**Una inmersión en la identidad digital corporativa y contemplar la emisión masiva de IPJ**



Publicado el julio 8, 2022 por [**Editor**](https://www.xbrl.org/news/a-dive-into-corporate-digital-identity-and-contemplating-bulk-lei-issuance/)

Un reciente documento de investigación del Banco de Pagos Internacionales (BPI) analiza en profundidad el concepto de identidad digital corporativa con un enfoque en el Identificador de Personas Jurídicas ([IPJ](https://www.xbrl.org/tag/lei/)). Examina cómo funcionan los identificadores, sus ventajas y limitaciones, y las oportunidades en el futuro. Como observa, *"la identidad digital corporativa tiene el potencial de simplificar drásticamente la identificación y verificación de las empresas",* y si bien el enfoque principal del documento es reducir los riesgos y los costos de hacer negocios, también hay mucho que pensar en términos de beneficios regulatorios.

Un punto que nos llamó la atención fue la discusión sobre la emisión masiva de IPJ. Esta es la idea de que los IPJ podrían emitirse, en una sola toma, a todas las empresas registradas ante una autoridad, lo que significa que los registros corporativos podrían servir como emisores de IPJ para todos sus solicitantes, siempre que cumplan con los requisitos de verificación pertinentes. *"Esto podría mejorar drásticamente la eficiencia y la confiabilidad de la recopilación de datos, ya que el registro corporativo ya debería tener información sobre los atributos centrales de cualquier empresa registrada".*

Lea más [aquí](https://www.bis.org/publ/bppdf/bispap126.pdf).

[IDENTIFICADORES BIS](https://www.xbrl.org/tag/bis/) [LEI](https://www.xbrl.org/tag/lei/)



Documentos BIS No. 126

Identidad digital corporativa: no hay una bala de plata, pero sí un lado positivo

por David Leung, Bénédicte Nolens, Douglas Arner y Jon Frost

Departamento Monetario y Económico

Junio 2022

Extracto

La identidad digital corporativa (ID) tiene el potencial de simplificar drásticamente la identificación y verificación de las empresas y reducir los riesgos y costos de hacer negocios. Forma una especie de boleto de admisión para que una empresa acceda a servicios financieros y no financieros y, al mismo tiempo, mejora el acceso a la información sobre la empresa para contrapartes, clientes, reguladores y proveedores de servicios financieros. Siempre que haya voluntad política, la innovación tecnológica y las políticas pueden ayudar en varias áreas a facilitar la identificación digital corporativa y, por lo tanto, mejorar la eficiencia general, la integridad del mercado, la estabilidad financiera y la inclusión. Sin embargo, no hay una bala de plata que pueda lograr todos estos beneficios a la vez. Tampoco una sola parte interesada puede impulsar todos los cambios necesarios; los registros corporativos, los bancos y otras instituciones financieras, los proveedores establecidos, las empresas emergentes de regtech y los reguladores y formuladores de políticas tienen un papel que desempeñar. El identificador de personas jurídicas (IPJ), los identificadores descentralizados (DID) y las reformas basadas en sistemas públicos de identificación digital individual son especialmente prometedores, en particular para las pequeñas y medianas empresas, apoyando así un desarrollo sostenible, un empleo y una innovación más amplios. En este documento, examinamos estas innovaciones en la identificación digital corporativa y exploramos caminos para el futuro.

Palabras clave: identificación, verificación de identidad, estructura corporativa, beneficiario efectivo, impuestos, identificador de personas jurídicas, regulación prudencial, lucha contra el lavado de dinero / lucha contra el financiamiento del terrorismo, pequeñas y medianas empresas, inclusión financiera.

Códigos JEL: D22, F23, G28, G38, L22.

Resumen ejecutivo

La identidad digital corporativa (ID) proporciona verificación electrónica de la identidad de una entidad legal. En otras palabras, para ser "digitales", los atributos asociados con una identificación digital corporativa deben capturarse electrónicamente, almacenarse y ponerse a disposición de los usuarios potenciales de datos.

En muchos aspectos de los negocios y las finanzas, la identificación y verificación del cliente (ID&V) es un primer paso necesario. En los servicios financieros, no solo está impulsado por los requisitos reglamentarios, en particular en torno a la integridad del mercado (como las normas contra el blanqueo de capitales) y los objetivos prudenciales, sino también por prácticas comerciales y de gestión de riesgos sólidas, es decir, para evitar pérdidas y fraudes y comprender mejor a los clientes y las contrapartes. La identificación digital corporativa tiene el potencial de simplificar drásticamente la identificación y la evolución de las personas jurídicas y, por lo tanto, reducir los riesgos y los costos de adquisición de clientes, análisis de contrapartes y hacer negocios. Forma una especie de boleto de admisión por la vía rápida para que una entidad legal acceda a servicios financieros y no financieros. Más allá de su función principal de proporcionar certeza de identidad, la identificación digital corporativa puede ofrecer más beneficios al vincularse digitalmente a otra información y atributos sobre esa entidad legal. Esto ayuda a facilitar el conocimiento de su cliente (KYC) y otros procedimientos obligatorios de diligencia debida, además de proporcionar información sobre contrapartes y clientes fundamentales para los riesgos y oportunidades que se evalúan, ya sean comerciales, financieros o relacionados con objetivos de desarrollo sostenible más amplios.

La identificación digital corporativa, como tal, es fundamental para la eficiencia operativa, la integridad del mercado, la estabilidad financiera y la inclusión. Al permitir que los actores privados demuestren quiénes son, sepan definitivamente con quién están realizando transacciones e integren datos de diferentes fuentes, la identificación digital corporativa supera las asimetrías de información, permitiendo una mejor evaluación por parte de inversores, acreedores, contrapartes y otros, y respalda la confianza. También apoya el trabajo de las autoridades públicas, por ejemplo, los bancos centrales, los reguladores financieros y las autoridades fiscales, que necesitan conocer las estructuras de propiedad y control totales de las empresas.

Hay una serie de paralelismos con la identificación digital para las personas, sin embargo, la identificación digital corporativa no es una mera extensión de la identificación digital individual. De hecho, una entidad legal puede ser parte de una estructura corporativa complicada cuyos atributos (como los directores) pueden cambiar con frecuencia. La privacidad de los datos tiene implicaciones muy diferentes para las "personas jurídicas" que, para las personas físicas, en particular porque la mayoría de los regímenes de protección de datos diferencian explícitamente entre datos personales y no personales (por ejemplo, empresas). Dicho esto, la identificación digital individual es un complemento muy significativo de la identificación digital corporativa, debido a la necesidad de los usuarios externos de identificar y autenticar a las personas que dicen representar a una empresa (por ejemplo, los directores que autorizan una transacción) y para permitir la interconexión de datos e identidades entre las empresas, sus representantes, propietarios y controladores.

Un identificador único de persona jurídica es esencial para cualquier solución de identificación digital corporativa, ya que a menudo es confuso identificar a una empresa solo por su nombre, especialmente porque un nombre puede aparecer en diferentes versiones y diferentes idiomas. Las corporaciones a menudo se identifican por su registro comercial o número de registro de la compañía. Sin embargo, estos sistemas no están estandarizados, generalmente no son interoperables y, a menudo, no están digitalizados. La información con frecuencia no se verifica y no se actualiza. El Identificador de Personas Jurídicas (IPJ), desarrollado a raíz de la crisis financiera de 2008 para simplificar la identificación de contrapartes en los mercados financieros, es un punto de partida más sólido para la identificación corporativa, ya que es global, único y ampliamente reconocido. Sin embargo, se necesitan mejoras para aumentar su tasa de adopción a fin de crear efectos de red, especialmente fuera de la industria financiera y en los mercados emergentes y las economías en desarrollo (EMDE) y las pequeñas y medianas empresas (PYME).

Relacionados con estos están los esfuerzos para desarrollar identificadores descentralizados (DID), liderados por el Grupo de Trabajo DID del World Wide Web Consortium (W3C). Esta iniciativa busca desarrollar un conjunto de estándares para interconectar diferentes fuentes de datos, bajo el control del individuo o entidad. Este es un marco "autosoberano" para permitir el control y el uso de datos dispares. Sin embargo, fundamentalmente, tanto los sistemas corporativos como los individuales requieren una forma básica de identificación. Cada vez se considera más que esto se sirve mejor como una infraestructura de bien público, proporcionada por las autoridades públicas (como en Aadhaar de la India o MyInfo de Singapur) o por el sector privado con estándares y regulaciones públicas. Hasta ahora, los sistemas corporativos se están desarrollando más lentamente, con la probabilidad de que un sistema híbrido que involucre tanto un ID base como enlaces a otros datos ofrezca el mayor potencial.

La innovación tecnológica puede ayudar en varias áreas a dar forma a la identificación digital corporativa y a mejorar la eficiencia general, la integridad del mercado, la estabilidad financiera y la inclusión. Sin embargo, según lo que sabemos hoy y podemos prever razonablemente en el futuro cercano, no hay una bala de plata que pueda lograr todos estos beneficios a la vez, ni una sola parte interesada puede impulsar todos los cambios necesarios. El lado positivo es que, trabajando juntos, estas partes interesadas pueden abordar los principales puntos débiles de ID&V corporativo:

• Registros corporativos: los registros son indispensables en cualquier solución de identificación digital corporativa ya que proporcionan datos de "fuente de oro" sobre las empresas. Para mejorar su papel, deben esforzarse por mejorar la apertura de los datos, la disponibilidad de los datos (en particular los datos de los beneficiarios reales), la calidad de los datos, la digitalización y la conectividad de los datos. Los datos deben verificarse para verificarse para verificar su exactitud, actualizarse periódicamente y facilitar el acceso.

• Bancos y otras instituciones financieras: recopilan y verifican grandes cantidades de datos corporativos para sus propias operaciones y para cumplir con los requisitos reglamentarios, y pueden usar estos datos para servicios de identificación corporativa. Pero compartir dichos datos, por ejemplo, en el contexto de las utilidades KYC, es un desafío. En muchos casos, esto requiere medidas legislativas o reglamentarias, como ha sido el caso de los sistemas de intercambio de información crediticia y los sistemas de divulgación de los mercados de capitales en todo el mundo.

• Proveedores / proveedores de servicios establecidos y empresas emergentes de regtech: las grandes empresas actualmente sustentan la mayoría de los procesos de KYC e incorporación de bancos y corporaciones, y ahora están construyendo capacidades nuevas e innovadoras. Mientras tanto, las nuevas empresas de regtech utilizan tecnología innovadora para resolver los puntos débiles en ID&V corporativo. Por ejemplo, proporcionan conectividad automatizada entre múltiples fuentes de datos y herramientas para extraer información de documentos corporativos o datos no estructurados.

• Reguladores y formuladores de políticas: en los últimos años, un número creciente de jurisdicciones están construyendo sistemas públicos de identificación digital individual, como lo destaca la iniciativa de Identificación para el Desarrollo (ID4D) del Banco Mundial y se refleja en los Objetivos de Desarrollo Sostenible (ODS) de las Naciones Unidas. Si bien estos sistemas se interrelacionan con los sistemas corporativos, están invariablemente separados, con oportunidades y desafíos en la creación de vínculos. Los reguladores y los responsables políticos tienen un papel clave en la coordinación, también a través de las fronteras. Esto se ve particularmente en el contexto de los procesos existentes relacionados con el intercambio de información fiscal y la divulgación de beneficiarios reales (coordinados por la OCDE), la lucha contra el lavado de dinero / la lucha contra el financiamiento del terrorismo (ALD / CFT) (coordinado por el GAFI), los derivados OTC y la infraestructura financiera (coordinados por el FSB, CPMI e IOSCO), y otros como los datos de los mercados de capitales (coordinados por IOSCO y el ISSB), informes de crédito (ICCR) y sostenibilidad (ISSB).

Este documento analiza las soluciones innovadoras de identificación digital corporativa y los facilitadores de políticas que pueden ser necesarios para respaldar su adopción. Documenta tanto la promesa como los riesgos de varias soluciones. De esta manera, busca apoyar los esfuerzos de política dirigidos a la eficiencia, la integridad del mercado, la estabilidad financiera y la inclusión financiera, y por lo tanto objetivos de desarrollo sostenible más amplios.

1. Introducción

El término "identidad corporativa" a menudo evoca una imagen de marcas comerciales, logotipos y marcas de la empresa. Con el fin de proyectar una apariencia consistente a los clientes, proveedores o inversores, las empresas a menudo utilizan tales símbolos para demostrar que las comunicaciones dispares (cartas, sitios web, publicidad), las personas (administración, personal) y las ubicaciones físicas (oficinas, tiendas, almacenes) pertenecen a la misma entidad, la empresa, y que esta empresa puede verse como la misma entidad en todos los lugares y a lo largo del tiempo.

De hecho, muchas empresas adoptan la forma de una "entidad jurídica", como una empresa. Una entidad legal es una criatura de jurisdicciones legales individuales. Las leyes de sociedades, fideicomisos y asociaciones y otros marcos legales permiten la creación de personas jurídicas y establecen los requisitos necesarios. Cada "persona jurídica" creada por las leyes nacionales y (en el caso de las organizaciones internacionales) las convenciones internacionales tiene una identidad única y formal. Sin embargo, a diferencia de las personas físicas (individuos), no tienen una identidad objetiva o un cuerpo físico sujeto a identificación física o biométrica. Para denotar un negocio específico, los actores tanto del sector público como del privado utilizan una gama de identificadores específicos para una empresa. Ejemplos comunes de identificadores son el nombre de la empresa, un número de registro asignado por un registro corporativo, un número de identificación fiscal emitido por una autoridad fiscal, licencias comerciales emitidas por departamentos gubernamentales específicos o registros de intercambio para empresas que cotizan en bolsa. El nombre de la empresa puede no ser un identificador confiable, ya que puede aparecer en diferentes versiones (por ejemplo, completo vs abreviado, acrónimos) y en diferentes idiomas, y puede no ser único. El número de registro corporativo es algo equivalente a un número de pasaporte o un número de licencia de conducir para un individuo. Sin embargo, la complejidad surge porque las corporaciones pueden contener muchas entidades de muchas jurisdicciones diferentes en un grupo determinado bajo un solo nombre, y cada entidad tiene su propio registro de empresa. Estos se pueden combinar con registros y licencias en una variedad de jurisdicciones diferentes.

La identidad corporativa (ID) es mucho más que un identificador. Es sobre todo una herramienta para la identificación y verificación (ID&V) de una empresa y de sus relaciones con otras empresas dentro de la misma estructura de propiedad. Funcionalmente hablando, la identificación corporativa es análoga a un boleto de admisión. Con este boleto, una empresa puede ingresar a un mercado que brinda una amplia gama de servicios financieros (por ejemplo, préstamos, seguros) y otros servicios (por ejemplo, aduanas y despacho fronterizo para importación / exportación). La identidad corporativa puede cumplir esta función porque está vinculada a la información corporativa (conocida como atributos) asociada a esa empresa. Dichos atributos permiten a las partes externas identificar y verificar de forma única la identidad exacta de la empresa y vincular esa identidad a otros atributos esenciales para "conocer a su cliente" (KYC), la diligencia debida y la evaluación de la contraparte y la gestión de riesgos. El ID corporativo, a su vez, se refiere también a la identificación individual y las firmas, ya sean físicas ("húmedas"), digitalizadas o digitales, que son necesarias para la autorización de transacciones individuales y acciones por parte de la empresa.4

Tal identificación única de las empresas es importante por una serie de razones. Fundamentalmente, al ayudar a los actores a saber con qué entidad están haciendo negocios, la identidad corporativa ayuda a reducir las asimetrías de información y a permitir la confianza en el intercambio económico. De hecho, en las sociedades preindustriales, la reputación y la confianza a menudo se construían entre grupos étnicamente homogéneos que podían identificarse entre sí a través de lazos culturales y de parentesco compartidos, lo que permitía que el comercio floreciera a largas distancias. Las innovaciones tecnológicas y las instituciones legales han ayudado a mejorar la ID&V de las empresas, tanto dentro de las jurisdicciones como a través de las fronteras. Esto hace posible el comercio internacional y las transacciones financieras complejas entre empresas que conocemos en la economía global moderna, gracias a la certeza que proporciona ID&V. La identificación corporativa desempeña un papel importante en la identificación de contrapartes con fines de regulación financiera, particularmente en el contexto de los derivados y créditos extrabursátiles (OTC), pero también en una gama cada vez mayor de otras áreas de regulación financiera, incluida la divulgación de información sobre los mercados de capitales y la presentación de informes y monitoreo ambientales, sociales y de gobernanza (ESG).

Además de estas necesidades comerciales y financieras básicas, las autoridades públicas deben identificar y verificar a las empresas privadas por razones de política. Además, los reguladores en muchas jurisdicciones también requieren ID&V de un cliente corporativo como punto de partida para los procesos para prevenir el lavado de dinero, el financiamiento del terrorismo y otras irregularidades financieras. Según el Grupo de Acción Financiera Internacional (GAFI), se debería exigir a las instituciones financieras que adopten medidas de diligencia debida con respecto al cliente (CDD) en muchas ocasiones, como al establecer relaciones comerciales. Las medidas de la DDC que deben adoptarse son las siguientes:

(a) Identificar al cliente y verificar su identidad utilizando documentos, datos o información de origen confiables e independientes.

(b) Identificar al beneficiario final (UBO) y tomar medidas razonables para verificar la identidad del UBO. En el caso de las personas jurídicas y los acuerdos, esto debe incluir que las instituciones financieras comprendan la estructura de propiedad y control del cliente.

c) Comprender y, según proceda, obtener información sobre el propósito y la naturaleza prevista de la relación comercial.

d) Llevar a cabo la debida diligencia permanente sobre la relación comercial y el escrutinio de las transacciones realizadas a lo largo de esa relación para garantizar que las transacciones que se realicen sean compatibles con el conocimiento de la institución del cliente, su negocio y su perfil de riesgo, incluida, cuando sea necesario, la fuente de los fondos.

Los procedimientos de KYC son relevantes no solo para los bancos y otras instituciones financieras reguladas. De conformidad con las recomendaciones del GAFI, los países deberían establecer una dependencia de inteligencia financiera (UIF) que actúe como centro nacional para la recepción y el análisis de: a) informes sobre transacciones sospechosas; y b) otra información pertinente para el blanqueo de dinero, los delitos determinantes conexos y la financiación del terrorismo, y para la difusión de los resultados de ese análisis. Los no bancos también están sujetos a tales obligaciones de cumplimiento, y están obligados a informar de las transacciones sospechosas a las UIF de sus jurisdicciones.

La ID&V corporativa y el cumplimiento de las leyes pertinentes requieren muchos recursos. Esto se debe en parte a que tales actividades son necesariamente antagónicas, y las empresas y las autoridades trabajan constantemente para mantenerse al día con las prácticas en evolución de los actores ilícitos. Los escándalos y revelaciones de alto perfil también han dado lugar a mayores demandas para combatir la actividad ilícita.7 La creciente demanda de cumplimiento de las normas contra el lavado de dinero / la lucha contra el financiamiento del terrorismo (ALD / CFT) conduce a una carga de trabajo significativa para las empresas afectadas. En una encuesta realizada a profesionales de tesorería y finanzas por EuroFinance y SWIFT en agosto / septiembre de 2019, el 93% de los encuestados dijo que las solicitudes de KYC eran más desafiantes ahora que hace cinco años, y el 59% dijo que las solicitudes de KYC son "mucho más desafiantes". En general, un tesorero corporativo generalmente tiene que pasar el 10% de su tiempo para cumplir con los requisitos de KYC.8 Esto fue, por supuesto, antes de la expansión masiva de la digitalización a nivel mundial impulsada por Covid-19.

Además de KYC y AML / CFT, la política fiscal proporciona otra razón para centrarse en la identidad corporativa. En 2015, a raíz de una solicitud del G20, la OCDE acordó un marco común para el intercambio automático de información sobre las cuentas de sus respectivos ciudadanos. El "Estándar Común de Informes" (CRS) ha sido implementado por más de 100 jurisdicciones en todo el mundo a partir de octubre de 2021. Una iniciativa similar que se aplica a la transparencia de la titularidad real. En octubre de 2021, 137 países acordaron una tasa impositiva corporativa mínima global del 15% para evitar que las empresas transfieran ganancias a jurisdicciones de baja tributación. Para hacer cumplir estas reglas, las autoridades fiscales de muchas jurisdicciones tienen un interés vital en comprender la propiedad completa y la estructura corporativa de las empresas que declaran impuestos. Esto es tanto más importante cuanto que, a efectos fiscales, las filiales de empresas multinacionales son tratadas como entidades independientes que compran y venden bienes y servicios entre sí. Estos problemas se han vuelto muy claros para las instituciones financieras y otros que buscan identificar la propiedad y el control de las contrapartes y los clientes que buscan cumplir con la miríada de sanciones contra individuos y entidades en el contexto de la guerra entre Rusia y Ucrania.

