INFORME SOBRE FRAUDE DE IDENTIDAD

De la democratización a la sofisticación: millones de intentos de fraude, cada uno más fuerte

AMÉRICA LATINA

2025-2026

Un informe completo de expertos de la industria basado en datos sobre las tendencias en materia de fraude de identidad y las técnicas de prevención

Introducción

En el Informe sobre fraude de identidad del 2024, identificamos la democratización del fraude: el rápido aumento de las plataformas de fraude como servicio y los kits de herramientas listos para usar que redujeron las barreras de entrada para los delitos de identidad. Esa tendencia aún no ha desaparecido. En todo caso, se ha integrado en el ecosistema del fraude, lo que mantiene el fraude de identidad generalizado y accesible, con millones de intentos registrados en nuestra plataforma cada año.

Pero, aunque el volumen de ataques sigue siendo abrumador, la naturaleza del fraude está cambiando. Los métodos "descuidados" de antes, como las falsificaciones de documentos desprolijas y los burdos trabajos de copiar y pegar, son reemplazados cada vez más por sistemas de verificación más sofisticados. Sin embargo, los estafadores se han adaptado y han reutilizado las mismas herramientas democratizadas para llevar a cabo operaciones más inteligentes y profesionalizadas. Hoy en día, los fraudes de identidad mediante deepfakes, las redes de identidades sintéticas y los abusos cuidadosamente orquestados tras el proceso KYC son mucho más habituales.

Nos referimos a este punto de inflexión como la evolución la sofisticación: un momento en el que los casos de fraude pasan de ser un ruido a alto volumen a ataques menos frecuentes, pero más precisos y dañinos. Esto es importante porque los porcentajes estables pueden crear una falsa sensación de seguridad. En realidad, cada intento de fraude exitoso representa ahora una mayor preparación, mayores costos y un impacto a más largo plazo tanto para las víctimas como para las instituciones.

Por eso es fundamental dar un paso atrás y ver el panorama general. En nuestro Informe sobre el fraude de identidad 2024, vimos cómo las nuevas tecnologías y los mercados de fraude como servicio han transformado el panorama de las amenazas. El informe 2025 continúa con esa narrativa, mostrando cómo esas tácticas democratizadas están madurando ahora en operaciones más específicas y profesionales. Mediante el análisis de millones de intentos de fraude en todos los sectores y la combinación de esos datos con los resultados de encuestas globales, este informe ofrece una visión completa de cómo está evolucionando el fraude de identidad y de lo que deben preparar las empresas, los reguladores, las plataformas y los proveedores de servicios de cara a 2026 y en el futuro.

Andrew Sever,
CEO de Sumsub

"Estamos siendo testigos de un cambio fundamental en la naturaleza del fraude. La IA generativa ha democratizado el engaño, pero también ha obligado a la verificación a innovar a un ritmo más rápido que nunca. Lo que estamos presenciando ahora no es un aumento en los niveles de fraude, sino ataques más inteligentes y deliberados, con múltiples capas de engaño.

La evolución de la **sofisticación** marca un punto de inflexión, ya que las empresas se enfrentan ahora a retos relacionados con su velocidad y la rapidez con la que pueden detectar amenazas y adaptarse. La próxima frontera en la prevención del fraude pertenecerá a aquellos que sean capaces de unir la perspicacia humana, la inteligencia de datos y la precisión de la IA para generar confianza a gran escala. Este informe recoge la evolución del fraude para convertir los datos en previsiones con el fin de construir un futuro digital más seguro."

Tabla de Contenidos

Metodología

Las principales fuentes de datos para el informe

Este estudio ofrece un análisis detallado de la dinámica del fraude de identidad en América Latina. El fraude de identidad se refiere al robo o la falsificación de información personal para llevar a cabo actividades fraudulentas, como abrir cuentas o realizar compras no autorizadas.

Más de 4 millones de

intentos de fraude analizados

En este informe, comparamos los datos internos de verificación de identidad y actividad de los usuarios de 2024 y 2025, que abarcan intentos de fraude en múltiples países y sectores. En algunos casos, también se incluyen datos de 2023 para resaltar las tendencias a más largo plazo.

