



La **evolución de la identidad** en un mundo digitalizado

Por qué es esencial un enfoque orquestado por capas para una verificación de identidad preparada para el futuro



Los cambios en la verificación de identidad

No hace tanto tiempo, abrir una cuenta bancaria, alquilar un apartamento, comprar un coche o incluso solicitar un empleo se hacía personalmente. La confianza que se establecía en estos intercambios a menudo dependía únicamente de un firme apretón de manos, un rostro honesto y un carné de conducir para demostrar quién eras.

Avancemos hasta hoy. Ahora trabajamos, compramos, jugamos, aprendemos y nos conectamos en un entorno digital. Determinar quiénes somos en línea es mucho más complejo y subyace a cada paso que damos en nuestra vida digital.

Las herramientas y técnicas de verificación de identidades en línea se han acelerado para seguir el ritmo de los nuevos tipos de fraude, las nuevas normativas y las mayores expectativas de los clientes. Sin embargo, a pesar de estos avances, las organizaciones siguen experimentando un aumento de las tasas de fraude, demasiada fricción en la experiencia del usuario y silos tecnológicos.

Lo que funcionaba en el pasado ya no basta para crear experiencias de cliente fiables, intuitivas y eficientes en la era digital.

QUÉ ENCONTRARÁS EN ESTE EBOOK

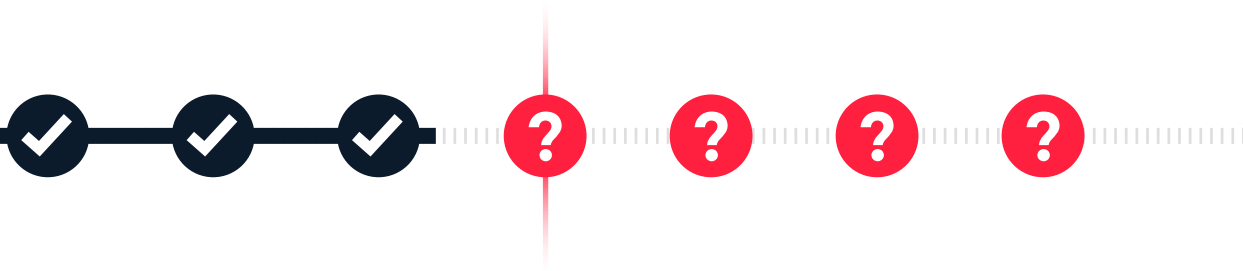
- De la identidad real a la digital
- Es hora de replantearse la verificación de la identidad
- La creciente importancia de la diversidad de señales
- La vida después de los documentos de identidad
- Las ventajas de un enfoque adaptativo para un mundo digital
- Descubre cómo Mitek puede ayudarte a orquestar el futuro de la verificación de la identidad

De la identidad real a la digital

Antes de la era digital, las empresas dependían de un documento de identidad físico para verificar la identidad de un cliente durante una consulta en persona en una sucursal u oficina. Un carné de conducir o un pasaporte ayudaban a responder a la pregunta: «¿Es esta persona quien dice ser?».

Incluso hoy en día, para muchas empresas que han trasladado el viaje del cliente a los canales en línea, los documentos siguen siendo la principal defensa contra los defraudadores, pero ahora en formato digital. Los documentos de identidad digitalizados pueden verificarse analizando una imagen o un vídeo del documento, o mediante la lectura de datos del chip integrado en el propio documento de identidad. Las mismas preguntas utilizadas para verificar la identidad en el mundo real se aplican en el ámbito digital, junto con otras nuevas que son más difíciles de responder. ¿El permiso de conducir presentado es real, falso o sintético? ¿La persona que presenta el documento de identidad es su verdadero propietario? ¿Está esa persona realmente presente durante el proceso?

