Resumen: Guía de Identidad Digital del GAFI Aspectos Relevantes

El creciente volumen de transacciones digitales, la ubicuidad de internet y la posibilidad de aplicar masivamente soluciones digitales motivó al GAFI a ofrecer una guía para lograr un mejor entendimiento de cómo los individuos están siendo identificados y verificados en la industria de servicios financieros digitales.

En este artículo se presentan sucintamente las consideraciones que plasmó el GAFI frente a los procesos de identificación digital en su guía emitida el mes de marzo y dirigida tanto al sector privado y público. Será imprescindible que el lector se encuentre familiarizado con *Las 40 Recomendaciones* del GAFI, esencialmente con la número 10.

Definiendo el concepto de Identidad

Para propósitos del GAFI, identidad se refiere a la identidad oficial. Esta es aquella basada en características de la persona que la hacen única en un grupo de población o contexto específico al tiempo que es reconocida por un estado para propósitos regulatorios y legales.
La forma de probar la identidad oficial varía entre jurisdicciones pero, generalmente, depende de la emisión de algún registro, certificado o documento creado por un ente gubernamental, tal como la *Cédula de Ciudadanía* (Colombia) o *Documento Nacional de Identidad* (Argentina, Perú), y que es ampliamente aceptado por distintas agencias.

Sistemas de Identificación Digital

Procesar la identidad para fines de debida diligencia y posteriormente para todo tipo de movimientos electrónicos exige el uso de Sistemas de Identificación Digital (SID); estos emplean medios digitales para corroborar y probar la identidad oficial de una persona que se desenvuelve en un entorno on-line, con ciertos niveles de seguridad.

Los SID involucran dos componentes básicos y un tercero opcional para su operación:

- **<u>Componente 1</u>:** Comprobación de identidad y enrolamiento (con vinculación y credencialización inicial).

La comprobación de identidad responde a la pregunta *¿quién eres tú?* y se refiere al proceso mediante el cual un proveedor de SID **recolecta, valida y verifica** información sobre una persona para finalmente establecer que se trata de una persona única dentro de un grupo de población o contexto específico. La siguiente gráfica ilustra las actividades al interior de este componente, van desde que el cliente es un aplicante hasta convertirse en miembro activo de la entidad (o suscriptor):

- **<u>Componente 2:</u>** Autenticación y gestión del ciclo de vida de la identidad.

Responde a la pregunta *¿eres el individuo con la identidad previamente verificada?* En otras palabras, se trata de establecer si la persona que está afirmando una identidad, es la misma que inicialmente se enroló y a la que se le asignaron ciertas credenciales y autenticadores.

Por autenticadores se entiende a los factores que pueden ser usados para confirmar una identidad, son ampliamente conocidos en la industria de prevención del fraude y se dividen en tres categorías:

1. De propiedad: claves criptográficas.
2. De conocimiento: contraseñas, preguntas clave.
3. Inherentes: biometría.

En la práctica se conoce como "algo que el cliente tenga, sepa y sea".

- **<u>Componente 3</u>:** Mecanismos de interoperabilidad y portabilidad.

La identidad portable significa que una credencial digital de identificación de un individuo pueda ser usada para probar la identidad oficial ante nuevos sectores, privados o gubernamentales, para acceder a nuevos servicios sin que estas últimas tengan que someter a un proceso repetitivo de identificación y verificación al cliente cada vez.
El GAFI resalta que parte del primer componente (la prueba de identidad y el enrolamiento) pueden ser digitales o físicos. Sin embargo, el resto de componentes como la credencialización, la autenticación y la portabilidad son siempre y necesariamente digitales para un SID.

Estándares GAFI y Procesos de Debida Diligencia

La Recomendación 10 requiere que las jurisdicciones impongan obligaciones sobre las entidades para que ejecuten procesos de debida diligencia usando ***<u>documentos, datos o información de fuentes independientes y confiables.</u>*** ¿cómo se relaciona esto en un entorno de identificación digital y qué rol cumplen los criterios "independientes y confiables"?

En el contexto de la identificación digital, ser "confiables e independientes" significa que el Sistema de Identificación Digital (SID) utilizado para llevar a cabo la debida diligencia de clientes debe basarse en procesos y

procedimientos tecnológicos con un adecuado gobierno, tal que proporcione resultados precisos con un nivel adecuado de confianza. De otro lado, significa que el SID cuenta con medidas de mitigación para prevenir los tipos de riesgos abordados más adelante.

Por supuesto, el enfoque basado en riesgo continúa siendo una directriz en el contexto de debida diligencia empleando identificación digital, tal como se viene trabajando años tras, por lo que el GAFI no plantea nada nuevo.

