FINTECH
IBEROAMÉRICA

LIBRO BLANCO IBEROAMERICANO DE LA

Identidad Digital.

Septiembre 2019

1. Introducción

La gestión de la Identidad Digital es una pieza clave en el sector financiero, especialmente cuando las iniciativas tienen una base electrónica y se fundamentan en procesos digitales.

Su adopción se fundamenta en la seguridad necesaria para hacer los negocios y cumplir con la regulación, al mismo tiempo que en las nuevas capacidades que crean en nuestros negocios para mejorar la vida de nuestros clientes y puedan contratar más y mejor con nuestra compañía. Ambas cosas: la seguridad y las oportinandes de negocio son sus impulsores.

Las nuevas tecnologías de identificación electrónica, en concreto: la identificación remota de clientes, la autenticación biométrica y las nuevas firmas electrónicas avanzadas y cualificadas están comenzando a cambiar las reglas del juego en el sector financiero en otras regiones. La Alianza Fintech de IIberoamérica (AFI) considera que es un buen momento para que nuestra región tome conciencia de los cambios y aproveche la oportunidades que impulsaran el sector, mejorando la inclusión financiera y la economía.

Este documento provee información sobre la definición de identidad digital así como describe un conjunto de buenas prácticas internacionales, requerimientos normativos estándar y otra serie de consideraciones, que serviran de guía base para el desarrollo del concepto de la identidad digital en las empresas financieras emergentes de base tecnológica o Fintechs.

a. Objetivos del documento

Los principales objetivos de este documento son los siguientes:

- Que la comunidad iberoamericana de tecnología financiera (Fintech) pueda aprovechar los beneficios que plantea el uso de las nuevas tecnologías de identidad digital y que tenga una gúia para implantaras de forma adecuada y según la normativa vigente.
- Para las instituciones y reguladores financieros locales de cada país: con el objetivo de que tomen conciencia de las buenas prácticas y regulaciones pioneras en otros países y regiones. El objetivo es que puedan adelantarse en la regulación haciendo acopio de ellas, favoreciendo así la inclusión financiera y el fomento de la innovación en el sector financiero. Cómo consecuencia se obtendrá una mejora en la economía de cada país.
- Recopilar las mejores prácticas internacionales en relación con la creación de sistemas públicos de identidad digital a efecto de informar las políticas a ser adoptadas por los países de Iberoamérica. Su intención es aportar a la investigación que deben hacer las autoridades locales y los organismos regionales previo a la implementación de sistemas de identificación digital estatales y atender los retos que deben sortearse en su diseño.

2. Definición de Identidad Digital

La Identidad Digital es el Alter Ego Electrónico de una persona y toda la información y atributos relacionada con la misma. Toma especial relevancia en un contexto de estilo de vida cada vez más digital y donde la confianza es clave va a la hora de construir relaciones.

Su gestión se define como el proceso de crear, mantener y eventualmente destruir identidades personales de los individuos. La identificación de clientes, la autenticación, la gestión de sus datos en la contratación son actividades fundamentales para lograrlo.

Uno de los retos asociados a la identidad digital viene de garantizar confianza en las transacciones en un medio como Internet, que por su naturaleza no lo hace. Otro de los retos es evitar el uso fraudulento o delictivo de la misma, así como garantizar derechos como la privacidad donde de nuevo, por la naturaleza electrónica y la posibilidad de una memoria perdurable en el tiempo de este medio, puede desembocar en perjuicio para las personas.

a. Identificación Vs Autenticación.

Es importante diferenciar estos dos conceptos, pues a veces dan lugar a confusión.

La **identificación es el proceso de garantizar que la persona es quien dice ser**. El proceso comienza el día en el que el cliente inicia su relación con una Institución Financiera (IF) y se prologa durante su ciclo de vida hasta que la persona deja de utilizar sus servicios. Cómo le registramos, cómo le vamos conociendo en el tiempo, cómo contrata y consume nuestros servicios forma parte de un proceso continuado donde vamos conociendo al cliente e intentamos construir una relación de mutuo beneficio. En el argot del cumplimiento normativo y negocio financiero este proceso es conocido como *Know Your Customer* (KYC).

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

Un ejemplo para ilustrar la diferencia entre estos conceptos:

Pongámonos en situación: una persona se compra un teléfono inteligente iPhone modelo X, que incorpora la última tecnología biométrica facial. El usuario activa el servicio Apple Pay para incluir una de sus tarjetas de crédito expedidas por su banco habitual. Esto facilitara los pagos en tiendas minoristas, tales como: tiendas de ropa, cafeterías, clínicas, etc…

Comenzamos por la autenticación: la estrategia de autenticación de Apple es una estrategia multi-factor. No ha cambiado desde primeros modelos ya que basa su seguridad en un primer factor que es la contraseña para acceder al *smartphone*. Cuenta además con un segundo factor biométrico, que es el factor biométrico facial (tecnología denominada FaceID). Cuando el usuario compra su terminal, lo abre y se registra

selecciona una contraseña para su acceso y registra su cara en el FaceID. Ambos registros quedan grabados de forma segura en el terminal. Las aplicaciones utilizan el sistema operativo y esta estrategia de seguridad combinando estos dos factores. Apple y por extensión todo su ecosistema de desarrolladores conoce que la persona que compro el teléfono es quien accede a las aplicaciones con una alta probabilidad, pero ¿conocen la identidad de la persona? Y la respuesta es que por solo estos métodos no. Lo que pueden garantizar con estos métodos de autenticación es que la persona que se registro inicialmente accede al teléfono y a sus aplicaciones, pero no conocen la identidad de la persona.

Cuando el usuario quiere activar su servicio Apple Pay (*e-wallet*) es por temas de confianza y cumplimiento normativo cuando Apple y sus socios financieros tendrán la necesidad de identificar inequívocamente al cliente. ¿Y como lo hacen? Pues todo se hace enlazando una cadena de confianza que tiene su origen en que la IF, dentro de sus procesos KYC y previo a 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 Apple permite al usuario activar el servicio Apple Pay a través de su tarjeta de crédito es cuando existe una vinculación entre una persona registrada inicialmente (no necesariamente conocida) y la confianza en la identidad que proviene de la IF y que por motivos regulatorios ha tenido que conocer la identidad real del cliente previamente. En todo este proceso esta presente la identificación.

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

¿Por qué la autenticación? La respuesta también es sencilla: por seguridad. La seguridad necesaria de conocer que las personas que supuestamente realizan las operaciones en el día a día son quienes dicen ser.

Como veremos más adelante en este artículo, en el sector financiero la combinación de un proceso continuado de identificación y una estrategia segura de autenticación son claves para la relación con nuestros clientes.

3. Buenas Prácticas, Tecnología y Normativa en Identificación Remota de Clientes.

a. Antecedentes de la identificación remota de clientes

Hasta la llegada de la primera normativa en el mundo que se liberó en Alemania en 2014, la única forma de identificar a un cliente con todas las garantías que requiere la contratación de alto riesgo o la apertura de cuentas en el sector financiero se realizada en presencia, cara a cara en la oficina comercial de la Institución Financiera (IF).

Esta normativa, que permitió a las IFs identificar a los clientes digitalmente y de forma remota por una entrevista por videoconferencia, marca un antes y un después en las relaciones a distancia por el canal digital. El proceso consiste en una entrevista que realiza un agente entranado, con el cliente: durante la entrevista el agente verifica la identidad a través de un documento expedido por un estado miembro (tarjeta de identidad o pasaporte). Se verifica la autencidad del documento a través de las medidas de seguridad, valida que la persona esta viva y que su identidad corresponde con la del documento. La entrevista se graba como principal evidencia de este acto de identificación y posterior a la misma, la IF realiza el resto del proceso KYC. Con todo esto en orden, finalmente procede a la creación de la cuenta o a la contratación.

Previo a este hito normativo ya existía tecnología de validación de documentos: fundamentalmente fabricantes de software anglosajones que permitían realizar y tratar fotografías o documentos de identidad escaneados (denominados selfies), los comparaban con pequeño streaming de video de la cara del cliente y realizaban lo que se denomina una acreditación de identidad. Como veremos más adelante, estas soluciones de selfies que tratan imágenes (no video) nunca ofrecieron una seguridad equivalente a identificación realizada en presencia. Se utilizaban y se siguen utilizando para procesos de verificación de un menor riesgo, como por ejemplo la verificación en la identidad en la contratación de pólizas de auto o seguros de hogar o microcréditos.

Con la circular del BaFIN alemán en 2014 el estándar de seguridad en la identificación remota para el nivel equivalente a la identificación realizada en presencia se establece de facto en la tecnología base de video en *streaming* y en la validación de todo el proceso por un humano entrenado.

Este hecho da lugar a la aparición de los primeros neo bancos, como es el caso de Number 26 (ahora N26) uno de los principales bancos puramente digitales a nivel mundial, con una valoración actual que

supera los 3bn de dólares y que marca el camino a otras muchas Fintech o insurtech que eventualmente se quieren convertir en un prestador de servicios financieros puro y regulado. Bancos como N26 hacen publicidad como los primeros bancos digitales, ofreciendo una cuenta sin limitación en las operaciones y una tarjeta de crédito. Su punto fuerte es que ya no necesita canal presencial, ofrece a sus clientes un servicio puramente digital, incluido el proceso de enrolamiento, que dicho sea de paso se convierte en su principal reclamo para los clientes, ya que pueden evitar por primera vez en la historia el inconveniente proceso de abandonar su "que hacer" diario e ir a la oficina comercial a realizar el proceso.