Por último, pero no menos importante, el ID&V corporativo es relevante para las entidades legales en el sector público, ya que muchas agencias del sector público se comportan como corporaciones, y las adquisiciones representan una parte significativa de los gastos públicos. Al igual que las empresas privadas, estas agencias del sector público experimentan puntos débiles en el proceso de ID&V corporativo, aunque a menudo en menor medida.

¿Qué es la identidad digital corporativa?

La innovación digital puede facilitar aún más la ID&V de las empresas, a través de la identidad digital corporativa (ID).

Para ser "digitales", los atributos asociados con una identificación digital corporativa deben capturarse, almacenarse y ponerse a disposición de los usuarios potenciales de datos electrónicamente. A diferencia de su equivalente en papel, un sistema digital ofrece una funcionalidad mucho mayor. En particular, la vinculación a atributos es potencialmente automática, lo que facilita la recuperación remota y la autenticación de los datos corporativos por parte de usuarios externos. Además, si los atributos están bien estructurados y son legibles por máquina, entonces pueden ser fácilmente recopilados y analizados por algoritmos informáticos. Para cumplir con este propósito, estos atributos deben ser verificados, verificables, seguros y de confianza por todas las partes involucradas, así como idealmente reconocidos para fines legales y regulatorios.

Aparte de estas características principales, un concepto relativamente nuevo pero digno de mención es la identificación digital "autoexprestigiada", que brinda a las empresas un mayor control sobre su identidad. Por ejemplo, pueden otorgar derechos de acceso a ciertos datos (por ejemplo, solo aspectos seleccionados de credenciales verificables) a partes seleccionadas. El derecho de acceso a estos atributos puede gestionarse de forma descentralizada para que los sujetos de ID no dependan de proveedores externos para almacenar y gestionar de forma centralizada sus datos. A través de estas soluciones, que a veces se basan en tecnologías de contabilidad distribuida (DLT), los propietarios pueden decidir qué partes de sus credenciales verificables se compartirán con qué partes. Es decir, todo el intercambio de datos debe llevarse a cabo sobre la base del consentimiento. Además de los sistemas privados, se han desarrollado sistemas similares para conectar en red información de identidad individual soberana distribuida en una gama de bases de datos diferentes, a menudo de "fuente dorada", a veces ofrecidas por empresas privadas, en otros casos sobre la base de la infraestructura pública de red como Aadhaar de la India, MyInfo de Singapur o el sistema iAMSmart de Hong Kong.

Tenga en cuenta que la definición anterior de ID digital corporativo se aplica a diferentes tipos de emisores de ID digital. En otras palabras, el emisor puede ser un gobierno nacional o local, un consorcio de empresas del sector privado o una organización sin fines de lucro. La clave es que los datos subyacentes son suministrados por un proveedor confiable (por ejemplo, una agencia gubernamental, organización internacional u otra parte de confianza) y vinculados a alguna forma de identidad digital central confiable para que los usuarios vean una identificación digital como confiable. En algunos casos, la identidad puede incluso ser emitida por la propia empresa, siempre que la identidad corporativa sea verificable por datos confiables, y las soluciones tecnológicas podrían garantizar que la identidad, una vez verificada, no pueda ser manipulada aún más.

¿Qué más facilita la identificación digital corporativa?

Un sistema de identificación digital corporativa bien administrado y ampliamente confiable ayuda a una empresa y a sus representantes a demostrar que son quiénes y qué dicen ser. Más allá de esto, una identificación digital corporativa sólida tiene beneficios en cuatro grandes categorías: (1) eficiencia operativa, (2) inclusión financiera, (3) estabilidad financiera y (4) integridad del mercado (Arner, Zetzsche, Buckley y Barberis, 2019).

Eficiencia operativa

En comparación con los enfoques tradicionales basados en papel o cara a cara para identificar y verificar una empresa, un sistema de identificación digital corporativo confiable tiene el potencial de aumentar la eficiencia operativa y reducir sustancialmente la carga de trabajo manual, reduciendo los costos de transacción. Tal reducción de costos le da a una empresa la capacidad de acceder a más servicios e interactuar con otras partes, sin tener que recurrir a la intervención humana o la documentación física. La evidencia anecdótica sugiere que podría acortar el tiempo requerido para que una institución financiera complete su KYC, CDD, AML / CFT y otros procedimientos de diligencia debida para incorporar a un nuevo cliente corporativo, de un período típico de cinco a seis semanas actualmente a unos pocos días o incluso menos para una PYME. En el contexto de los sistemas de identificación individual soberana como Aadhaar en la India, la reducción en el tiempo y los costos de apertura de cuentas bancarias ha sido dramática, de semanas a minutos y de $ 15 a 7 centavos por cuenta (D'Silva et al, 2019). Además, desde el brote mundial de la pandemia de Covid-19 a principios de 2020, la incorporación remota de clientes y el CDD en curso se han convertido cada vez más en necesidades y no solo en características agradables de tener. Esto se debe a que ha sido muy difícil realizar negocios utilizando el enfoque tradicional cara a cara y basado en papel cuando se imponen medidas de confinamiento y los viajes de negocios transfronterizos están severamente restringidos. En este contexto, lo más significativo es que el GAFI reconoció en 2020 que la identificación digital soberana es al menos tan buena como la identificación física soberana, sentando así las bases para el reconocimiento regulatorio de dichos sistemas a nivel mundial.

Las ganancias de eficiencia resultantes de la identificación digital corporativa no se limitan al sentido estricto de reducir el costo del cumplimiento por parte de los bancos y otras instituciones financieras reguladas. Además de la reducción de costos, también se pueden minimizar los errores debidos al procesamiento manual de datos y las inconsistencias en el juicio humano. De hecho, poder identificar mejor a los clientes y contrapartes tiene importantes beneficios para la integridad del mercado y la reducción del fraude y la delincuencia, así como para mejorar la gestión de riesgos de las instituciones financieras. En un sentido más amplio, facilita el comercio al acortar el tiempo de aprobación y reducir los requisitos para los documentos de credenciales durante un proceso de solicitud, esfuerzos que a veces se duplican innecesariamente cuando una empresa comienza una relación con otra institución financiera.

Inclusión financiera

La inclusión financiera a menudo se considera a la luz de los individuos, pero también es relevante con respecto a las pequeñas y medianas empresas (PYME). El acceso de las PYME a los servicios financieros puede mejorarse mediante la identificación digital corporativa, ya que un sistema de identificación digital corporativo confiable y bien administrado puede abordar las asimetrías de información. Tales asimetrías son a menudo más graves para las PYME que para las grandes corporaciones, ya que las primeras suelen carecer de registros contables y un largo historial operativo. Como tal, las instituciones financieras tienden a priorizar a las empresas más grandes, a menudo a expensas de las PYME, a pesar de que estas últimas también contribuyen significativamente a la economía mundial. Al reducir el costo de identificar y verificar una empresa, un sistema de identificación digital agiliza los costosos procesos de KYC y ALD / CFT, aliviando así un desincentivo significativo para proporcionar servicios financieros a las PYME. El sistema también puede integrarse con otras soluciones (por ejemplo, digitalización de documentos comerciales, elaboración de perfiles de riesgo de crédito mediante datos alternativos) que reducen aún más las barreras de información para que las PYME y los prestatarios corporativos en emDE obtengan financiación externa. Desde una perspectiva de todo el sistema, el resultado puede ser una asignación más eficiente de los recursos a través de la reducción de las fricciones del mercado. Como se destacó anteriormente, la identificación digital individual ahora se considera una herramienta central para mejorar la inclusión financiera, y las lecciones se dirigen cada vez más hacia los desafíos que enfrentan las PYME.

La identificación más fácil de las empresas también puede ayudar a formalizar actividades que actualmente son informales, es decir, ocultas a las autoridades por razones monetarias, regulatorias e institucionales. Particularmente en las economías de mercados emergentes y en desarrollo, las empresas de la economía informal son importantes productoras de bienes y servicios y una importante fuente de ingresos para muchas personas, pero a menudo encuentran que navegar por los procesos formales para abrir un negocio o presentar impuestos es indebidamente engorroso. La identificación digital corporativa puede reducir estos costos y proporcionar beneficios concretos a las empresas informales, abriendo así la puerta a protecciones y beneficios legales y servicios financieros formales (por ejemplo, ingresar a la economía formal, se puede establecer el historial crediticio y, por implicación, la mayor capacidad de endeudamiento para hacer crecer el negocio). De esta manera, tales reformas pueden apoyar un crecimiento económico más amplio, el empleo y las protecciones legales, y ayudar a incorporar las actividades actualmente no registradas en la contabilidad nacional.

Estabilidad financiera

Un sistema de identificación digital corporativo bien administrado también es propicio para la estabilidad financiera, ya que aumenta la transparencia de los mercados financieros. En particular, la identificación digital corporativa facilita la identificación de las interconexiones entre las contrapartes y, por lo tanto, la localización de riesgos potenciales de concentración excesiva. Dicha transparencia es un requisito previo esencial para la aplicación de los principios básicos de Basilea para una supervisión bancaria eficaz, en particular el Principio 19, que cubre el riesgo de concentración y los límites de gran exposición, y el Principio 20, que cubre las transacciones con partes relacionadas (BCBS, 2012). En la crisis financiera de 2008, las brechas de datos resultantes de la opacidad de los valores respaldados por activos hicieron que fuera muy difícil para los responsables de la formulación de políticas comprender el alcance de los riesgos de contagio, con importantes implicaciones macroprudenciales. Este fue también un elemento clave en las debilidades en el mercado global de derivados OTC que surgieron en el contexto de la quiebra de Lehman Brothers en 2008. La introducción del Identificador de Personas Jurídicas (IPJ) recomendado por el Consejo de Estabilidad Financiera (FSB) en 2012 es un sistema para remediar esta falta de transparencia a nivel de activos y empresas. Los id.i. digitales basadas en el IPJ podrían ser un mecanismo importante para ampliar el uso del ID digital corporativo (JERS, 2021).

Integridad del mercado

Una identificación digital corporativa confiable puede fomentar la integridad del mercado financiero, ya que mejora la efectividad de la detección de fraudes, reduce el uso criminal y terrorista del sistema financiero y ayuda a las autoridades y empresas a combatir la corrupción y la evasión fiscal. Tal mejora no se limita a la incorporación de un cliente corporativo (GAFI, 2020). La capacidad de las instituciones financieras para capturar digitalmente los cambios en la estructura de las entidades legales (incluido el cambio de los beneficiarios reales finales y los directorios), además de las soluciones para permitir el monitoreo de transacciones en tiempo real y de forma continua, puede ser un cambio de juego en el espacio ALD / CFT. Esto puede reducir el margen de maniobra para que los delincuentes y terroristas exploten las asimetrías de información entre los bancos ubicados en diferentes jurisdicciones. Estos sistemas también son fundamentales en el contexto de la transparencia a efectos de corrupción y fiscalidad, así como muy importantes en el contexto del fraude, la manipulación del mercado y los delitos financieros.

¿Cómo puede funcionar la identificación digital corporativa?

Conceptualmente, existen dos modos de operación para las soluciones de identificación digital corporativa: (1) un modelo centralizado y (2) un modelo descentralizado. El primero presupone una parte central, como un registro corporativo encargado de recopilar toda la información relevante sobre las empresas y coordinar las actividades de otras partes. El mérito de este modelo es que generalmente es consistente y eficiente. Además, la interoperabilidad podría no ser una gran preocupación, ya que los formatos y la estructura de datos similares permiten el uso de interfaces de programación de aplicaciones (API). Sin embargo, la exigencia para el partido central en términos de capacidad técnica es tremenda. También corre el riesgo de un solo punto de falla o un solo objetivo para posibles ataques de hackers, como ha surgido, por ejemplo, en el caso de Equifax, un importante proveedor de información crediticia.

Por el contrario, en un modelo descentralizado, los datos de identidad son proporcionados por múltiples partes, a veces coordinadas por el uso de DLT como blockchain. El mérito de este modelo es una mayor flexibilidad y un menor riesgo, de lo contrario aumentado por un solo punto de falla. Sin embargo, esto requiere un modelo de gobernanza bien definido, ampliamente aceptado y bien ejecutado para que todos los participantes tengan suficiente confianza en el modelo descentralizado. Y el acceso a los datos es otro problema: este enfoque no permite una visión holística para empezar, y puede requerir un proceso largo para que se agreguen todas las piezas del sistema.

Una tercera opción es un enfoque híbrido, donde puede haber una sola fuente de identidad corporativa (como un registro de empresas), pero los diversos atributos y datos se vinculan en una estructura de red, vinculando fuentes dispares de datos al punto central. Este modelo es cada vez más común en el contexto de la identificación individual, dado el riesgo de concentración en el modelo centralizado y los desafíos de coordinación inherentes al modelo descentralizado. MyInfo en Singapur y Aadhaar en la India proporcionan ejemplos útiles: una sola identidad individual soberana se vincula a una variedad de datos de fuentes de oro en varias fuentes; los datos no se agregan en un solo punto, sino que se vinculan según sea necesario para diferentes fines bajo el control del individuo. También está surgiendo en el contexto de la identificación digital corporativa.

ID digital corporativo vs ID digital individual

El desarrollo de la identificación digital corporativa jurisdiccional es mucho más desafiante que la identificación digital individual jurisdiccional. Las soluciones de identificación digital individual ya se han establecido bien en varias jurisdicciones (por ejemplo, sistemas del sector público en Estonia, hongkonés SAR India y Singapur, y sistemas público-privados en Dinamarca y Suecia) se están desarrollando. Sin embargo, no es sencillo extender y transferir sus experiencias a la identificación digital corporativa.

Algunos desafíos de la identificación digital corporativa incluyen:

1. Los atributos centrales de una empresa (por ejemplo, directores, accionistas principales y estructura de propiedad) suelen ser mucho más numerosos y complicados que los de un individuo (por ejemplo, nombre, sexo, país de nacimiento, fecha de nacimiento). Lo que cuenta como atributos esenciales también puede depender de la industria o sector en el que opera una empresa. Además, estos atributos suelen estar sujetos a cambios más frecuentes, lo que requiere una solución que se adapte a la actualización de datos de forma continua. Todo esto podría complicarse por la legislación de las jurisdicciones individuales.

2. Una empresa puede tener estructuras de propiedad complicadas y anidadas, con algunas de sus compañías afiliadas ubicadas y / o incorporadas en múltiples jurisdicciones, lo que dificulta la identificación de los beneficiarios finales. Esto es particularmente cierto si algunas de las empresas asociadas están incorporadas en registros corporativos que no requieren la presentación de información de UBO o restringen el acceso público a dicha información.

3. Para los procesos empresariales que impliquen más de una jurisdicción (por ejemplo, comercio e inversión extranjera directa), una solución de identificación digital corporativa puede necesitar una armonización transfronteriza de las normas de datos y un reconocimiento mutuo, además de los requisitos técnicos habituales. Si bien las personas en actividades transfronterizas también se enfrentan a tales problemas, la identificación digital corporativa es particularmente desafiante debido a la complejidad de los atributos corporativos. Por ejemplo, las diferentes jurisdicciones tienen diferentes formas de entidades jurídicas, lo que puede dificultar la armonización transfronteriza.

4. Existen demandas muy diferentes sobre la privacidad y confidencialidad de los datos. Mientras que las personas mantienen sus atributos (nombre, fecha de nacimiento), dirección y transacciones privadas por razones personales, relacionadas con los derechos fundamentales de las empresas de privacidad de datos lo hacen por razones comerciales, por ejemplo, para evitar que los competidores obtengan información sobre planes futuros o propiedad intelectual. Equilibrar estas demandas legítimas de confidencialidad, así como los requisitos de regulación de datos (como la localización) con la prevención del fraude y el abuso puede ser un desafío clave.

No obstante, una identificación digital individual bien establecida es un apoyo muy importante para la identificación digital corporativa. De hecho, una empresa lleva a cabo sus negocios a través de representantes como el personal, los agentes, los directores y los principales accionistas. Para lograr la identificación de extremo a extremo de una empresa, una solución de identificación digital corporativa idealmente debe integrarse a la perfección con una solución de identificación digital individual efectiva para que el proceso de identificación no falle cuando se trata de la tarea final de identificar a los representantes, directores y propietarios de la empresa (NCAPEC, 2022). Esto puede suceder si, por ejemplo, se necesitan documentos en papel para identificar a las personas que representan a la empresa. Esto puede considerarse particularmente importante en el contexto de las PYME, donde puede haber poca diferenciación entre el historial financiero y de otro tipo del propietario o propietarios individuales y la empresa.

Muchas jurisdicciones se están centrando en las plataformas corporativas de identificación digital después del desarrollo de un sistema de identificación digital individual. Por ejemplo, en la RAE de Hong Kong, la Oficina del Director de Información del Gobierno (OGCIO) ha estado trabajando con la Autoridad Monetaria de Hong Kong (HKMA) en una prueba de concepto (PoC) y en una investigación sobre la versión comercial del "iAM Smart", que es una plataforma de identificación digital individual.12 La primera fase del PoC se completó en el segundo trimestre de 2021. Sobre la base de los resultados del PoC, OGCIO está explorando actualmente la viabilidad de diseñar una propuesta de desarrollo sostenible a través de un enfoque de asociación público-privada y continuará deliberando con la HKMA y otras partes interesadas sobre la implementación de la próxima fase de autenticación digital de identidades comerciales. Los temas de deliberación incluyen la evaluación de la aceptabilidad por parte de la industria de la solución propuesta y la exploración de su aplicación, el marco de gobierno de la plataforma y el plan de implementación detallado. Una vez que se alcance un consenso entre las partes interesadas relevantes sobre el plan de implementación, se realizará una prueba de sandbox para evaluar, entre otras cosas, la seguridad del sistema, la protección de la privacidad de los usuarios y la compatibilidad con las plataformas relacionadas. con miras a determinar la viabilidad del desarrollo sostenible de la plataforma, así como a realizar la consulta legal y regulatoria correspondiente.

En resumen, la identificación digital corporativa puede respaldar muchos beneficios económicos y sociales, pero es un gran desafío. Las diferentes partes interesadas tienen cada una una pieza del rompecabezas, es decir, solo una parte de la solución general. Esto es muy diferente de los sistemas de identificación digital soberana individuales, que a menudo requerirán la centralización del control de los elementos centrales con un jugador en una jurisdicción individual. Debido a que la identificación digital corporativa involucra a una gama más amplia de participantes en diferentes jurisdicciones, está menos sujeta a la posible centralización a través de un solo actor en una sola jurisdicción. Las cuestiones interjurisdiccionales se vuelven aún más difíciles desde el punto de vista de la coordinación.

La innovación privada está en curso, aportando nuevas herramientas y enfoques potenciales. Además de los proveedores tradicionales que ofrecen servicios de KYC, algunos bancos han establecido recientemente consorcios para proporcionar servicios de identificación corporativa, capitalizando así los datos de identificación corporativa que recopilan y verifican para cumplir con los requisitos reglamentarios. Las grandes tecnológicas (por ejemplo, las principales plataformas de redes sociales y navegadores de Internet) también se están convirtiendo en guardianes de la identificación digital de facto. Utilizando los datos generados desde sus plataformas de comercio electrónico, ofrecen soluciones de identificación que permiten a sus usuarios (tanto individuos como empresas) autenticarse en sitios web y servicios de terceros con sus perfiles de usuario. Las nuevas empresas fintech exitosas en el espacio de pago están explorando eficiencias y economías de escala a través de ID&V corporativos mejor automatizados.

Dadas las soluciones de identificación digital corporativa actualmente disponibles, el resultado más probable en el futuro previsible es que se utilicen diferentes enfoques en diferentes áreas y casos de uso. Las soluciones de identificación digital corporativa adecuadas para grandes empresas multinacionales podrían no ser aplicables a las pymes. Aunque las nuevas tecnologías (por ejemplo, blockchain y API) podrían abordar algunos cuellos de botella, un sistema de identificación corporativa aún necesita superar los obstáculos de otras fuentes, como los problemas legales y regulatorios. Este trabajo está lejos de haber terminado, pero existe un consenso cada vez mayor en torno al valor y la importancia de que los sectores público y privado busquen enfoques y soluciones de desarrollo comunes.

