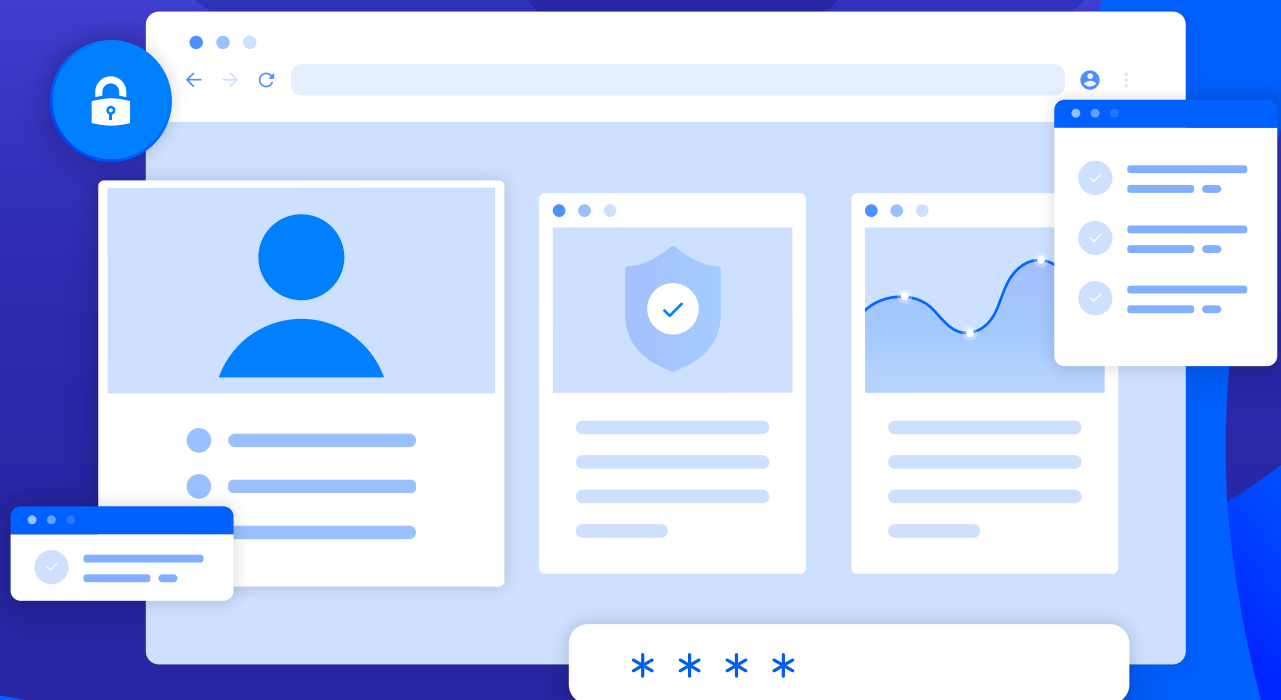


Onboarding digital

Creado por

**Iván Nabalón, Diego Herrera
y Sonia Vadillo**



Clasificaciones JEL: E42, G2, K2

Palabras clave: inclusión financiera, regulación financiera, abordaje digital, *onboarding* digital, identidad digital, Fintech, América Latina, Caribe, supervisión financiera

Copyright © 2021 Banco Interamericano de Desarrollo. Esta obra se encuentra sujeta a una licencia Creative Commons IGO 3.0 Reconocimiento-NoComercial-SinObrasDerivadas (CC-IGO 3.0 BY-NC-ND) (<http://creativecommons.org/licenses/by-nc-nd/3.0/igo/legal-code>) y puede ser reproducida para cualquier uso no-comercial otorgando el reconocimiento respectivo al BID. No se permiten obras derivadas.

Cualquier disputa relacionada con el uso de las obras del BID que no pueda resolverse amistosamente se someterá a arbitraje de conformidad con las reglas de la CNUDMI (UNCITRAL). El uso del nombre del BID para cualquier fin distinto al reconocimiento respectivo y el uso del logotipo del BID no están autorizados por esta licencia CC-IGO y requieren de un acuerdo de licencia adicional.

Nótese que el enlace URL incluye términos y condiciones adicionales de esta licencia.

Las opiniones expresadas en esta publicación son de los autores y no necesariamente reflejan el punto de vista del Banco Interamericano de Desarrollo, de su Directorio Ejecutivo ni de los países que representa.



Inter-American Development Bank
1300 New York Avenue, N.W.
Washington, D.C. 20577
www.iadb.org

El Sector de Instituciones para el Desarrollo fue responsable de la producción de la publicación.

Colaboradores externos:

Coordinación de la producción editorial: Sarah Schineller (A&S Information Partners, LLC)
Revisión editorial: Sol Dellepiane y Julia Gomila
Diagramación: Gabriel Ramírez

Índice

	Resumen Ejecutivo	1
1.	Introducción	2
2.	Objetivos del estudio	5
3.	Modelos de identidad digital que necesitan de <i>onboarding</i> digital	7
4.	Definición de <i>onboarding</i> digital	13
5.	Análisis de la regulación existente y situación actual del <i>onboarding</i> digital	21
6.	Experiencias en <i>onboarding</i> digital	26
7.	Beneficios del <i>onboarding</i> digital	33
8.	Marco jurídico	36
9.	Recomendaciones para que los reguladores implementen el <i>onboarding</i> digital en sus jurisdicciones	39
10.	Visión desde el campo ofrecida por los expertos	48
11.	Conclusiones y recomendaciones de política pública	52

Siglas y abreviaturas

ABD	American Business Dialogue
AFI	Alianza Fintech Iberoamérica
ALC	América Latina y el Caribe
AML	<i>Anti-Money Laundering</i>
APIs	<i>Application Program Interfaces</i>
BACEN	Banco Central de Brasil
BaFIN	Federal Financial Supervisory Authority
BCP	Banco Central de Paraguay
BCU	Banco Central de Uruguay
BID	Banco Interamericano de Desarrollo
BPR	Bien público regional
CAC	Costo de adquisición del cliente
CDD	Diligencia debida de cliente (por sus siglas en inglés, <i>Customer Due Diligence</i>)
CMF	Comisión para el Mercado Financiero de Chile
CNBS	Comisión Nacional de Bancos y Seguros de Honduras
CNBV	Comisión Nacional Bancaria y de Valores de México
CNV	Comisión Nacional de Valores de Argentina
COAF	Consejo de Control de Actividades Financieras
COVID-19	Sars Coronavirus mutación 19
DLT	<i>Distributed Ledger Technology</i>
EORI	<i>Economic Operator Registration and Identification Number</i>
FAFT	Financial Action Task Force
FCA	Financial Conduct Authority
FELABAN	Federación Latinoamericana de Bancos
FIAB	Federación Iberoamericana de Bolsas
FINMA	Swiss Financial Market Supervisory Authority
FinTech	Tecnología financiera
FSA	Japan Financial Services Agency
FSC	Financial Services Commission
FT	Financiación del terrorismo (por sus siglas en inglés, <i>Counter Financing of Terrorism</i>)

GAFI	Grupo de Acción Financiera Internacional
HKMA	Hong Kong Monetary Authority
IA	Inteligencia artificial
IDS	Identidad digital soberana
INTERPOL	Organización Internacional de Policía Criminal
KYB	<i>Know Your Business</i>
KYC	Conoce a tu cliente (por sus siglas en inglés, <i>Know Your Customer</i>)
LEI	<i>Legal Entity Identifier</i>
MAS	Monetary Authority of Singapore
MRZ	<i>Machine Readable Zone</i>
NIST	National Institute of Standards and Technology
OD	<i>Onboarding</i> digital
PBCFT	Prevención de blanqueo de capitales y financiación del terrorismo
PEP	Persona políticamente expuesta (por sus siglas en inglés, <i>Politically Exposed Person</i>)
PSCC	Prestadores de servicios de confianza cualificados
SBIF	Superintendencia de Bancos e Instituciones Financieras de Chile
SBPR	Secretaría de Bien Público Regional
SENACLAFT	Secretaría Nacional para la Lucha contra el Lavado de Activos y el Financiamiento del Terrorismo de Uruguay
SEPBLAC	Servicio ejecutivo de la Comisión de Prevención de Blanqueo de Capitales e Infracciones Monetarias de España
SEPRELAD	Secretaría de Prevención de Lavado de Dinero o Bienes de Paraguay
SIC	<i>Standard Industrial Classification Number</i>
SPID	Sistema público para la identidad digital
SSI	<i>Self Sovereign Identity</i>
UAF	Unidad de Análisis Financiero de Panamá
UIAF	Unidad de Información y Análisis Financiero de Argentina
UIF	Unidad de Inteligencia Financiera de Colombia
URF	Unidad de Regulación Financiera de Colombia

Prólogo

Jorge Castaño Gutiérrez

Presidente de la Secretaría Técnica FintechLAC.

Abril de 2019 - Mayo de 2021.

Dice un viejo proverbio que **“la oportunidad llama, pero una vez”**; en otras palabras, no deben desaprovecharse las situaciones fortuitas para afianzar los objetivos deseados. Como respuesta al sonado refrán, Milton Berle, actor y comediante estadounidense, propuso allá por los años cincuenta: **“si la oportunidad no llama, construye una puerta”**.

Esperamos que la pandemia de COVID-19 sea justamente eso: una oportunidad sin precedente para transformar el sistema financiero y desentrañar el potencial de una acelerada adopción digital que mejore las condiciones de la población más vulnerable por medio de los pagos electrónicos, el crédito digital y la canalización de ayuda del gobierno, entre otros.

A pesar de su impacto negativo sobre el crecimiento económico, los indicadores de pobreza y desempleo, algunas cifras de la era pospandemia nos muestran un panorama más alentador de cara a la anhelada reactivación de las economías de la región. De acuerdo con un estudio reciente de Minsait (2020), la acelerada adopción digital ha conducido a una reducción en el uso del efectivo en la región de América Latina y el Caribe, destacando su caída como principal medio de pago² entre 2018 y 2020 en países como Colombia (de 60% a 36%), Argentina (de 50% a 30%) e incluso Brasil (de 39% a 12%), que ya contaba con una alta penetración de pagos digitales antes de la llegada de la COVID-19. También se destaca la población que reporta un mayor uso de billeteras electrónicas (65% en Argentina y Perú) y de transferencias y pagos a cuentas (71% en Colombia y 67% en Chile). Asimismo, el documento revela la preponderancia del canal digital para el comercio electrónico, lo que aumenta la frecuencia de compras realizadas en línea (más de 50% de los encuestados en la región reporta al menos una compra por mes en 2020, en comparación con 43% el año anterior).

Pero mal haríamos, como responsables de las políticas, en delegar en un evento imprevisto de tal magnitud como ha sido la pandemia el logro de los objetivos deseados en materia de inclusión financiera, empoderamiento de los consumidores y sostenibilidad del sistema; **como sociedad, debemos también construir esa puerta.**

---

² Porcentaje promedio, según instrumento de pago, con el que se realiza la mayor parte de los gastos del hogar.

El *onboarding* digital (o “abordaje digital”) es precisamente esa puerta de entrada hacia el sistema financiero; una política pública transformadora que, apalancada sobre las nuevas tecnologías y las soluciones innovadoras, facilita la identificación de un consumidor financiero de forma remota, con seguridad, agilidad, e incluso a un menor costo que el mecanismo presencial.

Este estudio, oportunamente encomendado por el BID, identifica el *onboarding* digital como un marco de confianza determinante para impulsar al sistema financiero en su transformación digital y subsanar deficiencias de sistemas anteriores en materia de usabilidad, interoperabilidad y acceso. Tal como señalan los autores, los procesos de identificación, verificación y autenticación —basados en tecnología y de forma remota— generan eficiencias, favorecen la inclusión financiera, permiten un acceso abierto e incrementan la conveniencia para sus usuarios.

¿Alguna vez se han cuestionado cómo abrir o cerrar una puerta? Prácticamente cualquier persona, en casi cualquier latitud, intuitivamente sabe cómo ingresar a un recinto. Por razones de **seguridad** (por ejemplo, contra incendio), estas cierran hacia afuera; por cuestiones de **usabilidad**, abren hacia adentro (permitiendo así una calurosa bienvenida a los invitados); algunas incluso abren de forma automática e inclusiva, permitiendo la **accesibilidad** de la población discapacitada. También la tecnología ha revolucionado el diseño de puertas de acceso, con sistemas automatizados de apertura, mecanismos de identificación biométrica y aplicación de sistemas sin contacto (*contactless*) para garantizar estándares de bioseguridad, un aspecto particularmente relevante en la actual coyuntura.

Por último, la puerta del *onboarding* digital es apenas un elemento que debe tenerse en cuenta en la construcción de un ecosistema financiero inclusivo, confiable y sostenible. Aún tenemos por delante un inmenso desafío para asegurarnos de que quienes acceden al sistema permanezcan y prosperen allí dentro: la educación financiera digital quizás sea esa “llave en mano” para ingresar con paso firme.

Prólogo

Juan Antonio Ketterer

**Jefe de División de Conectividad, Mercados y Finanzas
Banco Interamericano de Desarrollo**

Es indudable que las sociedades del mundo entero han avanzado de forma extraordinaria hacia un proceso de digitalización que afecta a todos los sectores económicos. La situación excepcional derivada de la pandemia de COVID-19 ha acelerado este proceso, poniendo de relieve las fortalezas y también las carencias desde el punto de vista económico y social. En el ámbito financiero, tanto las entidades del sistema financiero tradicional como los nuevos operadores, tales como las plataformas Fintech o las denominadas Bigtech, han venido creando nuevos productos basados en el uso de tecnologías, y habilitando canales digitales que permiten realizar pagos o compras en línea, cobrar los subsidios del Estado, tener acceso a crédito, seguros, cuentas bancarias y otros servicios financieros. Según el informe del BID y Finnovista (BID y Finnovista, 2019), en el año 2019 fueron identificados en América Latina y el Caribe (ALC) 2.301 emprendimientos Fintech, que utilizan tecnologías diversas como móviles y aplicaciones (21%), big data y analítica (19%), interfaces de programación de aplicaciones, plataformas abiertas (17%), computación en la nube (8,6%), aprendizaje automatizado o inteligencia artificial (IA) (8,1%).

Con una [penetración móvil cercana al 100%](#) y una penetración de *smartphones* del 45% en ALC, la utilización de canales y productos financieros digitales, accesibles desde un terminal móvil, puede convertirse en una herramienta clave para avanzar en la inclusión financiera de la región y permitir el acceso al sistema financiero de sectores alejados de las grandes poblaciones, o tradicionalmente excluidos y con dificultades de acceso a financiamiento como las pequeñas y medianas empresas o los colectivos de mujeres. Si bien los países de la región han venido respondiendo con medidas como la habilitación de canales digitales para pagos de transferencias del gobierno o la autorización de la apertura simplificada de cuentas de forma remota, aún existen importantes barreras para la completa digitalización del sector financiero. El abordaje u *onboarding* de un cliente, entendido como el proceso electrónico que permite su identificación frente a una institución financiera y con una confianza equivalente a la de un proceso presencial, es un aspecto clave para avanzar en la digitalización y en la inclusión financiera, por cuanto se convierte en la puerta de entrada de los consumidores al sistema financiero.

De acuerdo con el GAFI¹, el uso de sistemas de identidad digital independientes y confiables podría facilitar la identificación y verificación en el *onboarding* del cliente y contribuir a la inclusión financiera, habilitando a personas que no han accedido a servicios a probar su identidad oficial en un rango amplio de circunstancias y reforzar la lucha en la prevención de blanqueo de capitales y financiamiento del terrorismo (PBCFT).

Desde el Banco Interamericano de Desarrollo (BID) hemos venido apoyando la inclusión financiera y el desarrollo de un ecosistema regional Fintech a través de diversas iniciativas, como la red [FintechLAC](#). Esta es la primera red público-privada de Fintech en ALC, conformada por reguladores y supervisores financieros así como por asociaciones de Fintech de 16 países. FintechLAC se ha constituido en una herramienta para el ecosistema de la inclusión financiera digital a través del apoyo decidido a los gobiernos en la creación de políticas públicas enfocadas en la digitalización de los servicios financieros. Esta publicación es el fruto de esos esfuerzos y pretende ser una herramienta que facilite a los gobiernos y responsables de políticas la adopción de medidas que permitan avanzar en la digitalización del sistema financiero. Aún existen importantes barreras legales, culturales, tecnológicas, de coordinación entre autoridades o de adopción, entre otras, así como riesgos de ciberseguridad y de confiabilidad de las tecnologías o sistemas empleados. Sin embargo, los beneficios son incuestionables. Desde la política pública los gobiernos pueden promover iniciativas de coordinación interinstitucional, medidas legales o reglamentarias que habiliten la utilización de métodos alternativos de identificación de clientes, el impulso de innovaciones regulatorias a través de *sandboxes* regulatorios, la promoción de estándares de interoperabilidad o la cooperación internacional que permita compartir experiencias, mejores prácticas y analizar de forma conjunta los riesgos y oportunidades asociados al uso de nuevas tecnologías. Es el momento de que los países de ALC aprovechen el impulso de las medidas adoptadas en respuesta a la pandemia y avancen de forma decidida hacia una estrategia de digitalización que permita el desarrollo de sistemas financieros robustos, modernos e inclusivos.

---

¹ <https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Guidance-on-Digital-Identity-Executive-Summary.pdf>.

Prólogo

Erick Rincón Cárdenas

Presidente de Alianza Fintech Iberoamérica.

Mayo de 2020 – Mayo de 2021.

Los autores han elaborado un texto que aborda el tema del *onboarding* digital con idoneidad y que brinda los conocimientos para que un lector mínimamente familiarizado pueda comprenderlos de manera fácil, así como reconocer la importancia de este tema en el ecosistema Fintech. Los principales cambios expuestos en el texto son la demanda creciente de la digitalización de los servicios como resultado de la pandemia de COVID-19, las modificaciones en la industria y la necesidad de revitalizar la economía considerando el papel determinante de la inclusión financiera.

En los últimos años, la industria Fintech se ha consolidado como una importante herramienta de bancarización dentro de la región de América Latina y el Caribe (ALC). Sin embargo, queda un largo camino por recorrer para incrementar la facilidad en el acceso a estos servicios, otorgando a su vez seguridad y confianza tanto a las empresas prestadoras como a los usuarios. Así, buscando mejorar la totalidad de la experiencia Fintech en la región al igual que su avance, el *onboarding* digital se presenta como un camino para la identificación de los consumidores financieros; es decir, una vía que otorga la seguridad tradicionalmente reconocida al sector, sumada a las facilidades de los procesos electrónicos.

Ante este panorama, el presente estudio describe el contexto del *onboarding* digital en ALC y expone sus beneficios y herramientas de aplicación, para luego ocuparse de manera sumamente clara e ilustrativa de recomendaciones puntuales que los organismos reguladores pueden tener en cuenta al momento de profundizar en la materia. En este mismo sentido, el texto presenta la principal normativa de los países que han desarrollado el *onboarding* digital, lo cual abre el camino para profundizar en su análisis y obtener un panorama general de su desarrollo que permita un estudio de aplicación en la región.

El texto se encarga de abordar diferentes modelos de identidad digital que se han implementado a fin de conocer los avances generados, el contexto y los aspectos clave que deben tenerse en cuenta para su evolución.

