El futuro de la identidad digital

Junio 2022

Biometría, ecosistemas e ID en el panorama digital pospandémico

Informe de iupana, en asociación con Jumio

iupana

jumio

iupana te muestra el futuro de las finanzas en América Latina y el Caribe a través de noticias, análisis y opinión. Te traemos información exclusiva y minuciosa sobre cómo nuestros colegas, competidores y clientes en servicios financieros de Latinoamérica y el Caribe están transformándose con tecnología.

iupana.com

Contenido

Carta a los lectores

A medida que se acelera la tendencia en torno a las transacciones digitales en toda América Latina, las empresas de tecnofinanzas, los bancos, las compañías de medios de pago y demás instituciones financieras deben permanecer un paso adelante en materia de seguridad y fraude, dos áreas en constante evolución.

Hasta hace no mucho tiempo, verificar la identidad de las personas con una herramienta sofisticada como la autenticación biométrica era suficiente. Hoy, en cambio, con nuevos esquemas de fraude y regulaciones cada vez más estrictas contra el lavado de dinero (o AML, por sus siglas en inglés), ya no basta con una simple validación de ID. Las empresas precisan una gama de herramientas digitales para confirmar adecuadamente la identidad de un cliente.

Ahora, la seguridad digital excede ampliamente la verificación biométrica: se trata de combinar distintas herramientas para contar con un sistema de gestión de identidad consolidado y coordinado. Este informe detalla la situación actual en materia de riesgo, fraude y AML en América Latina, y explora las demandas cambiantes respecto de la autenticación de identidad en el entorno digital de la región.

Este informe detalla la situación actual en materia de riesgo, fraude y AML en América Latina, y explora las demandas cambiantes respecto de la autenticación de identidad en el entorno digital de la región.

Katie Llanos-Small
iupana

La naturaleza cambiante de la confianza digital

El entorno financiero digital en América Latina ha crecido enormemente en los últimos años, con Brasil y México a la vanguardia de este proceso. En todos lados surgen empresas de tecnofinanzas, junto con bancos digitales, billeteras digitales y plataformas de criptomonedas, que obligan a todo el ecosistema financiero a repensar su enfoque para abordar las necesidades actuales y futuras de los clientes.

Hasta los bancos tradicionales, que en un principio se mostraron renuentes a pasar al mundo digital, ahora están efectivamente obligados a hacerlo. No solo para cubrir necesidades específicas de los clientes —necesidades que surgieron a partir de la pandemia de COVID-19—, sino también para satisfacer las demandas de generaciones más jóvenes y competir con nuevos bancos tecnológicos o *challenger banks*.

Si bien es cierto que la pandemia impulsó las finanzas digitales, la situación no es tan sencilla. Las innovadoras empresas de tecnofinanzas develaron nuevos modelos de negocios que arrasaron con los métodos tradicionales para efectuar transacciones financieras. Tal es el caso de las transferencias y los pagos transfronterizos, por ejemplo. Las empresas emergentes no solo introdujeron métodos más simples para mover dinero entre países que la típica transferencia electrónica a través de un banco, sino que también ofrecieron tipos de cambio mucho mejores.

Además, las empresas ajenas al sector financiero están diversificando sus actividades e incorporando gradualmente los pagos digitales, para lo cual aprovechan sus amplias bases de clientes. Tomemos como ejemplo el sector de las telecomunicaciones. Algunas empresas de telecomunicaciones tienen cientos de millones de clientes, de manera que la incorporación de una billetera digital a sus aplicaciones para habilitar pagos y proporcionar un servicio más completo parece ser el paso más lógico. Algo similar ocurre con el conjunto cada vez más numeroso de empresas que realizan integraciones verticales diferentes para mejorar sus negocios tradicionales.

Esta es una tendencia sumamente interesante, que cambiará todo el ecosistema financiero y que, en el mejor de los casos, hará que más personas ingresen al sector financiero formal. Sin embargo, esto también presenta nuevos problemas de seguridad que deben abordarse.

El fraude y el lavado de dinero se encuentran entre los principales riesgos a los que están expuestos las empresas. No basta con cumplir las normas: lo que necesitan las empresas es minimizar su vulnerabilidad ante el fraude. La cantidad de pasos necesarios para mejorar la seguridad de una empresa depende de su nivel de exposición al fraude y de su apetito por el riesgo.

Tanto en América Latina como en cualquier otra parte —y así se trate de un banco o de un negocio de comercio electrónico—, se debe tener la certeza de que la persona con la que se está haciendo negocios es quien dice ser. Dicho esto, los requisitos no son los mismos para un banco que para una tienda en línea. Desde la perspectiva de un banco, se debe saber si la persona que abre una cuenta se encuentra en una lista de terroristas, está involucrada en el lavado de dinero o tiene alguna sanción económica. Para determinar todo esto se debe conocer la identidad del usuario.

Desde la perspectiva del comercio electrónico, existen menos regulaciones y la prioridad máxima consiste en prevenir el fraude en la medida en que se pueda determinar si el cliente es realmente un delincuente que intenta usar el número de una tarjeta de crédito robada o una identidad robada.