Objetivos de la investigación

En este contexto, este documento busca investigar el panorama actual de la identificación digital corporativa. Nuestra investigación tiene una orientación práctica para que las partes interesadas, incluidos los responsables políticos y los profesionales de la industria, estén mejor informados sobre las posibles oportunidades, las innovaciones recientes y el camino a seguir. En concreto, los objetivos de la investigación son los siguientes:

• Comprender cómo las soluciones de identificación digital corporativa pueden aliviar los puntos débiles de ID&V corporativo, especialmente para las pymes que generalmente enfrentan un alto obstáculo para acceder a los servicios bancarios y financieros.

• Comparar las soluciones actuales de identificación digital corporativa y las próximas iniciativas, examinando sus fortalezas, limitaciones e idoneidad para diferentes tipos de casos de uso.

• Investigar por qué la adopción de la identificación digital corporativa es relativamente baja en muchos países, y explorar posibles remedios que potencialmente superarían los obstáculos para la adopción.

• Destacar las oportunidades potenciales para aprovechar los procesos de cooperación regulatoria internacional existentes a fin de apoyar los objetivos más amplios de eficiencia, estabilidad financiera, integridad del mercado, inclusión financiera y desarrollo sostenible.

Enfoque de investigación

Con el fin de investigar los puntos débiles de la identificación digital corporativa desde diferentes perspectivas y explorar las posibles soluciones a estos puntos débiles, realizamos entrevistas cualitativas con varias partes interesadas, como bancos, organizaciones relacionadas con bancos, e-KYC y otros proveedores de soluciones fintech, responsables políticos, organizaciones internacionales, académicos y expertos de la industria. Algunas de estas entrevistas fueron organizadas por la consultora Virtual Risk Solutions. También participamos en talleres de ideación organizados por el Grupo Asesor de la CCI sobre Financiamiento del Comercio (ATF) y el Grupo de Trabajo de Finanzas Abiertas de la Red de Innovación del BIS. Además, el Instituto de Finanzas Internacionales (IIF) estableció dos grupos focales para discutir los temas centrales de la identificación digital corporativa con los principales bancos e instituciones financieras. A través de estos canales, intercambiamos puntos de vista y obtuvimos información de profesionales de la industria y formuladores de políticas. Durante nuestro proceso de investigación, se llevaron a cabo más de 70 reuniones. Las opiniones obtenidas en estas reuniones se analizan y complementan con información de otras fuentes, como una revisión de la literatura y una encuesta escrita de las partes interesadas.

2. Panorama regulatorio y estándares digitales

Como punto de partida para identificar y verificar un negocio, la identificación digital corporativa es una parte esencial de la comprensión de una contraparte. Además de su centralidad desde el punto de vista de los procesos de negocio y la gestión de riesgos, también es un elemento importante de la regulación, en particular la regulación financiera, pero también de la regulación de datos y una serie de otros requisitos reglamentarios.

Desde un punto de vista regulatorio, la regulación de la integridad del mercado que aborda AML / CFT se centra en procesos de debida diligencia inicial y continua con el cliente. Los requisitos de AML son un foco importante de regulación financiera y cumplimiento a nivel mundial y, por lo tanto, un importante foco de atención para las empresas y los reguladores. Los requisitos de ALD/CFT son un costo, particularmente en el contexto de la adquisición de clientes. A menudo también constituyen una barrera para la inclusión financiera, tanto para las personas como para las empresas, en particular las PYME. Por lo tanto, es importante comprender el panorama regulatorio alD / CFT y cómo la identidad digital corporativa puede desempeñar un papel en él. A nivel internacional, los esfuerzos conjuntos en ALD / CFT tienen una larga historia, que se remonta a 1989, cuando las naciones del Grupo de los Siete lanzaron el GAFI. El GAFI y sus estándares han traído cambios significativos a las formas en que los bancos y las empresas de todo el mundo conducen sus asuntos a través de cambios regulatorios en las leyes y en las operaciones gubernamentales.

Además del papel directo del GAFI, una serie de otros organismos internacionales de normalización financiera también han incorporado normas conexas, entre ellas el Comité de Supervisión Bancaria de Basilea (BCBS) y la Organización Internacional de la Comisión de Valores (IOSCO). Como un hito en el panorama regulatorio, en 1997, el BCBS emitió los primeros "Principios básicos para una supervisión bancaria efectiva".13 Establece que "los supervisores bancarios deben determinar que los bancos cuenten con políticas, prácticas y procedimientos adecuados, incluidas estrictas reglas de 'conozca a su cliente', que promuevan altos estándares éticos y profesionales en el sector financiero y eviten que el banco sea utilizado. intencionalmente o no, por elementos criminales". También insta a las naciones a adoptar las 40 Recomendaciones del GAFI.

La crisis financiera de 2008 puso de relieve el riesgo sistémico dentro del sistema financiero mundial, lo que dio lugar a una serie de reformas regulatorias e iniciativas de mercado relacionadas para proteger el sistema financiero. Desde el punto de vista de la identificación digital corporativa, surgió una iniciativa importante para identificar mejor a las entidades legales involucradas en transacciones financieras complejas, como los derivados OTC y los valores respaldados por activos, particularmente aquellos involucrados en instituciones financieras de importancia sistémica a nivel mundial (G-SIFI). Como un aspecto, el G20 ordenó al FSB que estableciera un sistema global para la identificación de personas jurídicas con el fin de comprender mejor las interconexiones entre instituciones, transacciones y mercados. El identificador resultante se integró en los nuevos estándares internacionales del FSB, BCBS e IOSCO y su implementación en todos los miembros del G20 / FSB. Un aspecto de este proceso involucró la creación de nuevos "Identificadores de Personas Jurídicas" (IPJ) y su uso en una serie de reformas regulatorias financieras posteriores a la crisis.

En 2012, entró en vigor un conjunto revisado de medidas y recomendaciones del GAFI. Estas recomendaciones a un alto nivel exigen que todos los países cuenten con sistemas eficaces para prevenir y abordar el blanqueo de dinero, la financiación del terrorismo y la financiación de la proliferación. Establecen las medidas que los países deberían adoptar en el marco de sus sistemas de justicia penal y reglamentación; las medidas preventivas que deben adoptar las instituciones financieras y otras empresas y profesiones; medidas para garantizar la transparencia en la propiedad de las personas jurídicas y los mecanismos; el establecimiento de autoridades competentes con funciones apropiadas, poderes y mecanismos de cooperación; y arreglos para cooperar con otros países. Como los países tienen diversos marcos jurídicos, administrativos y operacionales y diferentes sistemas financieros, no todos pueden adoptar medidas idénticas para contrarrestar estas amenazas. Las Recomendaciones del GAFI, por lo tanto, establecen un estándar internacional, que los países deben implementar a través de medidas adaptadas a sus circunstancias particulares, con la implementación a su vez supervisada por el GAFI.

Al mismo tiempo, a partir de alrededor de 2016, también surgió un creciente reconocimiento internacional de posibles conflictos entre los objetivos de integridad del mercado en el contexto de la lucha contra el blanqueo de capitales y los objetivos más amplios de desarrollo e inclusión en el contexto de la inclusión financiera, lo que se refleja en la idea de "reducción del riesgo" tanto desde el punto de vista de la aparición de barreras significativas para las personas como para las PYME en los países individuales. en particular los países en desarrollo, y desde el punto de vista de la exclusión de grandes segmentos en el contexto de la reducción de las relaciones de corresponsalía bancaria (véase Rice et al, 2020).

2.1 Identificador de personas jurídicas (IPJ)

Corporate ID&V generalmente comienza con un identificador corporativo, que idealmente es un mecanismo único para distinguir una empresa de otra. Históricamente, la identificación corporativa ha provenido principalmente de registros de empresas en jurisdicciones individuales. Una empresa es una entidad jurídica, una criatura creada por la ley, en la mayoría de los casos bajo el marco legal estandarizado de la ley de sociedades de una jurisdicción determinada tal como se implementa en el registro nacional de empresas, pero en algunos casos directamente a través de la legislación. Por lo tanto, la creación de una empresa implica la presentación de ciertos documentos e información requeridos y el pago de las tarifas necesarias. A cambio, el registro mercantil registra – crea – la persona jurídica: la empresa. Cada empresa se identifica por un nombre y también típicamente por un número de registro de la empresa. Además del número de registro de la empresa para una entidad determinada (y un grupo podría incluir muchas entidades en una variedad de jurisdicciones), una empresa también suele tener un número de registro fiscal en una o más jurisdicciones y también posiblemente una gama de licencias y números de licencia, además de una dirección registrada, información de contacto, directores, etc. También puede haber números separados para acciones individuales en uno o más custodios, así como números para cualquier listado en bolsas. Si bien cada uno de estos números puede ser único en una jurisdicción determinada, generalmente no existe una estandarización entre jurisdicciones ni un sistema armonizado de identificación corporativa.

Con una mayor globalización de los negocios y las finanzas, esto se ha convertido en una fuente creciente de ineficiencia y riesgos desde el punto de vista de la estabilidad financiera, la integridad del mercado y la protección de los inversores.

En respuesta a las claras brechas en ID&V de las personas jurídicas en transacciones complejas antes de la crisis financiera de 2008, el G20 ordenó que el IPJ Global se lanzara en 2012 como un sistema global de identificación corporativa. Cada entidad registrada recibe un IPJ único en virtud de un sistema administrado por una organización sin ánimo de lucro, la Fundación Global del IPJ (GLEIF), y diseñado de acuerdo con la norma ISO 17442. El IPJ es un código alfanumérico de 20 caracteres que identifica de forma única a una entidad jurídica. No es necesariamente lo mismo que un número de registro de empresa, que es jurisdiccional por naturaleza, pero busca proporcionar un sistema universal de designación para entidades individuales para permitir su identificación y seguimiento en los mercados globales.

Utilizando el BIS como ejemplo, el IPJ se estructura de la siguiente manera (Gráfico 1):

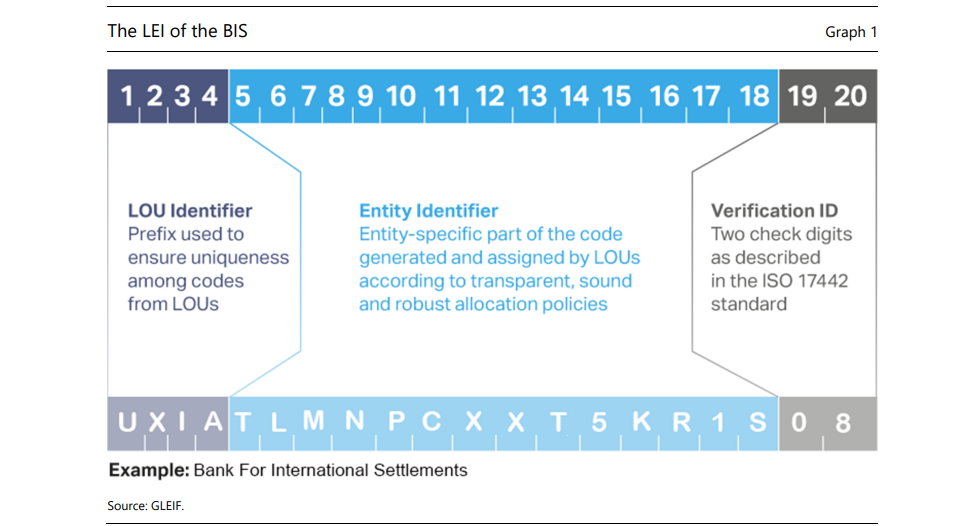
• Caracteres 1-4: representan el emisor de IPJ conocido como Unidad Operativa Local (LOU)

• Caracteres 5-6: dos caracteres reservados actualmente establecidos en cero

• Caracteres 7-18: parte específica de la entidad del código generado y asignado por las LOU

• Caracteres 19-20: dos dígitos de control como se describe en las normas ISO 17442

En este ejemplo, el BIS no es una entidad corporativa tradicional. Si bien en realidad es una sociedad limitada por acciones (en manos de 63 bancos centrales), también tiene las características de una organización internacional del sector público. Aun así, el formato utilizado es el mismo que el de otras entidades públicas y privadas, y puede usarlo para fines de ID&V. Tenga en cuenta que un IPJ representa una sola entidad jurídica y que muchos grupos empresariales formados por varias filiales tienen más de una entidad.



El IPJ cumple dos principios fundamentales:

1. Singularidad: Una vez asignado a una entidad única, el código no se asignaría a otra entidad, incluso si la entidad inicial deja de existir.

2. Exclusividad: Una entidad jurídica que ha obtenido un IPJ no puede obtener otro. Las entidades pueden transferir el mantenimiento de su IPJ de un operador a otro, pero el IPJ permanece sin cambios en el proceso.

Una característica clave del IPJ es que es un identificador global para personas jurídicas, lo que significa que los principios de unicidad y exclusividad se aplican a nivel mundial y la validez del IPJ no se limita a una jurisdicción, sector o industria en particular, y es bien reconocida en todo el mundo, con más de 220 países y jurisdicciones con disponibilidad de servicios de IPJ. Esto es diferente de los identificadores locales (por ejemplo, el número de registro emitido por un registro corporativo) que son válidos solo dentro de una jurisdicción en particular y no están estandarizados y son únicos en todas las jurisdicciones y, por lo tanto, generalmente no se reconocen más allá de las fronteras nacionales. Obviamente, a los efectos de las transacciones que involucran a múltiples partes a través de las fronteras, como la financiación del comercio y la inversión extranjera, un identificador global es preferible a uno local.

Además, la identidad global se vincula con el registro comercial local dentro de los datos de referencia del IPJ. El IPJ y sus datos referenciados están respaldados por una Fundación Suiza (GLEIF) sin ánimo de lucro supervisada por un Comité de Supervisión Regulatoria (ROC) compuesto por más de 65 reguladores de los mercados financieros y otras autoridades públicas y 19 observadores de más de 50 países. Los impulsores del IPJ (el G20, el FSB y muchos reguladores de todo el mundo) han hecho hincapié en que el IPJ es un bien público amplio. La GLEIF pone a disposición el IPJ y sus datos de referencia de forma cómoda y gratuita.

Más allá de su aplicación reglamentaria inicial en el contexto de la identificación de contrapartes en transacciones complejas (como las operaciones de derivados extrabursátiles) e instituciones (particularmente importantes en la insolvencia), los IPJ también se están utilizando para una serie de otros fines, incluidos los requisitos de integridad del mercado (ALD/CFT), los requisitos de protección de los inversores (identificación de cotización, requisitos de divulgación continua e informes comerciales) y la fiscalidad. Una nueva iniciativa del G20 centrada en la transparencia de la titularidad real de las entidades está siendo puesta en práctica internacionalmente por la OCDE y el GAFI e implementada sobre una base jurisdiccional, reuniendo muchas de estas piezas. También ofrecen oportunidades en el contexto de los nuevos requisitos de información ASG, también en el contexto del punto de acceso único (PAAS) de la UE propuesto, destinado a normalizar y centralizar la información de todas las empresas cotizadas de la UE que informan en virtud de los mercados de capitales y la regulación ASG.

Según un estudio conjunto de McKinsey y la GLEIF,14 el IPJ puede permitir ahorros de al menos el 10 % de los costes operativos totales para la incorporación de clientes y el procesamiento de operaciones para los bancos que lo adopten. Solo para la industria de la banca de inversión en general, esto produciría ahorros de más de $ 150 millones anuales. Los bancos en la financiación del comercio podrían ahorrar 500 millones de dólares adicionales al año en general mediante el uso del IPJ en la emisión de cartas de crédito. Es probable que haya más ahorros por la reducción del gasto en la identificación del vendedor para la facturación electrónica y por un proceso más automatizado para la extensión del crédito comercial.

Estos ahorros no solo mejoran la eficiencia, la estabilidad financiera y la integridad del mercado, sino que también reducen los costos y riesgos de la adquisición de clientes, y también pueden mejorar los objetivos de inclusión financiera y un desarrollo sostenible equilibrado más amplio, con un potencial particular en el contexto de las PYME.

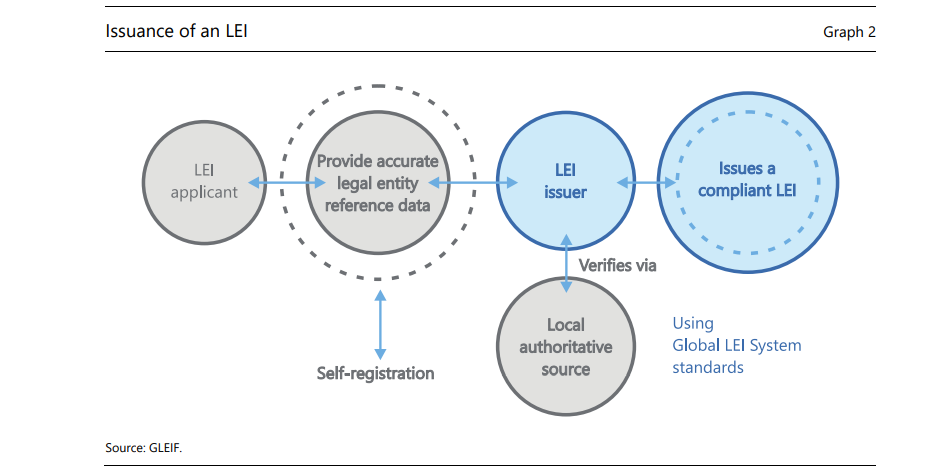
Datos de referencia

Cada IPJ está vinculado a un conjunto de datos de referencia sobre la entidad jurídica que se va a identificar. Básicamente, los datos de referencia consisten en: (1) información de la tarjeta de visita: responder a la pregunta "quién es quién" y (2) información de relación: responder a la pregunta "quién es dueño de quién". Como tal, cualquier persona puede ir al sitio web oficial de la GLEIF, ingresar el IPJ de una empresa en un cuadro y luego recuperar los datos de referencia sobre esta empresa, sin pagar ningún cargo. Como los datos ya son verificados por el emisor del IPJ, a menudo utilizando información de las autoridades de registro locales, los usuarios pueden confiar en la validez de los datos y tratarlos como el punto de partida para otros procesos comerciales, como las comprobaciones KYC y ALD/CFT.

¿Cómo funciona el IPJ?

Las empresas presentan una solicitud de IPJ mediante el autoregistro ante el emisor de IPJ (LOU) elegido, acreditado por la GLEIF. El proceso es análogo al proceso por el cual se incorporan e inscriben en un registro corporativo (Gráfico 2): El emisor del IPJ tiene entonces la función de validar la información autoinformada frente a una fuente autorizada local, como los registros de empresas, y garantizar la singularidad y exclusividad del IPJ. A partir de enero de 2022, hay 3.841 emisores de IPJ que prestan servicios a 226 países de todo el mundo, y una empresa puede elegir cualquier emisor de IPJ que esté acreditado para su jurisdicción para solicitar un IPJ. Este diseño tiene por objeto mantener la competencia entre los emisores de IPJ, de modo que la tasa de solicitud esté sujeta a la disciplina del mercado.

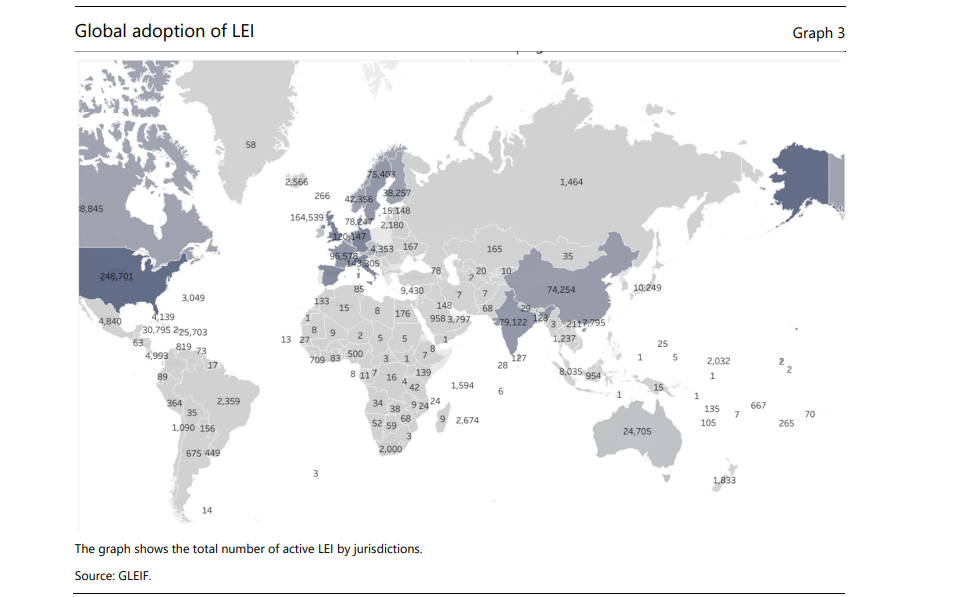
Se aplica un programa de control de calidad para garantizar la validez del registro de datos de IPJ. El programa incluye: (1) la validación anual de todos los elementos de datos en cada registro de IPJ, (2) una opción para que los usuarios externos impugnen los elementos de datos, y (3) un programa de calidad gestionado por la GLEIF que escanea diariamente el repositorio completo y publica los resultados mensualmente en informes de calidad gratuitos a nivel de emisores de IPJ globales e individuales. Tenga en cuenta que los registros de empresas generalmente no ofrecen tipos similares de programas de calidad para los datos corporativos que proporcionan. Más bien, la mayoría de los datos del registro de la empresa son declarativos, proporcionados por el solicitante de registro, y se verifican de forma independiente. Como resultado, a menudo requiere la validación por parte de las contrapartes y otros para errores simples como la falta de ortografía de los nombres de las ciudades.