Así, con un enfoque práctico y ajustado al panorama actual, el texto permite contar con elementos que apuntan al avance de la inclusión financiera en el contexto regional mediante facilidades de acceso en virtud de la identificación de los consumidores. Esto no solo representa ventajas en relación con la inclusión misma, sino también respecto del "conoce a tu cliente" (KYC, por sus siglas en inglés, *Know Your Customer*), facilitando garantías de transparencia.

El estudio reviste gran relevancia para el entorno Fintech, estableciendo aspectos que deben tomar en cuenta no solo la comunidad académica sino principalmente los encargados de la regulación en cada Estado y las empresas del sector. Se trata de un aporte de gran utilidad en épocas como la actual, donde la situación impone la necesidad de ampliar los procesos de virtualidad.

Resumen ejecutivo

Este documento describe los retos para la apertura remota de cuentas que impiden el acceso a servicios financieros digitales, y recomendaciones para superarlos. El proceso de digitalización de los servicios financieros se ha consolidado inesperadamente con la evolución de la pandemia global provocada por el Covid-19. Los cambios en las preferencias de los consumidores, la emergencia de plataformas Fintech, la adopción de tecnologías por parte de instituciones financieras tradicionales, entre otros factores, han llevado al sector financiero a ofrecer más servicios y productos digitales. Pese a esta rápida evolución, la inclusión financiera digital no se ha aumentado tanto como se hubiera supuesto por las dificultades con el “onboarding” digital, definido como el proceso electrónico que permite la identificación de un consumidor financiero frente a una institución financiera y cuyo resultado genera una confianza equivalente a un proceso presencial. Para que sea efectivo, requiere de una confianza equivalente a la que ofrecen los canales presenciales. Es decir, a la identificación realizada históricamente por parte de las instituciones financieras en las oficinas comerciales. Este texto identifica los retos para poder llevar a cabo el proceso, incluyendo aquellos relacionados con la identidad digital, los procesos para la prevención del lavado de activos y financiación del terrorismo, las tecnologías existentes, entre otros. También ofrece alternativas para la puesta en marcha de procesos de *onboarding* digital, y ofrece recomendaciones a reguladores y hacedores de política en la región.

1. Introducción

Como parte de la iniciativa FintechLAC³ se elabora el presente estudio general para conocer y analizar la situación actual sobre *onboarding* digital⁴ en América Latina y Caribe (ALC). Asimismo, se pretende brindar recomendaciones de política pública a los organismos reguladores y supervisores de la región para su implementación.

En este estudio se entenderá que el *onboarding* digital es el proceso que permite identificar al cliente y realizar los procesos de “conoce tu cliente” (KYC, por sus siglas en inglés, *Know Your Customer*) de forma remota y por el canal digital.

El proceso de *onboarding* del cliente, que está en vías de ser digitalizado (de ahí el nombre del proyecto), ha sido y continuará siendo clave en la industria bancaria y financiera. Su importancia radica en varios aspectos: i) es clave para comenzar una relación de mutuo beneficio donde la confianza en las partes intervinientes es primordial; ii) busca evitar el riesgo de fraude, y iii) permite prevenir delitos derivados del blanqueo de dinero y de financiación del terrorismo.

Entre muchos factores, existen tres que impulsan de forma determinante la digitalización del proceso:



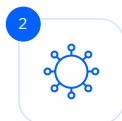
Una demanda creciente de la sociedad.

La necesidad del *onboarding* digital deriva de un contexto de digitalización inexorable de la economía. Con el paso del tiempo, la sociedad se ha ido adaptando, cada vez más, a un estilo de vida digital. Esta realidad demanda mayor inmediatez en el consumo de los servicios, y los servicios bancarios y financieros no son ajenos a este cambio. También demandan cada vez mayor conveniencia: hoy en día el proceso de identificación del cliente se sigue realizando en las oficinas comerciales de los bancos o prestadores de servicios financieros. Este desplazamiento es inconveniente dado su costo y tiempo en el canal presencial. En algunos casos también es complejo, dadas las circunstancias de poca accesibilidad de las personas o la lejanía, por ejemplo, en entornos rurales, donde no existe presencia física de los bancos o prestadores de servicios financieros.

³ <https://www.iadb.org/es/sectores/iniciativas/digital-finance-innovation/fintech>.

⁴ Dependiendo de la jurisdicción, el *onboarding* digital también se denomina “vinculación digital” o “abordaje digital”. Se ha optado por utilizar el término original en inglés dado que es el tecnicismo más utilizado.

La crisis sanitaria y económica de la COVID-19 ha puesto de manifiesto la necesidad de digitalizar determinados procesos y en especial la contratación a distancia en el sector, lo que podría impulsar de forma determinante esta demanda creciente de la sociedad. Según algunas referencias, como la de un artículo de la BBC (Millán, 2020), la necesidad en muchos países de tener una cuenta bancaria para acceder a ayuda gubernamental destinada a mitigar los daños económicos de la pandemia y la reducción de la circulación de dinero en efectivo impulsa el uso de soluciones financieras por el canal digital. Este podría ser uno de los principales impulsores que pueden hacer que América Latina —que posee un nivel de bancarización del 55% de acuerdo con un informe de la Alianza por la Inclusión Financiera (AFI, por sus siglas en inglés)— pueda progresar y alcanzar el nivel de regiones más maduras en este sentido, como Europa, con un 95% de bancarización.



Los cambios que está viviendo la industria.

La industria bancaria y financiera está sufriendo probablemente el mayor cambio de su historia. Las nuevas tecnologías impulsadas por internet, las nuevas formas de comercio electrónico y la movilidad, entre otros, hacen que las estructuras y el modelo de distribución actuales hayan quedado prácticamente obsoletos y requieran de una transformación profunda. Esta transformación no se realizará tanto en el qué se ofrece como servicio sino en el cómo se ofrece y distribuye, o en el cuándo relativo al momento de su consumo. Por otra parte, son muchos los actores nuevos que están desafiando el *statu quo* de los actores tradicionales en la industria bancaria y financiera, desde los líderes del comercio electrónico, las empresas de base tecnológica financiera (Fintech), las grandes tecnológicas (Bigtech), e incluso los operadores de telecomunicaciones o la industria del entretenimiento. Todos estos actores ven, de una forma u otra, una extensión de su negocio natural, y gracias a las nuevas tecnologías e internet se han dado cuenta de que es posible ofrecer este tipo de servicios. En consecuencia, podrían presionar al sector más tradicional y potencialmente disminuir la cuota de mercado en muchos segmentos que antes desarrollaban los bancos o los prestadores de servicios financieros. Todas estas circunstancias podrían poner en entredicho los modelos de negocio y distribución actuales basados en la presencia física; y ponen el foco en la transformación y el desarrollo de nuevas oportunidades comerciales en los canales digitales, como complemento de los canales presenciales.



La necesidad de revitalizar la economía allí donde la inclusión financiera será un factor determinante.

Sin excepción, todos los países incluidos en la región están de una forma u otra fomentando la economía digital y la inclusión financiera, con el objetivo de crear nuevas oportunidades de desarrollo económico y social en el futuro a corto plazo. El estudio “The Global Findex Database” editado por el Banco Mundial (Demirgüç-Kunt *et al.*, 2017) resalta que la región aún tiene un nivel de inclusión financiera bajo, si se la compara con otras regiones del mundo. En ALC solo 53% de los adultos (personas mayores de 15 años) manifiesta tener un servicio contratado en un banco o institución financiera. Por su parte, en la región, el 52% de los adultos sin una cuenta manifestó que tener una era demasiado caro. Sin embargo, el 95% de las personas encuestadas en la región manifestó contar con un documento de identidad y más de dos tercios cuenta con un teléfono celular. Esta realidad allana el camino para la digitalización del proceso de *onboarding* digital.

Así, se considera que el proceso de *onboarding* digital será clave en la superación de los grandes desafíos económicos y sociales antes mencionados. Las políticas públicas podrían llegar en un momento idóneo por el contexto social, político y económico de la región.

El principal objetivo de este informe es brindar apoyo a los reguladores y supervisores financieros en forma de recomendaciones de regulación y políticas para la implementación del *onboarding* digital.

El informe se estructura tal como se describe a continuación. Luego de este primer capítulo introductorio, el capítulo 2 contiene los objetivos del estudio, mientras que el capítulo 3 expone modelos de identidad que necesitan de *onboarding* digital. El capítulo 4 incluye la definición de *onboarding* digital. Por su parte, en el capítulo 5 se analizan la regulación existente y la situación actual del *onboarding* digital en el ámbito regional e internacional. Los capítulos 6 y 7 exponen, respectivamente, las experiencias y los beneficios del *onboarding* digital. El marco jurídico se describe en el capítulo 8, mientras que en el capítulo 9 se ofrecen recomendaciones de implementación del *onboarding* digital. El capítulo 10 presenta la visión de los expertos en este campo. Finalmente, el capítulo 11 ofrece conclusiones y una serie de recomendaciones de política pública para la implementación del *onboarding* digital en la región.

2. Objetivos del estudio

El objetivo general del estudio es explicar en detalle los fundamentos del *onboarding* digital en el contexto de América Latina y el Caribe (ALC). El objetivo particular es brindar recomendaciones de política pública a las entidades encargadas de la regulación y supervisión del sistema financiero que tengan facultades relacionadas con el *onboarding* digital en el sector financiero. Basándonos en los objetivos anteriores, se pretende impulsar la implementación del *onboarding* digital de la siguiente forma:



Segura, según los estándares internacionales.



Amplia, ya que afecta a todos los sujetos obligados que operan en el sector financiero definidos por el Grupo de Acción Financiera Internacional (GAFI).



Sin limitaciones en los montos económicos de las transacciones.



Universal, mediante una solución disponible y accesible para la gran mayoría de la población y las instituciones bancarias y financieras.

Alcance del estudio

Se centra en el *onboarding* digital de ciudadanos de ALC como clientes finales o como representantes de entidades legales. Aplica a entidades reguladas identificadas por el Grupo de Acción Financiera Internacional (GAFI), principalmente bancos, entidades bancarias de crédito, aseguradoras y prestadores de servicios financieros en mercados de capitales (en adelante Bancos o Prestadores de Servicios Financieros). Todas están obligadas a cumplir con regulación en el ámbito de la prevención de blanqueo de capitales y financiación del terrorismo (PBCFT) a la hora de identificar y realizar la diligencia debida de los clientes.

Principio de neutralidad tecnológica

Aunque el estudio describe algunas de las nuevas tecnologías existentes, así como requerimientos técnicos específicos del proceso de identificación del cliente extraídos de las regulaciones y buenas prácticas internacionales, se mantiene neutral en este sentido. Se entiende esta neutralidad como la libertad de las organizaciones de elegir la tecnología más apropiada y adecuada a sus necesidades dentro de requerimientos generales marcados por las administraciones que garantizarán la seguridad y el correcto desarrollo de la adopción de nuevas tecnologías.

3. Modelos de identidad digital que necesitan de *onboarding* digital

Debido a la necesidad de proporcionar un alto índice de confianza en la identidad de las personas al inicio de la relación, el *onboarding* digital es un proceso clave y obligatorio para el desarrollo de cualquier modelo de identidad digital, ya sea por parte de los Estados o de entidades privadas.

Este apartado describe los distintos modelos que se vienen desarrollando a nivel internacional en industrias reguladas, como por ejemplo en el sector financiero. Por su nivel de seguridad, los modelos de identidad digital que se describen en este apartado tienen en común el conferir una seguridad técnica y jurídica equivalente a las relaciones presenciales.

La importancia de la identidad legal expedida por los Estados en los modelos de identidad digital de industrias reguladas

En relación con la identidad de las personas, sean ciudadanos o representantes legales de empresas, las identidades expedidas y gestionadas por los Estados en forma de datos y atributos que se encuentran en los documentos de identidad, pasaportes, datos fiscales, laborales, etc. suelen ser la fuente más auténtica y fidedigna a la hora de responder quiénes somos. Esto ayuda a crear un entorno confiable para realizar transacciones, ya sean de carácter público o privado. Esta identidad de carácter legal ha marcado históricamente las bases para construir la confianza en las sociedades modernas y lo seguirá haciendo⁵ en la evolución digital de las mismas.

Esta identidad legal, sin restar importancia a otro tipo de información que arroje conocimiento y confianza sobre los ciudadanos, sigue siendo la piedra angular en la que se han construido las sociedades modernas. Hoy se viaja, se pagan impuestos, se accede a un sistema de salud y de educación, se tiene una relación laboral o se puede contratar un producto bancario o financiero en gran medida sobre la base de dicha identidad de carácter legal que gestionan los Estados. Como se verá más adelante, los documentos de identidad o pasaportes son la fuente principal de información fiable en los procesos de *onboarding* a la hora de determinar la identidad de las personas y comenzar cualquier modelo de identidad digital de una forma segura y confiable.

⁵ Se señalan dos estudios que pueden resultar de interés para el lector si desea ampliar esta información. El primero, un estudio editado por McKinsey Global Institute titulado "Digital Identification: A key to inclusive growth", que declara que los países emergentes pueden desbloquear hasta un 13,6% del valor de su producto interno bruto (PIB) gracias a la identidad digital (abril de 2019); y el segundo, editado por el Instituto de Empresa y su iniciativa de tecnologías gubernamentales (GovTech), PublicTech Lab, titulado "Identidad Digital: desbloqueando un efecto multiplicador del PIB en España" (septiembre de 2020).

La aparición de nuevas tecnologías tales como firma digital, *Big Data*, tecnologías biométricas, inteligencia artificial (IA) o *Blockchain*, sumadas a la creciente toma de consciencia de los ciudadanos acerca de la importancia de su privacidad –cada vez más en riesgo debido al uso de los datos por parte de organizaciones privadas y los Estados– está planteando un debate profundo e interesante en torno a los distintos modelos de identidad, así como una evolución importante de los modelos digitales. Tales modelos incluyen la nueva generación de servicios de firma digital o la aparición de otros en los que los Estados no son los únicos participantes garantes de la seguridad (por ejemplo, están los proyectos de identidad digital soberana sobre redes descentralizadas). Asimismo, como se verá más adelante, el *onboarding* digital descrito como un proceso en el que se digitaliza la verificación de la identidad del cliente para constatar que es la persona que reclama ser será de especial relevancia y común para todos estos modelos, ya que a través de él debe asegurarse que la transformación de la identidad analógica se convierta en digital de una forma segura y confiable.

Firma digital: modelo digital centralizado gestionado por los Estados

Este es un modelo que se da típicamente en sociedades que basan su modelo jurídico en el Derecho Romano, principalmente en regiones como América Latina y el Caribe (ALC) o Europa. El planteamiento de este modelo, basado en regulaciones de finales de los años noventa⁶, fue la búsqueda de un *alter ego* digital, que es el equivalente electrónico de los modelos de identidad analógica legal que tenían su base en los documentos de identidad o pasaportes expedidos por los Estados.

Estos sistemas se desarrollan a través de la firma digital, donde un documento electrónico (certificado electrónico de persona física o legal) es gestionado de forma segura a través de criptografía asimétrica⁷, para que el ciudadano tenga exclusivo control del uso de su identidad digital, típicamente para identificarse o para expresar su voluntad en contrataciones a través de la firma de documentos.

Este modelo, desarrollado desde finales de los años noventa y posteriormente en la primera década del siglo XXI, ha sido un modelo fracasado y con una penetración muy baja en la sociedad y en la economía digital. El principal motivo de este fracaso proviene de la falta de usabilidad de las soluciones técnicas por parte de los ciudadanos. Esto hizo que se abandonaran o no se trataran con suficiente atención cuestiones relevantes como las descritas a continuación.

⁶ Directiva 1999/93/CE del Parlamento Europeo y del Consejo del 13 de diciembre de 1999, por la cual se establece un marco comunitario para la firma electrónica.

⁷ Definición de criptografía asimétrica:

[https://es.wikipedia.org/wiki/Criptograf%C3%ADa_asim%C3%A9trica#:~:text=La%20criptograf%C3%ADa%20asim%C3%A9trica%20\(en%20ingl%C3%A9s,para%20el%20env%C3%ADo%20de%20mensajes.](https://es.wikipedia.org/wiki/Criptograf%C3%ADa_asim%C3%A9trica#:~:text=La%20criptograf%C3%ADa%20asim%C3%A9trica%20(en%20ingl%C3%A9s,para%20el%20env%C3%ADo%20de%20mensajes.)

Falta de usabilidad

La instalación de certificados electrónicos de personas físicas (firmas digitales) en las computadoras es extremadamente compleja para los ciudadanos comunes, que deben lidiar con la instalación de certificados en los navegadores o con tarjetas criptográficas, sus *drivers*, etc. Al mismo tiempo, las firmas digitales no eran portables: solo funcionaban en el dispositivo donde se instalaban y no funcionaban en los dispositivos móviles.

Falta de interoperabilidad

La falta de interoperabilidad ha sido un obstáculo importante debido a la complejidad para integrarse en aplicaciones de negocio como las de la banca electrónica. Existen también dificultades en su reconocimiento legal transfronterizo.

Falta de accesibilidad

La expedición y renovación de la firma digital requiere de la personación previa del ciudadano para una correcta verificación de la identidad. Esto implica una paradoja importante en el modelo: se trata de un instrumento digital que necesita del mundo analógico y a la vez este es el principal obstáculo para su aplicación en la mayoría de los casos que, por el contrario, requieren de un uso digital práctico e instantáneo.

No obstante, gracias a las lecciones aprendidas durante más de una década en este tipo de proyectos, el modelo de identidad digital basado en la firma digital atraviesa un renacimiento desde que se expidió el reglamento eIDAS (910/2014) en Europa (European Union, 2017)⁸. Este reglamento, en vigor en Europa desde el 1.º de julio de 2016 y cuyo modelo está siendo también fuente de inspiración en la región, propone algunos cambios interesantes que darán una nueva oportunidad al modelo. Propone una nueva generación de servicios de confianza electrónica y firma digital más fáciles de usar, portables, interoperables y accesibles que los de la primera generación. Los cambios son:

- Para una mayor usabilidad de las soluciones, la nueva regulación y las normas técnicas se deshacen del certificado descentralizado (tarjetas criptográficas o instalado en los computadores) y permiten un modelo centralizado que es interoperable y fácil de usar por parte de los ciudadanos.
- Para una mejor interoperabilidad, son más abiertos a la posibilidad de que entidades privadas puedan prestar servicios relacionados con la confianza electrónica. Aunque esto ya existía en las regulaciones anteriores, la computación en la nube y otros avances tecnológicos como la IA permiten abrir esta industria a un terreno de libre competencia y por lo tanto más adecuado para construir la interoperabilidad; a la vez, facilitan la implantación en otras industrias, más allá de las relaciones gubernamentales.

⁸ <https://ec.europa.eu/futurium/en/content/eidas-regulation-regulation-eu-ndeg9102014>.

- Introducen mejoras para el tratamiento de personas físicas (ciudadanos), pero también legales (empresas).
- Para una mayor accesibilidad, mejoran la expedición y renovación de la identidad digital y son precisamente los mecanismos de *onboarding* digital tratados en este estudio, en el que el sector financiero ha sido pionero. Esto permite la gestión de una identidad digital fuerte como es esta, concentrada en el canal digital y además sencilla y práctica para los ciudadanos.
- Introducen mejoras en la interoperabilidad entre Estados e industrias ya que, dado el marco de referencia de la seguridad, la identidad digital se extrapola para que las identidades digitales se puedan utilizar de forma transfronteriza y en cualquier industria que requiera de este nivel de seguridad.