Esta normativa es copiada ampliamente en países de Europa, Latinoamérica, Asia, incluso USA. Los beneficios son claros ya que mejoran la experiencia del cliente y evitan la necesidad de una oficina comercial para la IF. Sin embargo, es problemático a la hora de escalar para las IFs. Sobre todo, para las Fintech, ya que es un proceso muy complejo: más de 10 minutos de entrevista. Técnicamente genera muchos problemas: dos comunicaciones (voz y video) bidireccionales que requieren de una red muy estable y con un ancho de banda mínimo requerido. Finalmente, no es lo más eficiente y escalable para la IF ya que las altas de nuevos clientes están limitadas a las personas entrenadas que realizan el proceso.

En 2016 el regulador en España SEPBLAC da un paso en aras de optimizar este proceso en las dos vías: conveniencia para el cliente mejorando la inclusión financiera y para las IFs: por optimización de costes. El SEPBLAC lanza en marzo de 2016 un procedimiento de identificación no presencial por video identificación, manteniendo la seguridad de la circular del BaFIN, pero permitiendo un proceso asíncrono, donde el cliente se identifica en un proceso grabado de video que dura unos segundos y más tarde un agente cualificado verifica las pruebas del registro y valida la identidad. El proceso de registro mejora la experiencia de cliente: se identifica en segundos; mejora las ratios de adquisición por la facilidad técnica (una comunicación de video unidireccional). Finalmente tambien permite aumentar la escalabilidad del servicio ya que se optimiza los tiempos muertos de verificación por parte de los agentes y el uso de los mismos, sin restar en seguridad.

Timeline de la identificación remota

a. Consolidación del Video en Streaming y la verificación humana como estándar para la identificación remota de clientes.

A junio de 2019 la AFI contabiliza más de 38 países que permiten sistemas basados en video en *streaming* y la verificación por un humano cualificado como estándar para la identificación remota de clientes en la industria financiera. Y creciendo, ya que estimamos que sean más de 54 países que de una forma u otra lo adopten hasta final de año.

La lista de países por región hoy es la siguiente:

Región	Nº de Países	Nota
Europa	28	Todos los Estados Miembros
Norte de América	1	México, Estados Unidos de América
Sur de América	3	Brasil, Colombia
Asia	5	Armenia, Hong Kong, Japón, Singapur, Corea del Sur
Otros	1	Suiza

Esta estandarización se apuntala adicionalmente con estos acontecimientos:

El GAFI-Grupo Acción Financiera Internacional incluye la identificación a distancia por en sus recomendaciones en diciembre de 2016.

La Comisión Europea establece un reglamento de ejecución 2015/1502 que establece los niveles de seguridad en la identificación electrónica. El reglamento de ejecución es una extensión de la regulación eIDAS 910/2014, en vigor desde julio de 2016, que establece la norma comunitaria de obligado cumplimiento y aplicación directa para todos los estados miembros en lo relativo a los servicios de confianza electrónica, que, entre otros, regula la identificación y la firma electrónica para las relaciones digitales.

Por último y como hecho relevante para la industria financiera, la entrada en vigor de la 5ª directiva Europa de Prevención de Blanqueo de Capitales (AML5) en mayo de 2018, que confía en el marco de seguridad del eIDAS la identificación de clientes y medidas de diligencia debida a sujetos obligados, no solo homogeneizando las soluciones en Europa sino liderando la regulación AML que abre la puerta a las iniciativas Fintech, como por ejemplo las monedas virtuales, crédito o pagos.

b. ¿A quién aplica esta regulación en el sector?

La adopción de este conjunto de medidas para la identificación remota afecta, a modo de resumen, a distintos tipos de entidades, ya sean entidades con negocios tradicionales o entidades basadas en la tecnología (Fintech e insurtech, ITFs.). La denominación de estas puede variar de un país a otro.

- Las entidades e instituciones de crédito.
- Las sociedades gestoras de instituciones de inversión colectiva y las sociedades de inversión cuya gestión no esté encomendada a una sociedad gestora. (sociedades financieras populares, sociedades financieras comunitarias, organismos de integración financiera rural...).
- Las entidades aseguradoras autorizadas para operar en el ramo de vida y los corredores de seguros cuando actúen en relación con seguros de vida u otros servicios relacionados con inversiones
- Las empresas de servicios de inversión.
- Las entidades gestoras de fondos de pensiones.
- Las sociedades gestoras de entidades de capital-riesgo y las sociedades de capital riesgo cuya gestión no esté encomendada a una sociedad gestora.
- Las sociedades de garantía reciproca.
- Las entidades de pago y las entidades de dinero electrónico.

c. Niveles de Seguridad en la Identificación Remota Digital.

Haciendo una recopilación de las regulaciones PBCFT/AML conocidas se establecen tres niveles de aseguramiento de la identificación remota, que son los siguientes:

Nivel de Seguridad	Descripción	Casos de Uso	Sistemas
Bajo	La confianza requerida de que la persona es quien dice ser es baja. El nivel de seguridad puede ser comprometido con facilidad. El daño causado en el proceso proveniente de una identidad comprometida debe de ser mínimo	Comercio Electrónico.	Asunción de la información proporcionada por el cliente; Chequeos en el back con información pública del cliente; redes sociales.
Medio	La confianza requerida de que la persona es quien dice ser es moderada. El daño causado en el proceso proveniente de una identidad comprometida podría ser medio o alto.	Contratación con riesgo bajo: seguros de auto, hogar; microcréditos; transacciones acumuladas de hasta 999$ aprox.	Tecnología de verificación de la identidad a través de documentos por imágenes (selfies)
Alto	La confianza requerida de que la persona es quien dice ser alta. El daño causado en el proceso proveniente de una identidad comprometida podría ser serio o catastrófico.	Apertura de cuentas sin limite, contratación riesgo alto: crédito >999 $, hipotecas, pagos	Personación cara a cara en la oficina comercial; entrevista por video conferencia con agente cualificado; registro por video identificación con verificación posterior con agente cualificado; Documentos estatales de identidad electrónicos que cumplan con normativas de firma electrónica avanzada y cualificada.

d. Seis recomendaciones para preparar mi Fintech para la identificación digital de clientes.

1º ¿lo necesitas?

Quizás, con la contestación de esta pregunta, no necesitas avanzar más en esta materia, de momento. Muchos startups aprovechan espacios en la prestación de servicios financieros que no están regulados o simplemente intermedian entre los bancos o aseguradoras y los clientes. En estos casos la parte dura regulatoria o de seguridad corresponderá a los sujetos obligados, en este caso los bancos o aseguradoras. Por ejemplo, si tu Fintech es un buscador financiero que conecta los clientes con los servicios financieros probablemente no necesites identificar a los clientes ya que esto formara parte del proceso de contratación cuando llegue al prestador de servicios real.

Si lo dudas, es probable que lo necesites: la identificación de clientes no se realiza solamente por un tema de cumplimiento normativo, la identificación con garantías del cliente se hace sobre todo por un tema de seguridad, para evitar el fraude.

2º Busca una experiencia y seguridad graduada en el tiempo.

Es habitual que el proceso de apertura de una cuenta lleva asociado un proceso de KYC largo y con una experiencia costosa para el cliente: la identificación digital, el origen de los fondos, el chequeo con las bases de datos de fraude, contratación, etc.

Recomendamos pensar muy bien el proceso de *onboarding*/enrolamiento de cliente ya que tu startup va a vivir de adquirir nuevos clientes. Piensa como llegar al final, pero no necesariamente de una sola vez. Nuestra recomendación es que diseñes un camino de enrolamiento progresivo en el tiempo e incremental en la seguridad.

Aumentaras la inclusión financiera en personas menos acostumbradas a la tecnología y mejoraras tu ratio de adquisición de clientes.

3º El proceso de KYC, Conoce a tu cliente, va más allá de la identificación

Las buenas prácticas internacionales, tales como las guías de recomendaciones del GAFI ven el KYC un proceso prolongado y sistematico en la relación con el cliente, de forma que el análisis de su riesgo técnico, de solvencia y económico se convierta en una forma de entender al cliente y no en un proceso puntual al inicio de la relación.

4º Piensa en la privacidad

La privacidad no es una moda, si no una necesidad y un valor de largo plazo en la relación con tu cliente y todo el beneficio mutuo que podéis generar en el tiempo.

Si traicionas a tus clientes vendiendo sus datos sin su consentimiento probablemente estos lo noten y dejen de confiar en tu compañía. Recuerda que el servicio que vendes se basa en la confianza. Si no existe la confianza no existirá el negocio.