Y en las situaciones de mayor riesgo, como transferir los fondos de un plan de pensiones o solicitar un préstamo o una tarjeta de crédito, se requiere aún más información para generar confianza y bloquear a posibles defraudadores. Pero exigir simplemente más comprobaciones durante el proceso de verificación no es la solución. Añadir múltiples comprobaciones de identidad a la experiencia de incorporación puede crear mucha más fricción de la que sus clientes tolerarán, especialmente si estas comprobaciones no están bien orquestadas o no son fluidas para el cliente.



Desafíos en el paso a lo digital

“ Más transacciones digitales

Las organizaciones tienden 3 veces más ahora que antes de la pandemia a afirmar que al menos el 80 % de sus interacciones con los clientes son de naturaleza digital. [McKinsey Global Survey](#)

“ Aumento de los índices de fraude

Los casos de fraude y usurpación de identidad aumentaron en 2021, aparentemente impulsados por la explotación delictiva de la ansiedad y la confusión provocadas por la pandemia de COVID-19. Las pérdidas económicas derivadas de estos delitos también aumentaron en conjunto y por cada incidente. [Experian, October 2022](#)

Coste del fraude a largo plazo

“ El 67 % de los consumidores que sufren algún caso de fraude cambiarán de banco o cooperativa de crédito como consecuencia de ello. [The Great Payments Disruption Report, 2022](#)

Es hora de replantearse la verificación de la identidad digital

Las instituciones financieras llevan mucho tiempo a la vanguardia de la gestión de identidades, impulsadas principalmente por factores de riesgo financiero y de reputación. La capacidad de verificar que los clientes y empleados son quienes dicen ser es fundamental para proteger la confianza y prevenir el fraude.

Con la rápida digitalización de los productos y servicios acelerada por la pandemia, las mejores estrategias para gestionar la verificación de la identidad y prevenir el fraude se han convertido en una nueva prioridad. Y no solo para los proveedores de servicios financieros y las empresas de tecnología financiera. Los mercados, los minoristas y miles de otras empresas en línea se enfrentan ahora a un conjunto de herramientas de verificación de la identidad en rápida expansión (desde la verificación de documentos móviles hasta la geolocalización, la biometría y la detección de vida) y puede resultar difícil encontrar la solución más eficaz.

De hecho, muchos métodos de verificación ya establecidos o emergentes se centran en un único caso de uso o en unos pocos. El resultado es un conjunto de silos tecnológicos difíciles de integrar y mantener para la organización. Y lo que es más importante, estas herramientas y tecnologías dispares no trabajan juntas para adaptarse al fraude. Otro punto clave es que, al no trabajar juntas, estas herramientas han empezado a sobrecargar la experiencia del cliente con niveles inaceptables de fricción.



Es hora de replantearse la verificación de la identidad digital

Para hacer frente a esta situación, cada vez más empresas empiezan a adoptar un enfoque estratificado de la verificación, que les permite equilibrar mejor la tensión existente entre la comodidad del cliente y el riesgo empresarial. Con un enfoque por capas, estas empresas pueden incorporar “señales” adicionales según sea necesario, realizando una comprobación para determinar la edad de una persona, su perfil en línea o sus indicadores de riesgo. Las señales se han convertido en la base de un enfoque basado en el riesgo que puede ayudar a las organizaciones a adaptar el viaje del cliente de forma inteligente, a la vez que ofrece una mejor protección contra el fraude y el cumplimiento de los requisitos KYC.