En Europa, por ejemplo, la regulación eIDAS se ha configurado como el estándar para la Identidad Digital Europea, produciendo una armonización en esta materia comparable a lo que se hizo con el euro en relación a la armonización de la moneda en la región a finales del siglo XX. Esta regulación está creando el concepto de un Mercado Único Digital transfronterizo con potencial para homogeneizar los servicios en una región que, de forma agregada, es la segunda economía a nivel mundial, con alrededor de 500 millones de ciudadanos.

Entre las recomendaciones en este estudio se incluyen algunas dirigidas a los reguladores y supervisores en esta materia, que podrían activar una nueva generación de identidad digital también en la región. Se busca el desarrollo de un nuevo modelo de identidad digital fuerte que complemente al resto e impulse el uso común de identidades digitales fuertes en un contexto regional seguro, interoperable y para múltiples industrias.

Modelo digital centralizado gestionado por las organizaciones

Este modelo funciona principalmente en industrias reguladas como el sector financiero, donde el responsable de los datos de la identidad de los ciudadanos es el propio prestador de servicios (banco, Fintech, aseguradora, etc.). En este orden, el prestador de servicios asume el costo de la puesta en marcha de proyectos para conocer a sus clientes y realizar transacciones de forma segura y confiable.

Por ejemplo, entidades financieras internacionales implementan el *onboarding* digital y al mismo tiempo simplifican y digitalizan la experiencia de navegación de los usuarios. La nueva experiencia de incorporación digital les permite completar los requisitos de “conoce tu cliente” (KYC, por sus siglas en inglés, *Know Your Customer*), apertura de cuenta y producto en línea, así como rastrear su estado de manera más sencilla y ágil.

La principal virtud de este modelo es que la oferta y la demanda en un mercado abierto lo hacen evolucionar. Necesita regulación específica sectorial como en este caso, pero su crecimiento y penetración en la sociedad depende únicamente de solventar una necesidad y de poner en marcha mecanismos seguros que permitan este tipo de relaciones confiables, que cumplan con la normativa vigente en cada industria. Este modelo tiene una deficiencia por su falta de interoperabilidad: la información sensible de ciudadanos se puede encontrar en numerosas organizaciones, lo que puede suponer un riesgo por la cantidad de lugares donde la información de carácter personal de los clientes termina siendo procesada.

No obstante, se trata de un modelo maduro, ya que se viene utilizando hace mucho tiempo en el sector en los canales presenciales, y esta madurez le confiere una seguridad importante en tanto se ha estado ajustando a nivel técnico y regulatorio durante décadas.

Modelo digital descentralizado de identidad digital soberana

Este modelo denominado comúnmente “Identidad digital soberana” (SSI, por sus siglas en inglés, *Self Sovereign Identity*) propone un modelo de identidad cuya propiedad única de la información corresponde al ciudadano. Es el ciudadano el que va a tener el control de su privacidad y de sus datos de carácter personal, al mismo tiempo que puede gestionar los permisos relativos a una cuestión tan importante como es su identidad digital en relación con terceros. El modelo SSI aparece con la creación de las nuevas tecnologías de redes distribuidas *Distributed Ledger Technology* (DLT), en especial *Blockchain*, y tiene sentido dado el planteamiento que hace sobre la gestión de la privacidad y el control exclusivo de la información por parte de los ciudadanos.

Ya existen algunos casos reales basados en *Blockchain* donde se está comenzando a implantar este modelo. En Columbia Británica se ha puesto en marcha un directorio llamado OrgBook BC en el que se puede buscar información acerca de entidades legales que operan en la región. Además, los servicios gubernamentales podrán emitir permisos y licencias a través de esta plataforma distribuida y descentralizada. De este modo, organizaciones, gobiernos e individuos crean una red de confianza donde se pueden obtener, emitir y verificar credenciales (Jiménez, 2019).

Sin embargo, este modelo de identidad digital se encuentra actualmente en fase de experimentación en distintos países, por un lado por no existir todavía una cobertura legal sobre el modelo que permita desarrollarlo sobre redes de base distribuida como *Blockchain*, y por el otro por la inmadurez de las soluciones técnicas.

Otro ejemplo más tangible sería el de la ciudad suiza de Zug, donde se lanzó un servicio de identidad soberana —Zug eID— utilizando el protocolo uPort. Desde entonces, los ciudadanos pueden utilizar servicios relacionados, como por ejemplo la votación electrónica o la solicitud de certificados de residencia (Jiménez, 2019).

Uno de los principales retos del modelo es ver de qué manera puede crecer y obtener una masa crítica —un volumen de ciudadanos suficiente— para convertirse por sí solo en un modelo de uso común. Otro de los retos es ver cómo congenian el modelo técnico, en el que se descentraliza la gestión como valor clave, y el modelo político que le permita ofrecer un valor a la sociedad.

Conclusiones

La evolución de la identidad analógica para convertirse en identidad digital presenta distintas alternativas que se pueden considerar como una realidad. Asimismo, permite la diversificación de nuevos modelos que serán en el futuro complementarios con vistas a que la sociedad cree un sistema confiable para las relaciones y negocios entre personas e instituciones. El *onboarding* digital es una pieza clave que habilita cualquier modelo de identidad digital que la industria financiera pueda utilizar, ya sea que esté gestionado de forma pública o privada, o que sea centralizado o descentralizado.

4. Definición de *onboarding* digital

El *onboarding* digital es el proceso electrónico que permite la identificación de un consumidor financiero frente a una institución financiera y cuyo resultado genera una confianza equivalente a un proceso presencial. Para que sea efectivo, requiere de una confianza equivalente a la que ofrecen los canales presenciales; es decir, a la identificación realizada históricamente por parte de las instituciones financieras en las oficinas comerciales. El *onboarding* digital, por tanto, es un proceso que se realiza de forma totalmente remota y exclusivamente mediante el canal en línea.

Se lo engloba en la industria bancaria y financiera dentro de los procesos de Conoce a tu cliente (por sus siglas en inglés, *Know Your Customer*), y en la literatura y normativa financiera dentro de los procesos de Diligencia Debida de Cliente (CDD, por sus siglas en inglés, *Customer Due Diligence*).

Se considera como actividades clave dentro del proceso general de *onboarding* digital a las siguientes:

- Verificación de la identidad del cliente.
- Conocimiento sobre el origen de los fondos del cliente.
- Realización de chequeos antifraude.

Verificación de la identidad del cliente

La verificación de la identidad del cliente es el proceso que permite garantizar que la persona es quien dice ser. En general se realiza a través de una prueba de identidad oficial, típicamente un documento de identificación personal emitido por la autoridad gubernamental, como el documento único de identidad, la cédula de identidad o el pasaporte.

La definición del concepto de identidad es clave para la cuestión del *onboarding* digital. Dado que se trata de un concepto complejo y con múltiples significados, para el estudio se tomará como referencia la definición de identidad que propone el Grupo de Acción Financiera Internacional (GAFI) en su reciente *Guidance on Digital Identity* (la definición ha sido extraída de la sección “Digital ID Terminology and Key Features”).

Concepto de identidad oficial según el GAFI

Identidad es un concepto complejo con diferentes significados. Para los objetivos del GAFI, identidad se refiere a la “identidad oficial o legal” y es distinta de conceptos más amplios de una identidad personal o social que podrían ser relevantes a efectos no oficiales (por ejemplo: uso comercial no regulado o social, transacciones punto a punto en persona o en internet). La guía cubre el uso de sistemas de identidad digital para probar una identidad oficial para el acceso a los servicios financieros. En el marco de esta guía, identidad oficial es la especificación de una persona física única que:

- Se basa en características (identificadores o atributos) de la persona que le proporcionan una naturaleza única entre la población o en un contexto particular.
- Es reconocida por un Estado con un propósito regulatorio u otras finalidades oficiales.

Prueba de identidad oficial

Una prueba de identidad oficial generalmente depende de alguna documentación o certificación provista por un gobierno; por ejemplo, un certificado de nacimiento, una tarjeta de identidad o una credencial digital de identidad, que constituyen una evidencia de identificadores o atributos base (tales como nombre, fecha y lugar de nacimiento) para establecer y poder verificar una identidad oficial. El criterio para proveer una identidad oficial puede variar por jurisdicción. En el ejercicio de su soberanía, los gobiernos establecen los atributos requeridos, evidencias de la identidad y procesos para proveer la identidad oficial.

Origen de los fondos

El proceso permite obtener información del cliente sobre el origen de los fondos gestionados en el producto contratado, así como su residencia fiscal. Esta información hace parte de los procesos KYC determinados por el GAFI y puede ser utilizada para identificar y determinar la existencia de actividades sospechosas. En algunas jurisdicciones se complementa con una declaración jurada de fondos por parte del cliente, cuya responsabilidad de diligenciamiento recae en el consumidor financiero.

Chequeos antifraude

En este ámbito se determina si la identidad reclamada ha sido usada en actividades relacionadas con el fraude y si la persona que interviene en el proceso de identificación está o ha estado involucrada en actividades delictivas, bajo sanciones, o si es considerada una persona políticamente expuesta⁹ (PEP). Existen numerosas fuentes de información que permiten verificar que los ciudadanos previamente identificados no suponen ningún riesgo o amenaza para la organización o la sociedad siempre y cuando estas verificaciones sean complementarias a la verificación de la identidad de los clientes y no se hagan de forma aislada. Algunas de estas fuentes de información o verificaciones pueden ser las siguientes:

- Geolocalización: valida la autenticidad de las coordenadas del cliente a través de la revisión de la reputación de su dirección IP o del proveedor de servicios de telecomunicaciones.
- Validación de los primeros seis dígitos de una tarjeta de crédito, débito o prepago, lo que permite ver el nombre del banco que la expide, el país, y el nivel o tipo de tarjeta.
- Verificación de la dirección de correo electrónico: cuando se produce el proceso de alta, se verifica que la dirección de correo electrónico no sea de alto riesgo y que el servidor que la proporciona no haya sido comprometido o haya sufrido una brecha de seguridad en el último tiempo.
- Validación de una dirección física postal correcta.
- Verificación del teléfono móvil mediante la validación del tipo de número, el tipo de teléfono y el operador de telefonía, e incluso la precisión de la geolocalización de este número con la geolocalización del cliente.
- Verificación de listas vigiladas: se realiza una verificación con bases de datos que se actualizan con sanciones para reducir la exposición al riesgo, tales como PPE, lista de evasores extranjeros, listas de personas relacionadas con actos de terrorismo, personas cercanas y asociados, personas de interés especial, etc.
- Verificaciones de cuentas, validando la información de la cuenta del banco o las transacciones.
- Identidades suplantadas, manipuladas o robadas.

La existencia y actualización de este tipo de listas podría variar dependiendo de la jurisdicción.

---

⁹ En regulación financiera, una persona políticamente expuesta (PPE) es una persona a la que le ha sido confiada una función pública importante. Una PPE generalmente presenta un nivel más alto de riesgo ante un potencial involucramiento en actividades de corrupción, dada su posición y la influencia que podría mantener.

Otros temas

Los siguientes temas son importantes para tener en cuenta en las recomendaciones finales del estudio sobre *onboarding* digital. Sin embargo, su desarrollo tendrá una categoría secundaria de importancia. El motivo es que la normativa sobre prevención de blanqueo de capitales y financiación del terrorismo (PBCFT) los trata habitualmente como algo importante aunque no esencial. Estos son temas que afectan de forma general la realización de negocios privados y jurídicamente seguros con los consumidores. Pero cuentan con buenas prácticas y normativas específicas fuera de la legislación primaria PBCFT o de buenas prácticas internacionales en el *onboarding* digital.

Privacidad

Se trata de la correcta gestión de los datos personales de los clientes de forma de garantizar su privacidad en relación con los servicios prestados.

Contratación

La contratación es un proceso complementario al *onboarding* digital. Mientras el principal objetivo de este último es ofrecer confianza sobre la identidad del cliente y el origen de sus fondos, el de la contratación es garantizar que el acuerdo entre las partes —prestador del servicio financiero y cliente— se cumpla de una forma segura y de acuerdo con lo establecido en la ley en materia de contratación. La contratación a distancia se realiza a través de la firma electrónica, que es el concepto jurídico equivalente al proceso analógico de firma manuscrita. Tiene como meta que los acuerdos entre el cliente y el banco prestador de servicios financieros queden suscritos por vía telemática de una forma segura, inalterable y demostrable en cualquier momento. Las firmas electrónicas cumplen con estas características, lo que ayudará a solventar problemas en casos de impagos o repudios en la contratación. La contratación a través de la firma electrónica es un concepto ya extendido en América Latina y el Caribe (ALC). Los procesos de firma están vinculados a la confianza en la identidad de los firmantes. De este nivel de confianza en la identidad depende el grado de seguridad jurídica en la contratación. El cuadro 1 muestra el tipo de firmas existentes.

Definiciones de firma electrónica¹⁰

- **Firma electrónica:** son los datos en formato electrónico anexos a otros datos electrónicos o asociados de manera lógica con aquellos que utiliza el firmante para firmar.
- **Firma electrónica avanzada,** que cumple los siguientes requisitos:
  - Estar vinculada al firmante de manera única.
  - Permitir la identificación del firmante.
  - Haber sido creada utilizando datos de creación de la firma electrónica que el firmante puede utilizar, con un alto nivel de confianza, bajo su control exclusivo.
  - Estar vinculada con los datos firmados mediante la misma, de modo tal que puede detectarse cualquier modificación ulterior.
- **Firma electrónica calificada:** es una firma electrónica avanzada que se crea mediante un dispositivo cualificado de creación de firmas electrónicas y que se basa en un certificado cualificado de firma electrónica.

Las firmas electrónicas calificadas son las firmas electrónicas de mayor nivel jurídico, denominadas comúnmente firmas digitales. Este tipo de firma electrónica es la única que suele ofrecer una garantía idéntica a la de la firma manuscrita.

Cuadro 1. Tipos de firmas electrónicas existentes

	Identificación del firmante	Canales	Dispositivo	Equivalencia con manuscrita	Nivel de riesgo
Firma electrónica simple	No (Solo email, teléfono móvil)	En línea, oficina y teléfono	Cualquier dispositivo	No	No (Pólizas auto, coche, microcréditos)
Firma electrónica avanzada	Sí (Proceso realizado en presencia o con seguridad equivalente)	En línea, oficina	Cualquier dispositivo	No	Alto (Cualquier proceso de contratación, incluidos cualquier tipo de crédito, hipoteca, seguros de vida, planes de pensiones, etc.)
Firma electrónica avanzada y cualificada	Sí (Proceso realizado en presencia o con seguridad y cualificación equivalente)	En línea, oficina	Cualquier dispositivo	Sí	Alto (Administración pública)

Fuente: elaboración propia.

¹⁰ A efectos del presente texto, la definición de las firmas electrónicas ha sido extraída del reglamento comúnmente denominado eIDAS (European Union, 2017) relativo a la identificación electrónica y a los servicios de confianza para las transacciones electrónicas en el mercado interior (<https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32014R0910&from=ES>).

Identificación vs. autenticación

Con frecuencia, existe una confusión entre los conceptos de identificación y autenticación por su cercanía y por la terminología empleada. Entender los dos conceptos permite comprender en qué consiste el *onboarding* digital. En el *onboarding* digital, la identificación es el proceso de garantizar que la persona es quien dice ser. Comienza el día en que el cliente inicia su relación con el prestador de servicios financieros y se prolonga hasta que la persona deja de utilizar dichos servicios. Cómo se registra, cómo se lo va conociendo en el tiempo, cómo contrata y consume los servicios forman parte de un proceso continuo que permite construir una relación de mutuo beneficio entre las partes (el prestador de servicios financieros y el cliente).

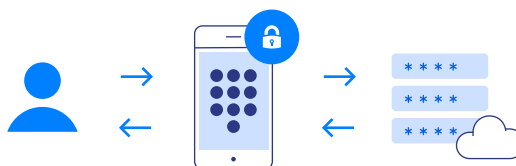
La autenticación tiene como misión garantizar que la persona accede y consume los servicios de base electrónica de una forma segura. La autenticación por sí misma no garantiza que la persona con la que se interactúa es quien dice ser, pero sí debe garantizar que los mecanismos o secretos que usa para acceder a las aplicaciones sean seguros para el acceso y también para la ejecución de transacciones financieras, tales como transferencias, pagos, contratación de créditos, etc.

Recuadro 1. Ejemplo de autenticación e identificación integradas

Una persona compra un teléfono inteligente modelo X, que incorpora la última tecnología biométrica facial. El usuario activa el servicio de pagos (*wallet*) para incluir una de sus tarjetas de crédito expedida por su banco habitual. Esto facilitará los pagos en tiendas minoristas tales como tiendas de ropa, cafeterías, clínicas, etc.

Autenticación

La estrategia de autenticación del fabricante del teléfono inteligente es una estrategia multifactorial. No ha cambiado desde los primeros modelos, ya que basa su seguridad en un primer factor que es la contraseña para acceder al teléfono inteligente. Cuenta además con un segundo factor biométrico, que es el facial. Cuando el usuario compra su terminal, lo abre y se registra, selecciona una contraseña para su acceso y registra su rostro en las características de biometría facial. Ambos registros quedan grabados de forma segura en la terminal. Las aplicaciones utilizan el sistema operativo y esta estrategia de seguridad combinando ambos factores. El fabricante del teléfono y por extensión todo su ecosistema de desarrolladores conoce que la persona que compró el teléfono es quien accede a las aplicaciones con una alta probabilidad. Pero ¿conocen la identidad de la persona? La respuesta es que no: estos métodos no son suficientes. Lo que se puede garantizar con estos métodos de autenticación es que la persona que se registró inicialmente acceda al teléfono y a sus aplicaciones, pero no se conoce de forma fehaciente la identidad de la persona que consume los servicios.



¿Por qué la autenticación? La respuesta es sencilla: **por seguridad**. La seguridad necesaria que permite conocer a las personas que supuestamente realizan las operaciones en el día a día, a fin de verificar si son las personas que dicen ser.

Identificación

Cuando el usuario quiera activar su servicio de pagos (*wallet*), por temas de confianza y cumplimiento normativo, el fabricante y sus socios financieros tendrán la necesidad de identificar inequívocamente al cliente. ¿Cómo lo hacen? Todo se realiza enlazando una cadena de confianza que tiene su origen en el prestador de servicios que, antes de dar de alta una tarjeta de crédito, ha tenido que identificar al cliente a través de su documento de identidad o pasaporte y firmar un contrato de términos y condiciones de uso de la tarjeta. Cuando el fabricante permite al usuario activar el servicio de pagos a través de su tarjeta de crédito es cuando se produce una vinculación entre una persona ya registrada (no necesariamente conocida) y la confianza en la identidad que proviene del prestador de servicios financieros que, por motivos regulatorios, ha tenido que conocer la identidad real del cliente con anterioridad. En todo este proceso está presente la identificación.