Origen y adopción del IPJ

El lanzamiento del IPJ se remonta a la crisis financiera mundial de 2008-9. Durante la crisis, uno de los problemas más difíciles fue identificar las decenas de miles de entidades que tienen exposiciones financieras o que son propiedad de una institución financiera al borde del colapso, con estas entidades ubicadas en múltiples jurisdicciones. En respuesta a este desafío, el G20 eligió un modelo federado compuesto por una unidad central, la GLEIF,15 y las LOU, supervisadas por la ROC.16 La misión de la GLEIF es apoyar, sin ánimo de lucro, la implementación de un Sistema Global del IPJ para que los datos de IPJ de alta calidad estén disponibles de forma gratuita para los usuarios tanto en el sector público como en el privado.

Reflejando su historia, el uso del IPJ se limitó inicialmente a las instituciones financieras y a los instrumentos financieros negociados en los mercados OTC. A 22 de marzo de 2022, 129 reglamentos y leyes del IPJ exigidos a nivel mundial utilizan en gran medida en la presentación de informes de servicios financieros.17 Sin embargo, el diseño del IPJ es independiente del tipo de industria. En los últimos años, la adopción del IPJ se ha extendido a las empresas no financieras. A nivel mundial, había 1,95 millones de IPJ activos a finales de enero de 2022, y la mayor parte de ellos se encontraban en economías avanzadas, por ejemplo, en Europa (Gráfico 3). China e India se encuentran entre las principales jurisdicciones por crecimiento en los últimos trimestres y ambos países tienen iniciativas en marcha que aprovechan el IPJ. En noviembre de 2020, el Banco Popular de China, la Comisión Reguladora de Banca y Seguros de China, la Comisión Reguladora de Valores de China y la Administración Estatal de Divisas publicaron conjuntamente una hoja de ruta, que describe los hitos clave de la adopción del IPJ para 2020-2022. Además, el Banco de la Reserva de la India ordenó que, a partir del 1 de abril de 2021, todas las entidades que realicen transacciones de pago por valor de INR50 millones (~ USD 650,000) o más para la liquidación bruta en tiempo real y la Transferencia Electrónica Nacional de Fondos deben identificarse con el IPJ. El 21 de abril de 2022, el RBI anunció además que los prestatarios no individuales de INR50 millones o más deberían estar obligados a obtener códigos de IPJ de acuerdo con un calendario 2023-2025, dependiendo del monto del préstamo. A largo plazo, la GLEIF estima que, con el tiempo, entre 200 y 400 millones de personas jurídicas podrían ser elegibles para un IPJ.



¿Cómo se puede mejorar aún más el IPJ?

Como herramienta para identificar entidades como las empresas, el IPJ es poderoso ya que es de naturaleza verdaderamente global. Además, a medida que se valida la información asociada con el IPJ, los usuarios tienen un mayor nivel de seguridad con respecto a su autenticidad. Sin embargo, los IPJ por sí solos solo pueden resolver ciertos puntos débiles en ID&V, lo que requiere una mayor mejora.

El IPJ tiene un papel crucial en la economía digital actual, dada su capacidad para proporcionar a las empresas una identificación única y permanente a nivel mundial. Esto es especialmente importante en el contexto de la identificación de entidades legales involucradas en transacciones digitales. El IPJ aporta valor tanto al producto más maduro (los certificados digitales) como a la innovación más reciente de credenciales verificables. En comparación con otras soluciones de identificación digital corporativa, está más avanzada en el llamado "ciclo de exageración" (Gartner, 2022), habiendo demostrado su efectividad a lo largo del tiempo. Aun así, se necesitan más esfuerzos para aumentar la adopción. Es probable que la clave de esto sea una combinación de:

- recomendaciones de orientación internacional:

• las recomendaciones relativas a las sanciones, la diligencia debida con respecto al cliente y las transferencias electrónicas podrían incluir el IPJ como información de identificación para las listas de sanciones o el principal medio de identificación para los clientes o beneficiarios de personas jurídicas (recomendaciones 6, 10 y 16 del GAFI),

• BCBS podría actualizar su recomendación actual del IPJ como información complementaria para formar parte de los requisitos mínimos establecidos en las Directrices para una gestión racional de los riesgos relacionados con el blanqueo de capitales y la financiación del terrorismo.

− requisitos reglamentarios (especialmente la banca, la integridad del mercado, los mercados de capitales, la información fiscal y normativa ESG), y

− la demanda del mercado, ya que los inversores y las contrapartes consideran que las eficiencias son cada vez más valiosas.

Centrándose en la demanda del mercado a corto y medio plazo, hay cuatro pasos críticos que podrían mejorar el IPJ y aumentar su tasa de adopción:

(a) IPJ verificable (vLEI)

• El IPJ per se es simplemente un identificador que separa a una entidad jurídica de otra. Cuando se proporciona un IPJ a usuarios externos, como bancos y proveedores, aún deben llevar a cabo el proceso de verificación y autenticación para garantizar que la empresa y sus representantes (por ejemplo, funcionarios, personal general, directores) sean realmente qué o quiénes afirman ser. Este proceso puede ser minuciosamente lento e ineficiente. Esta es posiblemente una de las principales razones que desalientan a los bancos a incorporar pymes, ya que los bancos generalmente perciben que no es rentable llevar a cabo el proceso de verificación, incluso si una pyme ya ha obtenido un IPJ.

• Con el fin de mejorar el proceso de verificación mencionado anteriormente y teniendo en cuenta las crecientes necesidades de empoderar a las entidades en la gestión de su identidad en contextos digitales, la GLEIF lanzó el IPJ verificable (vLEI) a principios de 2021, y el Marco de Gobernanza del Ecosistema vLEI se lanzó en febrero de 2022. Su idea básica es incrustar el IPJ en un documento digital de una empresa. El formato de documento digital para el vLEI se basa en los estándares W3C Verifiable Credential e Decentralised Identifier. Estos estándares proporcionan mecanismos interoperables para verificar la autenticidad del vLEI. En la sección B se proporcionan más detalles sobre estas normas.

• Al aumentar los beneficios esperados de un IPJ, la iniciativa vLEI podría aumentar potencialmente la tasa de adopción del IPJ, especialmente para las pymes. Para muchas pymes, la tasa de solicitud de un IPJ y las tasas anuales de renovación, aunque no son insignificantes, no son prohibitivamente altas. Una de las razones por las que tienen poco interés es que perciben pocos beneficios materiales en la obtención de sus IPJ. También hay relativamente pocos requisitos reglamentarios directos para las IPJ que se extiendan a las PYME. Esto podría ser apoyado por iniciativas de divulgación y digitalización con el apoyo de organizaciones internacionales y de otro tipo. Si se considera un bien público, los sistemas de registro corporativo podrían beneficiarse de una iniciativa similar a ID4D.

• La iniciativa vLEI puede beneficiarse de una mayor integración con las autoridades locales, que deben informar a la GLEIF inmediatamente (o casi inmediatamente) sobre cualquier cambio en la estructura de las entidades jurídicas. Esto podría hacerse, por ejemplo, mediante la digitalización de los procesos de los registros nacionales de empresas, incluidos los requisitos para la verificación y la ecologización constante de los datos presentados. Esto tendría un enorme valor para los usuarios de los datos de los registros de empresas individuales. Estaría facultado por la normalización y armonización internacionales. También podría fomentarse a través de los mercados de capitales y otras formas de requisitos reglamentarios para los IPJ y el acceso a la información, como en el contexto de los sistemas de información reglamentaria digital, como el EDGAR de la SEC de los Estados Unidos o el PAAS de la UE propuesto.

b) IPJ en certificados digitales

• Los certificados digitales se utilizan de muchas maneras, y los estándares y las plataformas tecnológicas están maduras y auditadas. Muchas jurisdicciones han incluido certificados digitales en su legislación de firma digital como herramientas legalmente respaldadas para la autenticación.18 Los productos y servicios están ampliamente disponibles.

• La GLEIF no pretende convertirse en una Autoridad de Certificación ni prevé que los emisores de IPJ existentes se conviertan en emisores de certificados digitales. Con el fin de fomentar el uso de IPJ en los certificados digitales, la GLEIF trabaja con las autoridades de certificación y los proveedores de servicios de confianza, los proveedores de aplicaciones posteriores, las empresas privadas y las autoridades públicas para alentar a las organizaciones a integrar IPJ siempre que se emitan certificados de representación legal y sellos electrónicos de empresas en un contexto empresarial. Esto se aplicaría a los sellos de la empresa, así como a los certificados para las personas que actúan en nombre de una empresa.

• La incorporación del IPJ en los certificados digitales facilita la verificación del comercio transfronterizo y permite a los titulares del sello electrónico de la empresa o del certificado de representante legal mejorar la seguridad y la credibilidad de sus operaciones. Los ejemplos de casos de negocio incluyen la facturación electrónica, el comercio electrónico y las compras electrónicas.

c) Emisión masiva de IPJ

• Otra iniciativa que puede acelerar potencialmente el proceso de adopción del IPJ es la emisión masiva. La idea es que los IPJ se emitan, en una sola toma, a todas las empresas registradas en una autoridad de registro. Efectivamente, esto significa que cualquier registro corporativo puede servir como emisor de IPJ y emitir IPJ a todos sus solicitantes, siempre que un registro cumpla con los requisitos de la GLEIF en relación con la verificación de los datos de referencia corporativos.

• Esto podría mejorar drásticamente la eficiencia y la fiabilidad de la recopilación de datos, ya que el registro corporativo ya debería tener información sobre los atributos principales de cualquier empresa registrada. Además, a través de economías de escala, una emisión masiva podría reducir el coste por empresa en la solicitud de un IPJ. Esto también reduciría la carga para la autoridad de registro local, ya que los datos de la empresa estarían disponibles públicamente a través del Índice Global de IPJ, lo que significa que la autoridad de registro local podría aprovechar este punto de acceso también para sus clientes.

d) Validación del agente

• En septiembre de 2020, la GLEIF introdujo un nuevo papel en el sistema global del IPJ conocido como agente de validación. Este movimiento podría simplificar y acelerar la emisión de IPJ. Un agente de validación suele ser una institución financiera o cualquier otra organización involucrada en la verificación y validación de identidad que se pone en contacto con los Emisores de IPJ en nombre de sus clientes para "validar" que se han realizado verificaciones y procesos de datos clave. La idea es capitalizar la información que el Agente de Validación ya ha adquirido con el fin de cumplir con los requisitos reglamentarios (por ejemplo, KYC, AML / CFT, impuestos, informes de datos) y los procesos de diligencia debida del cliente no solo para AML sino también para fines de evaluación de crédito y antifraude.

• Desde la perspectiva de los mercados emergentes, la GLEIF puso en marcha un proyecto piloto en agosto de 2021 que permitiría a los bancos africanos emitir IPJ a las pymes.

Además, en 2020, el GAFI publicó una nueva guía sobre identificación digital, destacando su valor, particularmente en el contexto de las personas físicas, pero también para las personas jurídicas. La guía permitió el reconocimiento de la identificación digital para fines regulatorios y de CDD. Del mismo modo, en 2022, el GAFI publicó una nueva guía sobre los requisitos de transparencia de los beneficiarios reales, destacando la necesidad de que las jurisdicciones establezcan mecanismos para garantizar la identificación de los beneficiarios reales de las personas jurídicas.

2.2 Identificadores descentralizados estándar (DID)

Algunas de las soluciones propuestas más recientes a los desafíos de la identidad digital corporativa se basan en el estándar de identificadores descentralizados (DID) propuesto por el consorcio World Wide Web (W3C). Diseñados como un protocolo técnico, los DID intentan resolver los desafíos de las soluciones de identidad digital que a menudo sufren cuellos de botella centralizados, desalentando así la adopción generalizada, especialmente en mercados subdesarrollados, en áreas jurisdiccionales o dentro de segmentos de mercado más pequeños. La propuesta de DID hace hincapié en los principios básicos de interoperabilidad, propiedad y control y verificación digital. En concreto, el W3C ha formulado los requisitos para este nuevo tipo de identificadores:

• Descentralizado: no debe haber un organismo emisor central;

• Persistente: los identificadores deben ser intrínsecamente persistentes, sin requerir el funcionamiento continuo de una organización subyacente;

• Verificable criptográficamente: debe ser posible demostrar el control del identificador criptográficamente;

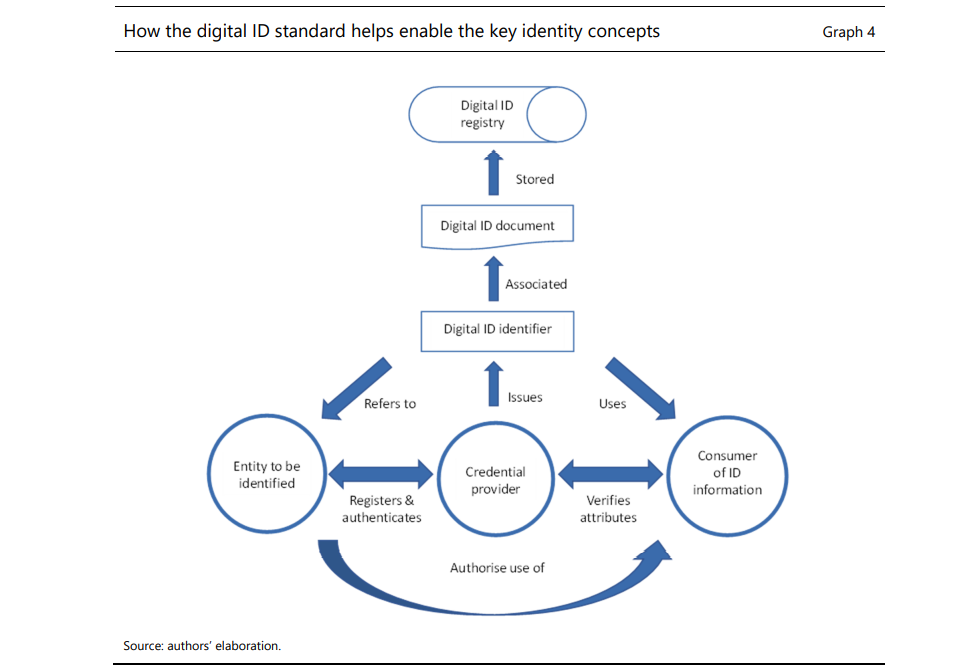
• Resoluble: debería ser posible descubrir metadatos sobre el identificador.

Con el fin de resolver los cuellos de botella de identidad tradicionales, la norma define un mecanismo descentralizado que desagrega los componentes comunes de un sistema de identidad digital corporativa y propone un nuevo modelo para que estos componentes trabajen juntos. Estos componentes incluyen: (1) las entidades a identificar, (2) los proveedores de credenciales que verifican la identidad de cada entidad, y (3) los consumidores de la información de identidad. En términos simples, los DID proporcionan un protocolo para conectar a estos actores de tal manera que cada parte exhibe una cantidad adecuada de control sobre las partes de la solución de identidad a las que son responsables.

Una de las características definitorias de los DID es la propiedad y el control del usuario, que también es una razón por la cual la solución se combina con la "identidad autosoberana". A diferencia de los identificadores tradicionales, los DID se construyen de tal manera que podrían desacoplarse de los registros centralizados, los proveedores de identidad y las autoridades de certificación. Si bien estas partes serían necesarias para el descubrimiento de información sobre la entidad detrás de un identificador descentralizado, DIDs garantiza que el propietario del identificador pueda probar el control sin requerir el permiso de ninguna otra parte. Los DID son identificadores uniformes de recursos (URI) que asocian un sujeto de IDENTIFICACIÓN digital, la entidad, con un documento DID, un conjunto o subconjunto de metadatos sobre la entidad. Esto permite interacciones confiables asociadas con ese tema. Tenga en cuenta que el W3C define un sujeto de identificación digital como "la entidad identificada por DIDS. Cualquier cosa puede ser un tema de identificación digital: persona, grupo, organización, cosa física, cosa digital, cosa lógica, etc."

¿Cómo funciona el modelo DIDs?

El modelo DIDs es independiente de la tecnología, aunque a menudo se asocia con el uso de redes de contabilidad distribuida como blockchain. Sucintamente, la norma funciona de la siguiente manera (Gráfico 4).



Supongamos que una corporación es una entidad que debe identificarse (abajo a la izquierda del Gráfico 4). Después de un proceso de registro y autenticación con el proveedor de credenciales, se registra un identificador de identificación digital descentralizado en un sistema de registro. Dentro del registrador, el identificador corresponde a un documento de identificación digital descentralizado, que contiene métodos de verificación opcionales que se utilizan para facilitar uno o más servicios relacionados con la identidad.21 Un consumidor de información de identificación (abajo a la derecha del Gráfico 4), como un banco que va a incorporar a un cliente corporativo, interactuaría con el proveedor de credenciales para verificar los atributos de esa corporación, con la condición de que la corporación proporcione autorización para el uso de dichos atributos. De esta manera, la combinación de los métodos de identificación, documento y verificación permite utilizar flujos de trabajo flexibles en torno a la creación, gestión y uso compartido de una identidad digital.

¿Blockchain o no?

Uno de los principios clave de los DID es el uso de una fuente de registro persistente y confiablemente disponible. El estándar W3C en sí mismo es independiente de la tecnología, pero dada la disponibilidad y el potencial de inmutabilidad propuesto por la tecnología blockchain, las redes basadas en blockchain son a menudo una fuente comúnmente utilizada para almacenar identificadores en implementaciones de DIDs.

Puede haber consideraciones económicas e institucionales sobre si una solución debe usar blockchain, tecnología de contabilidad distribuida autorizada o tecnologías de datos convencionales. En situaciones con un estado de derecho débil o una aplicación limitada de los contratos (por ejemplo, en estados frágiles o en desarrollo), blockchain o DLT autorizado podría ofrecer beneficios potenciales, pero es posible que deba lidiar con altas rentas para los validadores y límites a escala (Auer, Monnet y Shin, 2021). En otros casos, las consideraciones de seguridad y escala pueden favorecer un libro mayor centralizado. Esto puede estar respaldado por preocupaciones de privacidad y confidencialidad de datos, ya que un libro mayor inmutable y visible públicamente puede chocar con consideraciones como el derecho al olvido (Finck, 2018).

Beneficios de los DIDs

Los DID brindan la oportunidad de reducir los costos y las barreras de entrada, sirviendo como un protocolo de interoperabilidad entre las redes y soluciones de identidad existentes y proporciona una base escalable para proyectos a largo plazo. Estos beneficios se derivan del núcleo de la norma que proporciona un lugar único en el que se pueden registrar los identificadores y un método de comunicación establecido entre el número potencialmente infinito de entidades, proveedores de credenciales y consumidores. Las soluciones basadas en DID buscan mejorar la aplicación de los registradores y proveedores de identidad existentes, al tiempo que permiten la creación de un nuevo ecosistema de proveedores y participantes.