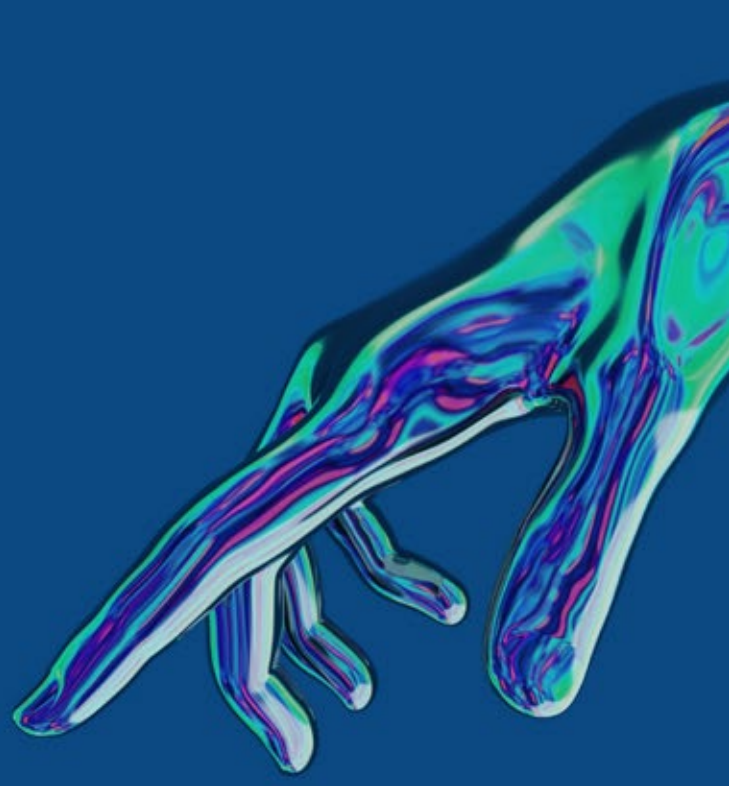
Los motivos pueden variar levemente, pero el desafío sigue siendo el mismo: conocer al cliente (o KYC, por sus siglas en inglés). En el mundo digital, asegurarse de que los clientes sean quienes dicen ser es esencial. Pero también es imprescindible que la experiencia del usuario sea positiva. ¿El objetivo final? Una solución que cumpla con las regulaciones y detecte el fraude, pero que al mismo tiempo evite cualquier tipo de fricción con el usuario. Si no le ofrecemos al cliente la mejor experiencia posible, le estaremos ofreciendo ese cliente a la competencia. ◆

Nuevos desafíos en la prevención del fraude digital

La pandemia ha acelerado el proceso de digitalización, y esto, a su vez, despertó más inquietudes con respecto al fraude, el delito cibernético, el lavado de dinero y la importancia de KYC, según afirma Patrick Aron Rinski, socio de McKinsey y experto en ciberseguridad y riesgos operativos. Rinski señala que las autoridades reguladoras están cada vez más interesadas en saber cómo protegen los datos y qué controles aplican las empresas. Se trata de un equilibrio delicado, ya que la implementación de controles más estrictos puede afectar negativamente la experiencia del usuario.

Otro efecto secundario de la pandemia es el rápido crecimiento de las transacciones en línea, que, desde el sector bancario hasta el comercio electrónico, crean el escenario perfecto para los delincuentes. El sector financiero ya ha sido objeto de muchos ataques cibernéticos o intentos de fraude digital, pero es una industria que se mantiene a la vanguardia de las últimas tendencias tecnológicas, según afirma Eder de Abreu, socio en Deloitte y especialista en temas cibernéticos. Otros sectores están menos preparados para el crecimiento de la demanda de servicios digitales. "Hoy en día, hay muchas empresas que trabajan con una serie de dispositivos y tecnología para mitigar y reducir el fraude y los ataques", además de cumplir con las leyes de protección de datos, señala.

Como parte de este proceso, las empresas están implementando controles adicionales para reducir las posibilidades de sufrir ataques cibernéticos y robo de datos. La autenticación de ID es un tema importante para las empresas que se han convertido a canales digitales. Una opción consiste en aplicar estrategias de verificación como las *selfies* de usuarios sosteniendo su ID o licencia de conducir. Otra es la incorporación de geolocalización y biometría (huellas digitales, reconocimiento de voz y rostro). El uso de un acelerómetro del teléfono móvil para evaluar cómo una persona usa su dispositivo también se convirtió en una tendencia.



"Otro efecto secundario de la pandemia es el rápido crecimiento de las transacciones en línea, que, desde el sector bancario hasta el comercio electrónico, crean el escenario perfecto para los delincuentes. El sector financiero ya ha sido objeto de muchos ataques cibernéticos o intentos de fraude digital, pero es una industria que se mantiene a la vanguardia de las últimas tendencias tecnológicas".

Eder de Abreu
Inteligencia cibernética en Deloitte

Prueba de vida: un recurso indispensable en la era digital

Si bien el impulso digital de la pandemia facilitó la apertura de cuentas bancarias, así como la solicitud y obtención de créditos de manera remota, también despertó más inquietudes sobre la verificación de la identidad de los clientes. Si no tenemos a una persona sentada frente a nosotros para ver su rostro e ID, y para verla firmar con su nombre físicamente, ¿cómo sabemos que es quien dice ser?