¿Por qué la identificación? La respuesta es sencilla: **confianza**. La confianza necesaria que es requerida desde siempre para realizar negocios y la confianza para evitar un uso delictivo del capital.

Conclusiones

Es común pensar que las nuevas tecnologías de autenticación —tecnologías biométricas (huellas dactilares, faciales, iris); tecnologías comportamentales (basadas en el conocimiento, en el comportamiento o asociadas a actividades de internet); vinculaciones con dispositivos móviles, o geoposicionamiento de los usuarios, entre otras— pueden, bien de forma aislada o combinada, proporcionar o sustituir un *onboarding* digital seguro. Todos estos mecanismos de autenticación (no de identificación) pueden aportar seguridad en el ciclo de vida de la relación con el cliente.

Sin embargo, es preciso remarcar que se trata de nuevas tecnologías que se utilizan con objetivos distintos, como se describió anteriormente, y en momentos distintos: la autenticación se realiza con posterioridad a la identificación y a la vinculación de la persona con los servicios prestados por las instituciones, que se da a través de la gestión de credenciales (diversos factores de autenticación) que ofrecen seguridad para su posterior relación transaccional.

5. Análisis de la regulación existente y situación actual del *onboarding* digital

En este apartado se identifica información relevante y actualizada para el estudio en general. Por un lado, se identifican las principales normas, estándares y buenas prácticas en el *onboarding* digital incluidos el país y el regulador que las ha publicado, una breve descripción, así como el mes y año de su entrada en vigor o publicación. Luego se realiza un análisis comparativo que identifica sistemas y buenas prácticas comunes en el *onboarding* digital en las distintas normativas existentes en la materia. Por último, se describen las principales conclusiones del análisis.

Toda esta información permitirá avanzar en apartados posteriores hacia el principal objetivo de este estudio: ayudar a los reguladores en la elaboración de políticas públicas y normativa con requerimientos concretos para habilitar el *onboarding* digital en cada jurisdicción.

Regulación existente en materia de *onboarding* digital

Los siguientes puntos identifican la regulación existente y en vigor que algunos países (ordenados alfabéticamente) han implementado para el *onboarding* digital. Incluyen normativas, procedimientos o autorizaciones que contemplan de forma específica la identificación no presencial o remota de clientes en el sector financiero, es decir un *onboarding* digital. La totalidad incluye un modelo técnico y de buen gobierno para que los sujetos obligados lo puedan implantar con las máximas garantías del *onboarding* digital.



Alemania

Tiene dos normativas que permiten el *onboarding* digital de clientes:

- Federal Financial Supervisory Authority (BaFin). Circular 3/2017 (GW) que permite un procedimiento de video identificación procedures-BaFin (todo el documento). Marzo de 2014.
- Federal Office for Information Security (FOIS). Guía Técnica TR-03147, Evaluación del Nivel de Aseguramiento de los Procedimientos para la Verificación de Identidad de las Personas Naturales, toda la sección 5 (págs. 20-25). Versión 1.0.4. Diciembre de 2018.

 Argentina

Financial Intelligence Unit (FIU). Resolution 28/2018 (art. 21 y sgtes.) y 21/2018 (capítulo III), en consulta con la Comisión Nacional de Valores (CNV): habilitó la implementación de plataformas tecnológicas a los sujetos obligados en el sector asegurador y de mercado de capitales, respectivamente, que permitan llevar a cabo trámites a distancia sin exhibición personal de la documentación, aplicando el enfoque basado en riesgos. Marzo de 2018 (28/2018 y 21/2018).

 Austria

Bundesgesetzblatt. Identification Ordinance, IVO, específicamente el punto 5 sobre uso de las tecnologías y medidas de seguridad para la identificación. Enero de 2019.

 Colombia

Circular Externa 027 de septiembre de 2020 de la Superintendencia Financiera de Colombia que imparte instrucciones relativas a la administración del riesgo de lavado de activos y la financiación del terrorismo. Estableció que las entidades pueden realizar los procedimientos de conocimiento del cliente de manera presencial o no presencial a través del uso de canales digitales o electrónicos. La norma permite que las entidades puedan obtener la información necesaria para realizar los procedimientos de conocimiento del cliente utilizando datos e información de fuentes confiables e independientes.

 Corea del Sur

Financial Services Commission (FSC): introduce un plan que permite el *onboarding* digital en el contexto de una ley para introducir bancos totalmente en línea en el país. Junio de 2015.

 España

Servicio Ejecutivo de la Comisión de Prevención de Blanqueo de Capitales e Infracciones Monetarias (SEPBLAC). Existen dos autorizaciones en España que permiten el *onboarding* digital:

- Autorización de procedimiento de identificación no presencial por videoconferencia. Febrero de 2016.
- Autorización de procedimiento de identificación no presencial por videoidentificación. Mayo de 2017.

 Estados Unidos de América

Departamento de Comercio – National Institute of Standards and Technology (NIST). El documento es una publicación especial 800-63.ª que provee los requerimientos para el enrolamiento y las pruebas de identidad para aplicantes que quieran obtener acceso a recursos en cada nivel de aseguramiento de la identidad. Se refiere específicamente a los apartados que son normativa. Junio de 2017.

 Hong Kong

Hong Kong Monetary Authority (HKMA) Remote Onboarding Authorization of Individual Clients. Circular de la autoridad monetaria del país. Febrero de 2019.

 Italia

Sistema Público para la Identidad Digital (SPID). La Agencia Digital de Italia define el estricto conjunto de medidas para obtener una identidad digital por canal en línea.

 Japón

Japan Financial Services Agency (FSA). Legislación sobre eKYC que permite la verificación de la identidad a distancia. 2007.

 Lituania

Law on the Prevention of Money Laundering and Terrorist Financing and amendments. Como parte de sus leyes AML, permite el *onboarding* digital no presencial. Diciembre de 2016.

 México

Comisión Nacional Bancaria y de Valores (CNBV). Resolución que modifica las disposiciones de carácter general aplicables a las instituciones de crédito, y refuerzan la identificación del cliente y permiten el *onboarding* digital a través de videoconferencia. Agosto de 2017.

 Portugal

Banco de Portugal (BdP). El procedimiento que permite el *onboarding* digital de clientes está incluido en la norma actualizada de PBCFT. Febrero de 2018.

 Reino Unido

Financial Conduct Authority (FCA). Establece una guía base con normativas en la Prueba de Identidad y Verificación de personas para el sector financiero, liberada por el Cabinet Office Government Digital Service. Enero de 2016.

 Singapur

Monetary Authority of Singapore (MAS). Regula el uso de las tecnologías para mejorar la experiencia del cliente en relación con las instituciones financieras y las leyes AML. Enero de 2018.

 Suiza

Swiss Financial Market Supervisory Authority (FINMA). Circular 2016/7. Establece los requerimientos para la identificación en línea por video y los requerimientos para el *onboarding* del cliente por canales digitales. Julio de 2016.

Literatura adicional

En este apartado se identifica otra literatura, como estándares, directrices o estudios alrededor del concepto de *onboarding* digital. Esta literatura no es normativa pero eventualmente puede ayudar a que el público amplíe el contexto en torno al concepto tratado.

- Comisión Europea y PWC. 2018. “Study on eID and digital onboarding: mapping and analysis of existing onboarding bank practices across the EU”. Este es un estudio preparado por PWC para la Comisión Europea.
- GAFI/FAFT. 2020. *Guidance on Digital Identity*. Es una guía base sobre la identidad digital publicada por el GAFI que recopila las buenas prácticas internacionales y estándares y los complementa con los beneficios y riesgos del *onboarding* y la gestión de la identidad digital.
- GAFI/FAFT. 2019. The FATF Recommendations. Buenas Prácticas Internacionales para combatir el blanqueo de capitales y la financiación y proliferación del terrorismo.

- Comisión Europea. 2018. AML5. La nueva directiva europea de PBCFT. Ya en vigor en la EU Directiva (UE) 2018/843 del Parlamento europeo y del Consejo del 30 de mayo de 2018 por la que se modifica la Directiva (UE) 2015/849 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifican las Directivas 2009/138/CE y 2013/36/UE.¹¹
- Comisión Europea. 2014. eIDAS. Reglamento (UE) 910/2014 del Parlamento europeo y del Consejo del 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.¹²
- Comisión Europea. eIDAS. Reglamento de Ejecución (UE) 2015/1502 de la Comisión del 8 de septiembre de 2015 sobre la fijación de especificaciones y procedimientos técnicos mínimos para los niveles de seguridad de medios de identificación electrónica con arreglo a lo dispuesto en el artículo 8, apartado 3, del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.¹³
- ISO/IEC 29115:2013 Information technology —Security techniques— Entity authentication assurance framework.¹⁴

Análisis comparativo de normativas de *onboarding* digital existentes

Dada una metodología predefinida, el siguiente capítulo intenta analizar la regulación regional e internacional existente en el ámbito del *onboarding* digital mencionada anteriormente, con el objetivo de establecer una serie de mínimos requerimientos técnicos y de buen gobierno que sean comunes. El análisis permitirá posteriormente realizar tanto recomendaciones concretas y objetivas como aspectos que deberán tener en cuenta los reguladores en la implementación del *onboarding* digital en sus jurisdicciones. La metodología utilizada desglosa los principales requerimientos técnicos y de buen gobierno de cada regulación. Asimismo, establece una serie de criterios y los enumera en cada regulación con el objetivo de que las recomendaciones que se ofrecen para el desarrollo de políticas públicas sean lo más precisas y objetivas posible. Para los interesados, en el anexo 1 se ha incluido el detalle de la metodología.

¹¹ <https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32018L0843&from=EN>.

¹² <https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32014R0910&qid=1575276936854&from=EN>.

¹³ <https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32015R1502&qid=1575276834942&from=EN>.

¹⁴ <https://www.iso.org/standard/45138.html>.

6. Experiencias en *onboarding* digital

A continuación, se describen las experiencias que han marcado los principales hitos en la historia del *onboarding* digital.

Verificación de la identidad a través de soluciones basadas en imágenes/selfies

Dada la creciente adopción de internet en un entorno que no ofrece confianza en la identidad por defecto (las personas que navegan y trabajan en la red no son identificadas previamente de forma natural), en 2010 aparecen las primeras leyes de sociedad de la información (EURO LEX, 2000)¹⁵ y comercio electrónico¹⁶, dando paso a la creación de soluciones para la verificación de la identidad legal de las personas físicas.

Estas soluciones comienzan a aparecer a partir de 2011. Funcionan tomando una fotografía de los documentos de identidad, las licencias de conducir o los pasaportes expedidos por los Estados, tanto del anverso como del reverso. Con el tiempo se ampliaron los sistemas para grabar un pequeño video en *streaming* del rostro de la persona y comprobar que está viva y que se corresponde con el documento en cuestión.

Aparecen las soluciones de *software* basadas en imágenes del documento, comúnmente llamadas soluciones de imágenes o *selfies*. Estas soluciones han tenido un recorrido importante en múltiples casos de uso, como la verificación de la identidad en determinados segmentos del comercio electrónico, el *check-in* o la verificación de la identidad en portales hoteleros o de economía colaborativa, tales como el alta en plataformas de *carsharing*. Gracias a su usabilidad han tenido una penetración alta en distintos sectores de la economía digital. Sin embargo, dado su bajo nivel de aseguramiento ya que son fácilmente manipulables y contienen grietas en el control y la integridad de su proceso a la fecha no han sido aceptadas en ninguna regulación específica¹⁷ de *onboarding* digital en el alto nivel de seguridad, equivalente a la identificación realizada en presencia.

¹⁵ <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=LEGISSUM%3AI24204>.

¹⁶ <https://www.consumer.gov/>.

¹⁷ Verificación realizada en el análisis comparativo de la normativa existente sobre *onboarding* digital en el sector financiero presentada en este estudio.

Existen casos de estudio con información pública en regiones que han regulado otros niveles de aseguramiento en la identidad que no permiten las soluciones de imágenes o *selfies*, que describen cómo algunos bancos o Fintechs —haciendo caso omiso de regulación más vigorosa existente en sus países en lo que hace al *onboarding* digital (por ejemplo, entrevista por videoconferencia) y tras varios casos de fraude— han sido denunciados por competencia desleal y por no cumplir con la regulación específica para el establecimiento de relaciones no presenciales con clientes. Estos casos han sido llevados a los inspectores de sus jurisdicciones, y actualmente se encuentran bajo inspección y vigilancia. En algunos casos graves, la licencia bancaria está siendo cuestionada. En otros casos de menor gravedad, las entidades demandadas han sido castigadas con multas abultadas y con el mandato de realizar nuevamente la identificación digital de la base de clientes captada durante el periodo en que se utilizaron sistemas no permitidos. Esto no solo ha puesto en duda la seguridad técnica de estas soluciones, sino también la reputación y valoración del banco o los prestadores de servicios financiero por parte de sus inversores y clientes. El impacto ha causado graves perjuicios para ambos.

La aparición de casos sonados de fraude, el avance de la tecnología y una regulación más garantista para el *onboarding* digital, que propone sistemas más sofisticados y seguros como el video en *streaming*, han limitado este modelo de *onboarding* digital a procesos de bajo riesgo en la verificación de la identidad y típicamente fuera del sector financiero. Los siguientes ejemplos avalan esta afirmación:

- El Departamento de Comercio de Estados Unidos, a través del National Institute of Standards and Technology (NIST), creó una guía para la identidad digital en junio de 2017, denominada *Guía sobre la identidad digital: enrolamiento y requerimientos para la prueba de identidad* (NIST SP 800-63). La guía establece tres niveles de aseguramiento para el registro y pruebas de la verificación de la identidad clasificados como bajo (IAL1), medio (IAL2) y alto (IAL3). El punto 5 de la regulación “Resolución de la identidad, validación y verificación” tiene la calidad de normativa (no informativa). El nivel alto de aseguramiento (IAL3) es el único equivalente en seguridad y cumplimiento normativo de todos los niveles a la identificación en presencia, y resulta válido para la apertura de cuentas de forma remota. Este nivel requiere la intervención humana (véase el punto 4.5 del documento) y establece la transmisión continua de video (*streaming*) como único sistema válido para realizar dicha verificación de la identidad (véase el punto 5.3.3.2 del documento). Esto deja fuera de juego las soluciones de imágenes/selfies y cambia el modelo legal anglosajón (*Common Law*), donde habitualmente existe un mayor espacio para la interpretación a un ámbito más explícito y garantista para el uso de los sistemas de *onboarding* digital por parte de los bancos y prestadores de servicios financieros.

- En marzo de 2020, el GAFI publica una guía para la identidad digital. Aunque esta guía es informativa (no normativa), favorece la implementación de procesos de *onboarding* digital por parte de los sujetos obligados y reguladores. La guía se apoya en el uso de nuevas tecnologías y recomienda explícitamente el uso de tecnologías de “transmisión de video en alta resolución” (GAFI/FAFT, 2020)¹⁸ (permitiéndolo para las identificaciones remotas y la verificación y prueba de vida).

Entrevista por videoconferencia

En 2014, el regulador alemán BaFIN creó la primera circular de la historia que permite el *onboarding* digital de personas físicas a través de una entrevista por video conferencia. Esta circular supone un hito, ya que regula por primera vez las relaciones no presenciales con el mismo nivel de seguridad y cumplimiento legal que una identificación y verificación de la identidad realizada en presencia, en una oficina comercial.

El proceso consiste en la grabación de una entrevista por videoconferencia, donde un agente cualificado guía al cliente para que muestre su documento de identidad a fin de verificar su autenticidad. Por otra parte, realiza algunas preguntas para validar la identidad de la persona.

El sistema marca un antes y un después en el sector financiero, desligando por primera vez en la historia la dependencia que tienen los bancos y prestadores de servicios financieros de las oficinas comerciales, al habilitar el canal en línea para el establecimiento de nuevos negocios y la contratación a cualquier nivel de riesgo, y poniendo el canal digital al mismo nivel que el presencial. La circular inspira a otros reguladores de otros países de la UE e incluso de otras regiones como América y Asia.

No obstante, y aunque el proceso es más práctico para el cliente que el desplazamiento y la espera en la oficina comercial, este sistema está cayendo en desuso debido a las siguientes circunstancias:

- El sistema necesita procesar cuatro caudales de información a través de la red: dos comunicaciones de audio y dos de video. La exigencia es alta en el procesamiento. Se originan problemas técnicos adicionales al no poderse gestionar la calidad de servicio de los paquetes de datos en internet. Estas complejidades provocan costos altos, inconveniencia para el cliente y una ratio baja de adquisición de clientes.
- La inconveniencia para el cliente sigue siendo alta. El *onboarding* digital, con una entrevista por videoconferencia, necesita al menos de ocho minutos para su realización completa.

---

¹⁸ <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/digital-identity-guidance.html>.

- El costo de adquisición de cliente (CAC) es el más alto de todas las soluciones estudiadas, dada la necesidad de disponer de un equipo humano permanente que atienda los procesos de entrevistas, tengan estas lugar o no, lo que significa una clara ineficiencia en términos de costos.
- Se trata de un sistema difícil de escalar si se suma la necesidad de contar todo el tiempo con agentes disponibles (a menudo, con necesidades de idiomas alternativos al nativo en cada jurisdicción para dar una respuesta inclusiva a ciudadanos extranjeros) y con la limitación natural del propio servicio. Ante una campaña de marketing siempre se encuentran limitaciones; por ejemplo, si un banco o prestador de servicios financieros realizara una campaña de captación de clientes en televisión o internet y se produjera un efecto llamada por el que varias decenas de personas quisieran contratar un servicio en ese momento. El servicio de *onboarding* digital para la verificación de la identidad estará limitado al número de personas formadas que estén disponibles para realizar la entrevista.

Videoidentificación

Dos años después de que lo hiciera el regulador alemán BaFIN, el Tesoro Público español creó —a través del Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias (SEPBLAC) de la Unidad de Inteligencia Financiera (UIF) de España— la primera autorización de un procedimiento de identificación no presencial por videoidentificación, gracias a la evolución de los sistemas de video en *streaming* y al avance de la inteligencia artificial (IA). La autorización que permite la identificación no presencial de clientes consiste en permitir el uso de sistemas de video en *streaming* asíncronos, que funcionan de la siguiente manera: primero se realiza un registro, que graba un video de inicio a fin en el que el cliente —guiado por el sistema— muestra su documento de identidad y su rostro para realizar una prueba de vida y una comparación biométrica con la imagen del documento de identidad. En un segundo paso, y a través de un proceso que garantiza la integridad, el video y los datos biométricos son enviados a una aplicación de autoridad de registro, donde un equipo humano cualificado verifica las pruebas del registro, pasando un protocolo de seguridad fuerte sobre las medidas de seguridad del documento y de la identidad de la persona. Esta verificación se realiza de forma asíncrona, en diferido.

El sistema propuesto de videoidentificación aporta una seguridad idéntica al proceso de entrevista por videoconferencia, pero mediante un proceso que es práctico para el usuario (dura unos segundos). Permite además un costo de adquisición de cliente (CAC) más bajo gracias a la IA, que eventualmente se traduce en una mayor eficiencia y en una mejora de la competitividad para el banco o prestador de servicios financieros. El cuadro 2 presenta un resumen de las experiencias de sistemas de *onboarding* digital.

