organización de los Estados Americanos (OEA). Se trata de una red para impulsar la cooperación entre los países para el desarrollo del Gobierno Digital, elaboración de políticas públicas participativas, formación de colaboradores públicos, intercambios de conocimientos para la construcción de estrategias nacionales de gobierno digital y el intercambio de soluciones y expertos en la región.

El objetivo general de la Red GEALC es el apoyo a políticas de gobierno digital con el ciudadano, y en particular las poblaciones más vulnerables, en el centro y posee diversos grupos de trabajo técnicos transversales entre los países miembros. Uno de los grupos, tiene como objetivo impulsar el reconocimiento transfronterizo de firma digital y la interoperabilidad transfronteriza de la identificación digital en la región. En este grupo, en los últimos dos años se han logrado avances sustantivos en la identificación digital transfronteriza.

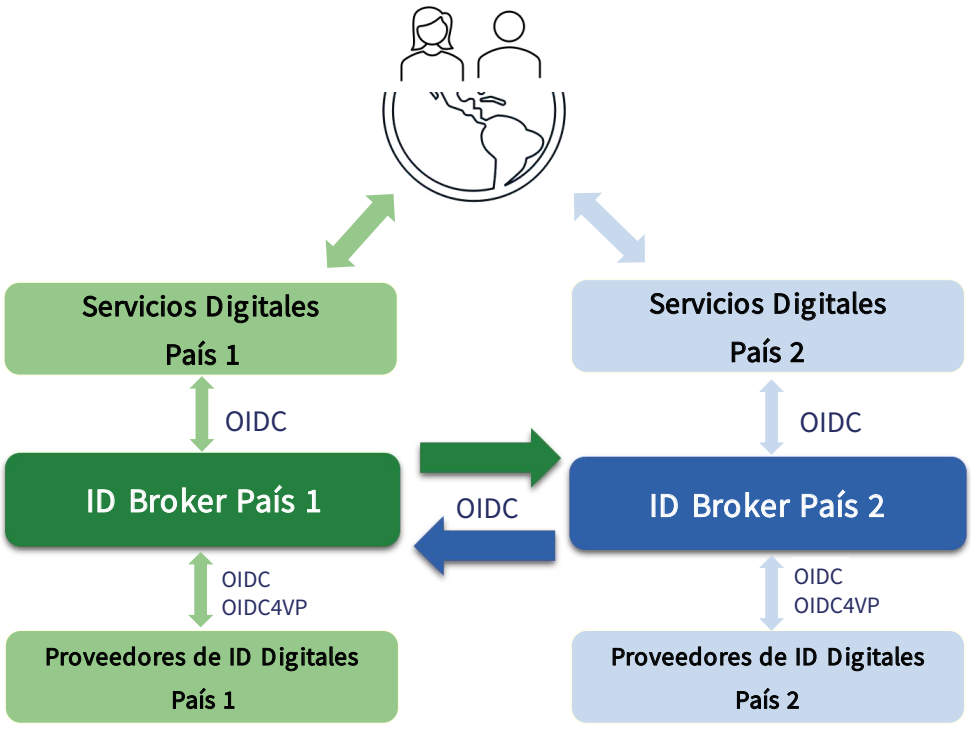
Argentina, Brasil y Uruguay poseen ecosistemas de identificaciones digitales a nivel país articulados cada uno por un *broker*, Autenticar, Gov.br e ID Uruguay respectivamente. Durante la pandemia COVID surgió la necesidad de comenzar a desarrollar la identificación digital transfronteriza, dado que muchas personas no podían salir de sus países de origen, pero necesitaban realizar trámites y servicios en países extranjeros. En estos países, no era posible validar la identidad de la persona, por lo que, si obtenía una identificación digital en el país extranjero, siempre iba a ser de baja confianza. A partir de esta situación, se llegó a la conclusión de que las personas deberían contar con identificaciones confiables de sus países y poder utilizarlas para identificarse digitalmente en servicios de otros países, tal cual se realiza con las identificaciones físicas, pero aprovechando todas las ventajas del mundo digital.

De esta forma, en el grupo de trabajo de Identificación y Firma transfronteriza de la Red, se comenzó a trabajar en definir cómo se podría hacer para lograr que una persona pueda acceder a servicios digitales de un país utilizando su identificación digital confiable nacional. En esta línea de trabajo, Uruguay y Argentina comenzaron a analizar a nivel técnico y a realizar pruebas para integrar los dos *brokers* de

identificación digital, es decir, Autenticar e ID Uruguay. Cada *broker* es el corazón del ecosistema federado de identificaciones digitales. Cada *broker* posee un conjunto de proveedores de identificación digital aptos para su ecosistema y estandariza la identificación (protocolos, datos que identifican a una persona y niveles de seguridad).