La evolución de las señales en la verificación de identidad

Era	Enfoque de verificación de la identidad	Señales comunes
Física pre-2000	Documentos de identidad presentados en una oficina o sucursal (pasaporte, permiso de conducir). Una persona inspecciona el documento de identidad y, si es necesario, lo coteja con una lista de vigilancia o una base de datos.	• Documentos de identidad oficiales • Comprobaciones forenses (manuales) • Comprobación de la base de datos (manual)
Física/Digital de 2000 a 2020 (prepandemia)	Los canales digitales complementan (o incluso sustituyen) a los servicios presenciales. Para acreditar su identidad y cumplir los requisitos KYC, los clientes presentan imágenes digitalizadas de sus documentos de identidad, que las empresas examinan y autentican mediante biometría y tecnologías asistidas por IA.	• Información personal introducida por el usuario • Captura y tratamiento de imágenes de documentos de identidad • Autenticación de documentos de identidad asistida por IA • Cheques con código de barras, MRZ y/o NFC
Digital-First postpandemia y más allá	La transformación digital seguirá dando rienda suelta a una nueva generación de productos y servicios en los sectores de servicios financieros, viajes, ocio, telemedicina, administración pública, jurídicos y otros. Las organizaciones se basarán en una amplia gama de señales para establecer la identidad de una manera que sea segura y sin fricciones.	• Biometría multimodal con detección de vida • Detección automatizada de PEP • Comprobaciones automatizadas de las listas de sanciones • Análisis de perfiles en línea • Geolocalización • Controles de agente por vídeo en directo • Credenciales digitales

La creciente importancia de la diversidad de señales

Cuando se trata de verificar la identidad, una señal es cualquier fuente de datos que pueda utilizarse para distinguir a un individuo único, ya sea en la vida real o en línea.

Una de las primeras y más comunes señales de identidad es la existencia de un documento de identidad emitido por el gobierno, como el permiso de conducir, el certificado de nacimiento o el pasaporte. Sin embargo, en el ámbito digital, ahora hay un número creciente de señales adicionales que las empresas pueden utilizar para corroborar la validez de una persona y detener las amenazas de fraude nuevas y emergentes, como las identidades sintéticas.

Mediante la superposición de una multitud de señales, las empresas pueden lograr un enfoque dinámico y basado en el riesgo para verificar las identidades digitales. Estas señales pueden incluir la validación de documentos de identidad, la comprobación de bases de datos, la detección de PEP y sanciones, la biometría facial o de voz, la detección de la vitalidad, la geolocalización, las alertas de fraude, el análisis de la huella digital, la biometría del comportamiento, la reputación del dispositivo, etc. Agrupar a las personas en función de las señales iniciales que se producen en tiempo real y, a continuación, añadir señales adicionales en función de los umbrales de riesgo, puede ayudar a las empresas a encontrar el equilibrio perfecto entre la prevención del fraude y la optimización de la experiencia del cliente.

Problemas creados por señales limitadas:

Comprobar únicamente una o dos señales limita a las organizaciones en términos del riesgo que pueden mitigar o de la experiencia personalizada que pueden ofrecer a los usuarios finales. Cada usuario se verá obligado a completar los mismos pasos, lo que se traducirá en el mismo nivel de seguridad. Sin señales adicionales, las organizaciones no pueden afinar el equilibrio entre el riesgo y la comodidad del cliente.



La creciente importancia de la diversidad de señales

¿Qué pueden indicar otras señales más allá de los documentos de identidad?

Un cliente potencial puede presentar una identificación verificable emitida por el gobierno, pero es posible que aún necesite saber más sobre él para tomar la decisión correcta para su organización en función de su tolerancia al riesgo o de la necesidad de cumplir con las normativas de KYC y PBC. He aquí algunos ejemplos de señales que pueden ayudar a satisfacer necesidades empresariales específicas.



	Geolocalización	PEP y sanciones	Comprobaciones de bases de datos de terceros	Huella digital	Banca abierta
Ejemplos	Datos extraídos sobre la ubicación física del dispositivo del individuo. Se pueden cruzar con la información de identificación personal proporcionada o con otros datos de señales para corroborarlos.	Detección de medios adversos, historial de transacciones ilícitas o conexiones sociales con personas incluidas en listas de vigilancia.	Comprobaciones de crédito, verificación de direcciones, historial laboral y registros gubernamentales.	¿Tiene esta persona una cuenta en LinkedIn o Facebook? ¿Las cuentas tienen muchos contactos? ¿Tiene una cuenta en Amazon? ¿Desde cuándo? ¿Con qué frecuencia se utiliza?	Historial de transacciones bancarias, datos generales de la cuenta e información sobre tarjetas.
Útil para	Detectar interacciones iniciales anómalas o un uso poco habitual de las devoluciones.	Cumplimiento de la normativa KYC y PBC para instituciones financieras.	Verificar que un documento concreto es válido (no ha caducado ni ha sido anulado) y evaluar la solvencia crediticia.	Ideal para empresas que desean una comprobación adicional de identificaciones recién creadas o posiblemente sintéticas. También es útil para verificar clientes con historiales de crédito poco sólidos.	Instituciones de apuestas en línea que están obligadas a verificar los medios financieros o la solvencia.