Desafíos con los DID

La adopción y el uso generalizado de los DID no están exentos de desafíos. Para los usuarios, puede haber costos iniciales para establecer una nueva infraestructura en forma de billeteras de identidad, servicios de identificación digital y registradores. Esto se combina con el desafío general de fomentar la adopción de una nueva norma. Debido a la dependencia de las tecnologías descentralizadas y la ausencia de un proveedor de servicios central, se requerirán soluciones técnicas a medida para realizar varios pasos clave para obtener y utilizar un DID. Cada una de estas soluciones necesitará tiempo para madurar su usabilidad, especialmente para los componentes de cara al usuario que requieren interacción con algunas de las áreas más desafiantes técnicamente, como cuando se utilizan claves criptográficas para firmas digitales. Problemas de madurez similares se pueden ver en soluciones que incorporan componentes tecnológicos emergentes, como las redes blockchain.

3. Aspectos legales y reglamentarios

Una empresa es una construcción jurídica, una "entidad jurídica" o "persona jurídica", creada bajo una forma estándar de marco estatutario o mediante promulgación legislativa. Si bien las empresas y otras formas de entidades legales tienen una larga historia, posiblemente desde el derecho romano, la ley islámica y el derecho canónico, su forma moderna comienza con las empresas establecidas por los soberanos para proporcionar servicios comerciales y otros servicios de tipo monopolio estatal en la Europa moderna temprana. Estas primeras compañías fueron generalmente creadas por carta real o parlamentaria, con ejemplos que incluyen las Compañías Holandesas y Británicas de las Indias Orientales y el Banco de Inglaterra. Este período de la historia culminó en la Burbuja de 1720. La reacción contra las empresas como resultado del colapso ralentizó el desarrollo durante un siglo, pero esto cambió durante el curso del siglo XIX a medida que se promulgaron una serie de leyes de empresas y corporaciones en las principales jurisdicciones para proporcionar marcos simples para la creación de empresas en ausencia de una carta real o parlamentaria específica. Como resultado, la empresa puede verse en el corazón de la revolución industrial y de la globalización económica y financiera moderna.

Bajo estos marcos legales estandarizados, las empresas tienen personalidad jurídica, existencia perpetua y sus propietarios tienen responsabilidad limitada, a cambio de ciertos requisitos, tanto iniciales como continuos. La personalidad corporativa establece que una empresa es una persona jurídica construida artificialmente, tratada como una persona física y separada de sus fundadores, directores y accionistas. Como una empresa posee sus propios derechos y pasivos, sus ingresos y activos están separados de los de sus propietarios. Tenga en cuenta que una empresa no realiza negocios en nombre de sus fundadores, propietarios, directores o accionistas; es una entidad separada.

Una empresa adquiere su personalidad corporativa solo después de que está debidamente constituida y recibe un certificado de incorporación emitido por un registro de la empresa. Antes de que se emita este certificado, una empresa no existe, legalmente hablando. Dado que la personalidad jurídica sólo existe en las sociedades constituidas, una PYME organizada como empresa unipersonal, sociedad u otra forma no constituida en sociedad no tiene personalidad jurídica propia. Desde el punto de vista jurídico, su identidad no es separable de las de su propietario o propietarios.

3.1 Cuestiones legales en la identidad digital corporativa

El principio de neutralidad tecnológica puede servir como principio rector para las leyes que rigen la identificación digital corporativa. Según este principio, las leyes solo consideran la sustancia de un proceso comercial en lugar de los medios tecnológicos adoptados para llevar a cabo este proceso. En otras palabras, hace poca diferencia si la identificación y verificación de una empresa se realiza de forma remota a través de una solución digital, o por medio de documentos tradicionales en papel en una reunión física.

Sin embargo, en el contexto de la identificación digital corporativa, el principio de neutralidad tecnológica por sí solo podría no ser suficiente porque los legisladores aún enfrentan una compensación sobre cuán detalladas y específicas deberían ser las leyes. Por un lado, si las leyes son muy detalladas y específicas, podrían reducir la inseguridad jurídica, pero corren el riesgo de quedar obsoletas por la rápida evolución de la tecnología. Como los procesos legislativos suelen ser largos, no es práctico modificar las leyes con frecuencia en respuesta a cada nueva pieza de innovación tecnológica. Por otro lado, si las leyes solo consisten en principios o criterios generales, los riesgos de quedar obsoletas podrían reducirse, pero podrían surgir muchas incertidumbres legales para los profesionales de la industria, así como para otras partes interesadas. En consecuencia, esto podría causar confusión y desalentar la adopción de nuevas tecnologías. Por lo tanto, es importante lograr un equilibrio adecuado entre estos dos extremos.

Hay otras cuestiones importantes que deben resolverse. En primer lugar, como las soluciones de identificación digital corporativa implican información sensible y posiblemente confidencial, es crucial que los datos se perciban como auténticos, verificables y ciberseguros. A fin de fomentar la confianza entre todos los participantes, es necesario contar con un marco de gobernanza ampliamente aceptado que se base en la legislación. En segundo lugar, también debe establecerse un mecanismo para delinear las posibles responsabilidades de las diversas partes, y establecer procedimientos bien definidos para resolver las controversias que puedan surgir. Finalmente, es muy útil considerar la integración entre la identificación digital corporativa y los aspectos relacionados, incluidas las firmas digitales y la identificación digital individual.

Las siguientes secciones destacan algunos de los marcos legales de identificación digital corporativa actualmente disponibles que podrían proporcionar información sobre cómo se podrían abordar estos problemas. Estos marcos incluyen: (1) el Proyecto de Disposiciones de la CNUDMI sobre el Uso y reconocimiento transfronterizo de la Gestión de la Identidad y los Servicios de Confianza, (2) el Marco Europeo de Identidad Digital (PCTF) y (3) el Marco de Confianza Pan-Canadiense.

3.2 Proyecto de disposiciones de la CNUDMI sobre la utilización y el reconocimiento transfronterizo de los servicios de gestión de la identidad y de confianza

A grandes rasgos, los servicios de gestión de identidades (IdM) consisten en gestionar la prueba de identidad o la identificación electrónica de personas jurídicas. Estos servicios esencialmente buscan responder a dos preguntas básicas: (1) "¿Quién o qué está tratando de probar la identidad?" y (2) "¿Qué tan confiable se prueba la identidad?" A menudo se relacionan con un tercer aspecto, que es la interconexión de la prueba de identidad con una serie de otros atributos para proporcionar detalles de las actividades de la entidad o individuo en cuestión.

Con miras a promover el IdM electrónico, la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI), que es el órgano de las Naciones Unidas que se centra en el derecho mercantil internacional privado, ha estado recibiendo presentaciones relevantes de los Estados miembros y las organizaciones internacionales desde 2016. Sobre la base de las aportaciones de esas partes interesadas, la CNUDMI publicó un proyecto de ley modelo sobre la utilización y el reconocimiento transfronterizo de la gestión de la identidad y los servicios de confianza ("Proyecto de ley modelo"). La última versión se distribuyó el 21 de febrero de 2022.

El proyecto de ley modelo no tiene por objeto establecer un régimen amplio de idM, que debería ser la labor realizada por las distintas jurisdicciones que tengan en cuenta sus circunstancias específicas. En cambio, está "diseñado para regular la provisión de IdM en la medida necesaria para dar reconocimiento legal y efecto a esos servicios". En otras palabras, no tiene capacidad legal ni signatarios. Su objetivo es proporcionar un patrón para que los legisladores de los gobiernos nacionales consideren la adopción como parte de su legislación nacional para los servicios de IdM y aclarar los principales problemas legales que podrían surgir.

Entre las cuestiones jurídicas de un sistema idm, la más importante se refiere a las obligaciones y responsabilidades de los proveedores de servicios IdM y los abonados a sus servicios. Esto es importante porque la falta de claridad sobre las responsabilidades de las partes involucradas a menudo constituye un impedimento importante para promover la confianza en el uso de los servicios de IdM. Todas las partes en el sistema de identidad digital deben poder definir claramente los derechos y obligaciones de acceso y asignar los riesgos. Básicamente, el proyecto de ley modelo postula el principio general de que los proveedores de servicios de IdM serán responsables de los daños causados a cualquier persona debido al incumplimiento intencional o negligente de sus obligaciones. No obstante, el proveedor de servicios idm no será responsable ante el abonado de los daños derivados del uso de un sistema IdM en la medida en que:

tiene. El uso excede las limitaciones en el propósito o el valor de las transacciones para las cuales se puede utilizar el sistema IdM; y

b. El proveedor de servicios de IdM ha notificado al suscriptor de esas limitaciones de conformidad con la ley.

Además, el proyecto de ley modelo trata de aclarar algunas cuestiones jurídicas que a menudo dan lugar a incertidumbres entre las partes interesadas. Por ejemplo, tiene disposiciones que especifican el estatuto jurídico de la identificación electrónica, la definición del consentimiento de los usuarios y el reconocimiento transfronterizo de los servicios de IdM. Específicamente:

• Situación jurídica de la identificación electrónica: No se denegará a la identificación electrónica de una persona el efecto jurídico, la validez, la fuerza ejecutiva o la admisibilidad como prueba por el único motivo de que la prueba de identidad y la identificación electrónica se realicen en formato electrónico (artículo 5).

• Consentimiento de los usuarios: Si bien el uso de IdM y/o servicios de confianza no debe imponerse a una persona que no haya aceptado utilizar estos servicios, el Proyecto de Ley Modelo sugiere que no es necesario el consentimiento expreso de los usuarios. La frase «el consentimiento puede inferirse de la conducta de la persona» sugiere que se otorga un consentimiento cuando los usuarios utilizan y se basan en el IdM (artículo 3).

• Reconocimiento transfronterizo de los servicios de IdM: Un sistema de IdM operado fuera de la jurisdicción promulgante tendrá el mismo efecto jurídico en la jurisdicción promulgante que un sistema de IdM operado o un servicio de confianza prestado en la jurisdicción promulgante si ofrece un nivel sustancialmente equivalente de fiabilidad (artículo 25).

De este modo, el IdM proporciona la base potencial de un marco jurídico acordado que, de hecho, podría funcionar conjuntamente con los DID y los IPJ para permitir la base de un sistema híbrido de ID de base vinculado a través de la tecnología y con una base jurídica adecuada. La posibilidad, en particular a nivel regional, queda ilustrada por el eIDAS de la UE y el marco europeo de identidad digital. Sin embargo, el desafío con las leyes y tratados modelo es a menudo el tiempo involucrado. En consecuencia, puede haber margen como opción para incorporar las normas en la orientación internacional o en los reglamentos de los sistemas. El Marco de Confianza Pancanadiense proporciona un ejemplo útil.

3.3 Identidad digital europea

El 3 de junio de 2021, la Comisión Europea propuso un marco para una identidad digital europea que estará disponible para todos los ciudadanos, residentes y empresas de la Unión Europea (UE) en la UE. Aunque se espera que este marco priorice la identificación digital individual durante sus primeros años, cabe destacar que también da cabida al establecimiento de la identificación digital corporativa.

En el marco de la identidad digital europea, los Estados miembros ofrecerán a los ciudadanos y a las empresas monederos digitales que podrán vincular sus identidades digitales nacionales con la prueba de otros atributos personales (por ejemplo, permiso de conducción, diplomas, cuenta bancaria). Estas carteras podrán ser facilitadas por autoridades públicas o por entidades privadas, siempre que estén reconocidas por un Estado miembro. Los servicios públicos y determinados servicios privados estarán obligados a reconocer la Identidad Digital Europea. Como tal, las nuevas carteras europeas de identidad digital permitirán a todos los europeos acceder a los servicios en línea sin tener que utilizar métodos de identificación privados o compartir innecesariamente datos personales. Con esta solución se espera que tengan el control total de los datos que comparten.

La identidad digital europea será:

• Disponible para cualquier persona que quiera utilizarlo: Cualquier ciudadano de la UE, residente o empresa en la Unión que desee hacer uso de la Identidad Digital Europea podrá hacerlo.

• Ampliamente utilizables: las carteras europeas de identidad digital serán ampliamente utilizables como forma de identificar a los usuarios o de demostrar determinados atributos personales, a efectos del acceso a los servicios digitales públicos y privados en toda la Unión.

• Usuarios que controlan sus datos: Las carteras europeas de identidad digital permitirán a las personas elegir qué aspectos de su identidad, datos y certificados comparten con terceros, y realizar un seguimiento de dicho intercambio. El control del usuario garantiza que solo se compartirá la información que necesita ser compartida.

El marco europeo de identidad digital se basa en el marco jurídico transfronterizo existente para las identidades digitales de confianza, a saber, la iniciativa europea de identificación electrónica, autenticación y servicios de confianza (eIDAS). Adoptado en 2014, el eIDAS proporciona la base para la identificación electrónica transfronteriza, la autenticación y la certificación de sitios web dentro de la UE.

Actualmente, aproximadamente el 60 % de los europeos ya se benefician del sistema actual. Sin embargo, no existe ningún requisito para que los Estados miembros desarrollen una identificación digital nacional y la hagan interoperable con las de otros Estados miembros. Esto conduce a altas discrepancias entre los países. La propuesta actual abordará estas deficiencias mejorando la eficacia del marco y extendiendo sus beneficios al sector privado y al uso móvil.

3.4 Marco de confianza pancanadiense

En septiembre de 2020, el Consejo de Identificación y Autenticación Digital de Canadá (DIACC), una coalición sin fines de lucro de organizaciones del sector público y privado comprometidas con el desarrollo de soluciones canadienses de identificación digital, lanzó el Marco de Confianza Pancanadiense (PCTF) como "un conjunto de reglas y herramientas diseñadas para ayudar a las empresas y los gobiernos a desarrollar herramientas y servicios que permitan verificar la información sobre una transacción específica o un conjunto particular de transacciones".

El PCTF se compone de siete componentes, cada uno de los cuales define procesos de confianza y criterios de conformidad relacionados con su área específica. El componente de organización verificada ("VOC") es el más relevante para la identificación digital corporativa. En general, desde una perspectiva operativa, el PCTF está bien estructurado y es bastante completo. Pero requiere más leyes y regulaciones para su implementación real.

Componente de organización verificada ("VOC"): fortalezas y limitaciones

El VOC define los procesos y criterios de conformidad para: (1) establecer y verificar la identidad de la organización y (2) crear la representación digital de confianza de una organización (es decir, identidad digital). Los criterios de conformidad son "los requisitos, especificaciones, recomendaciones y directrices que componen un estándar para evaluar la confiabilidad de procesos específicos. Los participantes pueden utilizar estos criterios para informar el diseño y desarrollo de sus productos y servicios". Un proceso de identificación que concuerda con los criterios de conformidad se convertirá en un proceso confiable que puede adoptarse como un sistema de identidad digital confiable.

Hay dos fortalezas principales del COV:

1. Es lo suficientemente amplio como para aplicarse a prácticamente todas las organizaciones, incluidas: (i) las organizaciones no incorporadas; ii) grandes organizaciones (por ejemplo, conglomerados multinacionales); y (iii) pequeñas organizaciones creadas por una sola persona (por ejemplo, empresas unipersonales).

2. Es un sistema multipartidista donde las organizaciones intercambian información confiable sobre sí mismas con las de las partes externas. Y el PCTF reconoce explícitamente el uso de la información para fines de KYC.

Sin embargo, el PCTF es sólo un marco muy amplio. Los siete perfiles de conformidad incluyen más de cien criterios de conformidad. Esto requerirá un mayor cumplimiento. Al ser solo un marco, los participantes adoptan voluntariamente el marco. No existe ninguna obligación legal para todos los expertos de la industria (incluidos los participantes) de observar estrictamente los criterios de conformidad. Además, el PCTF proporciona poca orientación para reducir la inseguridad jurídica derivada de los sistemas de identidad corporativa digital, ya que las obligaciones y responsabilidades legales de los participantes no se proporcionan explícitamente. Los participantes tienen que recurrir a las leyes existentes.

4. Registros de empresas

Los registros de empresas desempeñan un papel fundamental en cualquier ecosistema de identificación corporativa, sin importar cómo evolucionen las tecnologías o cualquier modelo operativo que se adopte. En primer lugar, estas agencias del sector público son el proveedor principal de identificación de la empresa, a menudo emitiendo un identificador único (por ejemplo, número de registro) para cada empresa bajo su registro. También son el proveedor más completo de credenciales corporativas, independientemente del tamaño de la empresa y los tipos de industria. En segundo lugar, solo un registro corporativo tiene el poder legal de obligar a las empresas a presentar datos precisos sobre sí mismas y actualizar estos datos de forma regular. Ninguna empresa de KYC del sector privado o proveedores de datos tiene tal autoridad legal, ni tienen los incentivos y las capacidades de investigación para administrar datos corporativos tan voluminosos para toda la economía. Por lo tanto, los registros corporativos a menudo se consideran la "fuente de oro" de información; por lo menos son la "fuente de oro" de la identificación corporativa y de sus atributos centrales, en particular sus directores y domicilio social. Es cierto que existen limitaciones para estos datos, en particular la falta de verificación de datos por parte de la mayoría de estos registros. Sin embargo, los usuarios como los bancos, los proveedores de datos y las empresas de KYC se dan cuenta de que los registros corporativos a menudo sirven como el primer paso de sus procedimientos de diligencia debida, además de lo cual pueden realizar análisis adicionales e investigaciones más profundas para verificar los datos del registro.

Para que los registros corporativos desempeñen mejor su papel en un ecosistema de identidad digital corporativa, deben abordar una serie de cuestiones básicas:

• ¿Recopilan toda la información necesaria sobre las empresas, en particular la información sobre la propiedad real que se requiere para KYC / AML en muchas jurisdicciones?

• ¿Llevan a cabo el control de calidad necesario de los datos de su empresa (por ejemplo, verificación de los datos presentados por las empresas, requisito de actualización más frecuente de los datos)?

• ¿Ponen la información de la empresa (incluida la información personal sobre sus directores y accionistas principales) a disposición del público, hasta el punto en que lo permitan las leyes de privacidad de datos?

• ¿Adoptan medidas para facilitar la recuperación de datos corporativos por parte de usuarios externos mediante el uso de tecnología de la información (por ejemplo, acceso remoto automatizado a los datos a través de API, datos almacenados en formatos legibles por máquina)?

En esta sección, primero damos una visión general de los registros de empresas en todo el mundo, evaluando los diferentes aspectos de su desempeño al proporcionar datos de la empresa. La siguiente sección se centra en su suministro de datos sobre la titularidad real, ya que las recomendaciones del GAFI especifican que la identificación y verificación de los beneficiarios finales de una empresa forman una parte importante del procedimiento de diligencia debida del cliente y también un requisito cada vez mayor de los miembros del G20 / FSB. Finalmente, examinamos las limitaciones y desafíos de los registros en general, y luego examinamos los principales problemas que deben resolverse.

4.1 Apertura de los registros de sociedades

Con el fin de evaluar el desempeño de los registros corporativos, hacemos uso del Open Company Data Index (OCDI) compilado por OpenCorporates con el apoyo del Instituto del Banco Mundial desde 2012. El OCDI cubre actualmente 208 registros de empresas en todo el mundo. Como los puntajes más actualizados de todos los registros de empresas están disponibles gratuitamente en el sitio web de OpenCorporates (https://opencorporates.com), este informe no enumeraría los puntajes de los registros de empresas individuales. En su lugar, se proporciona un análisis estadístico de todos los registros.

