eBook

Onboarding digital seguro y sin fricciones: cómo reducir el fraude sin perder clientes

SOVOS

sovos.com/es

Cómo reducir el fraude sin perder clientes

Probablemente has escuchado que cerca de un 38% de usuarios abandona los procesos de onboarding digital a medio camino. ¿Por qué? Las razones son varias: porque tienen muchos pasos, incluyen demasiadas preguntas o sencillamente son difíciles de entender. A veces hay que sortear demasiadas vallas que nos hacen la vida (mucho) más difícil.

Ciertamente, los riesgos de seguridad en los procesos digitales se han disparado y obligan a procesos más robustos. Las amenazas han existido siempre, pero con tecnologías como la IA, cometer un fraude es sencillo incluso para quienes no tienen alma de hacker.

¿Cómo hacer entonces si el onboarding es tan crítico para el negocio? Este es EL momento clave en que logramos -o fallamos miserablemente- al intentar conquistar a un nuevo cliente o usuario.

¿Se pueden equilibrar realmente seguridad y UX?

Ofrecer una experiencia rápida y fluida para maximizar la conversión, y al mismo tiempo implementar controles de seguridad sólidos para prevenir el fraude son dos prioridades que a menudo parecen contradictorias.

Esto es especialmente relevante en Latinoamérica, donde solo en el primer semestre de 2024, el fraude bancario digital aumentó 32% y se perdió un 20% de ingresos por fraude. Al mismo tiempo, hasta el 60% de los usuarios abandonó procesos digitales por considerar que presentaban demasiada fricción.

El equilibrio parece difícil de alcanzar:
Si los controles son débiles, el riesgo de fraude se dispara; si son demasiado estrictos, la experiencia del cliente se resiente.

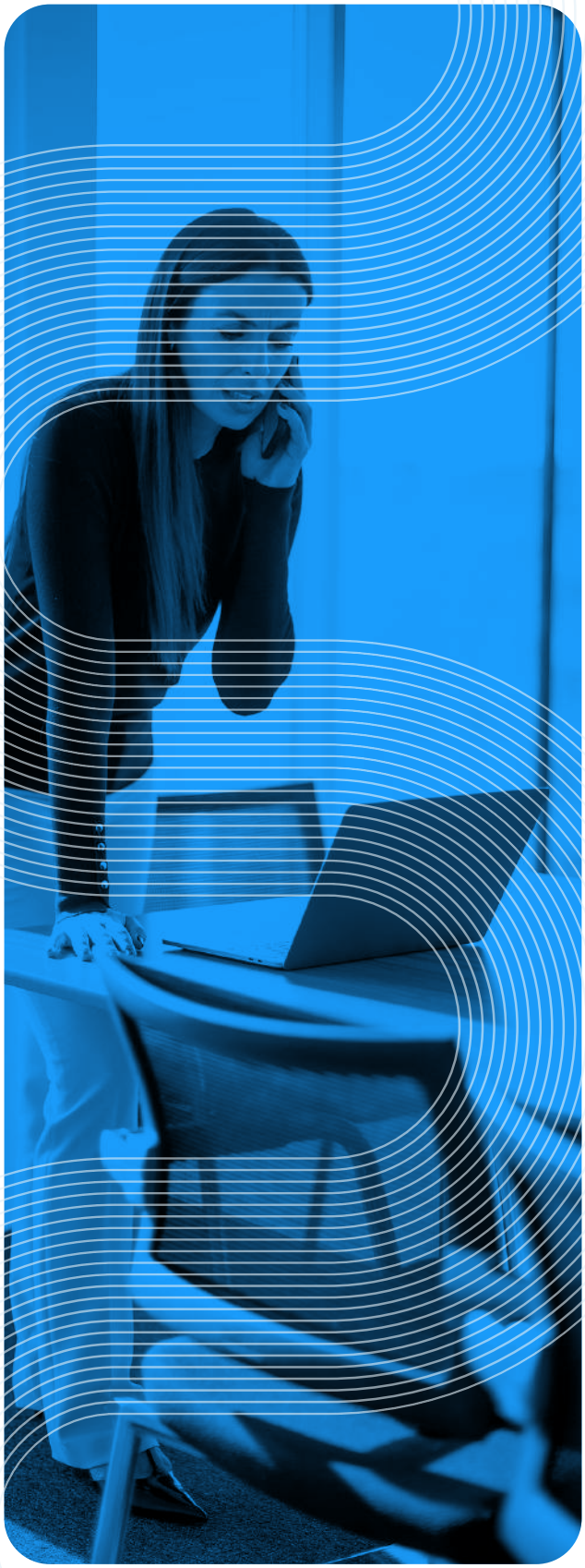
La clave está en diseñar procesos inteligentes que integren seguridad y experiencia de usuario desde el inicio, de manera que ambos objetivos se refuercen mutuamente. Seguridad y experiencia pueden coexistir, pero requieren de un enfoque planificado que priorice al usuario sin comprometer la protección.