Evalúa las buenas prácticas en los sistemas de información para guardar la información de tus clientes y aplícala en tus procesos y en los procesos de su ecosistema de clientes y partners. Recomendamos que veas como se trata la información como responsable de tratamiento de datos personales en leyes que avanzan en este campo. La nueva ley de privacidad europea o la nueva japonesa son bastante restrictivas y razonables para asegurar la privacidad y dando margen para desarrollar tu negocio.

5º Planifica la identificación digital

Algunas Fintech quieren ir rápido y adquieren clientes sin importarles si esos clientes son quienes dicen ser. Sobran las noticias en las que una Fintech arriesga creciendo, dando de alta clientes de una forma sencilla, pero sin seriedad y acaban saliendo en las listas negras de inversores, clientes y servicios de inspección regulatoria.

Hazlo bien y tendrás un beneficio. Por poner un ejemplo: las últimas rondas de financiación de los Unicornios Fintech arrojan la cifra media de 1100$ de valoración por cliente en las ampliaciones de capital[1]. Pero lo dicho: son serias y realizan bien su trabajo en la captación de nuevos clientes. Por tanto, no escatimes en el tiempo de preparación ni en el coste de captación ya que será rentable en el tiempo.

6º Prepara todo para evitar sorpresas.

Si el nivel requerido es el alto, te sugerimos que prepares o contrates a alguien para ayudarte en las siguientes tareas:

Consulta al regulador local acerca de la normativa vigente en materia de identificación de clientes no presencial. Algunos países de Iberoamérica ya cuentan con procedimientos PBCFT/AML para la

[1] Datos extraídos del análisis de últimas ampliaciones de capital en Crunchbase.

identificación de clientes no presencial. La mayoría de los reguladores conocidos están cada vez teniendo mayor apertura para atender solicitudes de sistemas que han sido validados y certificados en otras regiones para el mismo nivel de confianza.

Selecciona la mejor solución.

Documenta bien el proceso. Una buena preparación y documentación evita tener problemas con el regulador. Existe un conjunto de buenas prácticas que son comunes para preparar los procesos de identificación digital de clientes. Son las siguientes:

- Documenta el sistema que has contratado: como es el proceso desde el registro hasta la validación, que medidas de seguridad incorporas.
- Analiza los riesgos inherentes del canal online: pide a tu equipo de fraude o *compliance* que trabaje con los proveedores para identificar los riesgos específicos de este canal. Este trabajo te prepara para mitigar riesgos y te cubre de cara a una posible inspección.
- Prueba el sistema antes de salir a producción. Documenta las pruebas realizadas para que quede constancia que has tomado una decisión basada en unas pruebas del sistema positivas en la seguridad.
- Entrena, evalúa y certifica según la regulación al equipo de agentes de verificación e identidades. Si estas comenzando haz el esfuerzo y subcontrátalo a los proveedores que lo ofrecen. Tiene un coste, pero la seguridad tiene un retorno grande.

- Exige a tu proveedor las siguientes medidas técnicas y de seguridad del servicio:

    - Que cumple y este certificado con las políticas y buenas prácticas para prestar el servicio, como por ejemplo la ISO27001 en materia de seguridad de la información.
    - Que su sistema cumple y este certificado según la normativa actual para prestar servicios fiables en términos de privacidad de la información y gestión de datos de carácter personal como encargado del tratamiento.
    - Que su sistema realiza la seguridad requerida. Existen certificaciones funcionales de producto.

e. Solicitud a los reguladores locales respecto a la identificación electrónica remota de clientes en el sector financiero.

Por el impacto en la inclusión financiera de las personas y el impacto en la economía, la AFI anima a los reguladores a permitir los procesos de identificación electrónica remota, aceptando solicitudes de nuestra comunidad de Fintechs. Recomendamos hacerlo siempre que hayan garantizado el seguimiento de normativa internacional vigente en esta materia y las Fintech sigan las recomendaciones y buenas prácticas señaladas en artículos anteriores de forma seria y objetiva.

También les incitamos a analizar, poner en vigor y fomentar circulares o procedimientos de identificación no presencial en el canal online, fijándose en los países pioneros en la misma. En este último caso, disponibilizamos las autorizaciones de reguladores pioneras y más solidas en materia de seguridad, de todas las mencionadas en el trascurso de este documento. Se ordenan teniendo en cuenta la mejora de la conveniencia del cliente para la inclusión financiera y la eficiencia para la FI.

- Para el proceso de registro por video identificación más verificación posterior por humano cualificado, SEPBLAC, Servicio Ejecutivo de la Comisión de Prevención de Blanqueo de Capitales e Infracciones Monetarias, España, 2016. Actualizada en 2017 [enlace]

- Para el proceso de entrevista por videoconferencia, BaFIN, Federal Financial Supervisory Authority, Alemania 2014. Actualizada en 2019 [enlace]

Como mencionamos anteriormente, existen multitud de reguladores que han liberado procedimientos o circulares de este tipo, pero estas son las dos autorizaciones pioneras y en las que se basan el resto.

Adicionalmente a esto, la Unión Europea lleva casi una década trabajando en una nueva ley de servicios de confianza electrónica, denominada eIDAS. El eIDAS es la evolución a las antiguas leyes de firma electrónica y servicios de confianza que datan de finales de los años 90 y que dieron lugar a la mayoría de los proyectos estatales conocidos de identidad electrónica. El eIDAS no ha puesto foco en materia financiera y está enfocado en garantizar un esquema de seguridad de alto nivel para la creación de la identidad única digital europea. Esta identidad regional significa a la identidad lo que el euro significó a la moneda a principios de este siglo, estandarizando este concepto, haciéndolo transfronterizo y tanto para el ámbito público como privado.

Es un hecho relevante la conexión que los procesos KYC/AML tienen con el eIDAS. En mayo de 2018 entra en vigor la 5ª directiva Europea de Prevención de Blanqueo de Capitales (comúnmente denominada AML5). A falta de un esquema de seguridad especifico en la identificación electrónica, AML5 confía en todos los apartados del proceso de *Customer Due Dilligence* CDD e Identificación de clientes, en el esquema de seguridad del eIDAS. Esto significa que los sistemas validados y certificados eIDAS por cualquier laboratorio cualificado en las listas europeas (*Conformity Assestment Body* – CAB), cumpliría con las exigencias de las normas financieras para la identificación remota de clientes.

Entre las recomendaciones en este apartado a sus asociados, la AFI recomienda preparar a las Fintech para el cumplimiento de estas regulaciones tan exigentes, incluyendo la recomendación de solicitar a los proveedores de sistemas de identificación electrónica los certificados por los laboratorios cualificado.

4. Autenticación Biométrica

a. Datos clave para entender la entrada de la Autenticación Reforzada de Cliente y el emergente uso de las tecnologías biométricas.

Ofrecer seguridad en el acceso, al mismo tiempo que ofrecer una experiencia a los usuarios con las mínimas fricciones, esta siendo el caballo de batalla de cualquier iniciativa Fintech.

El concepto de Autenticación Reforzada de Cliente (ARC) es un concepto que viene de la nueva regulación, principalmente de la categoría de pagos, que es una de las más crecientes en esta explosión de regulaciones y nuevos servicios financieros. Se estima[2] que el volumen de transacciones de pagos digitales (sin efectivo) creció en 2016 un 10.1% para alcanzar los 482.6 billones de y que el volumen de transacciones para los pagos con carteras electrónicas (e-wallet) ya alcanza los 41.8 billones, siendo un 8.6% de todas las transacciones sin efectivo. Este crecimiento continuado en una economía que intenta eliminar la moneda física, sumado a la necesidad de prevenir el fraude, esta siendo clave para que los bancos y Fintech inviertan[3] en nuevas tecnologías, incluyendo la inteligencia artificial para alertar sobre fraude en tiempo real, así como tecnologías de reconocimiento facial, voz y huellas dactilares (tecnologías biométricas).

La ARC obliga y permite tener una estrategia de autenticación que se basa en el uso de dos o más elementos categorizados como: conocimiento (algo que solo el cliente conoce), posesión (algo que el cliente posee) y algo inherente al usuario (algo que el cliente es). Estos elementos son independientes, es decir, que el comprometimiento de uno no significa la falta de fiabilidad del otro. Las combinaciones múltiples de unos factores con otros, ofreciendo la mejor experiencia en el uso al cliente define la estrategia de autenticación de cualquier Fintech.

Y desde que en mayo de 2016 el NIST norteamericano (National Institute of Standards and Technology) publica unas líneas base en las que recomienda el abandono del las OTP-*One Time Password* a través de SMS como segundo factor de autenticación, los factores biométricos mencionados se están convirtiendo rápidamente en uso común en nuestra industria.

2 World Payments Report 2018, Cap Gemini BNP Paribas 2018
3 Global Banking Fraud Survey KPMG, May 2019

b. ¿Qué es la biometría?

La biometría es la ciencia del análisis de las características físicas de las personas. En el sentido más académico, la biometría significa: el estudio mesurativo o estadístico de los fenómenos o procesos biológicos.

En nuestro contexto Fintech el objetivo del uso de la biometría es confirmar la identidad de nuestros clientes de cara a asegurar el acceso a nuestras aplicaciones, a la operativa normal y a contratar nuevos servicios.