La identificación es el primer paso para iniciar transacciones financieras, asegura Paola Bustos Urrutia, gerente comercial de Sinacofi Buró, empresa de Experian y socia de Jumio. Esta compañía trabaja con reconocimiento facial y otros métodos de validación de ID. El proceso de autenticación debe ser lo suficientemente riguroso para que una empresa tenga la seguridad de que puede proporcionar un servicio o iniciar una relación con un cliente. Y eso incluye verificar que el documento de identidad que se presenta sea válido.

Akif Khan, analista de Gartner Research y especialista en fraude en transacciones de pago y verificación de identidad, comenta que una de las alternativas disponibles para abordar el problema de la verificación de identidad es trabajar con proveedores y empresas de terceros que cotejen los datos de identidad de una persona con la información que poseen estas entidades y el Gobierno.

Pero, como señala Khan, la segunda pieza del rompecabezas es saber si la persona que ingresa los datos es quien dice ser, y es aquí donde la biometría comienza a ganar terreno. Según comenta, es posible pedirle a un usuario que tome una fotografía de algún medio de identificación, como el pasaporte, la licencia de conducir o el documento de identidad, seguido de una *selfie* que permita ver el rostro de esa persona.

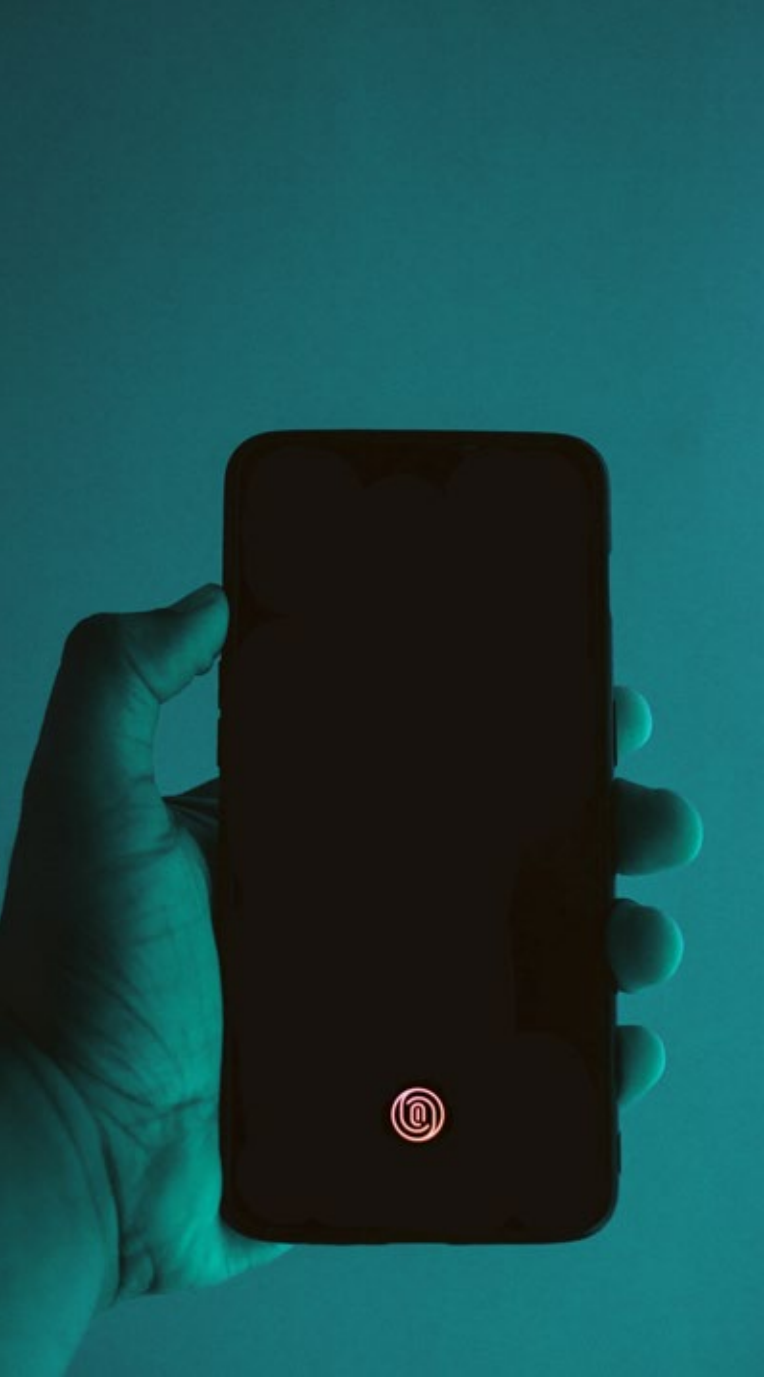
De hecho, con el marcado aumento de las transacciones por Internet, las empresas están agregando capas de seguridad para mitigar el riesgo de fraude. Samer Atassi, vicepresidente de Jumio para América Latina y el Caribe, señala que, aunque solicitemos una fotografía de la persona y su ID, no podemos saber con exactitud quién sostiene la cámara.