El OCDI puntúa los registros de empresas en una escala de 0 a 100 utilizando una metodología consistente descrita en su sitio web. En resumen, la puntuación total se basa en los siguientes criterios, con su ponderación entre paréntesis:

1. Búsqueda libre: Capacidad de búsqueda en línea con obstáculos mínimos en términos de costos u otras barreras (20%)

2. Licencias: Una licencia explícita de gobierno abierto que permite el uso libre de los datos obtenidos del registro (30%)

3. Datos disponibles gratuitamente: La información del registro está disponible como datos, ya sea como un volcado de datos gratuito o a través de una API gratuita (20%)

4. Profundidad de los datos: disponibilidad de datos para el público en general sobre las siguientes áreas:

tiene. Lista de directores de empresas (10%)

b. Lista de accionistas significativos (10%)

c. Cuentas anuales de la empresa (10%)

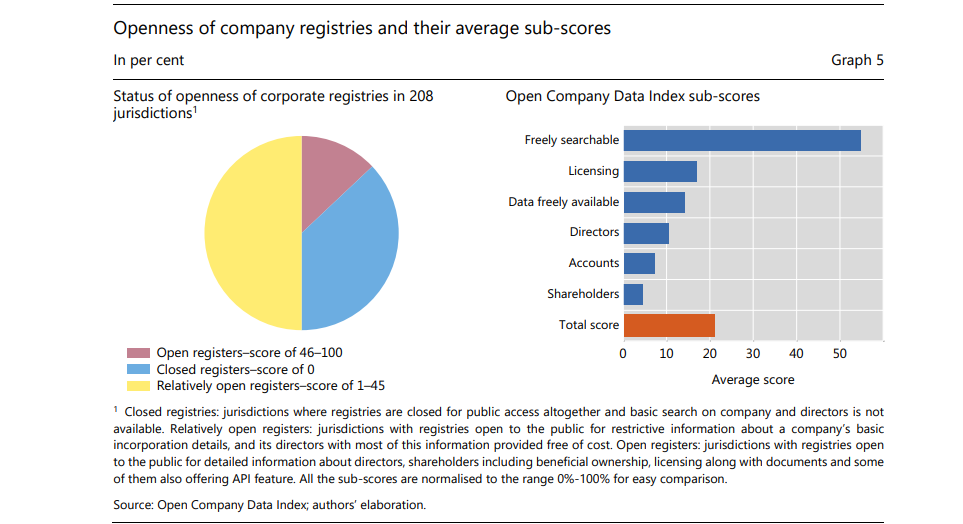
Sobre la base de la OCDI, la apertura de datos de los registros de empresas en todo el mundo es bastante divergente. A nivel mundial, 27 registros (13% del total) se clasifican como "Abiertos", con una puntuación total de 46-100. Los grupos más grandes se clasifican como cerrados (77 registros, 37% del total) o "Relativamente abiertos" (104 registros, 50% del total) (Gráfico 5, panel izquierdo).

El gráfico 5 (panel derecho) muestra el promedio de todas las subpuntuaciones de la OCDI. En primer lugar, es obvio que los registros de empresas se desempeñan relativamente bien en términos del Criterio # 1 (Libremente buscable), con un puntaje normalizado promedio de 54.9%, significativamente más alto que el puntaje promedio general de 21.1%. En otras palabras, la mayoría de los registros de empresas pueden proporcionar capacidad de búsqueda en línea sin costos prohibitivos u otros obstáculos. Por lo tanto, lo que hace que un registro de empresas abierto se destaque de uno cerrado es su desempeño en los criterios restantes. En concreto, para que los registros de empresas puedan dar un mejor soporte a los sistemas de identidad digital corporativa, hay mucho margen para que mejoren en lo que se refiere a:

(a) emisión de una licencia de gobierno abierto que defina claramente el libre uso de los datos del registro;

b) hacer que sus datos sean legibles por máquina; y

c) mejorar la profundidad de los datos en términos de información sobre los administradores de las sociedades, los accionistas significativos y las cuentas anuales de las sociedades.



4.2 Datos de titularidad real en los registros de empresas

En términos generales, un propietario beneficiario final (UBO) es un individuo que en última instancia se beneficia de una transacción iniciada por una organización. El beneficio se puede obtener directa o indirectamente a través de muchos métodos, como una red de propiedad anidada de las empresas. Si bien las diferentes jurisdicciones tienen diferentes definiciones de una UBO, una UBO generalmente se define como un individuo que posee un mínimo de capital o derechos de voto en la entidad subyacente. Ese mínimo es en su mayoría alrededor del 25%, pero también depende de las reglas de jurisdicciones específicas.

La identificación UBO es una parte importante en el proceso de identificación y verificación de una empresa, ya que esto puede prevenir el uso indebido de una persona jurídica para actividades ilegales como el lavado de dinero y el financiamiento del terrorismo. Esto es especialmente aplicable a los bancos y otras instituciones financieras que están sujetos a requisitos regulatorios con respecto a KYC y AML / CFT.

Como resultado, en 2014 el G20 acordó un nuevo conjunto de enfoques políticos para la transparencia de los beneficiarios reales, basándose en la orientación existente del GAFI: los Principios de alto nivel sobre la transparencia de los beneficiarios reales. En 2022, el GAFI publicó una guía revisada que requiere la implementación de la transparencia de los beneficiarios reales.

En esta sección, analizamos los principales problemas relacionados con la identificación de UBO haciendo uso de los registros de empresas en algunas jurisdicciones.

(a) Estados Unidos

En 2021, el Congreso de los Estados Unidos promulgó dos leyes relacionadas con la transparencia corporativa. Ellos son: (1) la Ley de Transparencia Corporativa ("CTA") y (2) la Ley de Autorización de Defensa Nacional para el Año Fiscal 2021 ("NDAA 2021"), que se convirtió en Ley Pública el 1 de enero de 2021. En resumen, estas leyes proporcionan la base legal para que ciertos tipos de empresas divulguen su propiedad real al público.

CTA impone la obligación a ciertas compañías de presentar un informe sobre la propiedad real a la Red de Cumplimiento de Delitos Financieros del Departamento del Tesoro ("FinCEN"). Básicamente, la propiedad real se refiere a cualquier individuo que (1) ejerce un control sustancial sobre la entidad o (2) posee al menos el 25% de los intereses de propiedad de la entidad. Tenga en cuenta que la CTA no define el "control sustancial" y no describe cómo deben medirse los intereses de propiedad. La información de la titularidad real debe incluir: (1) nombre legal completo, (2) fecha de nacimiento, (3) dirección residencial o comercial actual y (4) número de identificación único. Sin embargo, la información sobre la titularidad real presentada en el marco del CTA no está a disposición del público. El FinCEN solo compartirá la información con las agencias de aplicación de la ley e instituciones financieras estadounidenses y algunas globales para fines de diligencia debida.

La NDAA 2021 prevé el lanzamiento de un registro público de beneficiarios reales, es decir, la información relacionada con UBO de ciertas empresas estaría a disposición del público. Sin embargo, no todas las compañías estarán obligadas a proporcionar información de UBO porque la NDAA impone la regulación solo a las compañías que reciben contratos federales de más de $ 500,000. Además, no todos los tipos de beneficiarios reales serán conocidos públicamente porque la definición de propiedad real de la NDAA no es lo suficientemente amplia.

b) Unión Europea

La Quinta Directiva contra el blanqueo de capitales (5AMLD) estipula que todos los Estados miembros de la UE deben establecer registros públicos de titularidad real ("registros") antes del 10 de enero de 2020. La información contenida en estos registros debe ser accesible al público en general. El 5AMLD reemplaza al 4AMLD que no requería que la información fuera de acceso público. Para las personas jurídicas y otras entidades jurídicas, se requiere la siguiente información sobre sus beneficiarios reales: (1) nombre, (2) mes y año de nacimiento, (3) país de residencia, (4) nacionalidad, (5) naturaleza y alcance de los intereses beneficiosos mantenidos. Es notable por exigir a los fideicomisos que divulguen información de beneficiarios reales como lo hacen las empresas. A largo plazo, la Comisión Europea tiene el objetivo de interconectar los registros de los Estados miembros. Se espera que el marco europeo de identidad digital anunciado en 2021 facilite la identificación y verificación de los beneficiarios reales de una empresa una vez que este marco se implemente por completo. Sin embargo, el mecanismo y el plan exactos aún no se han anunciado.

En la práctica, sin embargo, pasará tiempo antes de que todos los Estados miembros puedan establecer un registro verdaderamente público. Según Global Witness, hasta marzo de 2020, solo 5 de los 27 estados miembros han implementado un registro público de acceso gratuito. Otros 5 Estados miembros cuentan con un registro centralizado de los beneficiarios reales de las empresas que está a disposición del público, pero con importantes restricciones que dificultan su utilidad en la lucha contra el blanqueo de capitales. Estas restricciones incluyen la creación de un muro de pago o solo poder buscar utilizando el número de identificación fiscal de una empresa. Mientras tanto, 17 de los 27 Estados miembros aún no tienen un registro centralizado de los beneficiarios reales de las empresas que esté disponible para el público. Esta categoría incluye algunos países que aún no tienen un registro de beneficiarios reales que sea accesible para los miembros del público con un interés legítimo, que se requería que se hubiera implementado en la 4ª Directiva AML para junio de 2017.

c) Reino Unido

El registro del Reino Unido se llama People with Significant Control Register (PSCR). Una característica notable es que toda la lista de beneficiarios reales de todas las entidades legales se puede descargar como un archivo .json y este archivo se actualiza diariamente. Esto es tremendamente útil para los proveedores de soluciones KYC, que simplemente pueden importar los datos del archivo .json a su propia base de datos sin más trabajo.

d) EIR de Hong Kong

El Registro mercantil de Hong Kong ya ha digitalizado en gran medida sus sistemas. El registro está abierto a consultas, proporcionando información corporativa general, incluidos los directores de la compañía y los cargos creados junto con los documentos. Dadas estas características, el requisito previo para un sistema de identidad digital corporativa ya está en su lugar. Actualmente, la Oficina del Director de Información del Gobierno (OGCIO) de Hong Kong está trabajando con la Autoridad Monetaria de Hong Kong (HKMA) en pruebas e investigaciones de Proof-ofConcept (PoC) sobre la versión comercial de "iAM Smart", que es una plataforma de identificación digital individual.

El equivalente de UBO en las leyes de Hong Kong se conoce como "controladores significativos". A partir de marzo de 2018, las empresas de Hong Kong deben mantener un registro de controlador significativo (SCR), en el que se registrarán los detalles requeridos (por ejemplo, nombre, fecha de convertirse en un controlador significativo, naturaleza del control sobre la empresa, dirección de correspondencia, número de documento de identidad o número de pasaporte) de cada controlador significativo de la empresa. Si bien la información de UBO está disponible para el Registro de Compañías, el acceso a la información está limitado a los funcionarios encargados de hacer cumplir la ley de diferentes departamentos o agencias gubernamentales. Los bancos y los proveedores de servicios KYC no pueden hacer uso del SCR directamente, y solo pueden inferir las UBO de una empresa utilizando otras piezas de información.

e) Singapur

El registro de empresas de Singapur, que forma parte de la Autoridad Reguladora de Contabilidad y Sociedades (ACRA), proporciona servicios de búsqueda en línea para el perfil comercial de las empresas bajo su registro. Desde diciembre de 2018, la conexión api a la información corporativa ha estado disponible. El servicio API también actualiza la información de propiedad compartida en el registro de ARCA directamente desde el origen para mejorar los plazos y la precisión de los datos. Mientras tanto, la identificación digital se proporciona tanto a individuos como a corporaciones. La identificación digital corporativa, conocida como CorpPass, se lanzó en 2016 y permite a las empresas y otras entidades (por ejemplo, organizaciones sin fines de lucro) realizar transacciones con agencias gubernamentales en línea. Tenga en cuenta que CorpPass no divulga datos sobre UBO, a pesar de que el gobierno está en el proceso de recopilar información sobre UBO, ya que las empresas deben enviar datos al gobierno sobre los accionistas que tienen una propiedad superior al 25%.

4.3 API de integración

La interfaz de programación de aplicaciones (API) es un conjunto de reglas y especificaciones seguidas por programas de software para comunicarse entre sí, y una interfaz entre diferentes programas de software que facilita sus interacciones. Al permitir que una utilidad o programa de usuario comparta datos y solicite servicios de forma segura, las API permiten que el sistema operativo acceda a diferentes sistemas de archivos y servicios. Un ejemplo incluiría la API de Google Maps. La API permite a los desarrolladores incrustar Google Maps en páginas web utilizando una interfaz JavaScript o Flash.

Los registros de empresas con integración de API pueden permitir el intercambio de las credenciales de una empresa, incluidos los detalles sobre accionistas y directores. Esto puede ayudar en la automatización y reducir significativamente el tiempo dedicado a investigar la identidad de un cliente corporativo. Por ejemplo, un registro integrado en api puede permitir que los detalles del director se integren en el sistema de una empresa. De esta manera, una vez que el usuario hace clic en el nombre, puede acceder a detalles adicionales sobre él o ella.

Los registros de empresas con integración de API incluyen los siguientes:

• Singapur: El portal de API de SingPass permite a los desarrolladores acceder a las especificaciones de la API de SingPass y utilizar el espacio aislado para experimentar, crear y probar soluciones de forma rápida y segura.

• Reino Unido: El registro permite a los usuarios registrarse en el Financial Services Register API Developer Portal. Este servicio es actualmente gratuito y permite a los usuarios generar una clave única para acceder a las API de Register, así como proporcionar materiales de soporte de autoayuda.

4.4 Limitaciones y desafíos a los que se enfrentan los registros

Hay una serie de limitaciones y desafíos que enfrentan los registros de empresas existentes:

1. Falta de verificación de datos: Dadas las limitaciones de recursos, generalmente no es factible que un registro de empresas audite y verifique cada dato presentado por las empresas. Además, muchos registros carecen de poder legal para eliminar información inexacta del registro. Como tal, los registros de empresas a menudo limitan su papel a tomar información de las empresas y ponerla a disposición de los buscadores. No obstante, hay espacio para mejorar la inexactitud de los datos a través de la verificación automatizada de las inconsistencias de los datos. Además, los registros pueden proporcionar una mejor conectividad de sus datos con otras fuentes (por ejemplo, las autoridades fiscales) para que los usuarios estén en una mejor posición para verificar los datos.

2. Falta de apertura de datos: Diferentes jurisdicciones han adoptado diferentes políticas con respecto a la accesibilidad de los datos de la empresa al público. Por ejemplo, mientras que los registros de los estados miembros de la Unión Europea deben estar abiertos bajo el 5º y 6º AMLD, muchos otros registros son menos abiertos por diversas razones, como la privacidad de los datos. Como resultado, el acceso a información confidencial sobre los directores y accionistas de una empresa a menudo se limita a ciertos agentes de la ley.

3. Falta de estándares comunes de datos: Es un proceso largo para que varias jurisdicciones definan y acuerden una línea de base común o un umbral básico para que todas las empresas se incluyan en el registro. Las reglas y regulaciones son diferentes para diferentes jurisdicciones, incluidos los umbrales para la propiedad de acciones de UBO, los requisitos fiscales, etc. Esto plantea un desafío para los procedimientos KYC y AML de una empresa que tiene múltiples subsidiarias incorporadas en diferentes jurisdicciones. También plantea un desafío para las soluciones corporativas de ID&V.

4. Costo y recursos: El escalado y la incorporación de datos KYC para registros junto con herramientas para actualizar continuamente los datos con los últimos cambios es una tarea enorme. Requerirá costos y recursos sustanciales de tal manera que el costo total incurrido pueda ser mayor que el resultado tangible que se espera.

5. Tecnología: Como se discutió, el acceso a la API puede ser altamente beneficioso. A falta de esto, la interfaz web regular sin una API también puede traer beneficios. Sin embargo, algunos registros corporativos no están conectados digitalmente en absoluto, de modo que el usuario necesita caminar a la ubicación física de la oficina para acceder a los datos. Es crucial que los registros que entran en esta categoría, sin ninguna digitalización, trabajen para invertir en tecnologías, al menos en una interfaz web.

6. Digitalización insuficiente: Muchos registros de empresas tienen una larga historia y muchos no han digitalizado completamente sus datos, registros, sistemas y procesos.

5. Iniciativas relacionadas con el Banco

En un ecosistema de identificación digital corporativa, los bancos y otras instituciones financieras a menudo se perciben como consumidores de información de identificación corporativa, ya que necesitan dicha información para identificar y verificar a los clientes corporativos, así como para realizar procedimientos para cumplir con los requisitos reglamentarios.

Sin embargo, conceptualmente, los bancos pueden desempeñar un papel más proactivo al servir como proveedores de servicios de identificación digital corporativa, convirtiendo así un centro de costos en un centro de ganancias. La Open Digital Trust Initiative es una iniciativa de este tipo, lanzada conjuntamente por el Instituto de Finanzas Internacionales y la Open ID Foundation.25 La justificación de tal enfoque podría ser múltiple:

• Monetizar la inversión KYC/AML: Con el fin de cumplir con los requisitos regulatorios y llevar a cabo la gestión interna de riesgos, los bancos ya han invertido mucho en los procesos KYC y AML/CFT. Como resultado, han acumulado una cantidad significativa de información sobre sus clientes corporativos. Como dicha información ya se verifica y actualiza regularmente para la debida diligencia del cliente, se puede utilizar fácilmente para proporcionar servicios a terceros.

• Superar la asimetría de la información: un banco solo puede tener una pieza de rompecabezas de datos sobre una entidad comercial, especialmente si la entidad es un grupo empresarial multinacional que abarca múltiples jurisdicciones. Si los bancos pueden agrupar y compartir los datos que poseen, pueden obtener una imagen más completa sobre la entidad comercial y, por lo tanto, reducir el margen de comportamiento malicioso que es posible al explotar las brechas de información entre los bancos.

• Servicio al cliente: Cuando una empresa busca incorporarse a otro banco, en lugar de repetir todo el proceso de KYC, la empresa podría proporcionar una base de consentimiento para obtener información verificada de su banco existente. Este tipo de portabilidad conduciría a una mejor experiencia del cliente.

• Reducir los procesos duplicados: La eficiencia operativa en el proceso KYC se puede mejorar y los costos se pueden reducir a través de la reducción de los procesos duplicados.

Los bancos también podrían colaborar entre sí mediante el establecimiento de una utilidad KYC para proporcionar soluciones de identificación digital corporativa. La primera generación de utilidades KYC compartidas se remonta a Clarient Entity Hub, que se formó en 2014 y se puso en marcha en febrero de 2015. Su objetivo era servir como un repositorio único de datos KYC de uso común de los clientes, que podrían ser utilizados por las instituciones financieras participantes. Fue adquirida por Thomas Reuters en 2017.26 SWIFT también tiene un registro KYC que se fundó en 2014.27 Otro ejemplo es que seis importantes bancos escandinavos lanzaron nordic KYC Utility en 2019, que luego se renombró como Invidem.28 Iniciativas similares en la etapa de PoC se llevaron a cabo en Singapur y Hong Kong, respectivamente.

Ninguno de estos esfuerzos de registro o utilidad de KYC es exhaustivo hasta ahora. A pesar de esto, existe un precedente para que los bancos compartan otros tipos de datos. Por ejemplo, en el contexto de los préstamos, se ha exigido a los bancos (y cada vez más a otros prestamistas) que compartan información crediticia sobre los prestatarios, individuales y corporativos, para prevenir el fraude y también para abordar las asimetrías de información (véase ICCR 2018). En el contexto de los derivados, los datos sobre las transacciones de derivados extrabursátiles deben presentarse a los registros de operaciones miembros del G20 / FSB. Del mismo modo, la información sobre las transacciones financieras que involucran acciones de la compañía es un enfoque central de la regulación financiera, con los registros y custodios de las compañías establecidos para mantener la información central. Finalmente, debido a que los directores de las empresas, los funcionarios responsables y los propietarios son individuos, los sistemas se interrelacionan no solo para la integridad del mercado, sino también para el intercambio de información fiscal, particularmente en el contexto del Estándar Común de Información (CRS) del G20 / OCDE.

De cara al futuro, cada vez más jurisdicciones están considerando cómo maximizar el valor de los datos agregados para la competitividad y el desarrollo, además de los objetivos regulatorios financieros básicos de estabilidad financiera, integridad del mercado, eficiencia, inclusión financiera y protección de clientes e inversores.

5.1 Desafíos de las iniciativas relacionadas con los bancos

Si bien la idea de una utilidad KYC es prometedora en principio, su implementación debe superar numerosos desafíos, incluidos los siguientes.