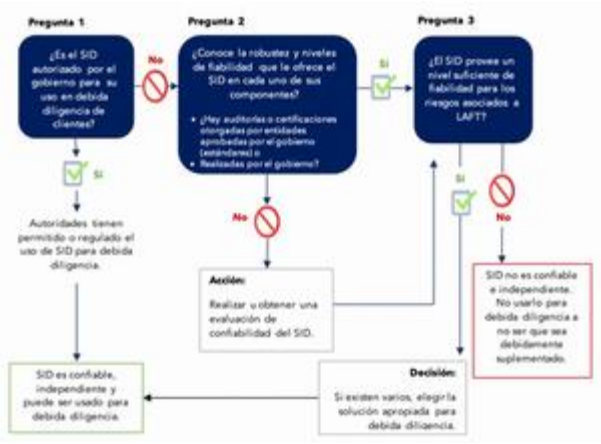
Un cambio detectado tiene que ver con la Nota Interpretativa de la Recomendación 10, que consideraba a las transacciones no presenciales (incluida la vinculación de clientes) como un ejemplo de circunstancias donde el riesgo LAFT podía potencialmente ser más alto.

Ahora el GAFI clarifica que en lo que respecta a identificación y transacciones que reposan sobre SID confiables e independientes, con medidas apropiadas de mitigación de riesgos, puede presentarse un nivel de riesgo normal o incluso más bajo. Esto sin duda es un cambio de posición frente al uso de tecnologías digitales.

En cuanto a la terciarización de procesos, el GAFI mantiene lo plasmado en la Recomendación 17, en ella se indican las condiciones que debe cumplir un tercero para proveer los servicios de debida diligencia a una entidad regulada, trasladándose casi íntegramente al contexto de identificación digital. Este hecho no es aplicable a las situaciones de outsourcing o relaciones de agencia, donde la Recomendación 17 no aplica y el GAFI lo deja bastante claro.

¿Cómo Identificar un SID confiable e independiente bajo un enfoque basado en riesgo aplicado a debida diligencia?

Las entidades reguladas (bancos, financieras, proveedores de activos virtuales, exchanges, otras) que estén en miras de emprender un Sistema de Identificación Digital para la vinculación de sus clientes y tratamiento de los actuales deberían cuestionarse lo siguiente.



Beneficios y desventajas de la identificación digital

Los beneficios del uso generalizado de la identidad digital tienen alcances más extensivos que la mera industria financiera, pueden ser aplicables a servicios de salud, tramites gubernamentales, entre otros. En relación puntual a los estándares GAFI se tiene:

- Facilitar la identificación y verificación de los clientes en el proceso de on-boarding (reducción del error humano por ejemplo al comparar dos fotografías y la reducción en los juicios de valor que pueden derivar en discriminación)

- Apoyar la debida diligencia continua y el escrutinio de transacciones durante la relación banca-cliente: todo ello al tiempo que se mejora la experiencia del cliente aumentando la retención del mismo.

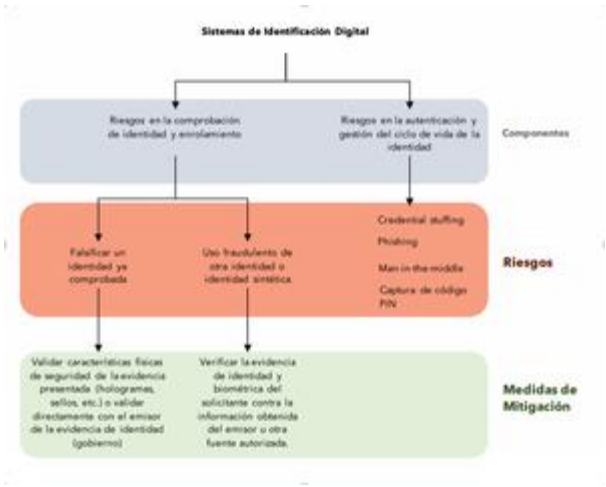
- Facilitar otras medidas de debida diligencia sobre el cliente.

- <u>Ayudar en la detección y reporte de transacciones sospechosas:</u> la entidad regulada puede establecer si la persona accediendo a una cuenta y realizando transacciones hoy, es la misma persona que accedió a la cuenta anteriormente. Aún más importante, dota a la entidad regulada de información adicional como geolocalización, dirección IP, dispositivo usado, entre otras permitiendo alcanzar mayor robustez en el reporte de operación sospechosa.

Riesgos de la Identificación Digital

Muy cautelosos, el GAFI aclara que los riesgos considerados deben acotarse exclusivamente a los SID en el marco de la debida diligencia y que de ninguna forma se pretende establecer que estos son mayores o menores que los beneficios.

La discusión se centra en dos de los componentes de SID: la comprobación de identidad y la autenticación. La siguiente gráfica sintetiza las previsiones del GAFI pero también incorpora juicios propios del autor.



En general, son consideradas las amenazas que enfrenta la digitalización a nivel global. Se incluyen en la guía obstáculos de conectividad, fricciones con la regulación de distintos países, desafíos en cuanto a la protección de datos y privacidad, así como la posible exclusión de ciertos grupos poblacionales al acceso de tecnología digital. Llama la atención que el GAFI deja espacio para lo que denominan “Riesgos Desconocidos” dando a entender que se espera una mayor evolución de los SID y la aparición de nuevos actores que exploten vulnerabilidades aún inexistentes.