El equilibrio se logra cuando las decisiones de seguridad se toman de manera inteligente, considerando riesgo, contexto y comportamiento del usuario, preparando el terreno para aplicar controles adaptativos que reduzcan el fraude sin afectar la conversión.

El fraude en el onboarding digital

El fraude en el proceso de incorporación de clientes no es nuevo, pero sí ha evolucionado con gran velocidad. Hoy, los atacantes aprovechan tanto vulnerabilidades tecnológicas como humanas para acceder a servicios financieros, plataformas de e-commerce o aplicaciones de pago. Entre los ilícitos más habituales se encuentran:

- Suplantación de identidad (mediante documentos robados o falsificados)
- Robo de credenciales reutilizadas de filtraciones anteriores
- Uso de deepfakes para engañar a los sistemas de verificación facial
- Fraude de primer pago, creando cuentas ficticias con tarjetas o medios de pago robados



La magnitud del problema en Latinoamérica es significativa en distintos frentes.
De acuerdo con el Latin America Identity Fraud Report 2024 de Experian, el fraude de identidad sintética creció un 27% interanual. Los intentos de ataques contra dispositivos móviles en 2024 sumaron 3.9 millones de intentos, afectando especialmente a países como Brasil, México y Chile, de acuerdo con el Financial Cyberthreats Report 2024 de Kaspersky.

El impacto en las empresas trasciende las pérdidas económicas directas.
La exposición temprana al fraude erosiona la confianza de los clientes y puede provocar un aumento significativo en las tasas de abandono. El estudio "Fraud vs. Friction" de Pi (Paytm Labs) muestra, por ejemplo, que un 71% de los consumidores desconfía más de un servicio fintech si ha sido víctima de fraude en el proceso de onboarding.

El desafío de la fricción

Si el fraude es uno de los grandes enemigos del onboarding, la fricción es el otro. A diferencia de los ataques externos, la fricción se genera desde dentro: surge cuando los controles de seguridad o los procesos de registro son tan complejos que el propio cliente decide abandonar antes de concluir.

La fricción puede tomar muchas formas

Desde formularios interminables y poco claros, hasta verificaciones que exigen múltiples contraseñas, códigos enviados por SMS que nunca llegan, o solicitudes de documentos que el usuario no tiene a mano en ese momento.

Lo que para la empresa puede parecer una medida de seguridad adicional, para el cliente se traduce en obstáculos que generan frustración y desconfianza.

De hecho, si un proceso de compra es percibido como demasiado complejo, el 74% de los clientes potenciales probablemente buscará otra opción. Los usuarios esperan procesos simples, rápidos y, sobre todo, consistentes en todos los canales.

El costo del abandono es alto

Cada registro que no se completa se traduce en ingresos que dejan de generarse y en la imposibilidad de construir relaciones duraderas con los clientes.

En sectores altamente competitivos como el financiero o el de e-commerce, donde los clientes tienen múltiples alternativas a un clic de distancia, una mala experiencia inicial suele equivaler a una oportunidad irrecuperable.

Lo más desafiante para las organizaciones es que seguridad y fricción suelen estar correlacionadas: a mayor número de pasos de validación, mayor probabilidad de abandono.

Por eso, el gran reto consiste en diseñar procesos que, sin relajar los estándares de protección, se perciban como sencillos y ágiles. Las tecnologías emergentes y los enfoques adaptativos permiten resolver este dilema. La clave está en lograr que la seguridad sea casi invisible para el usuario.

Estrategias para reducir fraude sin perder clientes

Reducir el fraude sin aumentar la fricción es posible si se adoptan estrategias inteligentes que combinan tecnología avanzada, análisis de riesgo y enfoque centrado en el cliente. No se trata de eliminar todos los pasos de seguridad, sino de hacerlos más inteligentes y adaptativos.