La biometría puede ser morfológica: huellas dactilares, forma de la mano, dedo, patrón de las venas, la retina o el iris del ojo o la forma de la cara o biológica: el ADN, la sangre, saliva o la orina. El desarrollo de la tecnología de autenticación ha comenzado por la morfológica, donde nos centraremos.

La autenticación biométrica es el proceso en el que se comparan los datos de las características de un cliente con una plantilla preestablecida que se establece en un registro inicial, con el fin de buscar su semejanza.

Confiabilidad de la biometría. La biometría se basa en algoritmos estadísticos, no determinísticos.
No es 100% infalible cuando se utiliza por sí sola. Motivo por el cual se combina con otros factores de autenticación para ser efectiva y segura.
En la precisión de las soluciones nos referimos a los "falsos positivos (False Match Rate-FMR)" o a las "falsos negativos (False NonMatch Rate-FNMR)". En estos casos los sistemas biométricos no pueden reconocer al cliente con precisión. Estos errores son síntomas que se producen con todas las técnicas utilizadas en la biometría. La precisión de un sistema biométrico depende no solo del rasgo relevante a identificar, sino también de las características del sensor, el número de individuos en la base de datos y las características poblacionales de la muestra, entre otros[4]
Las características biométricas no constituyen secretos ya que los rasgos biométricos de las personas podrían en último término copiarse.

Aunque la tecnología de autenticación biométrica ya está en una buena ratio de precisión y en el desarrollo de medidas de seguridad tales como (pruebas de vida, ataques *spoofing*, etc…) todos estos motivos hacen que la tecnología autenticación biométrica no vaya a ser por el momento una tecnología

[4] Para un análisis interesante sobre los distintos medios de identificación biométrica, incluyendo una comparación de los distintos rasgos que podrían utilizarse, véase: Anil K. Jain (2008). Biometric authentication. Scholarpedia, 3(6):3716.

para reemplazar primeros factores de autenticación, como por ejemplo las contraseñas (secretos). Sin embargo, se están convirtiendo en uso común en la estrategia multi-factor del sector Fintech, debido a la mejora en la experiencia del cliente con el concepto que se impone por seguridad de Autenticación Reforzada de Cliente.

c. Cuestiones clave para seleccionar la tecnología biométrica

Describimos las cuestiones que son clave para seleccionar la tecnología biométrica más adecuada para cada iniciativa Fintech.

Según el canal donde operes. La mayoría de las iniciativas Fintech comienzan en el canal online, concretamente contrayendo aplicaciones para el móvil. Sin embargo, existe una creciente conexión de las iniciativas como las de pagos y crédito que conectan los canales online y offline. Uno de los casos son las Fintech de pagos, que requieren de la conexión con el espacio físico minorista para ofrecer sus servicios de pago a personas o merchants. O el crédito que nace en el ámbito de la financiación en el e-commerce para ahora ofrecer servicios de financiación al consumo en el espacio minorista.

Pensar en el canal donde operas, pero también donde vas a operar en el futuro tiene implicaciones en la gestión de la identidad de tus usuarios y dado que la autenticación biométrica se convertirá en uso común es bueno que comiences a pensar en ello.

Esta tabla demuestra la cobertura de cada tecnología biométrica y su adaptación en cada canal.

TIPO DE BIOMETRÍA	CANALES NO PRESENCIALES			CANAL PRESENCIAL
	Móvil	Web	Telefónico	Oficinas Comerciales
Facial	Adecuado	Adecuado	Nulo	Adecuado
Dactilar	Adecuado	Nulo	Nulo	Limitado
Iris/Retina	Limitado	Limitado	Nulo	Limitado
Voz	Adecuado	Limitado	Adecuado	Adecuado

Adecuado: el tipo de biometría cubre de forma razonable y completa las necesidades del canal

Limitado: el tipo de biometría cubre de forma limitada técnicamente las necesidades del canal o necesitaría hardware propietario y soporte adicional para una seguridad razonable, más allá de los propios dispositivos estándar de los clientes.

Nulo: el tipo de biometría no puede utilizarse en este canal o tiene una limitación muy alta.

Para este análisis se han tenido en cuenta tecnologías biométricas que no tienen dependencia de un hardware especifico en un dispositivo, si no su seguridad se basa en el software con el objetivo de que sean independientes o no limitadas a dispositivos específicos. Por ejemplo: para la biometría facial se identificación tipos de biometrías que trabajan sobre cámaras de teléfonos inteligentes o tabletas. No se tiene en cuenta tecnología embebida (FaceID Apple). Para la biometría dactilar se tienen en consideración las tecnologías que utilizan la cámara del dispositivo, evitando tecnología propietaria que requiere una extensión de hardware especifico en el dispositivo del usuario.

Según el registro que realices:

El registro es un proceso esencial dentro de la experiencia del cliente. Un registro conveniente, con calidad y sin fricciones agradara a tus clientes. Si es algo complejo o inconveniente tendrá el efecto contrario.

Tipo de Biometría	Complejidad/Conveniencia del proceso de registro
Facial	**Baja**
Dactilar	**Media**
Iris/Retina	**Alta**
Voz	**Media**

Según la complejidad y la conveniencia para el usuario: asumimos la necesidad de un registro que garantice la calidad posterior de la autenticación.

Baja: el usuario no interactúa en el proceso de registro. El registro podría realizarse de forma automática y sin pasos extra en el proceso de enrolamiento KYC del cliente.
Media: el usuario interactúa en el proceso de registro adicional pero la interacción es mínima y sencilla por sus requerimientos técnicos.
Alta: el usuario interactúa en el proceso de registro y la interacción es alta y compleja por sus requerimientos técnicos.

d. Privacidad

El uso de datos biométricos de nuestros clientes debe de tener especial consideración ya que hay una tendencia actual de utilizar el uso de nuevas tecnologías biométricas al abuso más que al uso en relación con los clientes.

Cualquier dato biométrico descrito en este apartado tiene el tratamiento de dato de carácter personal especialmente sensible, requiriendo un consentimiento adicional al cliente para habilitar su uso, más allá

de las condiciones generales de privacidad para el uso de datos de carácter personal corrientes, como pueden ser sus credenciales de identidad.

Es importante que como responsables de los datos de carácter personal de los clientes sigamos buenas prácticas en el tratamiento del uso de la información y exijamos el cumplimiento adecuado en materia de privacidad a los terceros que nos proporcionen la tecnología de autenticación biométrica.

e. Tres recomendaciones para preparar mi Fintech con los *biométricos*

1ª analiza y selecciona tu biometría

Después de aceptar la necesidad de la ARC debes de pensar que tipo de biometría se adapta mejor a tus necesidades en la línea del tiempo y en relación con donde puede llegar tu negocio (canales) o la experiencia que quieres para tus clientes.

2ª piensa en los Customer Journey

Como los quieres registrar: si te lo puedes ahorrar para mayor conveniencia de tus clientes en el proceso de enrolamiento: si el registro se realiza incremental en el tiempo.

Piensa en los puntos de los procesos en los que requieres ARC o las tecnologías biométricas para hacerle la vida más fácil a los clientes: por ejemplo, vemos que hay Fintechs que utilizan la biometría facial o la voz como ayuda para identificar al cliente (el cliente no tendría que introducir o recordar el email como usuario), para firma de operaciones, contratación evitando una OTP al SMS o como un factor para recuperar la contraseña.

3º piensa en la privacidad

Empatiza con tu cliente y mira cual es la biometría que más le puede gustar. No debería de ser obligatoria y una idea puede ser que el seleccione la que le guste en cada momento o en cada canal.

Exige a tu proveedor las buenas prácticas contractuales, auditorias y certificaciones que te ayuden a cumplir con las leyes de privacidad. En este sentido es importante que el contrato con tu proveedor cuente con una extensión de privacidad (Acuerdo de Protección e Datos o Data Protection Agreement (DPA)) que regula las obligaciones con la gestión de datos de carácter personal. No existe una certificación global de privacidad, pero ten en cuenta que el proveedor cumpla con la legislación más exigente: por ejemplo, es mucho más exigente cualquier cumplimiento con leyes en Iberoamérica o GDPR en Europa, que son más garantistas porque están basadas en el derecho romano que el cumplimiento de leyes en USA o UK que se basan en la ley común y son menos exigentes.

Exige a tu proveedor que cumpla con las leyes existentes en materia de privacidad y además que lo tenga auditado y certificado. Por ejemplo, una certificación importante es la ISO27001. La ISO tiene un dominio de privacidad que, si tu proveedor tiene cubierto, te ofrecerá mayores garantías.

5. Contratación

La firma electrónica es el concepto jurídico equivalente al proceso analógico de firma manuscrita. Tiene el objetivo de que los acuerdos entre el cliente y la Institución Financiera (IF) queden suscritos por vía telemática de una forma segura, inalterable y demostrable en cualquier momento. Son caracteristicas que las firmas electrónicas cumplen que ayudaran a solventar problemas en casos de inpagos o repudios en la contratación.