Más de 300

profesionales encuestados especializados en fraude y riesgos

Todos los datos se basan en países con una actividad significativa de usuarios en nuestra plataforma. Para garantizar la fiabilidad de las estadísticas, solo hemos incluido jurisdicciones en las que hemos procesado más de 15 000 intentos de verificación durante el periodo del informe. Los países con menor tráfico quedan excluidos de este análisis, ya que el tamaño de sus muestras podría no reflejar con precisión las tendencias generales en materia de fraude.

Más de 1.2 mil

usuarios finales encuestados

Para analizar más a fondo la situación del fraude de identidad, Sumsub realizó una encuesta sobre la exposición al fraude en agosto de 2025, en la que recopiló opiniones tanto de empresas como de consumidores.

La encuesta sobre exposición al fraude de Sumsub para 2025 incluyó a empresas de diversos sectores, como banca, criptomonedas, pagos, comercio electrónico, comercio y juegos de azar en línea. Los participantes contaron sus experiencias con casos de fraude en 2025, el impacto que sufrieron y sus estrategias para combatir el fraude en 2026.

Todos los gráficos e infografías se basan en estadísticas internas elaboradas a partir de los datos de clientes que han dado su consentimiento. Los datos han sido agregados y se han mantenido en el anonimato.

Tendencias clave

La tendencia principal de este año: la Evolución de la sofisticación

¿Qué hay detrás de esta tendencia?

1 Fraude menos descuidado y que requiere menos esfuerzo, pero intentos más avanzados que causan daños más importantes. En comparación con 2024, hubo un 180 % de aumento en el 'fraude sofisticado' con el uso de técnicas de engaño, ingeniería social, e identidades generadas con IA.

2 Aunque la concietización y la educación públicas en materia de fraude mejoran, mantenerse al día con las tecnologías en rápida evolución es un desafío importante.

3 Las plataformas de verificación más sólidas han hecho que la simplicidad de las estafas amateur, de bajo esfuerzo y alto rendimiento del año pasado resulten en gran medida infructuosas. Como resultado, los estafadores están pasando a operaciones más estratégicas, invirtiendo más tiempo y recursos en ataques que puedan eludir estas defensas.

Tendencia 2: Fraude industrializado por IA

En años anteriores, los estafadores han utilizado principalmente la IA como herramienta para falsificar identificaciones, editar documentos o burlar los controles de autenticidad. En 2025, se ha convertido en algo más grande: un sofisticado ecosistema de producción de fraudes.

1 **Falsificación de documentos.**
Plataformas como las herramientas avanzadas de generación de imágenes de OpenAI ahora crean identificaciones con detalles casi perfectos, replicando fuentes, hologramas y texturas que antes requerían habilidades especializadas.

2 **Intentos de protección.**
Las grandes empresas tecnológicas han intentado implementar medidas de protección para combatir la desinformación y el plagio, incluyendo la adición de marcas de agua al texto generado por IA. Sin embargo, estas marcas de agua se pueden eliminar fácilmente, lo que permite a los delincuentes hacer pasar sus propias imágenes generadas por IA como auténticas o robarlas para utilizarlas en cualquiera de sus propias imágenes generadas por IA.

3 **Video sintético.**
Los sistemas de conversión de texto a video de última generación, como Google Veo y Sora y Sora 2 de OpenAI, pueden renderizar escenas dinámicas completas a partir de breves indicaciones, con microexpresiones faciales realistas, iluminación y profundidad. Estas herramientas permiten a los atacantes realizar comprobaciones de autenticidad convincentes que imitan los movimientos y reacciones de personas reales, lo que convierte la verificación visual en una de los niveles más vulnerables de la defensa de la identidad.