Cuadro 2. Experiencias de sistemas de *onboarding* digital

Sistema	Nivel de aseguramiento	Casos de uso	Tiempo de <i>onboarding</i> aproximado	Costo de adquisición de cliente (CAC)	Ratio de adquisición de clientes	Escalabilidad
Imágenes/ <i>selfies</i>	Bajo/ medio	- Comercio electrónico - Economía colaborativa	1-2 minutos	Bajo	Alta	Alta
Entrevista por videoconferencia	Alto	- KYC - Apertura de cuentas - Procesos de verificación de identidad de ciudadanos en gobiernos - <i>Onboarding</i> - firma electrónica - Viajes transfronterizos - Notario/Justicia Digital - Voto electrónico	8-12 minutos	Alta	Baja	Baja
Vídeoidentificación	Alto	- KYC - Apertura de cuentas - Procesos de verificación de identidad de ciudadanos en gobiernos - <i>Onboarding</i> - firma electrónica cualificada - Viajes transfronterizos - Notario/Justicia Digital - Voto electrónico	1-2 minutos	Medio	Alta	Alta

Fuente: elaboración propia.

Como consecuencia de estas experiencias de *onboarding* digital en el tiempo, los sistemas que utilizan la grabación de video en *streaming* de inicio a fin del proceso, tanto la entrevista por videoconferencia como la vídeoidentificación, se convierten en los sistemas de referencia en el nivel alto de seguridad, cuando el *onboarding* requiere un nivel de seguridad técnica y jurídica igual al que se realiza en presencia.

Otros casos de uso

Lo anterior se consolida además con el uso de la tecnología de video en *streaming* en otros casos de uso e industrias que tradicionalmente han requerido el nivel más alto de seguridad, a saber:

Gobiernos y proyectos de firma digital

Distintos países están autorizando el uso de tecnologías de video en *streaming* para la emisión de certificados electrónicos cualificados de personas físicas, permitiendo así el *onboarding* digital de un proceso que tradicionalmente se realizaba en presencia, en una autoridad de registro. Países como Italia¹⁹ o Austria²⁰ han sido pioneros en establecer normativa adicional al eIDAS (regulación de servicios electrónicos de confianza) y observamos cómo muchos otros países los están siguiendo en este modelo. Este hecho supondrá un avance importante en la digitalización de la administración pública y su relación con el ciudadano, ya que logrará que la firma electrónica tenga un mayor índice de penetración que cuando el *onboarding* era puramente presencial y se realizaba en las autoridades de registro de las administraciones.

- **Voto electrónico**

El registro del votante en procesos de voto electrónico y eventualmente la democracia participativa son casos de uso para el *onboarding* digital. Prácticamente la totalidad de los principales fabricantes de software líderes en el ámbito del voto electrónico tienen iniciativas de registro del votante a través de video en *streaming*.

- **Notario digital**

Son conocidos los avances en Europa para digitalizar el sector de los notarios públicos. El video en *streaming* está jugando un papel protagónico en la identificación de intervinientes (en su *onboarding* digital) pero también en los actos notariales para la generación de escrituras públicas y en su ejercicio de fedatario público y asesor jurídico de las partes intervinientes, ya que el acto notarial se graba como una entrevista por videoconferencia y se guarda como principal evidencia electrónica del proceso notarial.

- **Viajes transfronterizos**

La identificación remota del viajero por video en *streaming*, combinada con el uso de tecnologías biométricas, aunque en estado todavía experimental, avanza de forma imparable en vías de digitalización en la dinamización de la economía.

---

¹⁹ <https://www.spid.gov.it>.

²⁰ <https://www.buergerkarte.at/en/>.

Son muchas las noticias públicas de aerolíneas y Estados que progresan en esta línea de trabajo. Será cuestión de tiempo hasta que la inconveniencia de mostrar el documento de identidad o pasaporte en la aduana, en la puerta de embarque del avión o en el *check-in* del hotel dé paso a sistemas donde la persona se identifique una vez (*onboarding digital*) y así autentique varias instancias; por ejemplo, mediante tecnologías biométricas (rostro, huellas dactilares, iris, etc.)

Todos estos casos, impulsados por regulaciones que afectan a múltiples industrias, darán lugar a una economía digital mucho más eficiente, segura y práctica para la ciudadanía. Como se mencionaba en apartados anteriores, tal es la importancia de estas iniciativas que algunas regiones han dado pasos importantes en la creación de mercados digitales sobre la base de sistemas de identidad digital. Europa, por ejemplo, está avanzando significativamente en sus políticas públicas con el eIDAS, el reglamento de servicios de confianza electrónica, que regula la nueva generación de firmas electrónicas. El eIDAS ha creado el concepto de Mercado Único Digital.²¹ El proyecto se encuentra vigente después de varios años de trabajo replanteando un modelo obsoleto de seguridad de las antiguas leyes de firma electrónica, que habían fracasado con niveles de penetración muy bajos de los servicios, fundamentalmente por la falta de usabilidad de las soluciones.

El eIDAS es además un reglamento de aplicación obligada y directa por parte de los Estados miembros y en vigor desde julio de 2016. Es la semilla de un documento de identidad electrónico europeo y plantea un cambio en la identidad como el que supuso el euro en la estandarización de la moneda a finales del siglo pasado.

De interoperabilidad no solo habla el eIDAS. El propio GAFI, en su guía de identidad digital editada en marzo de 2020, ya plantea un componente importante en este sentido, en el apartado tres: “Portabilidad y mecanismos de interoperabilidad” (GAFI/FAFT, 2020). La interoperabilidad puede resultar un concepto muy interesante para desarrollar en ALC, ya que sentaría las bases para la creación de un Mercado Único Digital en la región, con todas las ventajas que esto traería para la economía de los países que la componen.

---

²¹ <https://ec.europa.eu/digital-single-market/en/conozca-eidas>.

7. Beneficios del *onboarding* digital

El *onboarding* digital mejora el acceso a los servicios bancarios y financieros, incrementando el nivel de inclusión financiera. Habilita además a los bancos y prestadores de servicios financieros a mantener relaciones digitales de inicio a fin, lo que se traduce en una mejor competitividad y en la posibilidad de ofrecer mayor variedad de servicios.

Como muchas veces ocurre frente a algo nuevo, los miedos y la resistencia al cambio a lo desconocido dan paso, con el tiempo y la experiencia, al reconocimiento de los beneficios del mundo electrónico para la sociedad. El propio GAFI ha pasado de considerar el *onboarding* digital como un riesgo hace años a incorporarlo dentro de sus recomendaciones a la industria, reconociendo sus ventajas. Prueba de ello es la siguiente declaración en su guía de identidad digital recientemente publicada, donde se afirma lo siguiente: “la guía clarifica que la identificación de cliente y transacciones no presenciales que confíen en sistemas de identidad digital fiables, con una apropiada planificación de los riesgos, podrían presentar un nivel de riesgo estándar o incluso un riesgo menor” (GAFI/FAFT, 2020, Sumario ejecutivo, punto 3).

Punto de vista del GAFI sobre los beneficios del *onboarding* digital

Los siguientes beneficios han sido extraídos de la forma en que se indica en la guía de identidad digital del GAFI (GAFI/FAFT, 2020, Sección I: Introducción. Potenciales beneficios).

- Los sistemas de identidad digital que se basen en alta tecnología y estándares de buen gobierno mantienen la gran promesa de mejorar la confianza, seguridad, privacidad y conveniencia de identificar personas físicas en una gran variedad de escenarios, tales como los servicios financieros, la salud y el gobierno electrónico en la economía global en la era digital. Estos sistemas de identidad digital se refieren a aquellos con altos niveles de seguridad.
- En relación con los estándares GAFI, el uso de sistemas de identidad digital independientes y confiables podría:
  - Facilitar la identificación y verificación en el *onboarding* del cliente.
  - Soportar procesos de diligencia debida en curso y el escrutinio de transacciones a través del curso de las relaciones de negocio.
  - Facilitar otras medidas de diligencia debida de cliente (CDD).
  - Apoyar la monitorización de transacciones, con el propósito de detectar y denunciar transacciones sospechosas, además de mejorar la gestión general del riesgo y los esfuerzos en la gestión del fraude.

- Los sistemas de identidad digital independientes y confiables pueden contribuir a la inclusión financiera, habilitando a personas que no han accedido a servicios para probar su identidad oficial en un rango amplio de circunstancias, incluso de forma remota, y así obtener servicios financieros regulados. Incorporar más personas dentro del sector financiero regulado refuerza la lucha en la prevención de blanqueo de capitales y financiación del terrorismo (PBCFT).
- Los sistemas tienen el potencial de reducir costos e incrementar las eficiencias para las entidades reguladas, permitiendo reasignar recursos en otras funciones para la PBCFT.

Además de los beneficios declarados en la guía publicada por el GAFI, se identifican los siguientes beneficios que fortalecen la seguridad de las transacciones:

- **La trazabilidad electrónica aporta importantes beneficios en detrimento de la analógica.**

Las pruebas del proceso de *onboarding* digital (video grabado de inicio a fin con la entrevista o videoidentificación, copias del documento de identidad, credenciales del cliente, *scoring* biométrico entre la persona y la imagen del documento, detección automática de medidas y características de seguridad de los documentos de identidad, así como el identificador del agente verificador, entre otros) que se guardan de forma perdurable e inalterable (con sellos de tiempo) hasta que termina la relación con el cliente son muy importantes no solo para la verificación de la identidad sino también como evidencia disponible en tiempo real cuando requiera investigarse alguna actividad sospechosa. Un ejemplo pionero que se basa en la trazabilidad electrónica financiera lo inició la INTERPOL (Organización Internacional de Policía Criminal) con su proyecto Titanium (*“Tools for the Investigation of Transactions in Underground Markets”*) (Horizon, 2020).²² El proyecto Titanium es un ejemplo de cómo monitorizar actividades fraudulentas en un ámbito internacional. Los datos de la identificación del cliente pueden ser tratados para fortalecer este proyecto, incluso preservando la privacidad de los clientes, pudiendo tratarse de forma anónima. La trazabilidad y el acceso a la información del *onboarding* digital en tiempo real puede suponer un antes y un después en la labor de la inspección, ya que dicha labor se sustenta hoy en papel, con la dificultad que conlleva su tratamiento. Con los sistemas electrónicos de *onboarding* digital, sumados a los nuevos estándares en la interoperabilidad entre aplicaciones, tales como las APIs (*Application Program Interfaces*), la función podría pasar a ejecutarse en línea. Incluso cabría la posibilidad de diseñar y desarrollar programas que permitan acceder a los datos en línea de los bancos y prestadores de servicios financieros y en facultad de las competencias de inspección, monitorizar de forma transversal y preventiva cualquier transacción sospechosa o mejorar la gestión del riesgo de las operaciones. Cabe destacar en este punto la versatilidad que puede ofrecer el proceso de *onboarding* digital en todo el ciclo de vida de los negocios para la institución financiera.

²² <https://www.interpol.int/es/Quienes-somos/Marco-juridico/Information-communications-and-technology-ICT-law-projects/Project-Titanium>.

- El modelo centralizado de verificación de la identidad fortalece el modelo de seguridad.

Tanto en el método de entrevista por videoconferencia como en el de videoidentificación, la seguridad recae sobre humanos anónimos para el público. Estas personas se capacitan para la función específica de la verificación de la identidad. Además, la asignación de verificaciones se realiza siguiendo buenas prácticas de seguridad, de forma aleatoria. Esto vuelve mucho más compleja la posibilidad de planificar en connivencia actos delictivos de suplantación de identidad. En el modelo presencial descentralizado, la capacitación de las personas que realizan la verificación no existe como buena práctica estándar y por lo tanto la posibilidad de planificar un acto delictivo es más factible.

- La grabación de un video de inicio disuade a las personas a la hora de planificar delitos en relación con la suplantación de identidad.

El hecho de solicitar el consentimiento de los clientes de forma explícita para la grabación del proceso de verificación de la identidad por temas de privacidad y que el cliente tenga que aceptar el uso de la cámara y el micrófono de su dispositivo genera un efecto disuasorio en quienes pretenden realizar un acto delictivo de suplantación de identidad, ya que son conscientes de que serán grabados cometiendo este acto de inicio a fin. Esta grabación puede ser una prueba irrefutable (que no existe habitualmente en el canal presencial) ante un posible juicio.

- El desarrollo de políticas públicas y nuevas regulaciones de *onboarding* digital en el sector financiero servirá de palanca para el desarrollo de otros modelos de identidad digital fuerte, como la firma digital o de identidad digital soberana, que ofrecerán valor a la sociedad.

8. Marco jurídico

La introducción del *onboarding* digital en el ordenamiento jurídico de cada país se podría facilitar al darse las siguientes circunstancias. Todos los casos internacionales de regulación que se han identificado y analizado en este estudio son actos administrativos emitidos por las autoridades de regulación o supervisión financiera o por la autoridad a cargo de la prevención del lavado de activos y financiación del terrorismo, habitualmente en forma de circular o autorizaciones. Esto simplifica la labor a la hora de regular, al tratarse de actos administrativos de rango inferior que afectan solamente a una industria y donde, en la mayoría de los casos, las entidades reguladoras tienen facultades claras y autonomía para poner en marcha iniciativas de este tipo.

El ordenamiento jurídico y los esquemas y jerarquías son diversos en la región de ALC. Sin embargo, hemos comprobado en diversos casos que los reguladores del sector financiero cuentan con facultades y autonomía para la publicación de normas específicas en dicho sector. Esto confiere capacidad para el establecimiento de resoluciones en forma de circulares o autorizaciones específicas para el *onboarding* digital. Se han escogido tres casos, a modo de ejemplo.

Chile

En el párrafo cuarto del artículo 35 de la ley orgánica constitucional se crea el Banco Central de Chile (BCC) como entidad reguladora del sistema financiero²³ y se le confieren las facultades de forma expresa para dictar normas: crear nuevas normativas, expedir o denegar autorizaciones y cartas circulares. La normativa que otorga facultades al BCC es la ley orgánica constitucional del Banco Central de Chile, ley 18.840 y dentro del artículo 35, en especial los numerales 1, 5 y 6. En Chile, la entidad supervisora en el ámbito de la PBCFT es la Superintendencia de Bancos e Instituciones Financieras (SBIF). La SBIF tiene atribuciones según la Ley General de Bancos (artículos 2 y 14 del título 1) que le confieren facultades expresas para supervisar las actividades que realizan las entidades reguladas por el BCC y requerir informes cuando sea necesario. La normativa otorga facultades adicionales al SBIF (fusionado desde 2019 con la Comisión para el Mercado Financiero) a través del artículo 4 de la Ley 21.000 para, por ejemplo, dictar las normas para la aplicación y el cumplimiento de las leyes y reglamentos y, en general, dictar cualquier otra normativa que le corresponda de conformidad con la ley para la regulación del mercado financiero.

²³ Ley Orgánica Constitucional del Banco Central de Chile de 2019 (<https://www.leychile.cl/Navegar?idNorma=30216#regular0>).

 Colombia

El ente regulador para el sector financiero es el Ministerio de Hacienda y Crédito Público, a través tanto de la Unidad de Proyección Normativa y Estudios de Regulación Financiera (URF) en lo que tiene que ver con la elaboración de proyectos de Decretos Reglamentarios finalmente expedidos por el Presidente de la República, como a través de la Superintendencia Financiera de Colombia (SFC) en lo relacionado con instrucciones generales o particulares que desarrollen las leyes y decretos reglamentarios que sean aplicables a las entidades vigiladas y conglomerados financieros y que se expiden a través de circulares externas o resoluciones. De esta manera, la SFC es un organismo técnico adscrito al Ministerio de Hacienda y Crédito Público, con personería jurídica, autonomía administrativa y financiera y patrimonio propio. A través de la SFC, el Presidente de la República ejerce la inspección, la vigilancia y el control sobre las personas que realicen actividad financiera, bursátil, aseguradora y cualquier otra relacionada con el manejo, el aprovechamiento o la inversión de recursos captados del público. La SFC tiene entonces por objeto supervisar el sistema financiero colombiano con el fin de preservar su estabilidad, seguridad y confianza, así como promover, organizar y desarrollar el mercado de valores colombiano; la protección de los inversionistas, ahorradores y asegurados, y la protección del consumidor financiero. Sus atribuciones generales están establecidas en los artículos 325 y 326 del Estatuto Orgánico del Sistema Financiero (Decreto Ley 663 de 1993)²⁴ y reglamentadas principalmente en el Libro 2 de la Parte 11 del Decreto 2555 de 2010²⁵. Dentro de sus funciones está la de instruir a las instituciones vigiladas sobre la manera en que deben cumplirse las disposiciones que regulan su actividad, fijar los criterios técnicos y jurídicos que faciliten el cumplimiento de tales normas y señalar los procedimientos para su cabal aplicación, así como instruir a las instituciones vigiladas sobre la manera en que deben administrar los riesgos implícitos en sus actividades. Ejemplos del ejercicio de estas facultades son la Circular Externa 029 de diciembre de 2019²⁶, a través de la cual la SFC impartió instrucciones con relación a los requerimientos mínimos de seguridad y calidad para la realización de operaciones incentivando el uso de factores biométricos como mecanismo de autenticación; y la Circular Externa 027 de septiembre 2020²⁷, a través de la cual la SFC impartió nuevas instrucciones sobre la administración del riesgo de lavado de activos y financiación del terrorismo con el propósito de promover la utilización de nuevas tecnologías en la gestión y administración de dicho riesgo, de acuerdo, entre otras, con las recomendaciones de la guía de identidad digital del GAFI.

²⁴ <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=1348>.

²⁵ <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=40032>.

²⁶ <https://www.superfinanciera.gov.co/inicio/normativa/normativa-general/circulares-externas-cartas-circulares-y-resoluciones-de-sde-el-ano-/circulares-externas/circulares-externas--10099659>.

²⁷ <https://www.superfinanciera.gov.co/inicio/normativa/normativa-general/circulares-externas-cartas-circulares-y-resoluciones-de-sde-el-ano-/circulares-externas/circulares-externas--10102740>.

 México

El ente regulador para el sector financiero es la Comisión Nacional Bancaria y de Valores y, en atención al artículo 78 de la Ley General de Mejora Regulatoria y con la finalidad de reducir el costo de cumplimiento de dichas disposiciones, la Comisión Nacional Bancaria y de Valores, mediante resolución publicada en el Diario Oficial de la Federación el 26 de diciembre de 2017, modificó las “Disposiciones de carácter general aplicables a las instituciones de crédito”²⁸ con el propósito de flexibilizar el plazo al que estaban sujetas las instituciones de banca múltiple para constituir sus requerimientos de capital por riesgo operacional. Para ello, a inicios del año 2020 convocaron a una propuesta pública de comentarios o diseño del marco regulatorio a la que se envió un proyecto. Los acápites más resaltantes de la normativa vigente sobre la materia son los siguientes:

Artículo 51 bis 6, sección III, que describe lo siguiente:

El formulario mencionado deberá incluir una manifestación que señale que su envío a la institución de que se trate constituye el consentimiento del solicitante para que su voz e imagen sean grabadas al establecerse una comunicación a través de un medio audiovisual. Dicha manifestación podrá realizarse por medio de herramientas automatizadas que permitan su grabación y posterior reproducción.