(a) Costar

El costo de configurar una utilidad KYC es significativo, incluido el costo general de construir la arquitectura de hardware de la computadora y el modelo de gobierno de la plataforma, y los gastos operativos continuos. Para operar con éxito, la empresa de servicios públicos debe lograr ganancias de eficiencia que sean suficientes para justificar estos costos. Un ejemplo revelador es la empresa de servicios públicos KYC de Singapur, que se propuso en 2017 pero se abandonó en 2018 ya que los ahorros esperados no fueron suficientes para cubrir los costos.

b) Procesos operacionales

Dado que los bancos tienen diferentes prácticas y apetito por el riesgo con respecto a sus procesos de KYC, es importante que puedan llegar a un consenso sobre los estándares de datos y el código de prácticas. Este proceso de creación de consenso y armonización de normas podría llevar una cantidad significativa de tiempo, especialmente si los bancos están ubicados en múltiples jurisdicciones y tienen que cumplir requisitos divergentes sobre sus procesos de KYC debido a diferentes regímenes regulatorios.

c) Ciberseguridad

La ciberseguridad es un problema a superar, ya que la utilidad KYC implica el almacenamiento y la transmisión de información corporativa confidencial. Este tema es de particular preocupación, especialmente si la utilidad está operando en un modo centralizado de tal manera que es fácil convertirse en una sola olla de miel para atraer los ataques de los piratas informáticos. El riesgo de un solo punto de falla es otra preocupación que debe abordarse.

d) Responsabilidades jurídicas

La empresa de servicios públicos KYC debe tener un modelo de gobernanza que especifique claramente los pasivos de varias partes. En particular, en caso de error, es crucial saber de antemano si es la empresa de servicios públicos KYC o el banco que confía en esta utilidad debe ser considerado responsable. De acuerdo con la Recomendación 17 del GAFI, los países pueden permitir que las instituciones financieras dependan de terceros para llevar a cabo algunas medidas de CDD si se cumplen ciertos criterios, y la responsabilidad final de las medidas de CDD sigue siendo de las instituciones financieras que dependen de los terceros. La incapacidad de transferir la responsabilidad sigue siendo una de las preocupaciones clave a medida que los bancos deciden si participarían o no en una empresa de servicios públicos KYC. Sin embargo, esto no ha demostrado ser un problema importante en el contexto de los registros de información crediticia, en los que se puede confiar en los datos a efectos de la evaluación crediticia, pero cualquier responsabilidad por cualquier decisión de préstamo recae en el prestamista y el prestatario. Un enfoque similar parecería sólido en el contexto de los posibles registros de datos corporativos: la información debe compartirse, pero la responsabilidad de las conclusiones extraídas sigue siendo de la institución en cuestión. Esto también reflejaría el enfoque de los sistemas de datos de los mercados de capitales, como EDGAR y el PAAS.

e) Privacidad de los datos

La utilidad KYC debe cumplir con las regulaciones con respecto a la privacidad de los datos. Por ejemplo, deben existir procedimientos bien establecidos para garantizar la transparencia de la recopilación y el procesamiento de datos. Además, la transferencia de datos debe estar basada en permisos. Este es un problema que está surgiendo cada vez más y que se está abordando de maneras muy diferentes en las principales jurisdicciones como la UE, China, los Estados Unidos y la India.

f) Dinámica competitiva

Los bancos son los custodios de la información de sus clientes. Esta información es estratégica y competitivamente valiosa. En ausencia de un requisito regulatorio o ahorros claros para el banco (el dilema de "qué hay para mí"), los incentivos para compartir pueden ser bajos. Sin embargo, esto puede cambiar a medida que nuevos competidores ingresan al mercado, ofreciendo nuevas soluciones y una incorporación de clientes sin fricciones, en parte debido a la alta digitalización de dichos procesos. Esto puede mover el objetivo para que los bancos ofrezcan una experiencia de incorporación de clientes más fluida. En la información sobre crédito y mercados de capitales, así como en la información ASG en la UE, esto se aborda a través de requisitos reglamentarios como la forma más adecuada de respaldar los datos como un bien público.

5.2 Registro KYC de SWIFT

La Society for Worldwide Interbank Financial Telecommunications (SWIFT) fue fundada en 1973 cuando 239 bancos de 15 países se agruparon para resolver un problema común sobre cómo comunicar información relativa a los pagos transfronterizos. Estos bancos formaron la empresa cooperativa de servicios públicos conocida como SWIFT, con sede en Bélgica. Su plataforma de mensajería, productos y servicios conectan a más de 11.000 organizaciones bancarias y de valores, infraestructuras de mercado y clientes corporativos en más de 200 países y territorios. También crea los estándares para que los miembros de SWIFT puedan operar de manera más efectiva. Según SWIFT, actualmente hay más de 1,3 millones de relaciones bilaterales de corresponsalía en toda la industria, lo que representa una carga administrativa considerable para los bancos cada vez que se forma una nueva relación o la información necesita actualizarse. Un enfoque comunitario es esencial para acelerar los procesos de cumplimiento y crear nuevas formas de colaboración para abordar los delitos financieros.

Lanzado en 2014, el Registro KYC de SWIFT se ha convertido en el estándar del sector para la diligencia debida de la banca corresponsal, permitiendo a más de 6.500 bancos optimizar sus procesos de cumplimiento de KYC. Y, tras un despliegue en las empresas conectadas a SWIFT en diciembre de 2019, el registro también ayuda a simplificar este proceso entre bancos y empresas.

KYC Registry es una plataforma global que permite a sus instituciones miembros intercambiar de forma segura información de diligencia debida verificada por SWIFT entre sí. Se basa en un conjunto estandarizado de información para los procesos de KYC, acordado en colaboración con bancos de todo el mundo. Por ejemplo, el cuestionario predefinido presenta preguntas relacionadas con ALD / CFT, incluido el último Cuestionario de Diligencia Debida de Banca Corresponsal del Grupo Wolfsberg, y evidencia documental para validar los datos que proporcionan los usuarios.

La línea de base del registro cubre una parte significativa de los requisitos globales de KYC, que contiene información de KYC tanto privada como públicamente disponible. Esta estandarización puede respaldar el proceso de diligencia debida y permite a los usuarios centrarse en un trabajo de mayor valor agregado, especialmente cuando se trata de múltiples solicitudes de datos. Para que el proveedor de datos conserve el control de los datos, el acceso al perfil KYC por parte de terceros se realiza con un permiso. Tanto los proveedores de datos KYC como los usuarios son voluntarios. Ninguno de ellos paga por los datos ni recibe recompensas por proporcionar los datos. El registro también habilita una conexión API.

5.3 Open Digital Trust Initiative y servicios relacionados

La Open Digital Trust Initiative (ODTI) es una iniciativa conjunta del Institute of the International Finance (IIF) y la Open ID Foundation. El objetivo de la iniciativa es crear una solución de verificación de identidad multipropósito proporcionada por los bancos bajo un estándar global común de código abierto que pueda usarse en los sectores público y privado. En septiembre de 2021, anunció un paradigma de identidad centrado en el usuario y de alta confianza conocido como Global Assured Identity Network (GAIN), que se espera que se lance en 2022. La idea básica de GAIN es aprovechar las inversiones bancarias existentes en KYC y autenticación multifactor, así como el papel de los bancos como protector confiable de los datos y la privacidad de los clientes. Conceptualmente, esto ayudará a los clientes a confiar unos en otros en línea sin comprometer la privacidad. Inicialmente, los servicios cubren eKYC y soluciones de inicio de sesión subcontratadas.

En los países nórdicos, BankID ofrece un tipo similar de servicio. La persona promedio en los países nórdicos usa BankID 198 veces al año. Las verificaciones de identidad cuestan entre 0,10 € y 1,00 € por llamada a la API exitosa. Existen oportunidades de ingresos adicionales para los productos de seguros asociados. La ODTI intenta implementar un concepto similar en una región más amplia, con miras a que eventualmente se practicaría a nivel mundial. Al mismo tiempo, busca crear un estándar gratuito de código abierto que pueda usarse para crear un mercado genuinamente competitivo para los servicios de confianza digital. Para impulsar el estándar, el equipo de ODTI se asoció con el IIF para alentar a otros bancos a considerar la prestación de servicios similares.

En el ecosistema de identificación digital de la ODTI, hay cuatro partes principales:

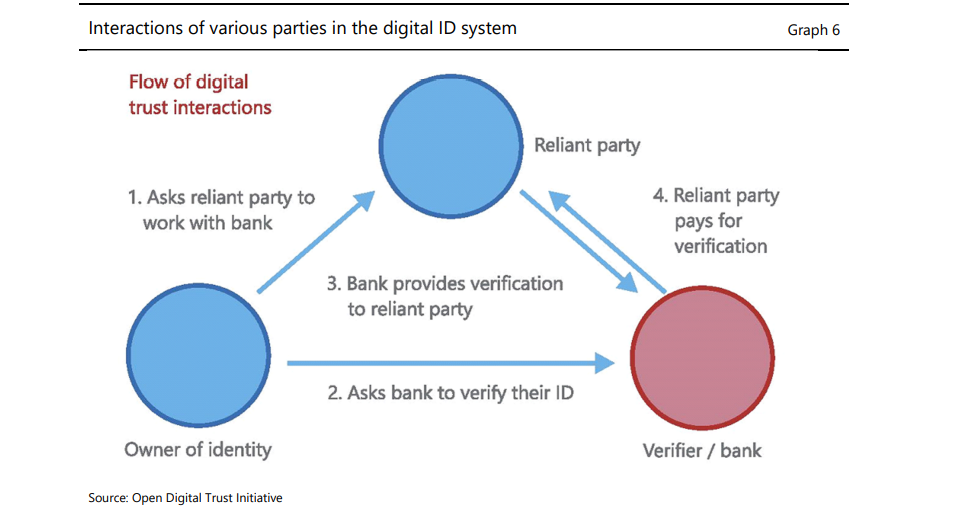
Bancos: Relación de confianza propia con sus clientes

Partes de confianza: Compre servicios de autenticación e-KYC y por sesión

Agregadores: Intermediarios para conectar a miles de partes de confianza con cientos de bancos. La clave para ser un agregador exitoso es hacer que sea muy fácil para los desarrolladores acceder a su red.

Proveedores de tecnología: Como este es un estándar de código abierto, hay muchas opciones para que los proveedores de tecnología participen.

Los flujos de interacciones se muestran esquemáticamente en el Gráfico 6. Primero, el propietario de la identidad (por ejemplo, una empresa) le pide a la parte que confía (por ejemplo, una compañía de seguros) que trabaje con el banco. En segundo lugar, el propietario de la identidad le pide al banco que verifique su identidad. En tercer lugar, el banco proporciona verificación a la parte que confía. Finalmente, la parte que confía paga una tarifa de servicio al banco para su verificación.



6. Proveedores establecidos y soluciones regtech

Tradicionalmente, una serie de proveedores establecidos han desempeñado un papel en id&V corporativo. Recientemente, una gama de empresas de regtech han comenzado a proporcionar soluciones para la identidad digital corporativa. Si bien las soluciones proporcionadas por estas empresas independientes no pueden sustituir a un sistema de identificación completo, pueden facilitar la realización de algunos aspectos de la diligencia debida del cliente. Los clientes de estas firmas de regtech suelen ser bancos y otras instituciones financieras reguladas que deben identificar y verificar a sus clientes antes de la incorporación, que suele ser el primer paso para KYC, AML / CFT y otros procedimientos de diligencia debida o control de riesgos. Más recientemente, los clientes de las empresas de regtech se extienden a las empresas e individuos que son sujetos a ser identificados, ya que la tecnología (por ejemplo, billeteras digitales portátiles, identidad autosoberana) está permitiendo cada vez más a estas empresas e individuos compartir sus datos de identidad verificados con usuarios de terceros de manera confiable y sobre una base de consentimiento.

Hay fortalezas y debilidades de las empresas emergentes de regtech en el suministro de soluciones de identificación digital corporativa. En primer lugar, estas empresas suelen tener una historia corta, y algunas de ellas son nuevas empresas fundadas en los últimos cinco años. En términos de recursos, están muy por detrás de los proveedores de datos bien establecidos y los bancos que ya han invertido significativamente en la adquisición y verificación de datos corporativos. La fortaleza de las empresas de regtech radica principalmente en el uso innovador de tecnología como la inteligencia artificial (IA), el aprendizaje automático, el procesamiento del lenguaje natural (NPL), el reconocimiento óptico de caracteres (OCR) y la cadena de bloques para resolver los puntos débiles en el proceso de identificación y verificación corporativa. Como son relativamente nuevos, no están gravados por sistemas de TI heredados que a menudo dificultan la adopción de nuevas tecnologías. Su pequeño tamaño también significa que son más ágiles y flexibles que las organizaciones bien establecidas para adaptarse a los últimos cambios tecnológicos.

Para comprender las propuestas de valor de las empresas de regtech, es útil comprender el flujo de trabajo del proceso KYC para identificar los puntos débiles en cada paso y cómo las soluciones tecnológicas podrían agregar valor. Sobre la base de entrevistas a estas empresas emergentes de regtech, sus flujos de trabajo se pueden resumir ampliamente en los siguientes cuatro pasos:

1. Recuperar datos de la empresa

• Ya sea a través del acceso directo a los registros oficiales y las cámaras de compensación gubernamentales o a través de API a los agregadores de datos y otros intermediarios

• El acceso debe ser en tiempo real, automático y con marca de tiempo

2. Extraiga y limpie los datos KYC relevantes

• La tecnología de PNL y OCR se utilizan para digerir documentos KYC y llevar a cabo la limpieza y mejora de datos

• Se destacan los puntos de datos clave y las personas de interés

3. Identificar a los beneficiarios finales (UBO)

• Se identifican las UBO y se destacan las conexiones con las empresas / accionistas

• Cálculo de la participación total en la propiedad y control de gestión de los individuos

• Visualización y analítica de gráficos

• Acceso a registros UBO compartidos

4. Realizar comprobaciones AML/KYC en individuos

• Personas políticamente expuestas (PEP), noticias negativas y herramientas de detección de sanciones

• Monitoreo automatizado posterior a la transacción y continuo con capacidades de bandera roja

• Análisis de redes para identificar partes relacionadas y UBO.

6.1 ¿Cómo pueden ayudar las soluciones regtech?

a) Conectividad de datos

Uno de los puntos débiles en la identificación y verificación de una empresa es que la información requerida está dispersa en múltiples fuentes, en algunos casos ubicadas en diferentes jurisdicciones. Incluso si un usuario de datos de identidad puede acceder a todas estas fuentes de información, se necesitaría mucho trabajo para recopilar y agregar la información requerida.

Con el fin de resolver los puntos débiles de la recopilación de información de múltiples fuentes, algunas empresas de regtech ofrecen soluciones para mejorar la conectividad de datos. Por ejemplo, Chekk, una empresa de regtech con sede en Hong Kong establecida en 2016, ofrece conectividad a fuentes de datos empresariales que cubren más de 350 millones de empresas en 200 países de todo el mundo. Estos datos empresariales provienen de una variedad de fuentes, como registros corporativos y proveedores de datos de terceros. Los usuarios de la plataforma Chekk pueden acceder a estos datos a través de una variedad de canales (por ejemplo, computadoras de escritorio, tabletas, teléfonos móviles). Junto con la conectividad de datos, también hace uso de varias tecnologías (por ejemplo, conexiones API, AI, NLP, OCR) para el acceso y análisis de datos.

Otro ejemplo es kompany, una firma de regtech con sede en Austria establecida en 2012 y adquirida por Moody's en 2022. Ofrece a sus clientes conexiones API en tiempo real a más de 200 registros comerciales, autoridades financieras y oficinas fiscales de todo el mundo para que sus clientes puedan acceder a datos y documentos originales de más de 115 millones de empresas. Mientras tanto, también se proporcionan servicios de valor agregado que incluyen monitoreo y alerta de cambios (PERPETUAL KYB), identificación fiscal y verificación de IBAN, y servicios de traducción de documentos.

En el contexto de los mercados de capitales y la información crediticia, los beneficios de la centralización han dado lugar al desarrollo de sistemas y procesos de normalización. El PAAS de la UE proporciona un ejemplo de cómo esto podría extenderse también a los datos ESG, que sufren muchos de los mismos problemas que los datos KYC.

b) Digestión de los documentos de la empresa

Con la adopción de las tecnologías digitales, los documentos de las empresas están cada vez más disponibles en formato electrónico. A diferencia de los documentos tradicionales en papel, estos documentos electrónicos son mucho más fáciles de almacenar, recuperar y transferir. No obstante, todavía se requiere una cantidad significativa de trabajo manual para leer estos documentos y extraer información relevante, ya que los datos contenidos en estos documentos electrónicos no están en un formato bien estructurado y consistente, lo que significa que no son fácilmente legibles por máquina. En este sentido, las firmas regtech han ofrecido soluciones innovadoras para reducir la carga de la lectura de estos documentos. Por ejemplo, la empresa belga complidata proporciona herramientas tecnológicas como OCR y PNL para digerir documentos de la empresa y extraer información útil. También ofrece soluciones para los controles de noticias negativas y sanciones de forma automatizada. En otros contextos, los requisitos de informes regulatorios digitales se están desarrollando rápidamente, ofreciendo el potencial de legibilidad de la máquina.

c) Descubrimiento de UBO

La identificación de la titularidad real se ha convertido cada vez más en un requisito reglamentario obligatorio para las instituciones financieras en muchas jurisdicciones, pero dicha información a menudo no está directamente disponible para el público en general. Aunque varios registros de empresas han exigido a las empresas en virtud de su registro que presenten información de UBO y proporcionen actualizaciones de dicha información de forma regular, a menudo solo se puede acceder a dicha información para determinados funcionarios encargados de hacer cumplir la ley.

En ausencia de información de primera mano proporcionada por fuentes autorizadas, muchas empresas de regtech ofrecen soluciones para identificar el UBO de una empresa. Por ejemplo, kompany hace uso de datos de fuentes primarias de registros gubernamentales y proporciona herramientas habilitadas para IA para descubrir las estructuras de propiedad transfronteriza de entidades legales de todo el mundo para que se puedan descubrir las UBO de una empresa multinacional. El resultado del análisis es fácil de usar, ya que se puede presentar visualmente en árboles de propiedad que son intuitivos de entender y fácilmente exportables.

d) Portabilidad de los datos

Desde el punto de vista de los sujetos a ser identificados y verificados, el punto de dolor es principalmente recopilar cantidades masivas de documentos para probar su identidad. Algunos de estos documentos aún pueden estar en forma de papel y se requiere una reunión cara a cara para verificar su autenticidad. Este tedioso proceso se repite cada vez que una empresa inicia una relación con un nuevo banco, proveedor u otro proveedor de servicios, introduciendo costes sustanciales. La portabilidad de datos del propietario de la identificación proporciona una solución eficiente para resolver este punto débil y potencialmente la transición a una interacción remota para la incorporación y el monitoreo. Por ejemplo, Chekk proporciona portabilidad de datos mediante una billetera digital que está encriptada de forma segura. Una empresa y sus representantes (por ejemplo, CEO, directores, accionistas principales) pueden almacenar sus datos de identidad en esta billetera. Sobre una base de consentimiento, el propietario de la billetera puede compartir cualquier parte de los datos con un banco u otros usuarios externos. Los usuarios pueden confiar en que estos datos son auténticos porque son verificados por una serie de fuentes de datos oficiales. Además, el uso de la tecnología también garantiza que los datos no puedan ser manipulados una vez que se verifican. Tenga en cuenta que el cifrado de datos es de extremo a extremo, de modo que incluso Chekk no puede ver los datos de sus clientes.

6.2 El ejemplo de ZOLOZ

Un ejemplo particularmente ilustrativo es la solución ZOLOZ eKYB en Asia. La solución incluye tres pilares: verificación empresarial (RealBID), verificación individual (RealID) y predicción de riesgos.

(a) Verificación de negocios

La verificación comercial de RealBID comienza a partir de documentos de registro, como certificados de registro comercial y estados de cuenta bancarios corporativos. Las imágenes de estos documentos son enviadas por los clientes en formato digital y luego se ejecutan a través de algoritmos OCR y antifalsificación para llegar a una puntuación de confianza de autenticidad. Si una PYME no puede proporcionar todos los documentos de registro, se utilizarán fuentes de datos alternativas. Por ejemplo, las empresas envían fotografías y direcciones de sus lugares operativos y / o las URL de sus sitios web. La IA junto con la supervisión humana derivará una puntuación de confianza.

b) Verificación de la identidad individual

El objetivo de RealID es verificar la identidad de las personas que actúan en nombre de una empresa, como sus directores, supervisores y altos directivos. Al igual que otras soluciones de identificación digital individuales disponibles comercialmente, RealID requiere que cada una de estas personas capture una imagen de documento de identificación y una imagen de selfie. Luego se realiza una verificación de calidad de primer nivel sobre estas imágenes.31 Después de que el individuo pasa esta verificación, ZOLOZ verifica la autenticidad de la identificación basada en algoritmos de IA. El siguiente paso es una verificación de la vitalidad para determinar si el individuo presentado es una persona viva. La tecnología de vida de ZOLOZ está certificada bajo la certificación ISO30107-3 nivel 2, lo que significa que la solución de vida de ZOLOZ es lo suficientemente robusta como para identificar la impresión facial, la reproducción de video (incluido el deepfake), así como los ataques de suplantación de máscara facial 3D. Como todo el proceso está completamente digitalizado, el tiempo de respuesta es de segundos.

c) Predicción del riesgo

RealID realiza una comparación cruzada en todos los documentos presentados para detectar si hay casos de falsificación de rostros (diferentes caras que aparecen en el ID con los mismos detalles), falsificación de detalles de ID (diferentes detalles aparecen en el ID con la misma cara), así como múltiples clientes que usan el mismo ID. Al mapear la relación de las empresas e ingerir actualizaciones de los proveedores de fuentes de datos, RealBID otorga una calificación de riesgo en la incorporación de clientes, elevando alertas cuando es necesario. Por ejemplo, cuando se marca a cualquier director, supervisor o alta gerencia de un cliente, todas las entidades relacionadas y sus respectivas entidades relacionadas de segundo grado también están sujetas a banderas de riesgo.