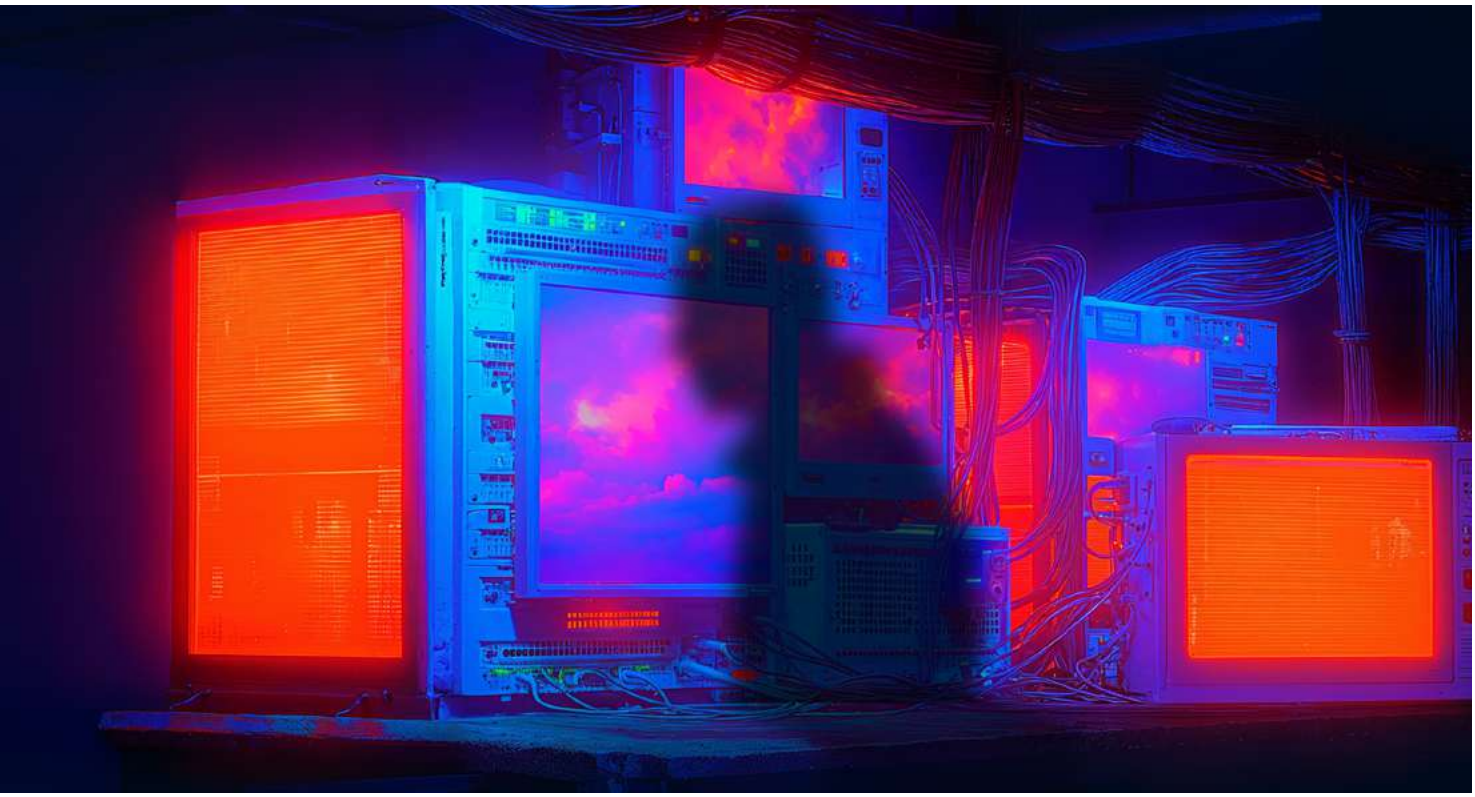
4 **La carrera hacia la cima.**
A medida que la IA alcanza su mayor nivel de adopción tanto entre empresas como entre consumidores, las grandes tecnológicas compiten por ser las más innovadoras en este ámbito. Tras el lanzamiento de Veo 3 de Google, OpenAI presentó Sora 2, seguido rápidamente por el lanzamiento de Veo 3.1 de Google, lo que supuso una escalada en la competencia por crear las herramientas de IA más realistas, acelerando así la evolución de la sofisticación.