Las empresas también deben contrastar la ID del cliente con una base de datos del Gobierno para asegurarse de que se trate de un documento válido. “Tenemos muchas maneras de probar que la ID que se presenta no ha sido manipulada. Una de ellas es la inteligencia artificial y el aprendizaje automático, que nos permiten asegurarnos de que todos los campos, como nombre, número de ID o edad, se hayan extraído correctamente y no haya una imagen superpuesta a la imagen de la ID. Pero eso no es suficiente”, comenta Atassi.

Para evitar que una persona abra una cuenta bancaria con el documento de otra, las empresas pueden utilizar soluciones de “prueba de vida” o “detección de vida”, que permiten verificar que la persona que sostiene la ID en la fotografía está realmente allí, y no es una fotografía o un video.

La detección de vida consiste en comprobar que la persona en la imagen sea real, y no una marioneta, una persona usando una máscara, un video o una fotografía. La fotografía se compara con la imagen de la ID mediante biometría. Las empresas también pueden verificar el nombre y la dirección mencionados en el documento.

A diferencia de los Estados Unidos o Europa, en América Latina “también existen servicios mediante los cuales se pueden contrastar estos datos biométricos con algunas fuentes del Gobierno”, expresa Khan. ◆



Priorizar la experiencia del usuario y la privacidad de los datos

Con cualquier solución que elijan, las empresas deben decidir qué experiencia del usuario desean ofrecerles a sus clientes, y cómo interactuarán con ellos a través de una aplicación móvil o un sitio web. La experiencia del usuario varía a la hora de detectar el robo de identidad, y en muchos casos exige realizar alguna acción para probar que el usuario está vivo: girar la cabeza, decir una palabra o parpadear durante el proceso de *onboarding* o identificación no presencial, por ejemplo.

Otros proveedores ofrecen un método denominado "detección pasiva de vida", donde el usuario no debe hacer nada. Simplemente mira a la cámara, y se toma una decisión acerca de si se trata de una persona real o no, según afirma el analista de Gartner.

Lograr un equilibrio entre una buena experiencia del usuario y la seguridad es esencial, y debe abordarse mediante una evaluación de gestión de riesgos. "El punto clave es que las empresas definan su apetito de riesgo y que, a partir de esto, desarrollen una metodología de riesgo y apliquen controles. Deben saber cuáles son para ellas las "joyas de la corona"; y aplicar más capas de protección a lo que consideran más importante", explica Patrick Aron Rinski, de McKinsey.

Cristian Galan, cofundador de Cellbank, una empresa de tecnofinanzas que proporciona servicios B2B2C digitales, menciona que los clientes están particularmente preocupados por la facilidad de uso. "La fricción cero no es algo que se queda en el

“Son muchas las conexiones que debemos controlar para saber si alguien se encuentra en alguna lista negra local o internacional”

Samer Atassi
Vice Presidente Latino América, Jumio

PowerPoint, sino que tiene que ser una realidad en todas las soluciones”, afirma.

Reconciliar las capas de seguridad con una excelente experiencia del usuario o UX, sin dejar de cumplir con las leyes de protección de datos, no es una tarea fácil. Ignacio Ardohain, director ejecutivo de Cellbank, afirma que un elemento clave para un *onboarding* digital seguro es autenticar la documentación del usuario. “No es *onboarding* si no tiene un proceso inteligente de prueba de vida. Las empresas deben tener un sistema confiable de prueba de vida”, menciona.

En cuanto a la protección y la privacidad de los datos, las empresas deben tener en cuenta tanto los procesos internos como los de sus proveedores en torno al almacenamiento de la información personal de los clientes para cumplir con las regulaciones nacionales. Se deben hacer preguntas importantes, como: ¿se borrarán todos los datos una vez que finalice la verificación de identidad? ¿O se almacenarán esos datos? Y en tal caso, ¿quién lo hará? “Como organización, debemos saber qué ocurre. Debemos saber si nosotros o nuestro proveedor está almacenando información personal de los usuarios o no”, señala Akif Khan de Gartner.

A las medidas preventivas para evitar el fraude y los riesgos relacionados, se le suma toda la serie de regulaciones independientes en materia de lavado de dinero. Por lo tanto, es importante cumplir con las leyes locales y adoptar la mejor práctica; por ejemplo, asegurarse de que el cliente no esté en una lista negra por lavado de dinero.

A medida que se envía más y más dinero por Internet, se crea un problema para los Gobiernos y autoridades reguladoras, ya que es posible que se muevan fondos ilícitos en pequeñas cantidades, con lo cual la capacidad de supervisar las transacciones resulta crucial. “Que alguien me pida un préstamo no implica necesariamente que ese dinero se utilizará con fines legales. Esa persona puede estar lavando dinero. Son muchas las conexiones que debemos controlar para saber si alguien se encuentra en alguna lista negra local o internacional”, asevera Samer Atassi, de Jumio. ◆

Más allá de la ID, la orquestación es esencial

En la era digital, es necesario validar mucho más que la ID de una persona y su biometría. Por lo tanto, se han desarrollado herramientas más sofisticadas para determinar si el dispositivo, el correo electrónico o el número de teléfono realmente pertenecen a la persona en cuestión, y si esta se encuentra en una lista negra. Las nuevas soluciones pueden controlar todo el universo de datos en torno a esa persona y ofrecen a las empresas una serie de controles para obtener una verificación de identidad infalible.

