DEBIDA DILIGENCIA E IDENTIDAD DIGITAL - ORIENTACIÓN SOBRE LA IDENTIFICACIÓN DIGITAL, GAFI[15]

KARINA MARIEL ARGÜELLO[16]

INTRODUCCIÓN

La transformación digital empujó inclusive al más reacio a su adopción en épocas pandemia, y esta situación, que multiplicó las transacciones digitales, llevó a acelerar la incorporación de los procesos de identificación digital, tanto en las empresas, como en los organismos gubernamentales. Los aliados estratégicos del sistema de prevención de lavado de activos y financiamiento del terrorismo, que en nuestro país denominamos sujetos obligados, debieron multiplicar sus esfuerzos para lograr verificar e identificar a sus clientes. Para comprender cómo funcionan los sistemas de identificación digital para la aplicación correcta de un enfoque basado en riesgo, en marzo de 2020, llegó la guía de Identidad Digital[17] publicada por el Grupo de Acción Financiera Internacional (GAFI), con los lineamientos para la implantación de sistemas de identidad digital, en las etapas de identificación, verificación y análisis de riesgo de individuos, y la misma, está "destinada a ayudar a los gobiernos, las entidades reguladas u otras partes interesadas relevantes, en determinar cómo se pueden utilizar los sistemas de identificación digital para llevar a cabo ciertos elementos de la debida diligencia de clientes (DDC) en virtud de la Recomendación 10[18]". Recordemos que esta recomendación está dentro de las medidas preventivas que involucran la debida diligencia de cliente, e incluye los siguientes puntos:

a) Identificar y verificar la identidad del cliente utilizando documentos, datos o información confiable, de fuentes independientes.
b) Identificar al beneficiario final y tomar medidas razonables para verificar la identidad del beneficiario final
c) Entender, y cuando corresponda, obtener información sobre el propósito y el carácter que se pretende dar a la relación comercial.
d) Realizar una debida diligencia continua de la relación comercial y examinar las transacciones llevadas a cabo a lo largo de esa relación para asegurar que las transacciones que se realicen sean consistentes con el conocimiento que tiene la institución sobre el cliente, su actividad comercial y el perfil de riesgo, incluyendo, cuando sea necesario, la fuente de los fondos.

[15] Grupo de Acción Financiera Internacional (GAFI o FATF, por su sigla en inglés)

[16] Licenciada en Marketing (UCES) con Especialización en Ciencias Sociales (FLACSO) y Especialización en Prospectiva Estratégica (TFI en elaboración) (UCES). Certificada en Ética y Compliance (UCEMA - AAEC- IFCA). Diplomada en Prevención de Lavado de Activos, Cibercrimen y Financiamiento del Terrorismo. (UCES). Soy idóneo en mercado de capitales, integrante del equipo de Aeromar Valores SA. Participó como docente adjunta de la materia "Sistemas de Información Gerencial" para las carreras: Lic. En Comercio Exterior y Lic. en Marketing (UCES). Desde el año 2020, formo parte del plantel docente de la Diplomatura en Prevención de Lavado de Activos, Cibercrimen y Financiamiento del Terrorismo y de la Certificación en PLA/FT orientada a sujetos obligados.

[17] Fuente: GAFI (2020), Orientación sobre Identidad Digital, GAFI. Recuperado el 17/04/2022 en:https://www.fatf-gafi.org/publications/fatfrecommendations/documents/digital-identity-guidance.html

[18] La Recomendación 10, forma parte de las 40 Recomendaciones emitidas por el GAFI, que establecen un estándar internacional, que los países deben implementar a través de medidas adaptadas a sus circunstancias particulares.

A los fines de este artículo, les comparto los puntos que consideré importantes de la guía, para la incorporación de clientes no presenciales, en cuanto a seguridad, privacidad y conveniencia, tanto en el momento de apertura de cuentas como a lo largo de la relación comercial.

¿QUÉ ES LA IDENTIDAD DIGITAL?