5 **Atomatización y escala.**
Los proveedores de fraude como servicio ahora agrupan estos modelos en kits de producción listos para usar, lo que permite incluso a los actores menos calificados generar cantidades industriales de falsificaciones de alta calidad.

Esto marca el salto de la IA como ayudante a la IA como motor detrás del fraude industrializado y escalable. Acelera tanto la cantidad (millones de intentos siguen inundando el sistema) como la calidad (ataques más sofisticados y difíciles de detectar), lo que alimenta la evolución de la sofisticación.

Tendencia 3: Agentes de fraude basados en IA

En 2025, vimos la primera aparición de los agentes de fraude basados en IA, sistemas autónomos que combinan contenido generativo, scripts y mimetismo conductual para ejecutar intentos de verificación completos de principio a fin. Lo que comenzó como experimentos aislados en el 2025, se espera que se convierta en una gran ola en 2026, a medida que estos agentes evolucionen hasta convertirse en bots fraudulentos autónomos capaces de ajustar sus estrategias en tiempo real.



Tendencia 4: La manipulación de la telemetría se convierte en la nueva evasión

A medida que mejoran los controles de incorporación y el análisis forense de documentos, los estafadores se centran cada vez más en los propios canales de datos, en lugar de solo en los artefactos de identidad. En lugar de limitarse a intentar engañar al ojo humano o a un clasificador de IA, trabajan para manipular las señales en las que se basan esos sistemas.

1 **Manipulación de SDK y API.**
Los estafadores crean flujos de verificación, reproducen sesiones pregrabadas o manipulan las llamadas SDK para engañar a los sistemas y hacerles creer que se ha producido una sesión auténtica.

2 **Enmascaramiento de dispositivos y entornos.**
Las granjas de emuladores, las máquinas virtuales y las capas de proxy permiten a los atacantes aparecer como usuarios "nuevos", ocultando las huellas digitales de los dispositivos y las señales de ubicación que suelen delatar los intentos repetidos de fraude.

3 **Interferencia en la señal de la cámara.**
Los estafadores intentan eludir las comprobaciones de vida inyectando fotogramas sintéticos o burlando las API de las cámaras, introduciendo videos pregrabados o generados por IA en lo que debería ser una captura en vivo.

Esto representa un cambio radical en la táctica. En lugar de atacar solo el contenido (una identificación falsa o un rostro deepfake), los estafadores ahora atacan el contexto (la forma en que los sistemas de verificación perciben y transmiten las señales).

Análisis Regional

Los siguientes insights regionales se basan en países con una actividad significativa de usuarios en nuestra plataforma. Para garantizar la confiabilidad estadística, solo se incluyeron las jurisdicciones en las que se procesaron más de 15,000 intentos de verificación durante el período del informe. Los países con menor volumen de tráfico se excluyen de este análisis, ya que el tamaño de sus muestras puede no reflejar con precisión las tendencias generales de fraude.

América Latina y el Caribe

América Latina sigue siendo uno de los entornos con mayor evolución en materia de fraude. La rápida expansión de los pagos digitales, el comercio electrónico y las plataformas de envío de remesas ha ampliado el acceso a los servicios financieros, pero también ha hecho que la región resulte muy atractiva para los estafadores.

En 2025, América Latina presentó claramente la Evolución de la sofisticación: Los intentos burdos están disminuyendo, pero las selfies generadas con IA, las sintéticas y las redes organizadas de fraude están ocupando ocupando un lugar importante.