La vida después del carné de identidad

La verificación adecuada de un individuo utilizando tantos factores como sea posible será esencial para incontables casos de uso empresarial. Algunos ejemplos son: evitar la venta de alcohol o cigarrillos a menores; denegar una solicitud de tarjeta de crédito a una persona con múltiples quiebras; facilitar el acceso a un coche de alquiler solo con la prueba de un seguro adecuado o verificar las credenciales educativas de un candidato antes de ofrecerle un empleo.

A medida que el mundo se aleja de un enfoque puramente centrado en los documentos para la verificación de la identidad, la pregunta que más nos hacen es: ¿Sustituirán las identidades y credenciales digitales a los documentos de identidad?, ¿y qué significa eso? Esto es lo que pensamos.

El escenario probable para las credenciales digitales

Es muy poco probable que exista una única credencial digital mundial. En su lugar, es probable que los marcos gubernamentales (como el TDIF en Australia, el DIATF en el Reino Unido o el gigantesco sistema de identificación electrónica Aadhaar en la India) establezcan las bases de un ecosistema interoperable de credenciales de uso universal. Las normas para confirmar las identidades y unas directrices estrictas para el intercambio de información digital entre sistemas serán el eje de la confianza dentro de este ecosistema.

La forma en que se desarrolle ese ecosistema dependerá, en gran medida, de las tecnologías que lo potencien, y creemos que hay tres avances tecnológicos clave que pueden servir de indicadores en el camino hacia unas credenciales digitales universalmente aceptadas.



La vida después del carné de identidad

Las señales en el camino hacia las identidades y credenciales digitales

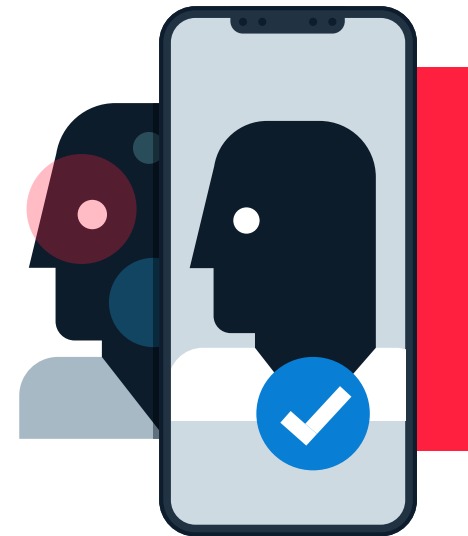
Hoy:
Biometría

Mañana:
Monederos digitales

Futuro:
Identidades autosuficientes

Las empresas que desean una solución más independiente de la plataforma implantan la autenticación biométrica directamente en su experiencia de cliente en línea o en su aplicación móvil. En este caso, la biometría permite un factor de autenticación independiente del dispositivo, un verdadero segundo factor. Utilizando cualquier smartphone u ordenador con biometría, los clientes acceden a sus cuentas de forma segura con su cara o su voz, que se coteja con la plantilla biométrica verificada del registro, sin necesidad de PIN ni contraseña. Y si el dispositivo se pierde o lo roban, nadie que consiga desbloquearlo tendrá acceso a las cuentas en línea de esa persona.