La orquestación de identidad se refiere al proceso de combinar diferentes elementos para un control multinivel: detalles acerca del dispositivo de la persona, su número de teléfono, su correo electrónico, bases de datos del Gobierno, listas de lavado de dinero, etc.

Cada vez más empresas están adoptando esta estrategia ante el aumento del fraude y las crecientes cargas regulatorias. Tener todos los datos y verificaciones de la persona en un solo lugar, con una única puntuación de riesgo, facilita el proceso de verificación.

Según Atassi, de Jumio, este único punto de orquestación es esencial y es lo que demandan las empresas. No desean pasar meses y meses en la integración con diferentes proveedores. La cobertura global también es importante, señala Atassi. “Piden simplicidad, piden todo en un mismo lugar, para una puntuación de riesgo unificada, para una gestión de casos, para una integración”, agrega.

En toda América Latina, las empresas —especialmente en el sector de finanzas—, están intentando reemplazar las contraseñas con niveles de seguridad adicionales, y la biometría va ganando terreno.

> “Hoy en día, los bancos ni siquiera confían en las contraseñas, sino en el dispositivo, en el uso de la información del entorno o el contexto en el que se autentica en la aplicación. Y confían en la biometría. Es por eso que el concepto de geolocalización, combinado con la geovelocidad, es importante”

Vinícius Fraga
Gerente senior de consultoría de seguridad y director de servicios de ciberseguridad en Accenture

También se observa una tendencia en torno a lo que se conoce como autenticación sin contraseña, que también apunta a mejorar la seguridad, asevera Patrick Aron Rinski, de McKinsey. Sin embargo, esto tiene sus obstáculos, comenzando con el hecho de que siempre habrá una contraseña detrás de cualquier método de autenticación, aunque el cliente no la “vea” muy claramente.

Actualmente, las empresas utilizan varios métodos para el *onboarding*, con identificadores únicos para que cada persona verifique su identidad, junto con la gestión interna de la identidad del cliente. Luego está la autenticación en sí misma, que puede ir desde algo físico, como un *token*, a soluciones más innovadoras, como el uso de IA para reconocer la manera en que una persona escribe y utiliza su teléfono celular, que es única e irrepetible. Otra opción es el análisis conductual para comparar diferentes puntos de datos; por ejemplo, la IP que el cliente utiliza para acceder a la banca móvil o geolocalización. “La biometría sigue siendo la más utilizada y, entre los diferentes tipos de biometría, el más utilizado es el conductual”, afirma Patrick Aron Rinski.

Por otro lado, Vinícius Fraga, gerente senior de consultoría de seguridad y director de servicios de ciberseguridad en Accenture, asegura que la autenticación sin contraseña es un concepto de confianza cero, pero puede utilizarse a nivel interno para el personal de una empresa. “En un futuro, la contraseña bancaria ni siquiera existirá. Hoy en día, los bancos ni siquiera confían en las contraseñas, sino en el dispositivo, en el uso de la información del entorno o el contexto en el que se autentica en la aplicación. Y confían en la biometría. Es por eso que el concepto de geolocalización, combinado con la geovelocidad, es importante”, explica Fraga.

Eder de Abreu, de Deloitte, agrega que, si bien la orquestación tiene una función importante en la mejora de la seguridad, es poco probable que haya una única solución para todos los problemas. “No creo que haya una solución milagrosa. Las empresas pueden tener diferentes opciones y, si existe una conducta inusual [del cliente], pueden cambiar la manera de hacer algo. Se pueden agregar dos o tres tecnologías, y utilizar una autenticación multifactor que ofrecerá un mayor nivel de comodidad”, comenta Abreu.

La autenticación multifactor se ha utilizado en el sector financiero durante décadas, aunque las tecnologías empleadas pueden haber cambiado con el tiempo. Este sistema puede incluir una contraseña combinada con biometría y un *token*. “El término “multifactor” implica una combinación, y generalmente se emplean al menos dos métodos”, indica Abreu.

El seguimiento es muy importante. Las empresas no deberían ver a las tecnologías de manera individual, sino como parte de un sistema integrado. Y deberían controlar continuamente el perfil del usuario, agrega Fraga. Este aconseja a las empresas que se concentren en la verificación cruzada de datos, y que unan la inteligencia y el análisis, y tomen decisiones usando la IA y el aprendizaje automático.

Además de las tecnologías de *onboarding*, que se centran mayormente en la verificación de identidad, la estrategia en torno a los pagos debe centrarse en el conocimiento del cliente. “Todas las personas deben tener herramientas de KYC y deben controlar la veracidad del documento, de la identidad, ya que es muy importante para el panorama de fraude”, afirma Fraga. “La seguridad, el fraude y la identidad van de la mano”.

¿Cuál es su apetito por el riesgo?