En esta guía, con el fin de "identificar al cliente y verificar la identidad de ese cliente", con el término "identidad" el GAFI se refiere a la identidad oficial, que es distinta de los conceptos más amplios de identidad personal y social que pueden ser relevantes para fines no oficiales (ej. información por interacciones comerciales o por redes sociales). Es decir, cubre el uso de sistemas de identificación digital para probar la "identidad oficial" para el acceso a los servicios financieros. Entonces, la identidad oficial se trata de una especificación de la persona humana que:

- Se basa en características (atributos o identificadores) de la persona que establecen la singularidad de esta, en la población o en un contexto particular.
- Es reconocido por el estado para propósitos reglamentarios y oficiales.
- Generalmente depende de alguna forma de registro, documentación o certificación proporcionada o emitida por el gobierno que constituye evidencia de los atributos básicos para establecer y verificar la identidad oficial.

Entonces, la identidad digital se trata de un conjunto de registros digitales que nos permite verificar que una persona es quien dice ser, pudiéndose autenticar de forma remota a través de canales digitales, que pueden ser independientes de la entidad emisora de la identificación y de la tecnología específica utilizada para la autenticación que va desde el uso de contraseñas, PIN[19], tokens[20], etc.

Hablamos de un sistema de identificación digital que utiliza medios electrónicos para afirmar y probar identidad oficial de una persona en línea, cubriendo el proceso de prueba/ registro de identidad y autenticación sin tener en cuenta los componentes del sistema, es decir, los tipos de tecnologías usadas, procesos o arquitectura que cada país logre desarrollar. Sin embargo, GAFI menciona como relevantes una gran gama de tecnología como: la biometría, que consiste en la medición estandarizada de los individuos (por ejemplo, las mediciones pueden estar basadas en el color de ojos o en la lectura del iris, o en los rasgos faciales, la marcha o la frecuencia cardiaca), también encontramos la casi ubicuidad de Internet y los teléfonos inteligentes, identificadores de dispositivos digitales e información relacionada (p. ej., direcciones MAC21 e IP[22];10 números de teléfonos móviles, tarjetas SIM[23], geolocalización del sistema de posición global (GPS)); escáneres de alta definición (para escanear tarjetas de identificación, licencias de conducir y otros documentos); transmisión de video que permiten la identificación, verificación y prueba de vida; inteligencia artificial/aprendizaje automático (p. ej., para determinar la validez de una identificación emitida por el gobierno).

[19] PIN: Personal Identification Number, se trata de una contraseña extra que se puede activar para proteger el ingreso a una cuenta.

[20] Tokens: también llamado clave electrónica, es un dispositivo físico para acceder a una cuenta y complementar la contraseña.

[21] MAC: Media Access Control, se trata de una dirección física y única para cada dispositivo.

[22] IP: Protocolo de internet, permite identificar una red o dispositivo en internet.

[23] SIM: Subscriber Identity Module, se trata de un dispositivo con un chip que almacena los datos telefónicos y claves de acceso del usuario.

El sistema de identidad digital tiene dos componentes básicos y un tercer componente opcional:

- Prueba de identidad e inscripción: ¿responde a la pregunta quién eres? Por lo tanto, es esencial, porque implica:
- Recopilación: se trata atributos de identidad y evidencia (ej. Completando un formulario en línea, cargando documentos o enviando una selfie
- Validación: inspección para garantizar la autenticidad (ej. Verificando atributos a través de otros servicios)
- Verificación: vincular al individuo con la evidencia de identidad proporcionada (ej. Usando soluciones biométricas como reconocimiento facial y detección de vida)
- Inscripción: crear la cuenta de identidad vinculando uno o más autenticadores (ej. Contraseñas o un generador de código de único uso)
- Autenticación y gestión del ciclo de vida de la identidad, responde a la pregunta: ¿es usted la persona que ha sido identificada y verificada? Y por lo tanto se trata de un componente también esencial en el sistema.

