VALIDACIÓN DE LA IDENTIDAD EN EL CONTEXTO DIGITAL

Vielky M. Álvarez Martínez

Santo Domingo, República Dominicana

30 de junio de 2023

RESUMEN EJECUTIVO

En el contexto empresarial, especialmente cuando se manejan fondos de terceros, es fundamental conocer la identidad de las personas involucradas para prevenir actividades ilícitas como el lavado de activos, el financiamiento del terrorismo y la proliferación de armas de destrucción masiva. La validación de la identidad es un requisito mínimo en los procesos de debida diligencia que busca garantizar la seguridad y cumplimiento normativo. A medida que la tecnología ha evolucionado, la identidad ha adquirido nuevas formas digitales, lo que ha llevado a la necesidad de implementar métodos de autenticación y seguridad más avanzados.

La inteligencia artificial ha surgido como una herramienta para mejorar la verificación de identidad, pero también plantea desafíos, como la aparición de identidades sintéticas o *deepfakes*. En ese sentido, es necesario abordar estos desafíos mediante sistemas robustos de autenticación y medidas de seguridad adecuadas, en colaboración con los reguladores, para crear un entorno digital seguro tanto para individuos como para empresas.

VALIDACIÓN DE LA IDENTIDAD EN EL CONTEXTO DIGITAL

En los negocios, especialmente cuando estos implican manejar fondos de terceros, es más que necesario, normativo, conocer la identidad de la persona implicada. Esto último es precisamente así, porque el negocio puede prestarse o servir de medio para el de lavado de activos, financiamiento del terrorismo y la proliferación de armas de destrucción masiva, entre otros.

La validación de la identidad como forma de conocer a los clientes no es más que un requisito mínimo dentro de la obligación de medios que procura asegurar la realización de un mejor esfuerzo dentro de los procesos de debida diligencia. Esto es que, además de seguir un requisito normativo, como en efecto lo es, busca agotar los procesos que ha de efectuar un buen hombre de negocios.

Tradicionalmente, desde que los procesos de apertura de cuentas en las entidades financieras han sido presenciales, las entidades han respondido a la necesidad de verificación de identidad exigiendo determinados documentos como son las cédulas de identidad o pasaportes, en el caso de las personas físicas. En ese contexto, era suficiente validar la identidad de una persona con su acto de presencia a la vez que un oficial de cuentas revisaba el documento de identidad.

Sin embargo, a medida que ha evolucionado la civilización, también lo ha hecho la identidad. Desde la introducción de los pasaportes, los números de identificación personal, la identificación fotográfica y ahora las identidades totalmente digitales, "*la verificación de la identidad se desarrolló paralelamente a la creciente necesidad de proteger y mantener registros precisos de*

datos, transacciones, créditos y normativas cada vez más complejos[1]". Por lo que, lo que tradicionalmente era aceptable y suficiente, hoy en día no necesariamente responde al ritmo / posibilidad de negocios y requerimientos normativos.

La tecnología, como fenómeno disruptivo, ha motivado sin duda alguna la automatización de procesos frente a revisiones manuales tendentes a generar mayores márgenes de error. En este sentido, y, por si fuera poco, la ola Covid-19 aceleró enormemente el proceso de digitalización, de modo que, para continuar con los negocios, por ejemplo, en el mercado de valores dominicano, todo lo que se hacía de manera presencial, pasó a ser digital.

Las nuevas tecnologías plantean retos para la identidad de las personas, siendo el primero de ellos una cuestión de autenticación y seguridad. La experiencia (a modo de ejemplo, en el mercado de valores) de un 2020 en República Dominicana, implicó incurrir en nuevas prácticas de validación de identidad como parte del proceso conozca su cliente.

En ese sentido, la presencia presencial pasó a ser la remisión de una foto sujetando el documento de identidad y/o la gestión de videollamadas. El sector de valores bien pudo haberse identificado con este proceso y encontrado en él una adecuada forma de "autenticación". Sin embargo, una de las tantas oportunidades de mejoras de eso (que en un momento bien pudo valerse de suficiente, pero que pronto comenzó a no serlo), aumentó y/o se destacó tan rápido como el Covid-19; se trata de la usurpación de identidad, la cual según la Comisión Federal de Comercio de Estados Unidos

[1] Joseph Burton, "Digital Identity: Where We Began, Where We Are And Where We Are Going". Forbes, 24 de mayo de 2022. https://www.forbes.com/sites/forbestechcouncil/2022/03/24/digital-identity-where-we-began-where-we-are-and-where-we-are-going/?sh=17e0351675a7

(FTC, por sus siglas en inglés) creció en torno al 45 % solo en 2020, lo que supuso enormes pérdidas económicas para los ciudadanos estadounidenses, llegando a un total de 56,000 millones de dólares en pérdidas, según Javelin Strategy[2].

Bajo el escenario anteriormente descrito, a fin de defender a sus clientes y datos ante los ataques y robos, las empresas empezaron a aumentar la seguridad exigiendo contraseñas más seguras, soluciones automatizadas y métodos de autenticación multifactor, procurando así garantizar la legitimidad de las transacciones y la identidad de los usuarios durante el proceso de incorporación[3]. De ahí que, el término identidad comenzó a acuñar el apellido "digital", de modo que se entendiera por este, toda la información y los datos que identifican a un individuo en el mundo digital; o toda la información relativa a una persona, una organización o incluso un dispositivo que se utiliza para realizar la autenticación en línea[4].