Al momento de definir las estrategias de seguridad, fraude o AML, las empresas suelen considerar su apetito por el riesgo. Los controles variarán según el nivel de riesgo que una organización esté dispuesta a aceptar en su intento por alcanzar sus objetivos. Las empresas tendrán diferentes requisitos para cada situación. Por ejemplo, si un cliente pide un préstamo de $100, la organización puede simplemente pedir una *selfie*. Sin embargo, para un préstamo de $10 000, se le puede exigir que envíe una prueba de dirección (como la fotografía de una factura de electricidad) en un correo electrónico.

"Cada empresa y cada integración vertical son diferentes. Todo depende de qué desean en términos de flujo y de la capacidad de personalizar los flujos de trabajo, creando su trayectoria en función de lo que desean. No tiene que ser lo mismo para cada persona", explica Atassi, de Jumio. Según la evaluación de riesgos, los requisitos pueden variar desde la solicitud de una ID y una *selfie*, hasta la verificación de que la información coincida con los datos del usuario en una base de datos del Gobierno, o algún método más refinado aun.

Cristian Galan, de Cellbank, observa que la complejidad de la comprobación de ID no solo depende de cuánto riesgo está dispuesta a asumir la empresa, sino también de su habilidad para interpretar los resultados. Paola Bustos Urrutia, de Sinacofi Buró, agrega que, para transacciones más pequeñas, la validación mediante preguntas, la ID o el reconocimiento facial pueden ser suficientes. Señala que "las compañías deben aclarar qué riesgos están dispuestas a tomar" al diseñar una estrategia de seguridad digital, y que es importante equilibrar el servicio, la experiencia del usuario y el riesgo.

> "La complejidad de la comprobación de ID no solo depende de cuánto riesgo está dispuesta a asumir la empresa, sino también de su habilidad para interpretar los resultados"
>
> Cristian Galan
> **CSIO y co-fundador, CellBank Group**

Esto depende en gran medida del tipo de servicio que se proporciona y, nuevamente, del apetito de la empresa por el riesgo. "Trabajamos con empresas grandes, como bancos, empresas de telecomunicaciones, financieras automotrices. El flujo de trabajo debe —justamente— fluir, y es importante saber que ningún servicio es totalmente infalible: algunos son más riesgosos y otros son más fáciles", explica Paola Bustos. Un ejemplo del proceso para mitigar los riesgos, asevera, es adoptar una validación facial híbrida que combine inteligencia artificial con capacidades humanas para abordar cualquier zona gris.

El futuro de la identidad digital

Según señala Akif Khan, de Gartner Research, el futuro de la validación de ID apunta hacia la creación de una identidad digital portátil. Ya no tiene sentido pedir a una persona que compruebe su identidad cada vez que visita un banco, proveedor de atención médica, portal del Gobierno o cualquier otro sitio web en línea.

"Estratégicamente, es más probable que, en un futuro, todo se base en la posesión de una identidad digital portátil que permita demostrar la identidad una vez, y que luego se utilice algún tipo de billetera digital, que contenga la identidad verificada", explica Khan. Eso significa que no se deberán repetir las validaciones cuando las personas realicen negocios en el espacio digital.

La identidad digital portátil también podría ser global: un pasaporte que se acepte en cualquier país del mundo. "Algunos proveedores, bancos y Gobiernos están intentando introducir este tipo de identidad digital portátil, pero aún falta mucho para que esto suceda" y no habrá una única solución predominante, asegura.

Khan cuenta que no se puede prever quién ganará esta carrera. "Pero mi sensación es que la confianza de los ciudadanos en un sistema de este tipo

"Debe haber un equilibrio entre el riesgo y la experiencia del usuario. Esto es algo particular para cada empresa y tiene que ver con el mercado en el que se encuentra, el nivel de riesgo que está dispuesta a tomar y la regulación."

Paola Bustos Urrutia
Sinacofi Buró, una compañia de Experian

probablemente vendrá de un esquema de identidad digital del Gobierno, en lugar de un esquema de un proveedor privado", agrega. Por supuesto, las personas deben confiar en su Gobierno para que un proyecto como este tenga credibilidad.

En ese sentido, Eder de Abreu, de Deloitte, comenta que el uso de cadenas de bloques o *blockchains* en identidad digital es algo que ya ocurre, aunque este método todavía se encuentra en una etapa inicial. "Tendremos una aplicación móvil que concentrará todos los datos, y podremos cifrarlos y utilizar *blockchains* con claves públicas y privadas", explica, y agrega que este enfoque introduce una serie de controles más confiables.

Entre los desafíos que deberán superarse en torno a las plataformas de verificación de ID se encuentran la facilidad de uso y las acciones basadas en controladores de inteligencia artificial, según señala Cristian Galan, de Cellbank. Otro desafío consiste en detectar las transacciones fraudulentas y el lavado de dinero de manera inteligente. "Tener un proceso y un flujo de trabajo inteligente con un alto grado de seguridad es clave, y eso es lo que busca el mercado", explica Galan.