Con este enfoque, las empresas pueden utilizar de forma rápida y segura la correspondencia biométrica alojada en la nube y en el servidor, sin depender del dispositivo exclusivo del cliente. Las soluciones de terceros pueden ofrecer a las empresas un mayor control sobre la inscripción y la configuración de los clientes, incluida la elección de modalidades biométricas (facial, de voz o ambas) para adaptarse a las tolerancias de riesgo y las necesidades empresariales.



La vida después del carné de identidad

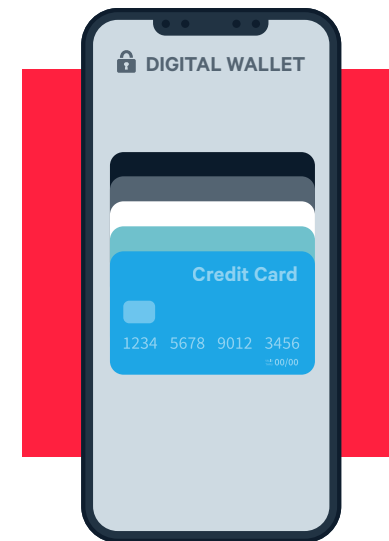
Las señales en el camino hacia las identidades y credenciales digitales

Hoy:
Biometría

Mañana:
Monederos digitales

Future:
Identidades autosuficientes

La biometría también se integrará en los monederos digitales (o eWallets) como señal de verificación almacenada. Las soluciones de monedero digital utilizarán una aplicación móvil segura para almacenar versiones digitalizadas y cifradas de documentos oficiales (documentos de identidad, registros de vehículos, credenciales sanitarias, etc.), además de plantillas biométricas. Estos eWallets permitirán a las personas demostrar su identidad y sus derechos en línea, así como en persona, ante las fuerzas de seguridad, los profesionales sanitarios o las empresas. Y lo que es más importante, los eWallets permitirán a su titular compartir únicamente la información necesaria para verificar una transacción concreta y nada más.



La vida después del carné de identidad

Las señales en el camino hacia las identidades y credenciales digitales

Hoy:
Biometría

Mañana:
Monederos digitales

Future:
Identities autosuficientes

A partir de las carteras digitales, las identidades autosuficientes serán el objetivo final de la verificación de la identidad descentralizada. La clave será el uso de tecnologías de cadena de bloques para crear credenciales “a prueba de manipulación” cuya autoría pueda verificarse, distribuirse y almacenarse criptográficamente. Podrían crearse credenciales de cualquier tipo a partir de organismos certificadores oficiales. Esto significa que los diplomas universitarios y las notas medias, los registros fiscales, las afiliaciones o certificaciones de asociaciones profesionales, los certificados de matrimonio o cualquier otro tipo de credencial podrían almacenarse en un único lugar y acceder a ellos a través del monedero una vez aprobados por el propietario de la identidad. Esto eliminaría la necesidad de repositorios de identidad centralizados (ya sean gubernamentales o a través de grandes empresas como Google y Facebook) y eliminaría la necesidad de crear nuevas cuentas con cada proveedor de servicios, minorista o agencia.



Las ventajas de un enfoque adaptativo para un mundo digital

La identidad seguirá siendo la base de la confianza que impulsa la economía digital mundial. Sin embargo, establecer la confianza en las credenciales digitales de un cliente al tiempo que se mitiga el riesgo de fraude nunca será una solución única.

En Mitek, creemos que las organizaciones están mejor equipadas con soluciones de identidad y ciberseguridad integradas y multicapa que ayudan a reducir el fraude, limitar la complejidad y abordar los requisitos KYC y PBC de forma más eficiente, a la vez que ofrecen experiencias de usuario fluidas en todos los canales.

La Plataforma de Identidad Verificada de Mitek (MiVIP) está diseñada para permitir a las empresas desplegar rápidamente soluciones de verificación de identidad y KYC contextuales y adecuadas, con toma de decisiones, activadores y umbrales basados en el riesgo.