La contratación a través de la firma electrónica es un concepto ya extendido y ampliamente aceptado en Iberoamérica prácticamente en la totalidad de países. Incluimos este apartado en el libro blanco para informar sobre las novedades que incorporan las nuevas regulaciones. Estas novedades pueden resultar de interés puesto que por primera vez en la historia hacen la firma electrónica avanzada y cualificada (la de mayor validez jurídica) más sencilla de usar para los clientes. Esto crea importantes oportunidades de negocio que anteriormente no eran posibles en el ámbito online, como la venta puramente electrónica de productos y servicios de alto riesgo, tales como: contratación de hipotecas, créditos de gran cuantía, planes de pensiones y seguros de vida, entre otros.

La firma electrónica se basa en la identidad digital del cliente ya que cuanto mayor es el nivel de confianza en la identidad del cliente mayor es el nivel de seguridad jurídica de la contratación.

La identificación alta del cliente realizada en los procesos de enrolamiento tiene un doble sentido: por un lado, atiende a la confianza en los negocios, forzada por las leyes de PBCFT/AML/KYC y los procesos de diligencia debida; por el otro lado una seguridad alta en la identificación, equivalente a la que se realiza cara a cara en las oficinas comerciales va a ayudar a garantizar la seguridad jurídica en la contratación en cuestiones legales.

Ilustramos con un ejemplo la importancia de garantizar ambas cosas: la identificación del cliente y una contratación con eficacia jurídica.

Pensemos en un cliente al que no identificamos en su enrolamiento o lo identificamos con un nivel bajo. Podremos hacer una contratación a través de una firma electrónica simple (la firma electrónica simple esta ligada a la identidad de la personas a través de su correo electrónico o teléfono móvil). Si eventualmente existiera un problema, por ejemplo, un impago o un repudio de una póliza, etc., la IF tendría dificultades para demostrar a un tercero que el cliente es quien dice ser (por la debilidad de los datos de identificación) y por lo tanto de recuperar el dinero invertido.

En otro caso tenemos una identificación del cliente alta, pero no se realiza bien el proceso de contratación electrónico o no existe una firma electrónica. Ante este caso el cliente podría repudiar su contrato. La IF podría identificar al cliente con exactitud pero no podría demostrar que el cliente ha dado su consentimiento expreso al contenido del contrato. Un juez podría darle la razón, al no existir pruebas exactas e integras de un acuerdo firmado.

Como vemos la identificación y la firma electrónica están intimamente ligados. Nuestra recomendación es buscar mecanismos de identificación y de contratación que permitan mitigar el riesgo del negocio y cumplir de inicio a fin con la legalidad.

a. Antecedentes de la firma electrónica

Las primeras leyes de firma electrónica datan de 1999, casi en paralelo a la creación y generalización del uso de Internet. Sin embargo, en el caso de la firma electrónica no es hasta hace una década que su uso se comienza a generalizar.

Las primeras leyes de firma electrónica impulsan el nacimiento en algunos países los documentos nacionales de identidad electrónicos, que incluyen un certificado electrónico de persona física preparado para que las personas puedan identificarse y firmar un contenido electrónicamente, con las mismas o incluso mayores garantías que la firma manuscrita.

Dada la falta de experiencia de los técnicos y reguladores por aquel entonces, la mayoría de estos proyectos acaban siendo un fiasco en la mayoría de los casos, debido a que la usabilidad de las soluciones (instalación de chipeteras; no funcionan en el móvil; certificados instalados con plugins en los navegadores) es muy bajo. En aquel entoncés, lo que pas, es que estas tecnologías descargan la complejidad de las soluciones en los usuarios, que necesitan ser avanzados tecnológicamente para hacerlos funcionar. El resultado es que después de una década, este tipo de firmas electrónicas (avanzadas y cualificadas) no llegan a generalizarse. Aún así, la idea de un alter ego digital ofrecido por un tercero confiable (Prestador de Servicios de Certificación) y la posibilidad de contratar a distancia, siguen siendo ideas magnificas para facilitar la vida de los ciudadanos y fomentar la inclusión financiera en nuestro sector.

En todos estos años, como pasa en muchas ocasiones, alguien más pragmático ve una oportunidad e introduce instrumentos más sencillos. En este caso este instrumento es la figura de la firma digital. La

firma digital se basa en las leyes de comercio electrónico anglosajón y confian en Terceras Partes de Confianza (TPC) una intermediación para realizar la contratación.

Son fundamentalmente los fabricantes y TPCs norteamericanos los que permiten extender este tipo de firmas porque son fáciles de usar: el usuario solo necesita un correo electrónico y un teléfono móvil para firmar un documento. Estas soluciones de firma digital tienen sus limitaciones y una seguridad jurídica limitada para procesos de alto riesgo debido a que el nivel de seguridad en la identificación no es alto. La firma digital de los TPCs se generaliza para procesos de bajo riesgo, tales como: las pólizas de un seguro de coche, de un hogar o incluso algunos microcréditos.

Con esta limitación, las IFs no son capaces de implantar sistemas en otro nivel de riesgo ya que pueden causar un daño para las compañías muy alto. Y es por esto por lo que la firma remota sigue siendo un reto para contrataciones de alto nivel de riesgo tales como: hipotecas, seguros vida, planes de pensiones, crédito, pagos, etc...

En este sentido, dada la aparición de las nuevas tecnologías como las mencionadas de video identificación anteriormente y el avance en el ámbito legal también se ha producido, además con importantes novedades en el ámbito de la usabilidad, su principal freno años atrás.

b. Novedades en la regulación de firma electrónica

En julio de 2016 entra en vigor en Europa la regulación eIDAS. eIDAS es la evolución de las antiguas leyes de firma electrónica. Regula todos los servicios de confianza electrónica: firma e identificación electrónica, sellos de tiempo, certificados web, etc. El eIDAS cambia la denominación de los Prestadores de Servicios de Certificación por Prestadores de Servicios de Confianza y hace pequeñas modificaciones en la norma para que las firmas electrónicas de mayor nivel jurídico (las firmas electrónicas avanzadas y cualificadas) puedan ser utilizadas ampliamente con una usabilidad semejante a la que un usuario puede tener al usar una tarjeta de crédito: a través de un PIN o con una Autenticación Fuerte Reforzada. Esto evita las complejidades de uso de las antiguas leyes y está haciendo resurgir las firmas avanzadas y cualificadas.

En su origen, prácticamente todos los países de centro y sur de américa bebieron del derecho garantista europeo para implantar las leyes de firma electrónica avanzada. En este momento vemos ya algunos en proyectos para dar entrada a las novedades incorporadas por el eIDAS, como las modificaciones en el exclusivo control del usuario que facilitan las firmas.

Esto permitira realizar una contratación remota con todas las garantías y para cualquier nivel de riesgo en lo que se refiere a la industria financiera.

c. Tipos de firmas electrónicas

Con la nueva regulación la firma digital provista por Terceras Partes de Confianza (TPC) desaparecen ya que la regulación les obliga a convertirse en Prestadores de Servicios de Confianza (PSC), aumentando así la seguridad jurídica y técnica para realizar las firmas electrónicas

No obstante, seguirán existiendo distintos tipos de firma, según su seguridad jurídica, que darán cobertura en el sector financiero a las distintas necesidades desde un nivel bajo hasta alto más garantista.

La siguiente imagen describe los distintos tipos de firma, incluyendo la nueva firma electrónica cualificada.

	Identificación del firmante	Canales	Dsipositivo	Equivalencia con manuscrita	Nivel de riesgo
e-Signature	No	Online, Oficina y Teléfono.	Cualquier dispositivo	No	Bajo (Polizas Auto, Coche, Microcréditos)
Advanced e-Signature	Sí	Online, Oficina	Cualquier dispositivo	No	Alto (Cualquier proceso de contratación, incluyendo cualquier tipo de crédito, hipoteca, seguros de vida, planes de pensiones, etc…)
Qualified e-signature	Sí	Online, Oficina	Cualquier dispositivo	Sí	Alto, Admon.Pública

6. Mecanismos de aseguramiento de la información y privacidad.

Desde el punto de vista de seguridad es crítico contar con mecanismos de captura, almacenamiento e intercambio de información sensible, que se basen en principios y políticas de privacidad frente a terceras partes.

Antes de aplicar estos mecanismos, es necesario establecer los metadatos obligatorios que debe incorporar el sistema y en su caso, los metadatos extendidos opcionales que podrían ser utilizados para otros sistemas que requieran la identidad, como servicios de e-health, licencia de conducción, votaciones, entre otros. Esta selección se debe realizar bajo el enfoque de fin del servicio que se quiera prestar, de manera que no se custodian datos que no tengan relación directa con este.

Por ejemplo, la Unión Europea en el Reglamento eIDAS[5] (910/2014) establece los metadatos obligatorios que un sistema de identidad debe solicitar, custodiar y compartir para personas naturales (nombre, apellidos, fecha de nacimiento y número de identificador único) y atributos adicionales (como lugar de nacimiento de los padres, lugar de nacimiento, género y dirección actual).