Al combinar una identificación individual y una solución de verificación empresarial, ZOLOZ persigue la incorporación digitalizada de pymes, apoyando la inclusión financiera de las pymes.

7. Iniciativas de identificación digital del sector público

El sector público tiene un papel importante que desempeñar en el apoyo a la identificación digital corporativa, sobre todo a través de su papel central en la habilitación de la creación de personas jurídicas y, en muchos casos, la extensión de la identificación digital individual. Además, muchas iniciativas gubernamentales apoyan explícitamente la inclusión financiera de las PYME. De hecho, los obstáculos para que las PYME accedan a la financiación están bien documentados. Según el Banco Asiático de Desarrollo (BAD), por ejemplo, las PYME representan sólo el 23 por ciento de la demanda de financiación del comercio, pero el 40 por ciento de los rechazos de la financiación del comercio. Su dificultad para acceder a la financiación del comercio es un factor clave para la brecha de financiación del comercio mundial que se disparó a un máximo histórico de 1,7 billones de dólares (o el 10% de los bienes comercializados a nivel mundial) en 2020, ya que la pandemia de Covid-19 asestó un golpe devastador a la economía mundial.

Uno de los principales obstáculos para que las PYME accedan a los servicios financieros es el costo prohibitivamente alto incurrido en el proceso de ID&V, que es obligatorio para todas las empresas reguladas por AML, como las instituciones financieras, las empresas dedicadas al comercio internacional y la mayoría de las empresas B2B. Este proceso está en marcha para disuadir el lavado de dinero, el fraude, el financiamiento del terrorismo y otras actividades delictivas. KYC / KYB generalmente implica dos pasos clave: primero, verificar el certificado de registro de la empresa, la licencia comercial y otros documentos relevantes para garantizar que el negocio sea real; segundo, identificar al beneficiario final (UBO), donde se realiza KYC para estas personas. Sobre la base de estos pasos clave, los procesos de diligencia debida del cliente llevan a cabo una investigación más amplia de las finanzas y el historial de las empresas y sus propietarios, tanto para el negocio (evaluación de crédito, gestión de riesgos, prevención del fraude) como para los requisitos reglamentarios (en particular, AML y también cada vez más protección de datos).

En esta sección final, discutimos iniciativas mediante las cuales el gobierno toma la iniciativa para proporcionar la infraestructura digital fundamental y el marco de intercambio de datos como un bien público para la identificación de empresas y / o individuos, aunque la participación de proveedores de servicios del sector privado no está excluida. Un ejemplo digno de mención es el sistema de identidad digital Aadhaar de la India, junto con su marco de gobierno de datos conocido como agregadores de cuentas. Por lo tanto, discutimos este y otros ejemplos seleccionados.

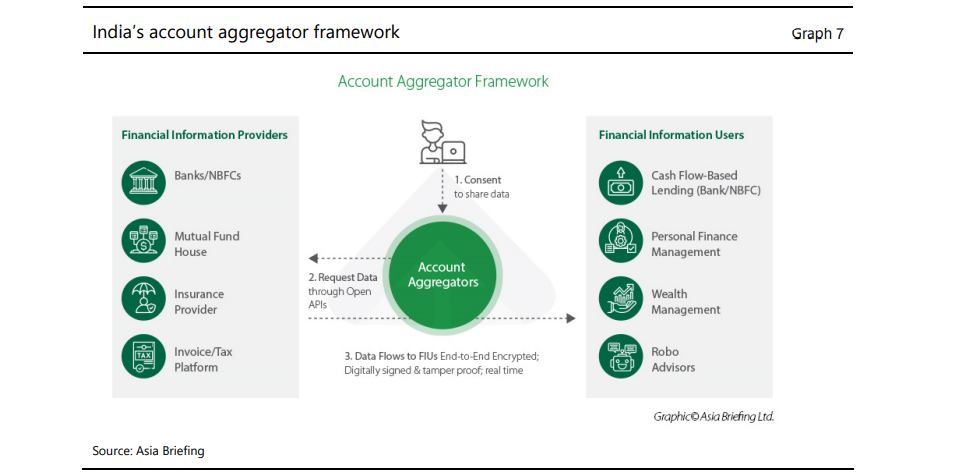
7.1 Aadhaar de la India, agregadores de cuentas e ID digital corporativo

El principio subyacente del enfoque de agregación de datos es que las personas y las PYME deben cosechar los beneficios de los datos generados por sus actividades comerciales. Estos datos no deben ser arrinconados por el estado o cualquier empresa del sector privado en "jardines amurallados" de datos, con los propietarios originales de los datos excluidos de los beneficios generados. Aplicando este principio a los servicios bancarios y financieros, esto significa que las personas y las PYME deberían poder hacer uso de sus propios datos para obtener un mejor acceso a estos servicios. Por ejemplo, las PYME deben poder proporcionar estos datos a los bancos para que su riesgo de crédito pueda evaluarse adecuadamente. Con el fin de poner en práctica este principio, la India introduce intermediarios de datos conocidos como agregadores de cuentas que facilitan la agregación y el intercambio de datos. Muchas jurisdicciones requieren el intercambio de información crediticia, tanto para reducir el fraude, el riesgo de crédito y las asimetrías de información, como para permitir prácticas crediticias más efectivas para apoyar la inclusión financiera y los objetivos de desarrollo más amplios.

El ecosistema de agregadores de cuentas se basa en la base de Aadhaar, que es un número de identificación de 12 dígitos emitido por la Autoridad de Identificación Única de la India. Lanzado en 2009, Aadhaar se ha desarrollado rápidamente en poco más de una década. A finales de octubre de 2021, 1.260 millones de indios (92,6% de la población total) ya tenían un Aadhaar.33 El rápido crecimiento en su tasa de adopción refleja los méritos del sistema, como el requisito mínimo de información, el bajo costo por identificación y varias características para proteger la privacidad de los datos. Por ejemplo, un solicitante de un número Aadhaar solo necesita proporcionar cuatro piezas de información, a saber, su nombre, fecha de nacimiento, sexo y dirección residencial. Las instituciones financieras pueden usar una API de eKYC para acceder a los detalles de Aadhaar para su verificación. Los estudios han encontrado que el sistema Aadhaar condujo a un aumento significativo de las cuentas bancarias y una reducción significativa en la exclusión de los grupos marginados, como las personas de bajos ingresos y las de las zonas rurales.

El marco del agregador de cuentas fue anunciado por el Banco de la Reserva de la India (RBI) en 2016 y entró en funcionamiento en septiembre de 2021. Los participantes clave del sistema consisten en agregadores de cuentas, proveedores de información financiera (FIP) y usuarios de información financiera (UIF) (Gráfico 7). Los agregadores de cuentas son intermediarios de datos registrados como empresas financieras no bancarias con el RBI. Su función es garantizar que la agregación y el intercambio de datos financieros procedan de manera segura, transparente y eficiente. Específicamente, recuperan o recopilan datos sobre los activos financieros de un cliente de los FIP y luego los agregan, consolidan y presentan a las UIF. La transferencia de datos está condicionada a un consentimiento explícito de los FIP. Una característica importante es que estos intermediarios de datos son ciegos a estos datos. Una vez aprobados, los datos fluyen directamente entre los FIP y las UIF de forma cifrada, y los agregadores de cuentas son incapaces de leer o almacenar los datos para su uso posterior. Además, las cuentas de agregador de cuentas son portátiles para que las personas puedan cambiar libremente sus agregadores de cuentas. También pueden restringir el consentimiento en términos de tiempo y categorías de datos, y revocarlo en cualquier momento. En las primeras 30 semanas desde que se puso en marcha, se procesaron 230.000 solicitudes de consentimiento de las UIF, o alrededor de 1000 por día. En el 90-95% de los casos, los FIP han abordado con éxito las solicitudes de consentimiento con un tiempo de respuesta promedio en segundos.

Aquí hay un ejemplo de cómo el marco del agregador de cuentas puede promover la inclusión financiera. Una PYME que busca un préstamo encuentra que sus datos financieros residen en múltiples instituciones, y es difícil para la PYME consolidar y compartir los datos con el prestamista. Bajo este marco, la PYME puede exigir que una lista de información (por ejemplo, declaraciones de impuestos, datos de cuentas bancarias, pagos de préstamos hipotecarios) se comparta con el prestamista (por ejemplo, un banco) con la intermediación de un agregador de cuentas. En comparación con los métodos convencionales de recopilación de información de múltiples fuentes, muchas de las cuales todavía se basan en papel, esto es mucho más eficiente. Esto también permite el uso de datos basados en el flujo de efectivo para procesar la solicitud de préstamo, a diferencia de los préstamos tradicionales basados en activos garantizados por garantías físicas como la propiedad. Para una PYME pobre en activos, a menudo es más factible demostrar su solvencia mediante pruebas basadas en el flujo de efectivo que prometiendo garantías para garantizar un préstamo. Además, dicha evidencia suele ser más actualizada y dinámica y, por lo tanto, más relevante para su salud financiera y un mejor insumo para el proceso de aprobación del préstamo.



7.2 Otras iniciativas del sector público

El sector público desempeña un papel en varias otras áreas importantes que apoyan la identificación digital corporativa. Por ejemplo, los reguladores y los responsables políticos tienen un papel clave en la coordinación de los procesos existentes relacionados con el intercambio de información fiscal y la divulgación de beneficiarios reales (coordinados por la OCDE), ALD / CFT (coordinados por el GAFI), derivados OTC e infraestructura financiera (coordinados por el FSB, CPMI e IOSCO) y otros como los mercados de capitales y los datos ESG (coordinados por IOSCO y el ISSB). En esta última subsección, examinamos algunas iniciativas relevantes del sector público.

MyInfo de Singapur

MyInfo proporciona un ejemplo útil de un sistema híbrido en el contexto de la identidad digital individual. Cuenta con una identificación digital soberana en la base, que luego se vincula a una gama de otros datos de fuentes doradas del gobierno y otras fuentes que se pueden compartir a través del sistema bajo el control del individuo. Esto, a su vez, puede apoyar la ID&V de las empresas. A través de la API de MyInfo Business, las empresas pueden consultar fácilmente datos y verificar características de empresas individuales en Singapur.

Países Bajos eHerkenning

En los Países Bajos, además de la plataforma de identificación digital para individuos (DigiD), el gobierno ofrece a las empresas un sistema de inicio de sesión estandarizado para acceder a más de 500 proveedores de servicios del sector público y privado. El sistema eHerkenning ("reconocimiento electrónico") ofrece cuatro niveles sucesivos de garantía, en función de las necesidades del caso de uso en cuestión. A partir de 2020, contaba con más de 600,000 empresas y 17 millones de autenticaciones exitosas. A principios de 2022, agregó funciones adicionales en torno a la autorización de la cadena.

Objetivos de Desarrollo Sostenible (ODS) de las Naciones Unidas

Los esfuerzos de política internacional también reconocen el vínculo entre la identificación individual y corporativa. A nivel mundial, se estima que 1.000 millones de personas carecen de credenciales de identificación formales. Reflejando la importancia de la identificación para la inclusión y el desarrollo, la identidad jurídica para todos se ha incluido como una de las metas de los ODS. Como se muestra en los ejemplos de países discutidos anteriormente, esto también puede apoyar la identificación digital corporativa para las PYME en particular.

ID4D

En apoyo de los ODS, el Banco Mundial lanzó su iniciativa identificación para el desarrollo (ID4D) en 2016. Como parte de este proceso, la iniciativa ha desarrollado Principios sobre Identificación para el Desarrollo Sostenible que comprenden 10 principios, abordando temas como la confianza, la seguridad, la interoperabilidad, la privacidad, la tecnología y la gobernanza. Si bien los Principios se centran en la identificación individual, los principios generales son también las preocupaciones centrales de la identificación digital corporativa. Además de los principios, la iniciativa coordina una variedad de organizaciones, proporciona asistencia y ha desarrollado una serie de estudios de casos y normas técnicas basadas en las experiencias de los países de todo el mundo.

8. Conclusión

La identificación digital corporativa puede acelerar significativamente la identificación y verificación de una empresa, lo que permite a sus contrapartes, como bancos y proveedores, gestionar los riesgos comerciales y cumplir con los requisitos reglamentarios de manera más eficiente. Como resultado, una empresa puede construir relaciones comerciales con estas contrapartes mucho más rápidamente con la identificación digital corporativa. Además, la identificación digital facilita el establecimiento de confianza, ya que la tecnología permite que los datos corporativos se verifiquen más fácilmente y se transmitan a los usuarios de manera más segura. Más allá de la eficiencia operativa o la experiencia del usuario, una identificación digital corporativa bien establecida también es un facilitador crucial para promover la inclusión financiera y salvaguardar la estabilidad financiera y la integridad del mercado.

En muchos sentidos, la identificación digital corporativa es paralela a la identificación digital individual, pero hay diferencias importantes. A diferencia de un individuo, los atributos de una corporación (por ejemplo, directores) pueden cambiar con mucha más frecuencia y, por lo tanto, requieren una actualización oportuna. Una corporación puede ser parte de una estructura corporativa complicada, con partes de ella ubicadas en múltiples jurisdicciones, lo que hace que sea un desafío identificar su propiedad real como lo requieren algunas regulaciones. Por lo tanto, la identificación digital corporativa no es una mera extensión de la identificación corporativa individual. Dicho esto, la identificación digital individual es un complemento muy significativo de la identificación digital corporativa, debido a la necesidad de identificar y verificar las identidades de las personas que dicen representar a la corporación.

Con el uso innovador de la tecnología y las políticas apropiadas, este estudio encuentra que una variedad de partes interesadas, incluidos los registros corporativos, los bancos y otras instituciones financieras, los proveedores y proveedores de servicios establecidos, las empresas de regtech y las autoridades públicas pueden lograr un progreso importante en la identificación digital corporativa. Algunas iniciativas son fundamentales, como el IPJ, que sirve como identificador global para conectar múltiples redes, cada una de las cuales puede aportar atributos importantes a un ID digital corporativo. El estándar de identificadores descentralizados (DID) puede ayudar a agregar información de diferentes fuentes. Mientras tanto, algunas soluciones están más hechas a medida para sectores específicos. Por ejemplo, las soluciones de identificación digital para pymes utilizan datos alternativos en lugar de documentos más oficiales que no están disponibles para algunas pymes. Como enfoque complementario, el sector público puede aspirar a construir nuevas infraestructuras, potencialmente basándose en la identificación individual proporcionada públicamente. Cada una de estas partes interesadas tiene su propia fortaleza en términos de recursos, sofisticación tecnológica y confianza por parte del público, pero también sus propios desafíos que superar.

Sobre la base de lo que sabemos hoy y podemos prever razonablemente en el futuro cercano, no hay una bala de plata que pueda lograr todos los beneficios potenciales a la vez, ni una sola parte interesada puede impulsar todos los cambios necesarios. Muchas partes interesadas están involucradas. Tampoco la solución es de naturaleza puramente tecnológica. La voluntad política es necesaria para impulsar el cambio y lograr los efectos de red necesarios. Los factores no tecnológicos, como los estándares de datos comunes, los modelos de gobierno y la aclaración de las incertidumbres legales o regulatorias, también son importantes para hacer realidad las promesas de la identificación digital corporativa. El lado positivo es que, trabajando juntas, estas partes interesadas tienen el potencial de abordar los principales puntos débiles de la ID&V corporativa.

Referencias

Arner, D (2002), "Development of the American law of corporations to 1832", 55 SMU Law Review, no. 23, pp 23-57.

Arner, D, G Castellano y E Selga (2022), "Financial data governance", European Banking Institute Working Paper no. 117, marzo.

Arner, D, D Zetzsche, R Buckley y J Barberis (2019), "The Identity Challenge in Finance: From Analogue Identity to Digitized Identification to Digital KYC Utilities", European Business Organization Law Review, 20, 55–80.

Banco Asiático de Desarrollo (BAD) (2021), "2021 trade finance gaps, growth and jobs survey", ADB Brief, núm. 192, octubre.

Auer, R, C Monnet y HS Shin (2021), "Distributed ledgers and the governance of money", BIS Working Papers, No. 924.

Comité de Supervisión Bancaria de Basilea (BCBS) (2012), Principios básicos de Basilea.

D'Silva, D, Z Filková, F Packer y S Tiwari (2019), "The design of digital financial infrastructure: lessons from India", BIS Papers, No. 106.

Grupo de Acción Financiera Internacional (GAFI) (2012), Normas Internacionales sobre la Lucha contra el Lavado de Dinero y el Financiamiento del Terrorismo y la Proliferación, París.

GAFI (2020), "Guidance on Digital Identity", París. GAFI (2021a), Oportunidades y desafíos de las nuevas tecnologías para ALD/CFT, París

GAFI (2021b), Revisiones a la Recomendación 24 y su Nota Interpretativa – Consulta Pública, París.

GAFI (2021c), Guía actualizada para un enfoque basado en el riesgo para los activos virtuales y los proveedores de servicios de activos virtuales, París.

Finck, M (2018), Blockchain Regulation and Governance in Europe, Cambridge: Cambridge University Press.

Garber, E, M Haine, V Knobloch, G Liebbrandt, T Lodderstedt, D Lycklama y N Sakimura (2021), GAIN DIGITAL TRUST: How Financial Institutions are taking a leadership role in the Digital Economy by establishing a Global Assured Identity Network, European Identity and Cloud Conference, Munich, septiembre.

Gartner (2022), "Gartner Hype Cycle", consultado el 1 de febrero.

Global Legal Entity Identifier Foundation (GLEIF) (2021a), «How can the LEI contribute to the technical implementation of the global minimum corporate tax rate and relocation of tax benefits of large multinational corporations (MNCs)?", Documento de Trabajo de la GLEIF.

GLEIF (2021b), "Introducing the Legal Entity Identifier (LEI)".

GLEIF (2021c), «Introducción del IPJ verificable (vLEI)».

Greif, A (1993), "Contract enforceability and economic institutions in early trade: the Maghribi traders' coalition", American Economic Review, Vol 83, No. 3, pp 525–48.

Instituto de Finanzas Internacionales (IIF) (2020), Identidades digitales en los servicios financieros - Parte 3: La oportunidad de negocio para la identidad digital.

Comité Internacional de Informes de Crédito (ICCR) (2018), Uso de datos alternativos para mejorar los informes de crédito para permitir el acceso a los servicios financieros digitales por parte de individuos y pymes que operan en la economía informal, Nota de orientación.

Organización Internacional del Trabajo (ISO) (2019), Small Matters: Global evidence on the contribution to employment by the self-employed, micro-enterprises and SMEs.

Landa, J (1994), Trust, ethnicity and identity: the new institutional economics of ethnic trading networks, contract law and gift-exchange, Ann Arbor: University of Michigan Press.

Mickelthwait, J & Woodbridge, A (2003), The Company: A Short History of Revolutionary Idea, Random House.

McKinsey Global Institute (2019), Identificación digital: una clave para el crecimiento inclusivo.

Autoridad Monetaria de Singapur (2021), Foundational Digital Infrastructures for Inclusive Digital Economies.

Murphy, H (2020), "SEC steps in after investors buy up the wrong Zoom", Financial Times, marzo.

Grupo de Trabajo sobre Firmas Electrónicas del Centro Nacional de Cooperación Económica de Asia y el Pacífico (NCAPEC) (2022), Advancing Digital Transactions in APEC: Enhancing e-signatures and digital signatures.

Rice, T, G von Peter y C Boar (2020), "On the global retreat of correspondent banks", BIS Quarterly Review, marzo.

Tiwari, S; Sharma, S; Shetty,S y Packer,F (2022), "The design of a data governance system", BIS Papers, No 124, 05 de mayo de 2022.

Society for Worldwide Interbank Financial Telecommunication (SWIFT) y EuroFinance (2019), Resolviendo el enigma de KYC.

Banco Mundial (2018), Panorama tecnológico para la identificación digital

Foro Económico Mundial (WEF) (2018), Identity in a Digital World - A new chapter in the social contract, septiembre.

WEF (2016), A Blueprint for Digital Identity – The Role of Financial Institutions in Building Digital Identity, agosto.