En su informe sobre identidad digital, el Grupo de Acción Financiera Internacional (GAFI) sugirió que el crecimiento de las transacciones financieras digitales requería una mejor comprensión de cómo se identifica y verifica a las personas en el mundo de los servicios financieros digitales. Esto es, como se puede autenticar la identidad. Del mismo modo, la precisión de que los documentos, datos o informaciones de origen digitales fueran "fiables e independientes" significaba que el sistema de identificación digital utilizado para llevar a cabo la diligencia debida con respecto al

[2] Sam Cook, "I Identity theft facts & statistics: 2019-2022". Comparitech, 20 de junio de 2023. https://www.comparitech.com/identity-theft-protection/identity-theft-statistics/
[3] Joseph Burton, *ibíd*.
[4] "Digital identity: The Complete Guide to Digital Identification". Adnovum, 12 de mayo de 2023. https://www.adnovum.com/blog/digital-identity

cliente debía basarse en la tecnología, una gobernanza adecuada y procedimientos que proporcionen niveles adecuados de confianza.

Como respuesta a este reto, surgieron empresas del sector *Regtech*[5] como Mati (MetaMap)[6] y VU Security[7], con herramientas y métodos para la identificación digital como son la autenticación de dos factores (2FA), la autenticación biométrica, el inicio de sesión único (SSO), OAuth y la identidad autosuficiente con carteras digitales[8]."

Sin embargo, cuando apenas el mercado dominicano va apropiándose de validaciones biométricas en los procesos de *onboarding* digital, vemos que el fenómeno de la inteligencia artificial (IA)[9] subvierte realidades en tiempo récord, apuntando a, por un lado, continuar fortaleciendo los métodos antes mencionados, y, por otro, ser el nuevo reto de mejora de estos.

Y es que, si bien la IA pudiera utilizarse para detectar anomalías en el comportamiento de los usuarios y mejorar la precisión de la verificación de identidad, también es la razón de que existan las identidades sintéticas o *deepfakes*. Es decir, un tipo de identidad que confunde lo real con lo no real mediante la manipulación de imágenes y vídeos para crear contenidos realistas pero inventados, que pueden ser utilizados para suplantar a alguien o crear identidades falsas a fin de obtener ventajas económicas, dificultando la detección de actividades fraudulentas.

---

[5] *Regtech* (tecnología reguladora) es una clase de aplicaciones de software para gestionar el cumplimiento normativo.
[6] Plataforma de verificación de identidad online https://es.metamap.com/sobre-nosotros
[7] Empresa de ciberseguridad especializada en la protección de la identidad digital y la prevención del fraude https://www.vusecurity.com/es/about-us
[8] Digital identity: The Complete Guide to Digital Identification, *ibíd.*
[9] Campo de estudio de la informática que se enfoca en la creación y el desarrollo de sistemas y programas capaces de realizar tareas que normalmente requerirían la intervención humana.

Esto último, plantea desafíos tanto legales como éticos. Desde una perspectiva legal, el uso de identidades sintéticas para cometer delitos puede ser considerado fraude, robo de identidad u otras formas de actividad delictiva. Además, el uso de información personal falsa o robada viola las leyes de privacidad y protección de datos.

Son muchos los retos que se suscitan a propósito de validar las identidades en un contexto digital. Garantizar la fiabilidad de las identidades digitales y protegerlas contra el robo, el fraude y el acceso no autorizado es fundamental. Los sistemas de autenticación deben ser robustos y confiables, y las medidas de seguridad adecuadas deben estar en su lugar para proteger la información personal y la integridad de las identidades digitales.

Las salidas o soluciones que surgen parecen no valerse en sí mismas como únicas e inquebrantables, sino que, confirman que, por el momento, la forma de afrontar este desafío es procurando el uso conjunto de métodos o autenticación de dos pasos (OTP, por sus siglas en inglés). Esto es que, en un escenario donde sea posible la validación de la identidad mediante autenticación biométrica, también se procure la confirmación de la persona mediante otro medio como llamada telefónica, mensaje de texto al teléfono registrado o proporcionado y/o al correo electrónico, a sabiendas de que un individuo pudiera crear un correo falso solo para estos fines.

En todo caso, será necesario contar con el apoyo de los reguladores, a fin de establecer directrices y requisitos claros que contribuyan a prevenir el riesgo sistémico, la promoción de la competencia, la mitigación de los riesgos asociados a la usurpación de identidad y la creación de un entorno digital más seguro para particulares y empresas.

BIBLIOGRAFÍA

1. Joseph Burton. "Digital Identity: Where We Began, Where We Are And Where We Are Going". Forbes, 24 de mayo de 2022. https://www.forbes.com/sites/forbestechcouncil/2022/03/24/digital-identity-where-we-began-where-we-are-and-where-we-are-going/?sh=17e0351675a7 (Consultado el 21 de junio de 2023)

2. Sam Cook, "I Identity theft facts & statistics: 2019-2022". Comparitech, 20 de junio de 2023. https://www.comparitech.com/identity-theft-protection/identity-theft-statistics/ (Consultado el 30 de junio de 2023)

3. "Digital identity: The Complete Guide to Digital Identification". Adnovum, 12 de mayo de 2023. https://www.adnovum.com/blog/digital-identity (Consultado el 20 de junio de 2023)

4. The Financial Action Task Force. 2020. Guidance on Digital Identity. París: www.fatfgafi.org/publications/documents/digital-identity-guidance.html