Uno de los mecanismos para garantizar la privacidad del dato es la aplicación de estándares. A continuación, mencionaremos algunos ejemplos:

- El estándar ISO/IEC 29115 proporciona a los sistemas de identidad un framework que permitirá asegurar los niveles de garantía de la identificación electrónica en relación con la confianza que merecen los procesos, las actividades de gestión y tecnologías utilizados para establecer y gestionar

5 eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32014R0910&from=ES

de forma efectiva la identidad de una entidad para su uso en las transacciones de autenticación de sus ciudadanos.

- El ISO/IEC 29100:2011 – provee un marco de trabajo de alto nivel para la protección de la Información de Identificación Personal (PII) que le permite a las organizaciones la definición de sus requerimientos de protección de la privacidad mediante la especificación de una terminología común, la definición de actores y sus roles en el procesamiento de datos, los requerimientos de privacidad y la referencia de una serie de principios orientados a la gestión de los aspectos organizativos, técnicos y procedimentales de esta estrategia.

- El ISO 19794 define el formato de intercambio biométrico entre diferentes sistemas, para varios tipos de datos biométricos (reconocimiento facial, iris, huella dactilar,), especificando los sistemas de encriptación y criptográficos necesarios para garantizar el intercambio seguro de esta información que es extremadamente sensible a ciberataques o robos de identidad.

7. Sistemas nacionales de identidad: casos de éxito internacionales.

Este apartado anima a los reguladores locales y estados a generar sistemas nacionales de identidad públicos que puedan llegar a fomentar la inclusión financiera y la economía domestica.

La gestión de la identidad de los ciudadanos no sólo es necesario para el propio individuo, sino también para el Estado y aún más para las terceras personas. Respecto al individuo, para poder probar su condición de ciudadano, hijo, cónyuge, pariente, mayor de edad, tutela, etc. Respecto del Estado, para la organización de muchos servicios administrativos. Respecto de los terceros, para dar certidumbre respecto al establecimiento de negociaciones entre sí.[6]

Tradicionalmente, los ciudadanos manifiestan su identidad repetidamente en distintas instituciones tanto público como privadas (en algunos países, este suceso se mantiene), cayendo en repeticiones innecesarias de verificación y autenticación. Además de ello, en muchos ecosistemas, la identidad ha surgido en contextos más sociales, como el de la religión, los procesos electorales o la gestión de comunidades culturales más pequeñas. Es así como uno de los retos más importantes del uso de la identidad son los ámbitos de aplicabilidad. Este indicador medirá si el mecanismo de identidad es capaz de utilizar para cualquier tipo de transacción pública y/o privada que lo requiera, así como independiente de la geografía o la voluntad de uso.

Dado este marco de relacionamiento, los sistemas nacionales de identidad requieren de un marco normativo robusto que parta de una definición de las competencias institucionales en la norma superior como puede ser la Constitución Nacional, y que se despliegue en normas como leyes a cargo del Congreso, y reglamentarias a cargo del ejecutivo a través de las distintas unidades orgánicas ejecutoras. Esta definición de competencias institucionales resulta fundamental, pues permitirá desplegar el documento de identificación y su uso en diversos procesos y trámites no sólo de la administración pública, sino también de particulares.

La AFI considera que la creación de sistemas nacionales -o regionales- de identidades digitales es una inversión de infraestructura sumamente importante que deben de considerar las autoridades de cada jurisdicción, toda vez que la identidad digital es un insumo para la prestación de diversos servicios que van desde el sistema financiero, el ámbito comercial y hasta los programas gubernamentales. La

6 http://www.derecho.usmp.edu.pe/cedetec/art_rptinv/29%20EVOLUCION%20DEL%20DNI.pdf

amplitud de servicios y actividades que se verían beneficiados al dotar a destinatarios de identidades digitales fiables nos lleva a afirmar con certeza que la identidad digital es condición necesaria del crecimiento en inclusión económica en la era digital.

Nos referimos a inclusión económica y no a inclusión financiera porque el primer concepto es más amplio y comprende tanto al segundo como a la garantía de acceso a productos y servicios distintos a los servicios financieros, por ejemplo:

- E-government,
- e-commerce,
- servicios médicos
- contratación electrónica.

Lo anterior se expresa sin negar que la inclusión financiera sería el objetivo más beneficiado por la implementación de sistemas adecuados de identidad digital.

Los principales beneficios de la inversión en infraestructura de identificación digital serían incrementar la productividad y el crecimiento económico, mejorar la tutela de la privacidad, avanzar en la prevención del robo de identidad y el fomento de la inclusión de sectores marginados. Para lograrlos, es necesario superar diversos retos en la creación de políticas públicas de avanzada; mismos que este documento buscará atender.

Adicionalmente y dada la naturaleza globalizada de los mercados actuales y la creciente integración regional entre los países que integran la Alianza Fintech Iberoamérica, consideramos esencial recalcar la importancia de que las políticas públicas que implementen los sistemas nacionales de identidades digitales se encuentren coordinadas entre sí.
A modo de referencia, se han revisado las siguientes experiencias de países, los cuales confirman la importancia de establecer un marco legal e institucional robusto para un eficiente funcionamiento del ecosistema de identidad:

Se realizan sobre las leyes de firma electrónica y ahora se actualizan de forma comunitario con la nueva regulación eIDAS, que se convierte en básica para entender los distintos desarrollos locales en la Unión Europea.

Estonia

Estonia cuenta con el sistema de identificación nacional de mayor alcance en todo el mundo, que facilita acceso a todos los servicios digitales como prueba de identidad en cualquier entorno digital. A finales de 2014 el gobierno estonio lanzó la iniciativa de e-Residency, un sistema de identidad digital transnacional que Estonia ofrecía a sus ciudadanos y ahora extendía a todo el mundo. La tarjeta de identificación permite, desde cualquier parte del mundo trabajar con el gobierno y bancos estonios, y para 2018 será aceptado como sistema de identificación en todos los países de la Unión Europea. Además, Estonia es pionera con el programa X-Road, que permite a sus agencias y partes del gobierno compartir datos de forma segura y privada. eliminando la necesidad de ir con fotocopias, duplicados, fotos nuevas, y datos básicos para cualquier gestión. Se cuenta adicionalmente con una ley de Identidad de Documentos (RT1 I 1999, 25, 365). Ley de Firmas Digitales (RT1 I 2000, 26, 150). Así como los principios generales del Código Civil, Código de Comercio y Ley de propiedad. Para utilizar los servicios electrónicos de identificación de tarjetas y e-ID se debe: i) Descargar Software de DNI, ii) Obtener un PIN, iii) Contar con un ordenador o teléfono móvil con conexión a Internet y iv) Tener un lector de tarjetas.

Estonia es el país de mayor referencia en este indicador, debido a que su gestión de la identidad se ha enfocado en mucho más que brindar una única identidad digital a la totalidad de sus ciudadanos, ya que también ha incluido en su ecosistema a no ciudadanos, es decir a los residentes de otras nacionalidades que tienen vínculos familiares o laborales en el país. Asimismo, otro componente positivo de su gestión es el otorgamiento de una identidad digital a través de un dispositivo móvil, como un Smartphone. La cobertura de población con identidad es del 98% y actualmente, el 12% de la población estonia gestiona su identidad a través de un dispositivo móvil, es decir autentifica su identidad para el uso de transacciones a través de un dispositivo.

Reino Unido

Reino Unido cuenta con un marco regulatorio definido a partir de buenas prácticas en materia de identificación nacional, que son emitidas por el Gabinete de Gobierno y los servicios de Gobierno Digital. GOV.UK Verfiy constituye un nuevo modelo de identificación, construido por el sector público en conjunto con el sector privado y el grupo asesor del consumidor y de la privacidad. GOV.UK Verify es un modelo federado - el Gobierno establece las normas y la Oficina del Gabinete gestiona el flujo de demanda del Gobierno y las relaciones comerciales con empresas previamente certificadas y autorizadas (proveedores IdP). Los proveedores IdP son las responsables de desarrollar y prestar servicios que

respondan a esas normas. Los trámites que se pueden realizar mediante el uso de este modelo son estatales únicamente.

La legislación del Reino Unido habilita de manera general mecanismos de autenticación y firmas electrónicas. Se trata de una legislación vanguardista cuyo modelo ha sido muy seguido por la reciente Directiva Europea de Autenticación Electrónica (julio de 2014).

Chile

El sistema de identidad nacional en Chile está definido por el Servicio de Registro Interno, que ha puesto a disposición el Carnet de Identidad cuenta con un Rol Único Nacional (RUN), que es el número de identificación único e irrepetible de todo chileno, y un Rol Único Tributario (RUT), asignado a toda persona nacional o extranjera inscrita en el Registro Civil. La credencial está conformada por una lámina de plástico de polimérico y su impresión es láser. En caso de robo o extravío se puede efectuar el bloqueo de la cédula a través de internet o vía telefónica, además de que sirve también de pasaporte para entrar a Argentina, Brasil, Colombia, Ecuador, Paraguay, Uruguay, Perú, Bolivia y México. Por otra parte, en materia de sistemas de identificación nacional, los Servicios de Registros Internos han puesto a disposición la Clave Única que es una firma electrónica de conformidad a lo dispuesto al artículo 2, letra f) de la ley N° 19.799.