El consentimiento a que se refiere el párrafo anterior deberá obtenerse en términos de la Ley Federal para la Protección de Datos Personales en Posesión de los Particulares a la que la sustituya. (...)

Artículo 51 bis 6, sección VI, que describe lo siguiente:

Si la institución valida que el solicitante no es su cliente, conjuntamente con el formulario a que se refiere la fracción III del presente artículo, deberá requerir al solicitante el envío de una fotografía a color de su credencial vigente para votar expedida por el Instituto Nacional Electoral, por el anverso y el reverso, y validar los elementos de seguridad de dicha credencial, a fin de detectar si dicho documento presenta alteraciones o inconsistencias, para lo cual deberán contar con la tecnología necesaria. (...)

Artículo 51 bis 6, sección VII, que describe lo siguiente:

Efectuar la comunicación en tiempo real y mediante el uso de herramientas automatizadas que permitan su grabación y posterior reproducción, y conforme a las guías de diálogo aleatorias que establezcan las instituciones. Asimismo, la comunicación deberá tener una duración de al menos 30 segundos continuos y sin interrupción, y ser grabada colocando el dispositivo de manera horizontal y conservada sin ediciones en su total duración por un periodo de, al menos, 10 años.

²⁸ https://www.dof.gob.mx/nota_detalle.php?codigo=5591405&fecha=09/04/2020.

9. Recomendaciones para que los reguladores implementen el *onboarding* digital en sus jurisdicciones

Las siguientes recomendaciones son la síntesis de todo el estudio realizado previamente, en especial del análisis comparativo de los actos administrativos que permiten el *onboarding* digital a nivel internacional.

Aunque forman parte de un todo, las recomendaciones se muestran ordenadas por distintas áreas: i) planificación y gestión del riesgo; ii) privacidad; iii) verificación de la identidad del cliente; iv) origen de los fondos, y v) chequeos antifraude. La intención es mostrar los aspectos más relevantes que son denominador común en las regulaciones de *onboarding* digital que se han identificado y analizado en este estudio. En ningún momento plantean una lista taxativa sino más bien una referencia adicional que pueda ayudar a los reguladores en su función.

Las recomendaciones se basan en el estudio pormenorizado de las regulaciones actuales que permiten el *onboarding* digital a nivel internacional, tanto en un ámbito de requerimientos y buenas prácticas técnicas como de buen gobierno.

Recomendaciones GAFI

Las recomendaciones realizadas se alinean con el GAFI a la hora de planificar las relaciones no presenciales con clientes. El siguiente texto se extrae de GAFI/-FAFT (GAFI/FAFT, 2020, pág. 5):

- Desarrollar guías y regulaciones claras que permitan desarrollar el uso de sistemas de identidad de forma apropiada y gestionando el riesgo inherente de las mismas. Como punto de partida, entender los sistemas de identidad digital disponibles en cada jurisdicción y cómo pueden encajar en los requerimientos existentes para la identificación y verificación del cliente y procesos de diligencia debida.
- Evaluar si las regulaciones existentes son apropiadas en un contexto jurisdiccional y su ecosistema de identificación. Por ejemplo, las autoridades deben considerar clarificar que las relaciones no presenciales y el *onboarding* digital podrían presentar un riesgo estándar o incluso menor para procesos de diligencia debida, cuando los sistemas de identidad digital, con niveles de aseguramiento apropiados son usados para la identificación y verificación remota de clientes.

Planificación y gestión del riesgo

La planificación y la gestión del riesgo juegan un papel importante en la puesta en marcha de iniciativas de *onboarding* digital. La inclusión de estos requerimientos en los actos administrativos ayudará a que las instituciones financieras planifiquen y gestionen mejor el riesgo inherente al proceso de *onboarding* digital. Los objetivos son que los sistemas utilizados sean documentados, analizados y testeados de forma que se pueda probar su eficacia antes de su utilización efectiva con clientes.

Analizar los riesgos del canal en línea

El banco o prestador de servicios financieros que implante un sistema de *onboarding* digital realizará un análisis de riesgos del proceso de identificación del cliente específico para el canal en línea. Este análisis identificará los casos que potencialmente podrían poner en riesgo un proceso de identificación y cuantificará el impacto y la probabilidad de que esto acontezca en el tiempo en cada caso. El análisis de riesgos establecerá un plan de mitigación específico para cada caso de riesgo potencial.

Documentar y probar el sistema

El banco o prestador de servicios financieros documentará el procedimiento y probará su eficacia, reseñando por escrito los resultados. No se procederá a la implantación efectiva del procedimiento si los resultados de las pruebas no acreditan su eficacia.

Capacitar el equipo humano de verificación

Los procesos de verificación deberán ser gestionados por personal con capacitación específica. Dicha capacitación será congruente con las funciones desempeñadas.

Asegurar la privacidad del cliente

El banco o prestador de servicios financieros asegurará la privacidad del cliente conforme con las normas establecidas en la jurisdicción donde opera.

Privacidad

El siguiente apartado intenta establecer requerimientos que garanticen el correcto tratamiento de los datos de carácter personal de los clientes, así como la obtención del consentimiento expreso antes de la verificación de su identidad.

Consentimiento

Al inicio y antes del comienzo del proceso de videoidentificación, a fin de ser identificada, la persona debe dar su consentimiento expreso al responsable del tratamiento de datos que utiliza los datos de carácter personal compartidos, de conformidad con la legislación local.

Cumplimiento de la ley de protección de datos de carácter personal

Como responsable de los datos, el banco o prestador de servicios financieros se exigirá internamente —y lo extenderá al ecosistema de socios de negocio con los que trabaje— el cumplimiento de la normativa local en materia de protección de datos de carácter personal. Se recomienda realizar o solicitar certificaciones específicas en materia de protección de datos de carácter personal. Asimismo, se establece la obligación de cooperar en esta materia con las agencias responsables de la protección de datos en cada jurisdicción.

Verificación de la identidad

La verificación de la identidad del cliente no presencial la realizará un humano cualificado, a través de una prueba de identidad oficial con fotografía. Los objetivos son los siguientes:

- Realizar un proceso de verificación de la identidad técnicamente seguro y con calidad.
- Describir las medidas de seguridad que permitan una asignación correcta e impredecible de los agentes verificadores de la seguridad del proceso.
- Describir los distintos métodos de verificación de la identidad a utilizar.
- Gestionar una correcta custodia de la información.
- Garantizar que las medidas de seguridad puestas en marcha en el proceso de *onboarding* digital aseguren con alta fiabilidad la autenticidad del documento de identidad.
- Garantizar que la persona es quien dice ser, su fecha de nacimiento y una prueba de vida.
- Garantizar una correcta capacitación de los agentes verificadores.

El proceso de verificación se realizará a través de la grabación de un video en *streaming*.²⁹ El video grabado de inicio a fin en el proceso de *onboarding* digital será la principal evidencia electrónica del proceso de verificación de la identidad oficial del cliente.

Control exclusivo de la grabación del video

- El control de la grabación del proceso de video en *streaming* debe estar bajo el exclusivo control del prestador de servicios financieros o, en su defecto, del prestador de servicios subcontratado para el proceso de verificación.
- No se admitirán videos pregrabados.
- No se admitirán videos realizados en el dispositivo local del cliente.
- El proceso de grabación del video se realizará en directo.

Identificación realizada por un equipo humano cualificado

El proceso de verificación de las pruebas de identidad lo realiza un equipo de empleados entrenados en el tema. Los empleados, sean internos o de un tercero, deben contar con una capacitación concreta en la verificación de la identidad de personas. Asimismo, deben estar ubicados en una localización dentro de la jurisdicción del sujeto obligado o, en su defecto, en una localización que cumpla con los requerimientos de privacidad exigidos por la normativa local vigente o por una normativa reconocida en el ámbito internacional, igual o superior en requerimientos a la local.

Asignación aleatoria de agentes de verificación

La asignación de los casos de verificación al agente cualificado se debe realizar con mecanismos que no puedan ser previsibles para evitar cualquier posibilidad de manipulación del proceso.

Calidad suficiente del entorno de la videoidentificación

La calidad de la iluminación del ambiente donde se realiza el proceso de video identificación así como la calidad del propio video y del sonido deben ser suficientes para permitir un estricto control en el proceso de revisión de las pruebas por el equipo humano cualificado.

²⁹ El proceso de verificación a través de la grabación de un video en *streaming* es el principal requerimiento técnico común en cada una de las normativas existentes identificadas en el estudio. Además, el video en *streaming* es una de las nuevas tecnologías mencionadas por el Grupo de Acción Financiera Internacional (GAFI) en su documento *Guidance on Digital Identity*, apartado "Recommendations for digital ID service providers" (GAFI/FAFT, 2020).

Documentos de identidad aceptados

Se admitirán solo documentos con medidas de seguridad a prueba de falsificaciones, claramente identificables y verificables, que contengan una imagen del individuo a identificar y que incluyan verificación por Zona de Lectura Mecánica (MRZ, por sus siglas en inglés, *Machine Readable Zone*). El regulador tiene que identificar y regular si lo requiere, de forma precisa, qué documentos son admitidos para este tipo de procesos por el derecho en vigor para esta clase de transacciones en su jurisdicción.

Custodia de la información

El proceso de identificación completo, así como las credenciales y otras evidencias electrónicas recogidas durante el proceso, deben ser grabadas y guardadas. Esta información debe ser firmada electrónicamente con un sello de tiempo para demostrar su inalterabilidad en el tiempo, y también encriptada, para evitar un uso inapropiado. Los datos deben estar guardados y custodiados al menos 10 años desde el cese de la relación con el cliente.

Verificación del momento de la grabación

Se utilizarán medidas tales como preguntas aleatorias (si la verificación es síncrona) o medidas automáticas de seguridad tipo *catch-up* (si la verificación es asíncrona), a fin de comprobar que el proceso de identificación se realiza en el momento actual previsto y no con anterioridad.

Métodos de verificación de la identidad del video

Síncrono

El proceso de verificación de la identidad se realiza a través de una entrevista por videoconferencia. El equipo humano cualificado que verifica las pruebas lleva a cabo el proceso de registro y verificación en línea al mismo tiempo.

Asíncrono

El proceso de verificación de la identidad se realiza a través de un primer paso que consiste en un registro de videoidentificación grabado por video en *streaming* de inicio a fin, en el que la persona muestra el anverso y el reverso de su documento de identidad y su rostro. Luego habrá una verificación de todas las pruebas recogidas en el proceso de registro por parte de un equipo humano cualificado que revisará todas las pruebas con un protocolo de seguridad que garantice la verificación de la autenticidad del documento de identidad, así como la verificación de la identidad de la persona.

☒ **Verificación de medidas de seguridad del documento de identidad**

El proceso debe asegurar que el documento usado como prueba de la identidad contenga todas las medidas de seguridad esperadas según el tipo y la versión del propio documento, específicamente: medidas de óptica de seguridad variables tales como hologramas, identigramas³⁰ y kinegramas³¹; customizaciones tipográficas o de imágenes láser; materiales, tales como ventanas transparentes, tinta de óptica variable, microescrituras, *chip* o patrones *guilloché*.

☒ **Características del documento**

El proceso debe asegurar que el documento de identidad tenga el tamaño, la tipografía y el diseño esperados y correctos. El proceso verificará que el documento no haya expirado (este requisito solo aplica a documentos que ofrezcan dicha información).

☒ **Comparación anverso-reverso**

El proceso verificará que el anverso y el reverso del documento de identidad correspondan entre sí.

☒ **Comparación de imágenes y criptogramas**

El proceso verificará que el documento de identidad y los patrones de imágenes del fondo sean presumiblemente correctas.

☒ **Verificación de la integridad de la zona MRZ**

El proceso verificará que los datos extraídos de la zona MRZ tengan los algoritmos adecuados y que el cómputo de su construcción sea íntegro.

☒ **Verificación de que el documento no haya sido dañado o alterado**

El proceso debe revisar y verificar que el documento de identidad no haya sido dañado o modificado, especialmente la fotografía. Ante cualquier duda razonable planteada en esta verificación, el proceso debe ser rechazado.

---

³⁰ Identigrama: nivel de atributos de identidad a proyectar, al servicio de la imagen, que generalmente se sitúan entre el ideograma actual y el ideal. Fuente: Website Gestipolis (<https://www.gestipolis.com/imagen-e-identidad-como-recurso-estrategico-en-la-gestion-de-hoteles/#:~:text=El%20identigrama%3A%20Nivel%20de%20atributos,ideograma%20actual%20y%20el%20ideal>).

³¹ El kinegrama consiste en una estructura de difracción microscópica. La imagen, no obstante, no es tridimensional como en el holograma, sino que al moverla muestra animaciones gráficas. Fuente: Banco de España (<https://www.eleconomista.es/diccionario-de-economia/kinegrama>).

Nota: algunas de las características de seguridad de los documentos de identidad podrían variar de un país a otro. Por tanto, para alcanzar un mayor nivel de seguridad se recomienda que el acopio de estas recomendaciones generales se adapte a las circunstancias de cada país, jurisdicción y tipo de documento nacional de identidad o documentos soportados.

☒ **Verificación de la identidad**

El proceso verificará, con un alto grado de probabilidad, que la persona de la fotografía del documento de identidad y la persona que mantiene el documento de identidad durante el proceso de identificación sean la misma y que la edad, el género y otras circunstancias inherentes a la identidad correspondan con la identidad reclamada por la persona durante el proceso.

☒ **Fecha de nacimiento**

El proceso verificará que la fecha de nacimiento es apropiada por el tipo de servicio a contratar y consistente con las características de la persona.

☒ **Prueba de vida**

El proceso verificará que la persona está viva y en un espacio suficientemente iluminado.

☒ **Origen de los fondos y chequeos antifraude**

En este caso los objetivos son los siguientes:

- Obtener la residencia fiscal y conocer el origen de los fondos del cliente

El proceso permite obtener información del cliente acerca del origen de los fondos y de su residencia fiscal en el momento del *onboarding*.

- Verificar la exposición política de la persona

El proceso permite obtener información acerca de si se trata de una persona políticamente expuesta (PEP, por sus siglas en inglés, *Politically Exposed Person*), a través de fuentes propias o listas de terceros.

- Corroborar que los datos aportados por el cliente son fiables y que la persona no ha estado potencialmente involucrada en actividades delictivas o fraude

El proceso permite verificar por fuentes propias o de terceros que la persona no ha estado involucrada en actividades delictivas o fraude.

Consideraciones sobre personas físicas y legales

Todas las normativas y la literatura recogida en el estudio han sido desarrolladas con el foco puesto en el *onboarding* digital de personas físicas. Sin embargo, existen algunas consideraciones sobre las personas legales que se describirán, ya que pueden ser de vital importancia para generar desarrollo en los países de la región a través de la financiación del ámbito productivo.

Personas físicas

La identidad de una persona física se basa comúnmente en una serie de atributos extraídos del proceso de verificación de su identidad legal, tales como nombre, dirección, país de residencia, fecha de nacimiento. Es importante enfatizar que el identificador único utilizado por las instituciones financieras suele representarse con el número del documento de identidad expedido por el Gobierno o identificadores únicos expedidos por la administración, como norma habitual y siempre que el país cuente con ellos. Como elementos sustitutivos del identificador único o como complementos al mismo, también existe una serie de atributos pertenecientes a la identidad legal de la persona que podrían diferir de una jurisdicción a otra, como podría ser el género, la ocupación, el lugar de nacimiento, el correo electrónico o el número de teléfono. Los últimos suelen ser datos prácticamente obligatorios y confirmados en los procesos de *onboarding* porque sirven de punto de contacto y comunicación en toda la relación.

Personas legales

En la normativa y literatura consideradas en el presente estudio, la identidad de una persona legal es, a menudo, una extensión de la persona física que, a través de los documentos que le confieren derechos y de identificadores y documentación relacionada con la entidad legal, suele actuar como representante.

Los atributos adicionales comunes que identificamos para una persona legal son el nombre legal, el identificador único y la dirección. Además, se identifican algunos alternativos que, aún divergiendo, se encuentran presentes en la mayoría de la literatura, como el número de referencia fiscal, el correo electrónico, el Standard Industrial Classification Number (SIC), Economic Operator Registration and Identification Number (EORI) o Legal Entity Identifier (LEI). Asimismo, suelen ser requisitos mínimos para el *onboarding* de una persona legal la identificación de los distintos beneficiarios de la entidad y los poderes de representación que permiten a las personas físicas actuar en nombre de las entidades legales. La recolección de información adicional a la expuesta en el *onboarding* digital de personas físicas puede suponer una complejidad extra en los procesos de *onboarding*, no solo porque añade otros pasos, sino además porque en muchos casos la documentación podría no estar en formato electrónico, lo que supondría un esfuerzo suplementario por parte de los clientes, así como de revisión por parte del banco o prestador de servicios financieros.

Para los interesados en el *onboarding* digital de personas legales, se recomienda la lectura del documento preparado por PWC para la Comisión Europea (Comisión Europea y PWC, 2018), identificado en el apartado “Literatura adicional”, ya que describe de forma detallada una serie de flujos de trabajo, mapas y atributos que podrían ayudar a entender este concepto con mayor detalle y que tiene como principales características las que se citan textualmente a continuación:

Los objetivos específicos del estudio SMART 2016/0094 son los siguientes:

- *Identificar las prácticas de embarque actuales, así como las mejores prácticas, incluyendo los requisitos legales de los Estados Miembros, las posibles directrices utilizadas y los requisitos reglamentarios de los organismos reguladores nacionales.*
- *Identificar dónde hay medios de cumplimiento comunes o divergentes, y dónde los procesos digitales podrían sustituir a los procesos no digitales existentes. Donde estos fueran considerados como no posibles, las razones por las que no se puede utilizar un proceso digital necesitan ser indicadas.*
- *Mapear los procesos físicos existentes frente a los digitales y los potenciales procesos digitales contra los niveles de garantía (LoAs) del eIDAS.*
- *Producir un flujo de proceso y un comentario de texto que ilustre el cumplimiento de los posibles procesos digitales frente a los requisitos reglamentarios específicos del sector.*

10. Visión desde el campo ofrecida por los expertos

Para la elaboración de este informe sobre *onboarding* digital se ha contado con el encomiable aporte de expertos³² de la región con los que se ha trabajado en forma conjunta a través de entrevistas, encuestas e informes relativos al proyecto.

Identificación de beneficios y riesgos del *onboarding* digital

Es prácticamente unánime la identificación de los principales beneficios del proceso por parte de los grupos de expertos:

- Genera eficiencias en la contratación.
- Favorece la inclusión financiera al lograr incrementar la penetración de los servicios en lugares remotos.
- Favorece el desarrollo y perfeccionamiento de los mercados, permitiendo un acceso abierto y eficiente a la contratación de productos y servicios.
- Incrementa la conveniencia para el usuario y abre la posibilidad de nuevos canales (dispositivos móviles) así como su disponibilidad, por ejemplo, las 24 horas, los siete días de la semana.
- Disminuye costos de transacciones para el usuario.

Principales barreras y riesgos detectados:

- Requiere de inversión por parte de las entidades financieras.
- Se pueden incrementar los riesgos relacionados con la seguridad de la información o con la privacidad de los ciudadanos.
- Se pueden incrementar los riesgos relacionados con temas de prevención de blanqueo de capitales y financiación del terrorismo (PBCFT).