1. Verificación multifactor inteligente

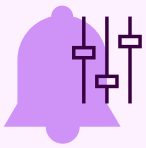
La autenticación multifactor (MFA) ha dejado de ser solo un requisito extra: hoy puede aplicarse de manera adaptativa según el riesgo. Por ejemplo, si un usuario se conecta desde un dispositivo o ubicación habitual, el sistema puede requerir menos pasos. En cambio, si detecta patrones inusuales, activa controles adicionales.

La MFA ha demostrado su capacidad para proteger a las organizaciones frente a las ciberamenazas, lo que se traduce en una mayor seguridad. Por ejemplo, Microsoft informó de que su uso redujo los robos de cuentas hasta en un 99,9 %.

2. Validación de documentos y biometría avanzada

La detección automática de documentos falsos y la verificación biométrica avanzada (como reconocimiento facial y liveness detection) permiten asegurar la identidad del usuario sin requerir revisiones manuales prolongadas.

Esto reduce la fricción, acelera la conversión y mantiene altos estándares de seguridad.



3. Tecnologías de análisis de riesgo, IA y machine learning

El machine learning y la analítica avanzada permiten detectar patrones sospechosos en tiempo real. Sistemas que analizan cientos de señales -como ubicación, velocidad de llenado de formularios o consistencia de datos- pueden bloquear intentos de fraude antes de que se materialicen.

Además, la IA puede realizar comprobaciones instantáneas de autenticidad en documentos: algoritmos de aprendizaje automático pueden analizar las características de seguridad y detectar anomalías o falsificaciones en los documentos. Si se detecta alguna discrepancia o manipulación, el sistema lo señala para su revisión posterior.

4. Orquestación de identidad digital

Más allá de tecnologías individuales, la clave está en integrar todos los controles dentro de un flujo dinámico y coordinado:

- **Mapear el recorrido del usuario:** identificar puntos críticos de fraude o abandono.
- **Definir reglas de riesgo:** asignar niveles de riesgo según ubicación, dispositivo y comportamiento.
- **Aplicar verificaciones adaptativas:** activar pasos adicionales solo cuando sea necesario.
- **Orquestar alertas y revisiones:** automatizar notificaciones y asignar revisiones manuales solo en casos sospechosos.
- **Monitorear y ajustar continuamente:** medir tasas de fraude y abandono, y optimizar el flujo basado en datos reales para evaluar el éxito del onboarding.

Este enfoque permite ofrecer un onboarding fluido para la mayoría de los clientes, mientras se intensifica la seguridad donde se requiera.

Buenas prácticas estratégicas

Para reforzar las estrategias anteriores, se recomiendan estos principios:

1. Experiencia primero: mantener la fluidez del registro para la mayoría de los usuarios.

2. Tecnología como habilitador: biometría, IA y machine learning previenen fraude sin fricción visible.

3. Feedback al usuario: informar de manera clara y amigable cuando se requiera verificaciones adicionales.

En conjunto, estas prácticas muestran que seguridad y experiencia de cliente no son objetivos excluyentes; más bien se refuerzan mutuamente cuando se aplican estrategias inteligentes y tecnología avanzada.

¿Cómo ayuda Sovos?

Sovos combina tecnologías avanzadas de verificación de identidad biométricas y no biométricas -incluyendo liveness detection- y procesos de autenticación multifactor con análisis de riesgo inteligente que permiten a las empresas proteger su onboarding y operaciones sin sacrificar la experiencia del cliente.

Esto permite

• Detectar documentos y credenciales falsas en tiempo real.

• Verificar la identidad de los usuarios de manera robusta sin pasos engorrosos.

• Aplicar controles dinámicos según el riesgo y comportamiento del cliente.

Estas capacidades reducen los intentos de fraude y agilizan el onboarding, asegurando que los usuarios legítimos se registren rápido y sin fricción.

Rol estratégico para la empresa

Más allá de la tecnología, Sovos ayuda a convertir la prevención del fraude en valor estratégico, no solo operativo. Contar con sistemas de onboarding seguros y sin fricción:

• Protege la reputación de la marca.
• Mejora la conversión y la retención de clientes.
• Permite cumplir con regulaciones locales e internacionales de manera eficiente.

El onboarding digital es la primera impresión, el inicio de la relación y la primera línea de defensa contra el fraude. El gran desafío consiste en equilibrar seguridad y experiencia, evitando exposición a ataques y la fricción que aleja a usuarios legítimos.

Transforma tu onboarding digital: protege a tus clientes, reduce el fraude y mejora la conversión. Con Sovos, es posible. Hablemos.