La idea de que cada *broker* posee un conjunto de proveedores de identificación, permitió concluir que, si se integraba un *broker* con otro, se estarían habilitando los proveedores de identificación de un país en el otro país y viceversa. Además, al integrar un *broker* a otro lo que en realidad se está realizando es habilitar un grupo de proveedores de identidad en un *broker* y viceversa. Esta situación permitió concluir que para integrar un *broker* con otro solamente bastaba con utilizar el protocolo *OpenID Connect* desde un lado y luego desde el otro. El siguiente esquema muestra esta situación:

Figura 13. Esquema simplificado de integración transfronteriza de ecosistemas de identificación digital.



Fuente: elaboración propia

La lógica para integrar ambos ecosistemas es hacer dos flujos, tal como se muestra en la figura anterior. El país 1 ve al otro *broker* cómo un grupo de proveedores de identificación digital federados y se integra de esa forma mediante *OpenID Connect*. Lo mismo sucede con el país 2.

Esta solución, sumamente simple y segura (con algunas condiciones) es la forma de integrar un ecosistema con otro, por lo que los ciudadanos de un país podrían utilizar las identificaciones de su país para ingresar a los servicios de los dos países. A mediados de 2023 se realizó el primer prototipo entre Uruguay y Argentina para validar esta idea y se comenzó a trabajar con Brasil.

El desarrollo entre Uruguay y Brasil fue más simple, porque la forma de hacerlo ya fue validada con la experiencia previa. En octubre de 2024 se puso en producción el primer caso de identificación transfronteriza de la región, donde ciudadanos brasileños podían identificarse digitalmente utilizando sus identificaciones confiables brasileñas en 40 servicios digitales uruguayos de la Unidad Reguladora de Servicios de Agua y Energía (URSEA) y la Solicitud de constancias para transporte de yerba mate del Ministerio de Salud Pública de Uruguay. En diciembre de 2025, se habilitaron todos los trámites y servicios de la Ventanilla Única de Comercio Exterior (VUCE) de Uruguay, alcanzando más de 360 trámites y servicios digitales en Uruguay habilitados para identificaciones digitales confiables brasileñas.

Esto despertó el interés de varios países de la región en desarrollar un *broker*, por lo que se planteó esta oportunidad a la Red Gealc. La oportunidad consistía en desarrollar un *broker* modelo, actualizado y minimalista, diseñado entre todos los países para que cada uno lo implemente en forma local. Esto no solo ahorraría costos al hacer un único desarrollo, sino que, más importante aún, crearía una plataforma estandarizada regional compuesta por todos los *broker* de cada país. Al contar todos los países con el mismo *broker*, se desarrollaría un ecosistema de identificaciones digitales en cada país, pero se construiría una capa de estandarización en la región, compuesta por todos los *brokers*.

Ante esta oportunidad, la Red Gealc anunció un proyecto para el desarrollo del *broker* modelo financiado por el Banco Interamericano de Desarrollo, el Banco Mundial y Co-Develop, con el apoyo de la Organización de Estados Americanos y otras organizaciones destacadas en la materia. En paralelo a esto, se formó un equipo de trabajo integrado por 13 países para establecer los requerimientos e ir diseñando el modelo de identificación digital de la región.

El proyecto IdLAC se compone del *broker* como pieza para facilitar y estandarizar la identificación digital de la región y el modelo que establece protocolos, niveles de seguridad, equivalencia de términos, requerimientos de seguridad y el conjunto de datos a utilizar para identificar a una persona. Se espera finalizar el desarrollo del *broker* durante el primer trimestre de 2026, para luego comenzar con las primeras implementaciones, dentro de los 13 países que integran el grupo de trabajo.

De esta forma, se está co-diseñando un modelo de identificación digital de América Latina y el Caribe llamado IdLAC. Este modelo, contempla métodos de identificación digital basados en Credenciales Verificables de identidad, por lo que se espera desarrollar el protocolo OIDC4VP, con el fin que el *broker* habilite credenciales

verificables para identificarse digitalmente. Una ventaja de este modelo es que este protocolo se va a implementar una única vez, y se va a distribuir entre los países que implementen el *broker*, pero tal como está diseñado el modelo, no es necesario que el *broker* posea las listas de confianza de todos los países. Cada persona va a utilizar su credencial como proveedor de identificación frente al *broker* de su país y a través de la integración entre los *broker* accederá a servicios digitales de otros países. Cada *broker* confía en las identificaciones de los otros y de esa forma se simplifica considerablemente el modelo.

ciat@ciat.org

ciat.org

MINISTERIO
DE ASUNTOS EXTERIORES, UNIÓN EUROPEA
Y COOPERACIÓN

aecid

cooperación
española