Suecia

Las tarjetas electrónicas eIDs en Suecia están reguladas por la Ley 2000: 832 (SFS 2000) sobre firma electrónica reconocida, que implementa la Directiva 1999/93/CE (un marco comunitario de firma electrónica y su aplicación a nivel nacional) de la Unión Europea. Todas las tarjetas electrónicas eID existentes en Suecia cumplen los criterios para firmas electrónicas avanzadas.

Estructura institucional.

Uno de los elementos más importantes que garantiza un eficiente funcionamiento del ecosistema de identidad es la estructura institucional, factor clave que determina la existencia, competencias, coordinación, comunicación y cooperación de instituciones intervinientes en la ejecución del ciclo de vida de identidad de manera armoniosa y congruente, bajo lineamientos técnicos.

Estudios o experiencias de referencia que avalan la importancia del indicador en el nivel de madurez de los Sistemas de Identidad Nacional son:

- El Banco Asiático de Desarrollo en su reporte Identity for development in Asia and The Pacific, establece como elemento crítico en los Sistemas de Identidad la existencia de una agencia que centralice y coordine a las diferentes instituciones implicadas en la gestión de la identidad y su uso, tales como las entidades de registro, de emisión, de validación, de certificación de calidad, entre otros.
- El Banco Mundial en el estudio ID4D. Technical Standards for Digital Identity señala, "This [institucional structure] aspect of is concerned with defining government goals, modelling business processes and bringing about the collaboration of administrations that wish to exchange information and may have different internal structures and processes". Es así como el rol principal de la agencia reguladora del sistema será el de definir una visión y enfoque unificados que superen toda iniciativa particular o fragmentada de identidad.

  Asimismo, en el estudio Identification for Development (ID4D) Integration Approach se afirma que los países más avanzados en la gestión de identidad desarrollaron un factor de éxito en común, el de definir e implementar la necesidad de contar con un organismo o agencia independiente que supervise el ecosistema de manera integral, con el rol de propietario del sistema nacional de identidad. Con ello, se asegura que el sistema desarrolle de manera independiente los intereses individuales otorgándole un mandato único y nacional a este organismo. De forma complementaria, esta estructura nacional tendrá que establecer los mecanismos de cooperación entre las agencias involucradas en el ciclo de vida de identidad digital, buscando garantizar la contribución formal de estas instituciones.

- Referente al mayor estadio de madurez de este indicador, el Banco Asiático de Desarrollo en el documento Identity for development in Asia and The Pacific señala lo siguiente: "Example of an activity with reference to digital ID interoperability across organizations/countries would be to map the identity lifecycle processes of that organization with the ISO Authentication assurance framework levels". Es decir, el escenario de mayor madurez de este indicador se da cuando las estructuras de generación y uso de la identidad están basadas en estándares internacionales y permiten el uso de identidades de otros países. Por ejemplo, este escenario ya existe en la realidad; las más representativas es la ejecutada por la Unión Europea, como STORK, STORK2.0, eSENS y eIDAS.

Experiencia de Usuario.

Como servicio brindado al ciudadano y por ser uno de los derechos fundamentales de la persona, la experiencia del usuario está muy relacionada con la experiencia que finalmente el ciudadano percibe durante el registro, validación, emisión y uso de esa identidad. Esta experiencia es percibida de manera integral, no sólo se enfoca, por ejemplo, en los procesos o en la tecnología disponible, sino también en la cercanía de los puntos de registro, el catálogo de transacciones que puede realizar, las capacidades de los asesores de servicios, los tiempos de entrega, entre otros. En ese sentido, la experiencia del usuario se convierte en uno de los retos más integrales y que se relaciona de manera directa con los demás elementos del ecosistema de identidad de cualquier país; por ejemplo, la experiencia de usuario que se busque establecer para el ciudadano, no sólo tendrá que resolver las dificultades que el ciudadano mencione, sino también con la regulación del sistema, así como con el cumplimiento por parte del Estado de otorgamiento de un derecho fundamental como la identidad.

En los estadios de madurez de un sistema respecto a la experiencia de usuario, se consideran como puntos críticos al enfoque con el que se implementen mejoras a la operación del ecosistema; es decir, en base a qué estrategia, se desarrollan las mejoras al ciclo de vida en el que el ciudadano solicita, registra y usa su identidad. En un primer momento, cuando se empiezan a establecer mejoras, estas se desarrollan identificando dificultades higiénicas que resuelven problemas puntuales y en su mayoría, no tienen mayor impacto en la percepción del ciudadano. Un paso siguiente, es diagnosticar las principales problemáticas de la operación de manera integral; con este input, las iniciativas que se desarrollen tendrán un alto impacto, ya que se eliminarán retrabajos, duplicidades y vacíos, se automatizarán tareas, pero aún de manera interna. El estadio más maduro de este indicador implica incorporar la voz del ciudadano a través de la realización de encuestas, cuestionarios, entrevistas a profundidad que develen las expectativas y las principales dificultades que tiene el ciudadano para la utilización de su identidad en distintos escenarios y ámbitos. Con este input, es posible lograr un alto impacto en la experiencia del usuario.

En ese sentido, existen estudios o experiencias de referencia que avalan la importancia del indicador en el nivel de madurez de los **Sistemas de Identidad Nacional**, los cuales son:

- **El Banco Interamericano de Desarrollo elaboró el estudio "Simplificando Vidas. Calidad y satisfacción con los servicios públicos"**[7] que tiene el objetivo de analizar

[7] publications.iadb.org/bitstream/handle/11319/7975/Simplificando-vidas-Calidad-y-satisfaccion-con-los-servicios-publicos.pdf

cuantitativa y cualitativamente los índices de satisfacción de los ciudadanos latinoamericanos respecto a los servicios que les brinda el Estado; es decir comprobar la existencia entre la gestión de los servicios y la experiencia que el ciudadano vive al realizar alguno de ellos. Este racional permitirá que, al desarrollar alguna iniciativa de optimización del servicio, esta pueda estar respaldada o validada por la necesidad o percepción que el ciudadano tenga acerca de la problemática que esta iniciativa quiera resolver, evitando la asignación de recursos a iniciativas que el ciudadano no valore o finalmente no resuelvan la dificultad identificada.

El objetivo del estudio no es establecer planes de acción para cada trámite realizado en los países analizados; sin embargo, sí de determinar líneas de acción en función a un mismo formato de medición para todos los países y todos los trámites. Por ejemplo, se analizó bajo el mismo marco de evaluación los procedimientos de registro de nacimiento y la renovación de los documentos de identidad. A pesar de que la evaluación tenía los mismos campos a evaluar, no es cierto que todos los países necesiten implementar grandes proyectos tecnológicos para optimizar sus sistemas, tal es así que Chile busca optimizar de manera electrónica más que implementar tecnología que robustezca el sistema; por otro lado, Panamá optó no solo por modernizar la captura de la identidad, sino de otorgarle calidad bajo la implementación de estándares internacionales al sistema de identidad.*8*

- La Secretaría de Gestión Pública de la Presidencia del Consejo de Ministros del Perú se encuentra realizando arduos esfuerzos en estandarizar las políticas y estándares de atención al ciudadano9 para todas las entidades que tienen esta competencia, dentro de ellas el Registro Nacional de Identificación y Registro Civil (RENIEC), quien se encarga del registro, validación y emisión de la entidad en este país. En ese sentido, estos estándares aplican de manera general a los siguientes ámbitos de la operación de cualquier entidad que atienda a un ciudadano: **a) estrategia y organización, b) usuario de la entidad, y c) accesibilidad y canales, d) infraestructura y mobiliario para la atención, e) medición de la gestión, f) reclamos y sugerencias, y g) diseñar e implementar un proyecto para mejorar la atención a la ciudadanía.**
  Con estos estándares definidos, se establecen marcos de referencia integral para toda la operación de cara al ciudadano.

8 blogs.iadb.org/gobernarte/2017/01/24/calidad-y-satisfaccion-ciudadana-con-el-registro-civil-y-la-gestion-de-la-identidad/
9 sgp.pcm.gob.pe/wp-content/uploads/2016/10/manual-atencion-ciudadana.pdf

Sistemas y tecnología.

Uno de los retos más importantes en los sistemas de identidad es asegurar la interoperabilidad en todo el ciclo de vida de la identidad (enrolamiento, validación, emisión y uso), a través de organismos e instrumentos de coordinación que diseñan y definen el uso de estándares internacionales aplicables a sistemas de identidad de cualquier país. El uso de estos estándares internacionales permite garantizar la interoperabilidad de la tecnología utilizada, incluso hasta niveles que traspasan las fronteras nacionales.

Es así como existen organismos internacionales y también países que han realizado esfuerzos en materia de diseño de estándares de aplicabilidad.
A continuación, algunos ejemplos:

- European Commitee for Standarization (CEN) and National Institute of Standards and Technology (NIST), así como organizaciones privadas como International Organization for Standarization (ISO), Open ID Foundation, FIDO Alliance, GSMA y Secure Identity Alliance, entre otras, tienen el objetivo de incrementar la interoperabilidad de los sistemas de identidad, construyendo o definiendo estándares aplicables.