Sin embargo, ciertas particularidades de los documentos, como una calidad de imagen deficiente, pueden exigir la intervención humana, agrega Ignacio Ardohain, director ejecutivo de Cellbank. "Preferimos soluciones que no estén totalmente automatizadas. En cambio, buscamos soluciones híbridas, ya que algunos documentos no se pueden escanear. En algunos casos no está presente el factor humano", comenta.

Otro desafío es el *onboarding* guiado por el reconocimiento de voz, con la ayuda de inteligencia artificial. En esto está trabajando Cellbank, en asociación con Amazon y Google, quienes tienen una fuerte capacidad de registro de voz, según comenta Galan. "Estamos buscando maneras de tener un acceso inteligente a este registro de voz para aplicarlo a los usuarios".

Las tecnologías avanzan más rápido de lo que pensamos; cada una contribuye de maneras diferentes y, lo que es más importante, se complementan, según señala Bustos. Pero lo que deben tener en común es el enfoque en la experiencia del usuario para evitar que los clientes abandonen su transacción. "Debe haber un equilibrio entre el riesgo y la experiencia del usuario. Esto es algo particular para cada empresa y tiene que ver con el mercado en el que se encuentra, el nivel de riesgo que está dispuesta a tomar y la regulación", detalla Paola Bustos Urrutia. ◆

Caso de uso:

Cómo mejorar el proceso de onboarding o identificación no presencial

Paulo Valdiviezo es codirector ejecutivo de Kambista, un sitio web de cambio de moneda en línea basado en Perú. Esta empresa de tecnofinanzas modificó su proceso de *onboarding* de clientes al sustituir un sistema basado únicamente en el número de ID por otro más amplio y fuerte. Kambista tenía aproximadamente 30 000 usuarios activos y llevó a cabo 40 000 transacciones en febrero. "Creemos que el mercado es mucho más amplio. Creemos que, en Lima, el mercado debería ser de 100 000 clientes que realizan intercambios cada mes", comenta.

Kambista ingresó en el mercado en un momento en el que el negocio de cambio de moneda tenía fallas de atención. Hasta hace poco, las personas podían cambiar dinero únicamente en bancos, en agencias de cambio o mediante personas que realizaban esta operación de manera informal, en la calle. Conocidos como cambistas, estas personas ofrecían buenas tasas, pero aceptaban únicamente efectivo y no proporcionaban ningún tipo de recibo. Kambista vio la oportunidad de realizar operaciones de cambio de moneda en línea mediante transferencias bancarias, con tasas transparentes y de manera ágil. Comenzó con un sitio web y luego lanzó una aplicación, que incluyó una opción para transacciones a través de WhatsApp.

Además de verificar la identidad de un cliente, Kambista deseaba mejorar los controles contra el lavado de dinero para evitar que los delincuentes utilizaran las cuentas de otras personas para cambiar dinero.

"No hemos detectado demasiados casos, pero creo que es mejor implementar controles y evitar esas situaciones", asevera Valdiviezo.

Valdiviezo señala que hay múltiples maneras de verificar la identidad de un cliente, como hacer preguntas de seguridad, validar correos electrónicos y números de teléfono, y controlar que una ID sea válida y coincida con los datos almacenados en bases de datos del gobierno o de terceros. "Cada vez más personas tienen acceso a teléfonos inteligentes y mejores cámaras; por lo tanto, deberíamos utilizar soluciones más desarrolladas para tener la mayor certeza posible de que la persona con la que estamos tratando es realmente quien dice ser", agrega.

El negocio de Kambista creció considerablemente cuando comenzó la pandemia. Durante meses, las personas no podían cambiar dinero en la calle, por lo que comenzaron a hacerlo en línea, comenta Valdiviezo. Las personas jóvenes se adaptaron rápidamente, pero algunos clientes mayores tuvieron dificultades con el proceso de ***onboarding***: les costaba tomarse fotos de manera correcta con una calidad de imagen adecuada y mantenerse al día con los mensajes. "Esto sigue siendo un desafío; a muchos se les complica el ***onboarding*** por estas cuestiones, pero creo que cada vez más personas ven los beneficios de hacerlo. Les preocupa la seguridad y confían en que usamos el proveedor correcto", afirma Valdiviezo.

Actualmente, todos los clientes de Kambista realizan el *onboarding* con una solución biométrica. "No hemos observado filtraciones de seguridad. También estamos haciendo muchas cosas con respecto a la experiencia del usuario. Trabajamos con los tres pasos para la validación de la identidad de Jumio", menciona.

Valdiviezo asegura que, en un mundo ideal, habría un único repositorio de identidades accesible para las diferentes integraciones verticales, de manera de garantizarle mayor comodidad al usuario: todo en un mismo lugar, ya sea para pagar por un producto y conseguir una hipoteca, o para hacer una transacción en línea e incluso registrarse en un hospital. Sin embargo, existen muchas inquietudes con respecto a quién almacenaría la información, y cuáles serían las mejores prácticas en materia de privacidad y la protección de datos, señala.