Este paso se puede llevar delante de acuerdo con 3 factores:

I. factores de propiedad (ej. claves criptográficas)
II. factores de conocimiento (ej. una contraseña)
III. factores inherentes (ej. datos biométricos)
IV. Es importante tener presente que la "autenticación" de los clientes existentes también es una medida de seguridad importante para la diligencia debida continua y la autorización del acceso a la cuenta.
    - Mecanismos de portabilidad e interoperabilidad. (opcional). Donde la prueba de identidad es portátil, es decir que la identificación digital se puede usar para probar la identidad oficial para nuevas relaciones con clientes en entidades gubernamentales o del sector privado relacionadas.

IDENTIDAD DIGITAL Y DEBIDA DILIGENCIA DEL CLIENTE

La recomendación 10 no impone restricciones sobre la forma física o digital para tomar las pruebas de identidad y en el contexto de la identificación digital, el requisito de que los "documentos, datos o información de origen" digitales deben ser "confiables e independientes" se traduce en que “el sistema de identificación digital utilizado para llevar a cabo la debida diligencia del cliente se basa en tecnología, gobernanza adecuada, procesos y procedimientos que brindan un nivel adecuado de confianza en que el sistema produce resultados precisos”. Por otra parte, la nota interpretativa de la recomendación 10 incluye las relaciones comerciales o transacciones que no son cara a cara como un ejemplo de una situación de riesgo potencialmente mayor, sin embargo, no requiere que se las catalogue como de mayor riesgo y tiene en cuenta además, la evolución tecnológica, los procesos y estándares técnicos para aclarar que la identificación del cliente y las transacciones que no son cara a cara, que dependen de sistemas de identificación digital confiables e independientes y con medidas apropiadas de mitigación de riesgos, pueden presentar un nivel de riesgo menor.

Otra consideración importante es la posibilidad de dependencia de terceros en el contexto de identificación digital (donde las entidades reguladas también actúan como proveedores de servicios de identificación digital), en cuyo caso, la entidad designada sigue siendo responsable de llevar adelante los pasos de identificación/verificación efectiva del cliente y una autenticación efectiva, utilizando el sistema de identificación digital proporcionado por el proveedor de servicios de identificación digital, y tendrían que aplicar el enfoque basado en riesgo al uso de sistemas de identificación digital, para la identificación/verificación y autenticación del cliente.

Como cierre no quiero dejar de considerar los beneficios potenciales que se marcan en la guía:

- Los sistemas de identificación digital tienen el potencial de mejorar la confiabilidad, seguridad, privacidad, conveniencia y eficiencia de la identificación de personas en la prestación de servicios financieros, en beneficio de los clientes, las entidades reguladas y la integridad del sector financiero.
- La posibilidad de minimizar las debilidades en las medidas de control humano.
- Mejorar la experiencia del cliente y generar ahorros en costos.
- Y una de las más importante, la inclusión financiera.
- Algunos riesgos y desafíos:
- La confiabilidad podría verse socavada por el robo de identidad, la información podría falsificarse o manipularse o se podrían perder datos o usar de forma indebida.
- Los procesos y tecnologías empleados por los sistemas de identificación digital presentan múltiples oportunidades para ataques cibernéticos.
- Desafíos de conectividad, de ciberseguridad y privacidad en el espacio digital que pueden afectar la integridad o disponibilidad de los sistemas de identificación digital para llevar a cabo la DDC.

CIERRE

En base lo visto considero pertinente sumar otra pregunta para reflexionar: ¿el sistema de identificación digital que usamos: es apropiado para la identificación/verificación del cliente y la debida diligencia continua, a la luz de los posibles riesgos de LA/FT asociados con el cliente, los productos y servicios, y el área geográfica de las operaciones?

La respuesta queda en mano de los aliados estratégicos o sujetos obligados, que deben hacer coincidir la solidez de la prueba de identidad y/o autenticación del sistema, con el tipo de posibles actividades ilícitas y el nivel de riesgos de lavado de activos y financiamiento del terrorismo.