- En ese sentido, existen países que cuentan con entidades que regulan y aseguran que los diferentes proveedores de servicios de identidad, siguen estos estándares para durante el ciclo de vida de la identidad (como T-Scheme en el Reino Unido).

  Adicionalmente, encontramos organizaciones e instrumentos supra-nacionales, como The European Data Protection Board (EDPB) y electronic IDentification, Authentication and trust Services (eIDAS), que establecen unos requerimientos mínimos que los países miembros deben cumplir para asegurar la interoperabilidad de sus sistemas, introduciendo en este concepto el nivel de madurez más alto para este indicador, es decir la interoperabilidad transfronteriza del sistema de identidad de un país.

Por otro lado, el uso de estándares de encriptación de datos, intercambio de información, biometría y otros, hace posible que sistemas externos puedan verificar la información del sistema de identidad y utilizarlo en transacciones. Ello dependerá de la tecnología utilizada para la emisión de la identidad y de los mecanismos de enrolamiento que se utilicen, así como si se utiliza biometría en el proceso o se emiten tarjetas SmartCard o similares, para la generación de la identidad.

A continuación, se listarán los estándares que corresponden a un estadio maduro tanto para los sistemas que utilizan sistemas biométricos, como los que utilizan credenciales físicas.

En el caso de países que utilicen sistemas biométricos, existen 3 estándares de mayor alcance internacional y cobertura:

- El ISO 19794 define el formato de intercambio biométrico entre diferentes sistemas, para varios tipos de datos biométricos (reconocimiento facial, iris, huella dactilar,), especificando los sistemas de encriptación y criptográficos necesarios para garantizar el intercambio seguro de esta información que es extremadamente sensible a ciberataques o robos de identidad;
- El ISO/IEC 29794-X (donde X identifica el algoritmo biométrico correspondiente) define la calidad de la biometría. En este sentido, también son importantes seguir los niveles de calidad de captura definidos en "U.S.- National Institute of Standards and Technology's (NIST) y Fingerprint Image Quality (NFIQ)";
- El ISO 29109 define la metodología de prueba que debe realizar un sistema para intercambiar información biométrica, siguiendo los formatos definidos en el ISO/ IEC 19794;

Para los países que sus sistemas de identidad estén basados en la emisión de una credencial física, los estándares internacionales que mayor madurez son los siguientes:

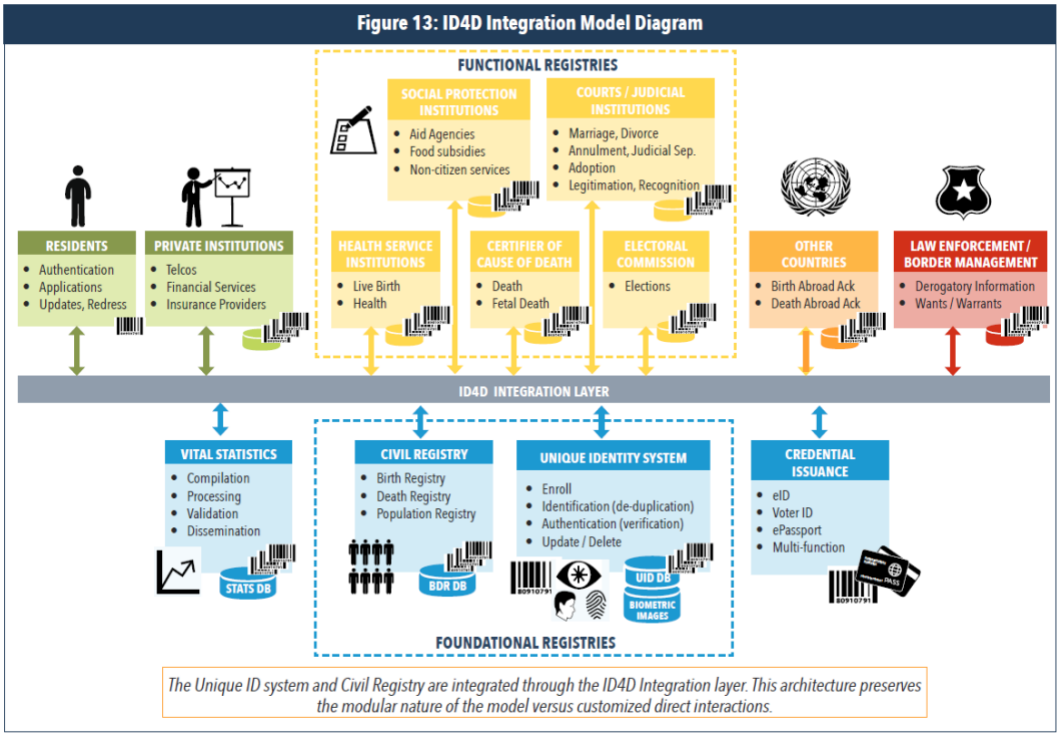
- Los ISO-7810 e ISO- 7813 son importantes para asegurar la interoperabilidad y conectividad de credenciales como el SmartCard;
- El ISO/IEC 7816 utilizado en su mayoría para tarjetas de contacto;
- El ISO/IEC 14443 diseñado para contact less (tipo NFC: Near-field communication);
- El ICAO 9303 es estándar complementario si se adiciona el atributo de utilizar la credencial como documento de viaje, permitiendo que pueda ser leído y verificado de forma automática en el paso de las fronteras (MRTD: Machine Readable Travel Documents);
- El Estándar EMV (Europay, Mastercard y Visa) permite el uso de la credencial para sistemas de pago;
- El ISO 18103 es un atributo de uso para licencia de conducción.

Además de la capacidad del mecanismo de identidad para ser utilizado para cualquier transacción independiente de la geografía, propósito y ámbito de uso; el desafío aún más complejo, es el nivel de

integración de este mecanismo con los servicios brindados al ciudadano tanto el ámbito privado como público.

En ese sentido, se busca que el nivel óptimo de un sistema de identidad tenga un nivel de integración completo de la información relacionada a la identidad con las transacciones a realizar en el ámbito público y privado. Para ello, los estadios menores refieren a niveles intermedios o parciales de esta integración, pudiendo utilizar esta identidad en algunos sectores comerciales o públicos.
En ese sentido, existen estudios o experiencias de referencia que avalan la importancia del indicador en el nivel de madurez de los Sistemas de Identidad Nacional, los cuales son:

El Banco Mundial en el estudio *ID4D. Technical Standards for Digital Identity* [10] describe a un sistema de identidad en su mayor nivel de desarrollo, como un sistema capaz de integrar la información que lo compone con otros ámbitos. Para ello, el registro fundacional deberá ser lo suficientemente potente para fungir de infraestructura troncal para entregar servicios a los usuarios finales.



10 pubdocs.worldbank.org/en/579151515518705630/ID4D-Technical-Standards-for-Digital-Identity.pdf

Actualmente, la implementación de Gov.UK Verify permite realizar 782 servicios que cubren diferentes sectores como (Banca, Finanzas, Administración Tributaria, Justicia, Transporte, Vivienda, entre otros), habiéndose realizado 892 millones de transacciones por año, en promedio. Es así que la experiencia de este país es uno de los más referentes para este indicador, debido a que el programa de GOB.UK Verify, el cual permite a través del uso de los mecanismos portables de identidad, realizar las siguientes transacciones:

- Gestión de créditos financieros (Sector Banca y Finanzas)
- Nacimientos, muertes, matrimonio, sociedades civiles y otorgamiento de poderes (Sector Público)
- Votación y participación comunitaria (Sector Público)
- Procesos legales, tribunales y policiales (Sector Justicia)
- Impuestos vehiculares, licencias de conducir (Sector Transporte)
- Admisión a escuelas, pasantías y créditos vehiculares (Sector Educación)
- Pasaportes, viajes, visas e inmigración (Sector Público)
- *Pago de impuestos (Sector Público*

8. Bibliografía y Referencias

- Autorización de procedimentos de vídeo-identificación. SEPBLAC, Servicio Ejecutivo de la Comisión de Prevención de Blanqueo de Capitales e Infracciones Monetarias, España, 2016. Actualizada en 2019

- Circular 3/2017 (GW) - video identification procedures BaFin, Federal Financial Supervisory Authority, Alemania 2014. Actualizada en 2019

- The Forrester Banking Wave™: European Mobile Apps, Forrester Report Q2 2019

- A.T. Kearney Retail Banking Radar Report, A.T. Kearney 2019

- World Payments Report 2018, CAP Gemini BNP Paribas 2018

- Global Banking Fraud Survey KPMG, May 2019r

- Anil K. Jain (2008). Biometric authentication. Scholarpedia, 3(6):3716.

- **(Regulación eIDAS)** REGLAMENTO (UE) No 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 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.

- **(Regulación PSD2)** Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo de 25 de noviembre de 2015 sobre servicios de pago en el mercado interior y por la que se modifican las Directivas 2002/65/CE, 2009/110/CE y 2013/36/UE y el Reglamento (UE) no 1093/2010 y se deroga la Directiva 2007/64/CE.

- **(Directiva AML5)** DIRECTIVA (UE) 2018/843 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 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 (PSD2)

- **(Regulación GDPR)** Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (GDPR)