En cuanto al futuro, Valdiviezo cree que las industrias financieras y de verificación van en la dirección de las pruebas de ADN, dadas las limitaciones que el software de biometría puede enfrentar cuando intenta reconocer a un usuario que ha perdido o ganado mucho peso, por ejemplo. "Es posible que esa sea la solución definitiva", sostiene. ◆

Comentarios finales

Como observó McKinsey, el acceso a datos e información a demanda va creciendo a medida que las plataformas móviles, el trabajo remoto y otras tendencias dependen cada vez más del acceso rápido a grandes conjuntos de datos, lo que aumenta la posibilidad de que se produzcan filtraciones.

Patrick Aron Rinski, de McKinsey, recomienda que las empresas consideren todos los potenciales sacrificios que están dispuestas a hacer por los controles de seguridad al crear una plataforma, en lugar de simplemente optar por la marca más popular. Deben evaluar sus procesos internos y decidir qué tecnologías son las más adecuadas para sus necesidades. Los bancos utilizan un promedio de seis a ocho soluciones diferentes para la identificación y la gestión de fraude. Pero dicha combinación puede ser difícil de manejar, agrega Rinski.

La mejor opción es elegir la herramienta que más se alinee con el proceso comercial de la empresa y su apetito de riesgo, y que al mismo tiempo aborde el riesgo de lavado de dinero, fraude y robo cibernético de una manera integrada. "En su preocupación por tener las herramientas más avanzadas, las empresas terminan olvidando lo básico: asegurar un proceso de autorización eficaz", indica Rinski.

Vinícius Fraga de Accenture agrega que algunas empresas, entre las que se incluyen bancos, están desarrollando soluciones a nivel interno en lugar de adquirir una plataforma externa. "Están reinventando la rueda y no invierten tanto como deberían en soluciones empresariales", afirma.

> "Los bancos utilizan un promedio de seis a ocho soluciones diferentes para la identificación y la gestión de fraude. Pero dicha combinación puede ser difícil de manejar"
>
> Patrick Aron Rinski
> **Socio de McKinsey y experto en ciberseguridad y riesgos operativos**

Fraga agrega que la biometría por sí sola ya no es suficiente: la verificación de documentos está en alza debido a las mejoras en la IA y las tecnologías de aprendizaje automático.

La autenticación basada en geovelocidad y la geolocalización surgen ahora como importantes herramientas para controlar la conducta del usuario. El reconocimiento facial combinado con la validación de prueba de vida también se ha hecho más frecuente.

Ya sea que se trate de minimizar el riesgo de fraude o de cumplir con las regulaciones contra el lavado de dinero, las empresas deben invertir en mejorar sus controles de ID y adoptar soluciones de seguridad fáciles de usar. ◆

Sobre nosotros

jumio

jumio.com/es

Cuando la identidad es lo que importa, confíe en Jumio. La misión de Jumio es convertir a internet en un lugar más seguro, protegiendo a los ecosistemas de las empresas a través de una plataforma AML y eKYC unificada que ofrece una verificación de identidad de punta a punta. La plataforma KYX de Jumio ofrece mútltiples comprobadores de identidad y servicios AML para establecer con precisión, mantener y reafirmar la confianza desde la apertura de la cuenta hasta el monitoreo continuo de transacciones.

A través de tecnología avanzada, incluyendo IA, biometría, aprendizaje automatizado, detección de vida y automatización, Jumio ayuda a organizaciones a luchar con el fraude y el crimen financiero, atendiendo más rápido a los clientes y cumpliendo con las normativas incluyendo KYC, AML y GDPR. Jumio ha realizado más de 500 millones de verificaciones en más de 200 países y territorios, entre la web en tiempo real y transacciones móviles.

Ubicada en Palo Alto, Jumio opera globalmente con oficinas en Norteamérica, América Latina, Europa y Asia-Pacífico y ha sido el receptor de numerosos premios por la innovación. Jumio es respaldado por Centana Growth Partners, Great Hill Partners y Millennium Technology Value Partners.

iupana

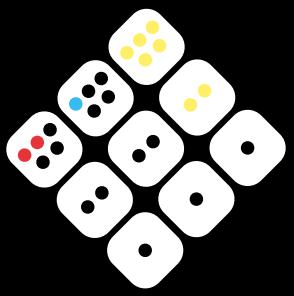
iupana.com

iupana es una empresa de servicios de información centrada en la transformación digital de las finanzas en América Latina y el Caribe.

iupana ofrece información valiosa acerca de los cambios que la nueva tecnología, combinada con modelos innovadores de negocios, está produciendo en la industria de los servicios financieros de la región.

A través de nuestro sitio web y de nuestros boletines informativos, eventos y iupanaPRO —un servicio de primera calidad centrado en la evolución regulatoria—, ayudamos a los líderes de la industria a mantenerse a la vanguardia de un mercado en constante cambio.

Altos ejecutivos del sector bancario, empresas emergentes empresas de tecnología y firmas de inversión confían en ***iupana*** para comprender las oportunidades, los riesgos y las tendencias existentes en relación con el crecimiento de la tecnología financiera en América Latina.



iupana

Katie Llanos-Small
Founder
katie@iupana.com
www.iupana.com

@iupana
@iupananoticias

jumio

Michelle Whiteford
Director, Global Online Marketing
marketing@jumio.com
www.jumio.com

@jumio
@jumio-corporation