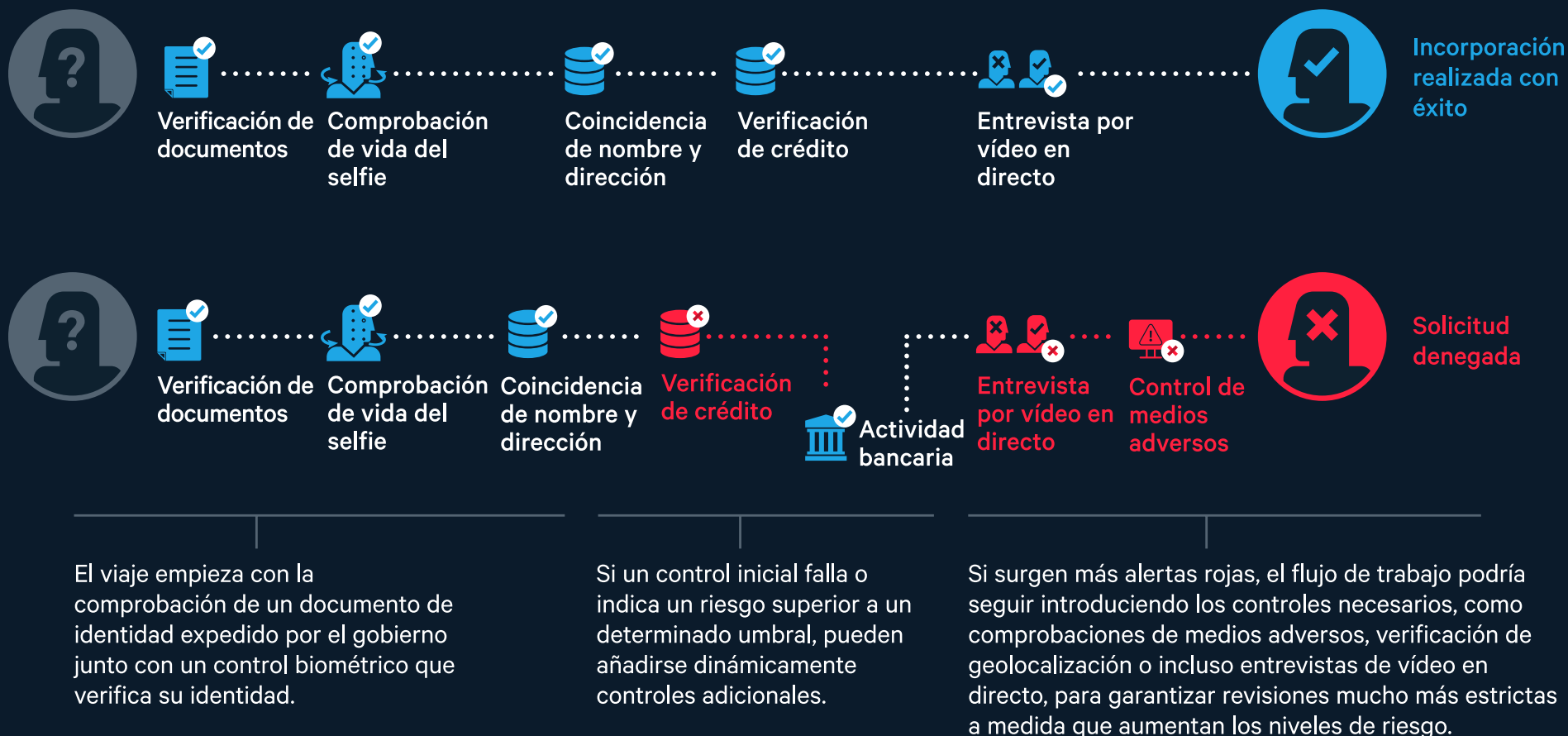
MiVIP combina un conjunto completo de señales de verificación de identidad originales y externas con potentes herramientas de orquestación y configuración, lo que permite a las organizaciones crear flujos de trabajo de incorporación a medida en cuestión de horas, reducir los costes operativos al disminuir la sobrecarga de los desarrolladores y acelerar el tiempo de creación de valor al reducir la fricción de la incorporación de clientes.