---

³² Las instituciones expertas que han realizado sus aportes formales al estudio son las siguientes: Banco Central de Reserva y Superintendencia y Sistema Financiero del Gobierno (El Salvador); Secretaría de Hacienda y Crédito Público y Comisión Nacional Bancaria y de Valores (México); y gremios o asociaciones transnacionales como Federación Latinoamericana de Bancos (FELABAN), Federación Iberoamericana de Bolsas (FIAB), Alianza Fintech Iberoamérica (AFI), y American Business Dialogue (ABD).

Necesidades y preocupaciones en relación con la puesta en marcha de políticas públicas

De las reuniones virtuales y posteriores respuestas formales por parte de los grupos de expertos, se han extraído las principales necesidades y preocupaciones en relación con la puesta en marcha de las políticas públicas descriptas. Cabe destacar que se consignan por orden de importancia.

Buenas prácticas y regulaciones a nivel internacional

Es importante conocer los requerimientos técnicos, así como los organizativos, para poner en marcha proyectos o desarrollar políticas públicas.

Usabilidad/Experiencia del usuario

Se manifiesta el interés de prestar atención a sistemas reconocidos que sean fáciles de usar por parte de los ciudadanos. En este tema se puede incluir también la necesidad de que los sistemas respondan a su vez a los requerimientos no solo de prevención de lavado de activos, sino también a las necesidades legales en la contratación; y que se aproveche la oportunidad para agilizar los procesos de contratación como en los mercados de capitales, que actualmente tienen una alta complejidad por la cantidad de documentos distintos en los que se debe asegurar la integridad, autenticidad e identidad de los firmantes de los contratos.

Seguridad

Desarrollo de políticas que permitan eliminar la incertidumbre en cuanto a la seguridad del sistema económico del país, y que al mismo tiempo lo hagan más inclusivo. Describir el desarrollo de requisitos técnicos, organizativos o de certificación de las soluciones que permitan planificar el riesgo inherente en el canal en línea.

Tiempo de acceso al mercado y costos de las soluciones

Se solicita mejorar el tiempo de acceso al mercado para acortar el número de trámites y los tiempos en la contratación, y tener en cuenta el costo de los sistemas, pues la región, el sector y determinados casos de uso son muy sensibles a los costos de las operaciones.

Interoperabilidad

Se plantea la necesidad de que el desarrollo de las políticas sea interoperable entre las instituciones financieras y no se generen silos de información.

Privacidad

Se solicita que los sistemas puedan dar respuesta a la gestión segura y confiable de los datos de carácter personal de los ciudadanos.

Riesgo de las operaciones y limitaciones en transacciones monetarias

Se solicita contextualizar el tema del *onboarding* digital en el ámbito del enfoque de los procesos de conoce a tu cliente (KYC, por sus siglas en inglés, *Know Your Client*) y de su aproximación en riesgos, cómo impacta al riesgo de las operaciones, y si existen limitaciones, ya que en algunos países se pusieron en marcha iniciativas para el *onboarding* digital o la contratación remota de productos y servicios aunque con limitaciones en cuanto al riesgo de las operaciones: productos simplificados de bajo riesgo (auto, hogar) y productos con cuentas limitadas económicamente por montos. Es importante aclarar que el *onboarding* digital planteado es por primera vez equivalente a la identificación que se realiza en presencia, en la oficina bancaria, y que por su nivel de seguridad no tiene limitaciones en el riesgo de las operaciones o es limitado por montos.

Accesibilidad

Se solicita que el sistema no solo sea seguro y cumpla con la legislación para equipararlo al presencial, sino que también sea un instrumento que pueda llegar a un amplio sector de la población, no quedando excluido ningún colectivo o, habiendo riesgo de exclusión, que este sea el mínimo posible; por ejemplo, personas que no tengan acceso fácil a internet o a un dispositivo portátil o teléfono inteligente.

Armonización de conceptos

Existe una confusión importante sobre el fundamento de la identidad digital y muchos de sus componentes o sistemas desarrollados en el mercado, tales como el *onboarding* digital, la autenticación, la firma electrónica o digital, o conceptos como la identidad digital soberana.

Firmas electrónicas para el *onboarding* digital

No se entiende qué valor pueden proporcionar las firmas electrónicas en estos procesos, el nivel de seguridad y la confusión entre nombres (firmas electrónicas, digitales, simples) y la falta de penetración de estos instrumentos digitales.

Transversalidad y armonización del sistema

Se solicita que el proyecto describa cómo dar una respuesta al sector y de qué manera puede ser desarrollado para cualquier vertical dentro del sistema bancario y financiero (banca, Fintech, crédito, mercados de valores, seguros, pagos, etc.) a través de políticas públicas transversales en países con jerarquías complejas y fragmentadas en su alcance. El sistema debe de ser aplicable a cualquier entidad facultada para abrir cuentas en el sistema financiero. De nada sirve que los bancos adopten un estándar regional si existen “puertas traseras” en otro tipo de entidades (empresas de telecomunicaciones, Fintech, etc.)

Personas físicas y personas legales

Es deseable que el sistema pueda responder en base a requerimientos para el KYC o también para personas legales (*Know Your Business*).

11. Conclusiones y recomendaciones de política pública

En el presente apartado se presenta un conjunto de recomendaciones que pueden orientar a responsables de las políticas, reguladores y supervisores financieros de los países de América Latina y el Caribe (ALC), con el fin de permitir la implementación del *onboarding* digital en el sector financiero. El objetivo es poner de manifiesto los aspectos que deben tenerse en cuenta desde el punto de vista regulatorio y proporcionar criterios claros que puedan orientar las políticas de los gobiernos en esta área. Lo mismo sucede desde la perspectiva de la supervisión. Conviene señalar que en las presentes recomendaciones no se han tomado en consideración aspectos puramente técnicos, referidos a las tecnologías a utilizar, ni las particularidades de cada uno de los segmentos de negocio o verticales que existen en el ámbito financiero de la región. Lo anterior se ha desarrollado en el apartado 10 con algún nivel de detalle.

Las entrevistas mantenidas con reguladores y supervisores financieros de la región, actores del ecosistema Fintech, representantes de bolsas, mercados de capitales, sector bancario en conjunto con el análisis resultante de la investigación revelan los principales retos identificados para la implementación del *onboarding* digital en el sector financiero.³³ Si bien pueden existir diferencias en los marcos regulatorios aplicables en los distintos países de ALC, así como en las competencias o atribuciones de los respectivos organismos supervisores y reguladores en el sector financiero, las recomendaciones pretenden proporcionar criterios generales para tener en cuenta que sean de utilidad para los países de la región. Del mismo modo, se reconocen las diferencias en los procedimientos de abordaje para los diferentes sectores; por ejemplo, los contrastes y las necesidades diferentes para abrir una cuenta de ahorros o un contrato de comisión en una casa de bolsa. Teniendo en cuenta estos factores, no se pretende ser prescriptivos, sino más bien ofrecer alternativas para generar políticas públicas para el sector financiero, orientadas al *onboarding* digital.

Barreras al *onboarding* digital en ALC

A continuación se presentan de manera esquemática las barreras identificadas para la implementación del *onboarding* digital en la región desde una visión de política pública.

³³ Se agradece la participación y el apoyo de la Asociación de Supervisores Bancarios de las Américas (ASBA), la Federación Latinoamericana de Bancos (FELABAN) y la Federación Iberoamericana de Bolsas (FIAB) por su colaboración en la realización de entrevistas con actores del mercado. En particular, se reconoce el esfuerzo de los señores Pascual O'Dogherty, Giorgio Trettenero y Roberto Belchior.



Legales y reglamentarias

Hacen falta acuerdos, estándares y lineamientos supranacionales en materia de *onboarding* digital que orienten la discusión y permitan tomar decisiones a los organismos de regulación y supervisión financiera nacionales. El *onboarding* digital debería ser un tema clave de política pública, tal y como lo ha demostrado la pandemia de COVID-19, por ser un habilitador al acceso y uso de servicios financieros como los pagos o el crédito. Asimismo, la visión se debe compadecer con un sistema financiero que es cada vez más intensivo en tecnología y por necesidad basado en transaccionalidad remota y digital. La consecuencia de esta carencia es, por una parte, el temor de adoptar enfoques regulatorios y de política pública locales que eventualmente deberían modificarse en el futuro en caso de la aparición de estándares con potenciales efectos sobre los costos regulatorios. Por otra parte, la multiplicidad de enfoques en las regulaciones nacionales hace difícil la movilidad entre jurisdicciones para involucrados y entrantes.



Culturales

En muchas de las jurisdicciones de la región existe la percepción de que la identificación de las personas depende de un sistema centralizado y gubernamental de identificación personal. En el caso de las empresas, se tiene la percepción de que únicamente el sistema de administración de impuestos es válido para identificarlas. Algo similar ocurre con la tecnología de firma electrónica, que fue muy popular en las primeras décadas de este siglo. Como se ha comentado y se comentará más adelante en la sección de oportunidades, existen mecanismos alternativos de identificación que permiten llevar a cabo un proceso completo y suficiente, similar al presencial.



Tecnológicas

El *onboarding* digital es un proceso intensivo en tecnología. Se requiere de inversión de capital por parte de las entidades y de las autoridades financieras. Las entidades deben disponer de sistemas tecnológicos robustos, documentados y testeados que permitan realizar de forma segura la identificación del cliente, así como la autenticación. Ello requiere llevar a cabo procesos de verificación de la identidad, análisis de riesgos de las operaciones, y también el registro de los procesos de identificación.

Por ejemplo, es necesario tener procedimientos para la grabación y el almacenamiento de las videollamadas o sistemas de identificación remotos realizados, las verificaciones de la autenticidad de los documentos identificativos aportados (tales como el documento de identidad), y los controles o cotejos de información con fuentes alternativas de datos, como registros públicos o privados. Para ello debe utilizarse tecnología con una alta capacidad de procesamiento, tratamiento y almacenamiento de la información durante el periodo de tiempo exigido por la normativa correspondiente (usualmente suele ser como mínimo de cinco años), lo que puede resultar costoso especialmente en entidades o mercados de pequeña escala.

Por otra parte, los supervisores financieros también requerirán llevar a cabo ajustes tecnológicos que les permitan ejercer sus facultades en materia de identificación de los consumidores financieros y de exámenes prudenciales a entidades financieras. Esto se relaciona con la práctica de supervisión sobre los sistemas de *onboarding* que adopten las instituciones financieras, y también con sus propias facultades administrativas y de protección del consumidor.

Finalmente, hay que señalar que la tecnología deberá ser adoptada por más instituciones que las entidades y autoridades financieras. Debe existir un ecosistema completo en el que posiblemente haya una decisión de país de avanzar en la identificación de las personas, involucrando otras autoridades distintas a las financieras y a los proveedores de servicios de la industria financiera, entre otros.



De adopción

Algunos mecanismos utilizados para realizar la vinculación digital de usuarios de servicios financieros son confusos, lentos o difíciles de utilizar, lo cual obstaculiza y disminuye la efectividad y el número de transacciones digitales. El tiempo requerido en los procesos y la necesidad de realizar algunos trámites presenciales también puede actuar como limitante. Algunos sistemas de identificación, como la firma electrónica, no tienen presencia suficiente en ciertos países de ALC, por temas de costo o por falta de claridad en cuanto a su plena validez jurídica. Esto hace que los usuarios no perciban de forma clara las ventajas asociadas a su uso. Aun así, será fundamental el trabajo con las habilidades digitales de los consumidores financieros, especialmente aquellos en condición de vulnerabilidad, grupos minoritarios y tercera edad.



De interoperabilidad

La ausencia de una identidad digital reconocida para las transacciones electrónicas supone que el consumidor financiero debe llevar a cabo un proceso de vinculación digital por cada empresa o servicio financiero al que desea acceder. Esto resulta poco eficiente y puede limitar el acceso a servicios financieros y la inclusión de los sectores más desfavorecidos de la población. La arquitectura tecnológica de los estándares de *onboarding* digital es a menudo cerrada, lo que contribuye a crear silos de información dentro de cada una de las entidades. La existencia de soluciones interoperables que puedan integrarse en los sistemas de distintas entidades permitiría optimizar los procesos y contribuiría a la consecución de los objetivos de desarrollo sostenible, al garantizar el acceso de poblaciones vulnerables a los recursos y reducir los costos de las remesas.



De dificultad de identificación de las personas legales

Cuando los clientes financieros son personas jurídicas, el proceso de identificación no presencial resulta en general más complejo que para las personas naturales o físicas. Usualmente, para la identificación de las personas legales se requiere el nombre legal, el identificador único y la dirección. Además, se suelen requerir otros datos, tales como el número de referencia fiscal, el número de clasificación industrial o económica, o el identificador legal de identidad. Asimismo, es necesario identificar los distintos beneficiarios de la entidad y acreditar los poderes de representación y la identidad de las personas físicas que pueden actuar en nombre de las entidades legales. La principal barrera se constituye en la digitalización de la documentación, así como en la posibilidad de verificar la información con registros públicos como registros de sociedades, de compañías o de comercio.



De coordinación

Desde el punto de vista de política pública, la intersección entre tecnología, identidad y servicios financieros hace que al menos tres tipos de entidades públicas tengan que intervenir en la toma de decisiones. Por una parte, están presentes las autoridades encargadas de las tecnologías de información desde la perspectiva de infraestructura, políticas públicas para la adopción digital de la población y habilitación de las tecnologías para la identificación y digitalización de datos.

Otras autoridades que participan en el tema del *onboarding* digital son las de identificación o registro civil para el caso de personas naturales, pero también aquellas que llevan los registros de empresas e incluso las autoridades impositivas. Por último, están las autoridades financieras, los reguladores y los supervisores.

La coordinación entre estos tres tipos de autoridades puede ser compleja por las definiciones de sus facultades y atribuciones legales y por las intersecciones que se pueden dar entre los sectores, generando "zonas grises" que impiden la adecuada definición de las políticas públicas encaminadas al *onboarding* digital. Sin embargo, esta barrera se convierte para los sectores públicos de la región en una oportunidad para actuar de manera conjunta con políticas nacionales y regionales que habiliten los servicios financieros.

Propuestas de política pública

Como ya se ha señalado, existen diversos factores que pueden actuar como barreras para los procesos de abordaje digital en los países de ALC. Los gobiernos, los reguladores y los supervisores financieros pueden promover acciones o medidas de política pública que faciliten estos procesos y permitan aprovechar las oportunidades que existen. A continuación se señalan algunas:



Legales y reglamentarias

Ante todo, debe existir la apertura y la voluntad política y de colaboración entre agencias para desarrollar políticas públicas que habiliten las tecnologías, los procesos y la digitalización documental, entre otros aspectos. En este orden se recomiendan acuerdos entre agencias gubernamentales que atiendan problemas puntuales, como por ejemplo la identificación de los consumidores financieros que son personas naturales (o morales, según la jurisdicción). Con base en esos acuerdos, se podrán pactar condiciones técnicas y financieras que deriven en actos administrativos según las competencias de las entidades para permitir, siguiendo el ejemplo, la identificación de este tipo de clientes.

En cuanto a los métodos de identificación, la regulación debería ser capaz de permitir el uso de métodos complementarios de identificación que complementen a los documentos nacionales o federales, en caso de que existan. Si la jurisdicción carece de documentos centralizados de identificación, un conjunto de documentos podría servir como prueba de la existencia de la persona y de que es quien dice ser. Como es de esperarse, estos documentos deben estar digitalizados y corresponder a un acuerdo de industria y de autoridades para cumplir con los requisitos de conocimiento del cliente, como mínimo.

En este sentido, y sobre la base de un consenso entre agencias gubernamentales e industrias, se podrían utilizar para la identificación de los consumidores financieros fuentes de información alternativas, tales como licencias de conducir, credenciales electorales, etc., que individualmente o en conjunto sumen datos suficientes que permitan verificar la identidad y los datos de residencia, por ejemplo.

A este respecto, se recomienda la utilización de todos los repositorios de identidad que permitan probar la existencia de una persona física o legal. Para ello se debería generar una política pública que facilite el acceso remoto a las bases de datos gubernamentales permitiendo el cotejo de los documentos oficiales de identidad, así como la verificación de la autenticidad de las actas constitutivas de las sociedades, los poderes y documentos que obran en los registros públicos de comercio, como el nombre de los accionistas y socios. Además, se debería facilitar el acceso a otras bases de datos públicas tales como registros fiscales, de seguridad social y de subsidios, o ayudas de gobierno (específicamente para el caso de las empresas).

Finalmente, y de manera similar a las plataformas de puntaje crediticio alternativo, se recomienda explorar la realización de validaciones adicionales utilizando bases de datos privadas, tales como cámaras de comercio, bureaus de crédito, compañías de telecomunicaciones, proveedores de energía y otros prestadores de servicios. Incluso recibos de servicios públicos o bancos y registros de pagos de impuestos pueden resultar útiles a la hora de verificar la existencia de la persona.

Para concluir, la política pública podría incluir también la combinación de métodos tradicionales de verificación con otros basados en tecnologías digitales, lo cual permitiría complementar la verificación de la identidad basada en documentos con una verificación basada en datos. Por ejemplo: el proceso de abordaje digital de un cliente podría consistir en: i) la identificación personal mediante la presentación del documento de identidad nacional, electoral o la licencia de conducir; ii) un video de la persona exhibiendo el documento identificativo a través de medios electrónicos; iii) la verificación de información de cuentas bancarias, registros de seguridad social y registros de subsidios del Gobierno, y iv) la certificación laboral o de ingresos y otros.

En línea con lo anterior, la validación de la identidad podría realizarse utilizando diversos elementos como:

- Atributos digitales como los asociados al dispositivo utilizado para la conexión (tipo de dispositivo, momento de conexión, duración, etc.), dirección de correo electrónico, perfil en redes sociales, teléfono celular u otros.
- Datos comportamentales, dinámicos o basados en conocimiento, como los asociados a la actividad en internet o redes sociales del usuario.

- Datos estáticos, como los contenidos en un documento oficial de identidad.
- Datos biométricos o de reconocimiento facial.
- Documentos.



Consenso con la industria: innovaciones regulatorias

Parte de la política pública debe consistir en analizar las prácticas de la industria en relación con el *onboarding* digital; los procedimientos empleados, las tecnologías (tales como inteligencia artificial [IA], aprendizaje automático, análisis de datos, cómputo en la nube, *Blockchain*) con el fin de identificar los riesgos y oportunidades asociados a su uso. A esos efectos podrían ponerse en marcha iniciativas tales como oficinas o *hubs* de innovación, o la realización de pruebas en el marco de *sandboxes* regulatorios. La utilización de nuevas tecnologías permite realizar un seguimiento comportamental de los clientes (a través de la navegación, geolocalización, etc.), lo que reporta enormes ventajas. Por un lado, las entidades pueden analizar la transaccionalidad de los clientes y orientar su oferta de productos o servicios a las necesidades de cada uno de ellos. Por otro, permite un seguimiento dinámico del riesgo, no solo en el momento de la contratación de un producto sino en la relación con el cliente en general, lo que es más eficiente a los efectos de detectar operaciones fraudulentas. La realización de pruebas en el marco de un *sandbox* serviría para orientar opciones de política pública o regulaciones que puedan facilitar el abordaje digital de los clientes de forma segura y con las máximas garantías.



Interoperabilidad

Se recomienda promover y facilitar la interoperabilidad tecnológica, permitiendo la utilización de sistemas abiertos para evitar que se creen silos de información. La arquitectura tecnológica de los estándares de *onboarding* digital debe ser abierta, con neutralidad tecnológica e interoperabilidad, de forma que se facilite la integración de sistemas de distintas entidades, permitiendo simplificar los procesos de vinculación digital de los clientes.



Colaboración público-privada

Aunque se ha mencionado de manera implícita anteriormente, la política pública debe buscar promover la colaboración entre las autoridades públicas (reguladores y supervisores financieros) y el sector privado (entidades bancarias, intermediarios financieros, operadores del mercado de capitales, bolsas, aseguradoras, entidades Fintech, operadores de tecnología) a fin de definir los estándares mínimos que puedan resultar eficientes desde el punto de vista de los costos para las entidades, y garanticen un adecuado nivel de confianza.



Coordinación interinstitucional entre agencias del Estado

La política pública debe promover la comunicación y coordinación de los supervisores financieros (bancarios, de valores, seguros, pensiones) con los reguladores y las autoridades públicas a cargo de la protección de datos, la protección del consumidor, la competencia y la seguridad nacional, con el objetivo de garantizar que las entidades que utilizan tecnologías innovadoras cumplan con las leyes y los reglamentos aplicables. Asimismo, se recomienda promover iniciativas entre supervisores financieros, autoridades responsables de la identidad nacional (como registro civil, registro de votantes u otros) y organismos responsables de la vigilancia y prevención de operaciones de lavado de activos y financiamiento del terrorismo (PBCFT), como Unidades de Inteligencia Financiera (UIF) u otros, con el fin de habilitar procesos tecnológicos para la identificación de los clientes, que cumplan con las normas de Diligencia Debida y Conocimiento del Cliente, y de la PBCFT.



Mejoramiento de la capacidad institucional de los supervisores y reguladores financieros

Para comprender y supervisar los riesgos asociados a las nuevas tecnologías y los modelos de negocio innovadores, son necesarios tres ejes principales:

- **Recursos humanos:** las autoridades deben contar con funcionarios capacitados en el uso de tecnologías emergentes y ciberseguridad, entre otros. En algunos casos quizás necesiten incorporar personal con habilidades específicas que complementen los conocimientos y las experiencias existentes. También sería recomendable evaluar los programas de capacitación vigentes con el fin de incorporar formación especializada en tecnologías emergentes.
- **Tecnología:** se requiere de tecnología que permita a las autoridades verificar las prácticas de la industria, crear consensos sobre las metodologías aplicables para la identificación y, en ocasiones, verificar directamente la identidad de las personas. En caso de que se considere la realización de pruebas en el marco de un *sandbox* regulatorio, es necesario disponer de tecnología para la realización de pruebas de penetración y controles de ciberseguridad y para el envío y recepción de información de las entidades que operen en el *sandbox*, como mínimo.
- **Organización o arquitectura institucional:** es preciso que las entidades de supervisión financiera creen instancias (departamentos, delegaciones, divisiones u otros) y asignen recursos personales y materiales para la supervisión de las innovaciones tecnológicas. Sin embargo, es importante reconocer, como se vio anteriormente, que la mayoría de las autoridades financieras de la región cuentan con arquitecturas institucionales que permitirían el avance del *onboarding* digital en el futuro.



Coordinación y cooperación internacional

Dado que la internacionalización de las operaciones en el sector financiero es cada vez más frecuente, resulta necesario avanzar hacia principios o estándares comunes. Mientras las autoridades supranacionales progresan en estos consensos, la prioridad es trabajar con lo que se tiene disponible a nivel local en materia de regulación y, mediante acuerdos transfronterizos, lograr consensos en la supervisión. En lo que se refiere a la identidad digital no existen todavía tratados internacionales de reconocimiento, aunque hay iniciativas muy avanzadas en el ámbito de la Unión Europea, como la regulación eIDAS. Si bien ALC está aún lejos de una identidad digital única, sí podrían promoverse mecanismos de cooperación multilateral en el ámbito de la supervisión financiera que permitan compartir experiencias, mejorar prácticas y analizar de forma conjunta los riesgos y oportunidades asociados al uso de las nuevas tecnologías (Herrera y Vadillo, 2021).

Riesgos asociados a las políticas públicas

Por último, resulta apropiado señalar que existen riesgos asociados a las potenciales políticas públicas que se mencionan en este estudio como alternativas para solucionar las brechas en cuanto al *onboarding* digital. A continuación se señalan algunos:



De privacidad y manejo de datos de individuos y empresas

Los operadores financieros manejan gran cantidad de datos personales de sus clientes (información laboral, financiera, fiscal, civil, transaccional, patrimonial) que están sujetos a requerimientos muy exigentes en materia de protección de datos, privacidad y seguridad de la información. La utilización de tecnologías para captura, manejo, tratamiento y almacenamiento de la información puede simplificar los procesos, pero requiere que las entidades cuenten con una estrategia de tratamiento de datos y de seguridad de la información que asegure el cumplimiento de la normativa aplicable. Para ello, las entidades deben diseñar e informar sobre las políticas de tratamiento, control y uso de datos, y definir de forma clara las responsabilidades frente a la protección de datos. Esto impone la necesidad de una regulación clara, que en muchos países aún no existe, lo que representa otro desafío en términos de *onboarding* digital. En el caso de la prestación de servicios por parte de terceros, es necesario establecer procedimientos que permitan la supervisión de las actividades llevadas a cabo por ellos, y atribuir de forma clara las responsabilidades de cada una de las partes. Este tipo de relaciones contractuales también debe definirse de manera simple en la regulación correspondiente.



De seguridad de la información

Es necesario que los procedimientos utilizados para el abordaje de los clientes cumplan con los más altos estándares internacionales en términos de prevención frente a ciberataques, protección de la información y manejo de los datos de los clientes de acuerdo con las respectivas legislaciones nacionales. La tercerización de actividades en empresas especializadas en tecnología puede resultar más eficiente y permitir un aumento de costos, pero también puede incrementar los riesgos en materia de ciberseguridad, en caso de que no se establezcan controles y procedimientos de supervisión adecuados.



De lavado de activos

Es necesario que las tecnologías empleadas y los procedimientos de debida diligencia de los clientes (CDD) permitan identificar quién es el titular real y beneficiario de las operaciones, así como comprender la estructura de control de la sociedad, en caso de operaciones con personas morales. Asimismo, los procesos utilizados deben investigar y, cuando corresponda, obtener información sobre el carácter, el propósito y el objetivo de la relación comercial del cliente con el fin de prevenir conductas fraudulentas o la utilización para fines delictivos.

Conclusiones finales



La pandemia de COVID-19 ha transformado de forma radical los hábitos de los ciudadanos del mundo entero, que se han visto forzados a realizar de forma remota actividades que antes se hacían de manera presencial.

Ello ha puesto de manifiesto la necesidad inmediata de buscar canales alternativos, no presenciales sino remotos, que permitan a los consumidores acceder a crédito, pagos y todo tipo de productos y servicios financieros. Los sistemas de identificación digital tienen el potencial de mejorar la confiabilidad, seguridad, privacidad, conveniencia y eficiencia de la identificación de los clientes en la provisión de servicios financieros, beneficiando tanto a los consumidores como a las entidades que prestan u ofrecen servicios financieros, y al sistema financiero en su conjunto. La digitalización del proceso de abordaje de los clientes tiene numerosas ventajas para las instituciones financieras: simplificación de los procesos operativos, reducción de errores humanos en procesos manuales de control, ahorro de costos, y mejoramiento del monitoreo de las transacciones, al tiempo que facilita el acceso a una base de clientes más amplia, lo que contribuye a la inclusión financiera de sectores más desfavorecidos de la población. Para los consumidores financieros es indudable que la digitalización puede reportar enormes ventajas, permitiendo el acceso a servicios financieros en cualquier momento, desde cualquier lugar.

Desde la perspectiva de los riesgos, el principal reto de la digitalización es la confiabilidad del sistema que depende en última instancia de la fortaleza de los documentos, procesos, tecnologías y medidas de seguridad empleados para la prueba de identidad, uso de credenciales, autenticación y seguimiento de las transacciones. El riesgo de ciberseguridad requiere implementar medidas adecuadas, salvaguardas y sistemas de gobernanza y rendición de cuentas robustos.

El avance hacia una digitalización de la economía es hoy una necesidad y el sector financiero no es ajeno a ello. El *onboarding* digital puede ser una solución que permita avanzar en la inclusión financiera de la población, al tiempo que facilite el acceso a nuevos productos y servicios financieros digitales de forma más eficiente. Los gobiernos y los responsables de las políticas pueden contribuir en este sentido mediante la adopción de políticas que faciliten y promuevan el uso de las tecnologías, dentro de un marco ordenado, con garantías suficientes que salvaguarden de forma adecuada los derechos de los consumidores financieros.

Si bien es posible que esta visión no sea necesariamente exhaustiva, es el resultado de la interacción con la industria. Queda claro que la peor política pública es no tenerla, sobre todo en el caso del acceso a los servicios financieros, tal como ha demostrado la pandemia de COVID-19.

Referencias

- AFI (Alianza Fintech Iberoamericana). 2019. Libro Blanco de la Identidad Digital. Alianza Fintech Iberoamericana.
- BID y Finnovista. 2019. Fintech: América Latina. De próxima publicación.
- Bundesamt für Sicherheit in der Informationstechnik-BSI. Guía Técnica TR-03147.
- Bundesgesetzblatt. 2019. Identification Ordinance. IVO.
- Comisión Europea. 2017. EIDAS Regulation (Regulation [EU] N.º 910/2014). FUTURIUM. Disponible en: <https://ec.europa.eu/futurium/en/content/ei-das-regulation-regulation-eu-ndeg9102014>.
- Comisión Europea y PWC. 2018. Study on eID and digital onboarding: mapping and analysis of existing on-boarding bank practices across the EU. Disponible en: <https://op.europa.eu/en/publication-detail/-/publication/8-da08249-49cd-11e8-be1d-01aa75ed71a1/language-en>.
- Demirgüç-Kunt, A. et al. 2018. Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution. Washington, D. C.: Banco Mundial.
- EURO LEX. 2000. Directiva 2000/31/CE: Comercio electrónico en la Unión Europea. Disponible en: <https://eur-lex.europa.eu/legal-content/ES/TX-T/?uri=LEGISSUM%3AI24204>.
- Federal Financial Supervisory Authority. BaFIN. Circular 3/2017 (GW).
- Financial Services Commission. FSC plan de onboarding digital. Grupo Acción Financiera Internacional (GAFI/FATF). 2020. Guidance on Digital Identity. Disponible en: <http://www.fatfgafi.org/publications/fatfrecommendations/documents/consultation-digital-id-guidance.html>.
- Herrera, D. y S. Vadillo. 2021. Sandbox regulatorio multi-jurisdiccional para América Latina y el Caribe. Washington D. C.: Banco Interamericano de Desarrollo. Disponible en: <https://publications.iadb.org/publications/spanish/document/Sandbox-regulatorio-multi-jurisdiccional-para-America-Latina-y-el-Caribe.pdf>.
- Horizon. 2020. Titanium: Tools for the Investigation of Transactions in Underground Markets. Unión Europea e INTERPOL. Disponible en: <https://www.interpol.int/es/Quienes-somos/Marco-juridico/Information-communications-and-technology-ICT-law-projects/Project-Titanium>.

ISO/IEC. 29115:2013 Information Technology. Security techniques. Entity authentication assurance framework.

Jiménez, P. M. 2019. Manejo de datos y privacidad - Identidad soberana: El camino hacia una red segura. Digital Biz. Disponible en: <https://www.digitalbizmagazine.com/manejo-de-datos-y-privacidad/>.

Millán, A. 2020. Coronavirus y economía: por qué la pandemia ha llevado a millones de latinoamericanos a abrir una cuenta de banco (y cómo puede ayudar a la recuperación). BBC News Mundo. Disponible en: <https://www.bbc.com/mundo/noticias-america-latina-54296617>.

Minsait Payments. 2020. X Informe de Tendencias en Medios de Pagos 2019-20. Indra Company.

Nabalón, I. 2020. Identidad digital: desbloqueando un efecto multiplicador del PIB en España. IE Public Gov Tech Lab.

White, O. *et al.* 2019. Report: A key to inclusive growth. McKinsey Global Institute.

Anexo 1. Metodología utilizada para el análisis

Se describe a continuación la metodología utilizada para realizar el estudio comparativo. Se utilizará una matriz para identificar los conceptos que figuran en la imagen A1.1.

Imagen A1.1. Matriz de análisis comparativo

DESCRIPCIÓN REQUERIMIENTO		Normativa	Guías Base	Estadística
Tema Onboarding Digital	Requerimientos técnicos y organizativos de la Verificación de la Identidad de cliente	Identificación de Normativas		
		Control exclusivo de la grabación del video		
Verificación de la Identidad de cliente	Tipos de Requerimientos	Descripción de Requerimientos		
		Datos de análisis y comparativos		

Fuente: elaboración propia.

Tema onboarding digital

Ejemplos: i) verificación de la identidad; ii) origen de los fondos; iii) chequeos antifraude, iv) privacidad, etc.

Tipos de requerimientos

Describen en detalle cada uno de los requerimientos que son comunes en las normativas identificadas, llevando la descripción al detalle. Ejemplos: i) verificación de la autenticidad del documento nacional o pasaporte; ii) custodia de la información, iii) gestión de los datos de carácter personal, etc.

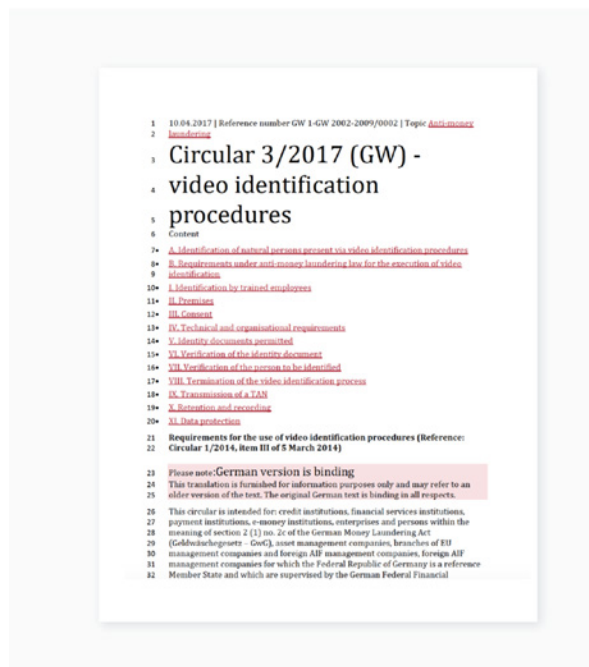
Tipos de requerimientos

Describen en detalle cada uno de los requerimientos que son comunes en las normativas identificadas, llevando la descripción al detalle. Ejemplos: i) verificación de la autenticidad del documento nacional o pasaporte; ii) custodia de la información, iii) gestión de los datos de carácter personal, etc.

Identificación de normativas

En las columnas de la matriz se identifican por orden alfabético cada una de las normativas encontradas en el estudio inicial. Se enlazan las normativas a un documento que se ha traducido al español y al que se ha incorporado el número de líneas, para más tarde poder realizar una referencia concreta en la presente matriz.

Los documentos traducidos y numerados están actualizados y enlazados en la matriz de resultados del análisis comparativo, anexo I.



Datos de análisis y comparativos

En el campo de datos de la matriz, el trabajo se realizará identificando cada requerimiento y cómo este se cumple en cada normativa. Ejemplo: el requerimiento se identifica en las líneas 64-69 del artículo 25 de la Ley 10/2010 y el artículo 39 de la Ley 10/2010.

Además, en el campo de datos se realizará un código de colores de cómo cada normativa cumple con los requerimientos:

- **Color verde:** cumple con el requerimiento.
- **Color amarillo:** cumple parcialmente con el requerimiento.

Con el análisis completo se obtendrá:

- Una fuente fiable y contrastada de información sobre temas y requerimientos comunes extraídos al revisar minuciosamente la regulación específica en materia de *onboarding* digital.
- La identificación de buenas prácticas de seguridad comunes.

Resultados del análisis

Los resultados del análisis se han incluido en la matriz del estudio (anexo: Matriz análisis comparativo). El detalle de las buenas prácticas de seguridad comunes se describe ampliamente en el apartado “Recomendaciones para que los reguladores implementen el *onboarding* digital en sus jurisdicciones”.

DESCRIPCIÓN REQUERIMIENTO	
Verificación de la identidad del cliente	El cliente debe ser capaz de verificar su identidad de forma segura y confiable.
	El cliente debe ser capaz de verificar su identidad de forma segura y confiable.
	El cliente debe ser capaz de verificar su identidad de forma segura y confiable.
	El cliente debe ser capaz de verificar su identidad de forma segura y confiable.
Verificación de la autenticidad del contenido de la identidad	El cliente debe ser capaz de verificar la autenticidad del contenido de la identidad.
	El cliente debe ser capaz de verificar la autenticidad del contenido de la identidad.
	El cliente debe ser capaz de verificar la autenticidad del contenido de la identidad.
	El cliente debe ser capaz de verificar la autenticidad del contenido de la identidad.
Verificación de la integridad de la información	El cliente debe ser capaz de verificar la integridad de la información.
	El cliente debe ser capaz de verificar la integridad de la información.
	El cliente debe ser capaz de verificar la integridad de la información.
	El cliente debe ser capaz de verificar la integridad de la información.
Verificación de la privacidad de la información	El cliente debe ser capaz de verificar la privacidad de la información.
	El cliente debe ser capaz de verificar la privacidad de la información.
	El cliente debe ser capaz de verificar la privacidad de la información.
	El cliente debe ser capaz de verificar la privacidad de la información.

Conclusiones del análisis



El *onboarding* digital es una realidad a nivel internacional.

Existen 14 normativas en vigor que describen en detalle los requerimientos de los sistemas permitidos, así como otros requerimientos técnicos y de buen gobierno necesarios para su adopción por parte de los bancos y prestadores de servicios financieros.



El *onboarding* digital es un proceso consolidado.

Desde la aparición de la primera circular del BaFIN en Alemania en 2014 se ha observado un importante desarrollo del *onboarding* digital por parte de los reguladores. Se estima que antes de finalizar el año 2020 el *onboarding* digital será una realidad aplicada al menos en 38 países y cuatro regiones³⁴ del mundo (AFI, 2019).



El conjunto de buenas prácticas comunes extraídas de las normativas analizadas ha ayudado a establecer un conjunto de requerimientos técnicos y de buen gobierno que se detallan en este estudio. **Este conjunto de requerimientos puede ayudar al fomento de políticas públicas y al establecimiento de resoluciones en forma de circulares o autorizaciones por parte de reguladores del sector financiero** que permitan la puesta en marcha del *onboarding* digital por parte de bancos y prestadores de servicios financieros en sus jurisdicciones.

³⁴ <http://fintechiberoamerica.com/wp-content/uploads/2019/11/Libro-Blanco-IberoAmericano-para-la-Identidad-Digital.pdf>.