Lo mejor de todo es que MiVIP permite a las organizaciones preparar su enfoque de la verificación para el futuro mediante una orquestación de señales flexible y por capas, ya que la plataforma puede absorber fácilmente nuevas señales a medida que estén disponibles para combatir el fraude en constante evolución.



Ejemplos de un viaje dinámico del cliente basado en factores de riesgo

Con un enfoque basado en el riesgo para la incorporación del cliente, se pueden añadir, eliminar o personalizar señales para crear viajes a medida en los que solo se introducen fricciones adicionales para el cliente si está justificado.



MiVIP permite a los bancos, las empresas de tecnología financiera y otras empresas crear viajes digitales de clientes adaptados a factores de riesgo individualizados con mayor eficiencia y mejores resultados.

BANCA DIGITAL



Señales utilizadas:

- Validación de documentos de identidad
- Captura de selfie
- Comprobación de vida
- Biometría facial
- Prueba de dirección
- Geolocalización

“Nuestras herramientas digitales inteligentes permiten a nuestros clientes tener el control, y el viaje MiVIP les ayuda a superar con éxito las comprobaciones KYC en las que fallan las comprobaciones tradicionales de nombre y dirección”.

Linda Robertson

Director de experiencia digital de cliente

BANCA MINORISTA



Señales utilizadas:

- Validación de documentos de identidad
- Captura de selfie
- Prueba de dirección
- PEP y sanciones
- Huella digital

“Sabemos que los clientes quieren poder abrir cuentas a la hora y en el lugar que más les convenga, sin tener que preocuparse de enviar por correo los documentos de identidad más importantes ni de dedicar tiempo de su día a ir a una sucursal. Por eso estamos haciendo que la apertura de cuentas sea más fácil, segura y rápida, para que los clientes puedan dedicarse a lo que más les importa”.

Frans Woelders

Director Digital

Verificación de identidad preparada para el futuro

El cambio es lo único constante

Las empresas seguirán evolucionando hacia un mundo digital. Esta transformación exigirá un nuevo enfoque de la verificación y corroboración de la identidad, capaz de satisfacer las expectativas de los clientes digitalmente avanzados y, al mismo tiempo, adelantarse a los defraudadores y superar los obstáculos normativos.

Aunque es imposible predecir qué nuevos tipos de fraude o riesgo pueden surgir (o qué nuevas señales de verificación pueden surgir para combatirlos), contar con una plataforma de verificación flexible que pueda adaptarse y evolucionar fácilmente es una de las mejores inversiones que puede hacer ahora para adelantarse a los cambios en el futuro.

Descubre cómo puede ayudar Mitek

MiVIP es una solución de verificación de la identidad de bajo código que permite a las empresas digitales verificar a los clientes y detectar el fraude fácilmente y en tiempo real. Con MiVIP, los clientes pueden crear más rápidamente una experiencia de usuario intuitiva y orquestar una gama completa de tecnologías de autenticación, como la biometría, la geolocalización, las personas políticamente expuestas (PEP) y las sanciones, y las comprobaciones de agencias para proteger todo el ciclo de vida de las transacciones.

Empresa de NASDAQ® | miteksystems.com Copyright © 2023 Mitek Systems, Inc. Confidencial. Todos los derechos reservados.

Este documento tiene únicamente fines de información general y no pretende ser ni debe ser tomado como asesoramiento jurídico y/o normativo sobre hechos o circunstancias específicos. Toda la información facilitada en este documento se proporciona "como está" sin garantía de ningún tipo, ya sea expresa o implícita. El contenido de este documento no puede citarse ni mencionarse para ningún fin sin el consentimiento previo por escrito de Mitek o sus filiales.