Evolución de los tipos de fraude en América Latina

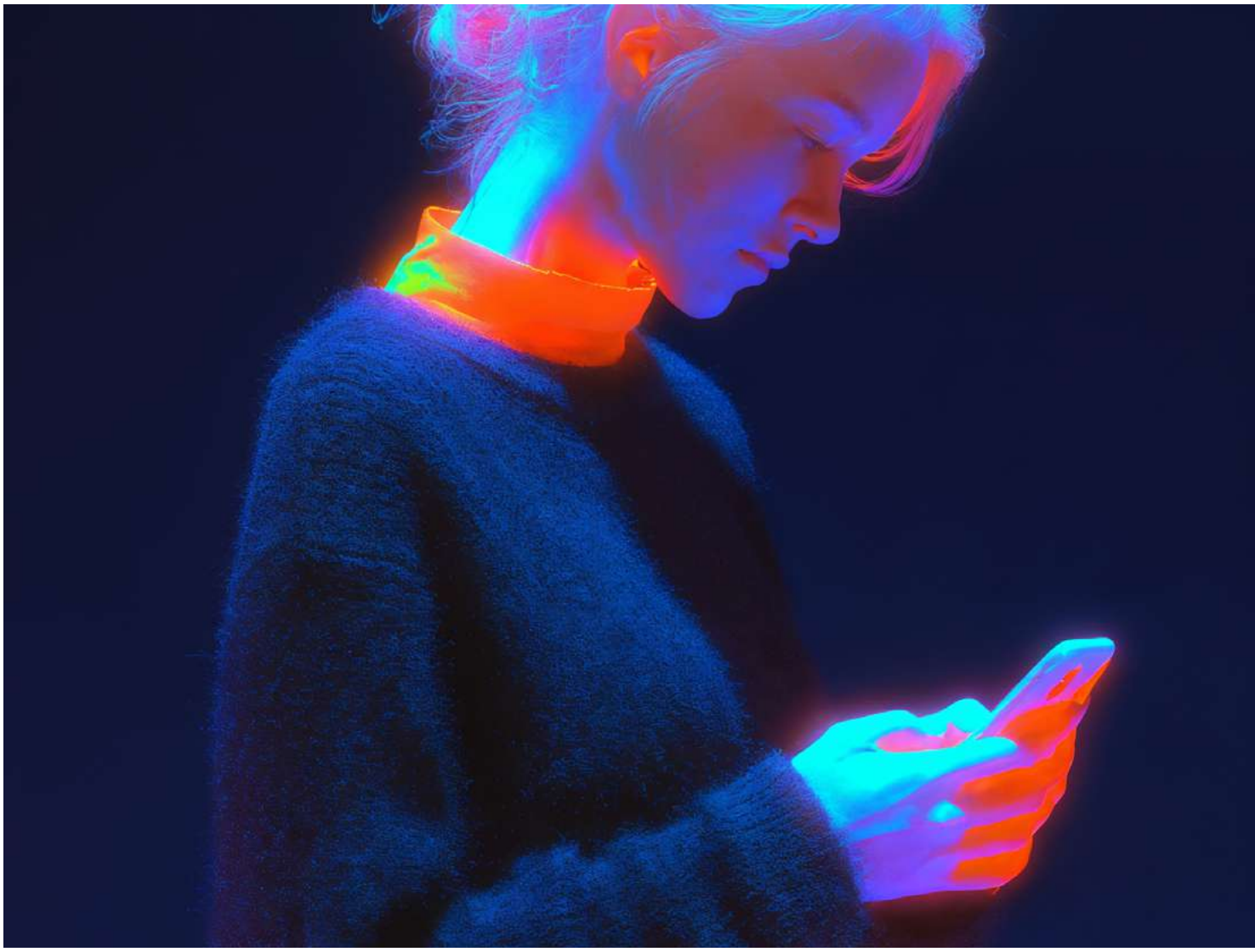
Los patrones de fraude en América Latina evolucionaron considerablemente en 2025:

Los fraudes con selfies son los que predominan.
El fraude relacionado con inconsistencias entre la selfie de un usuario y la imagen de su documento de identidad es la categoría más importante, ya que representa el 42 % de todos los fraudes, aunque su porcentaje ha disminuido en comparación con 2024. Esto refleja el auge explosivo de los deepfakes, muchos de los cuales se clasifican en estas categorías cuando eluden la clasificación directa.

Los fraudes de identidad sintética se expanden rapidamente.
Los datos personales falsos se triplicaron en un año, representando el 7,3 % de todos los fraudes. Los estafadores están creando identidades digitales totalmente falsas (con nombres, direcciones y fechas de nacimiento inventados) y combinándolas con selfies falsas para superar los controles de incorporación.

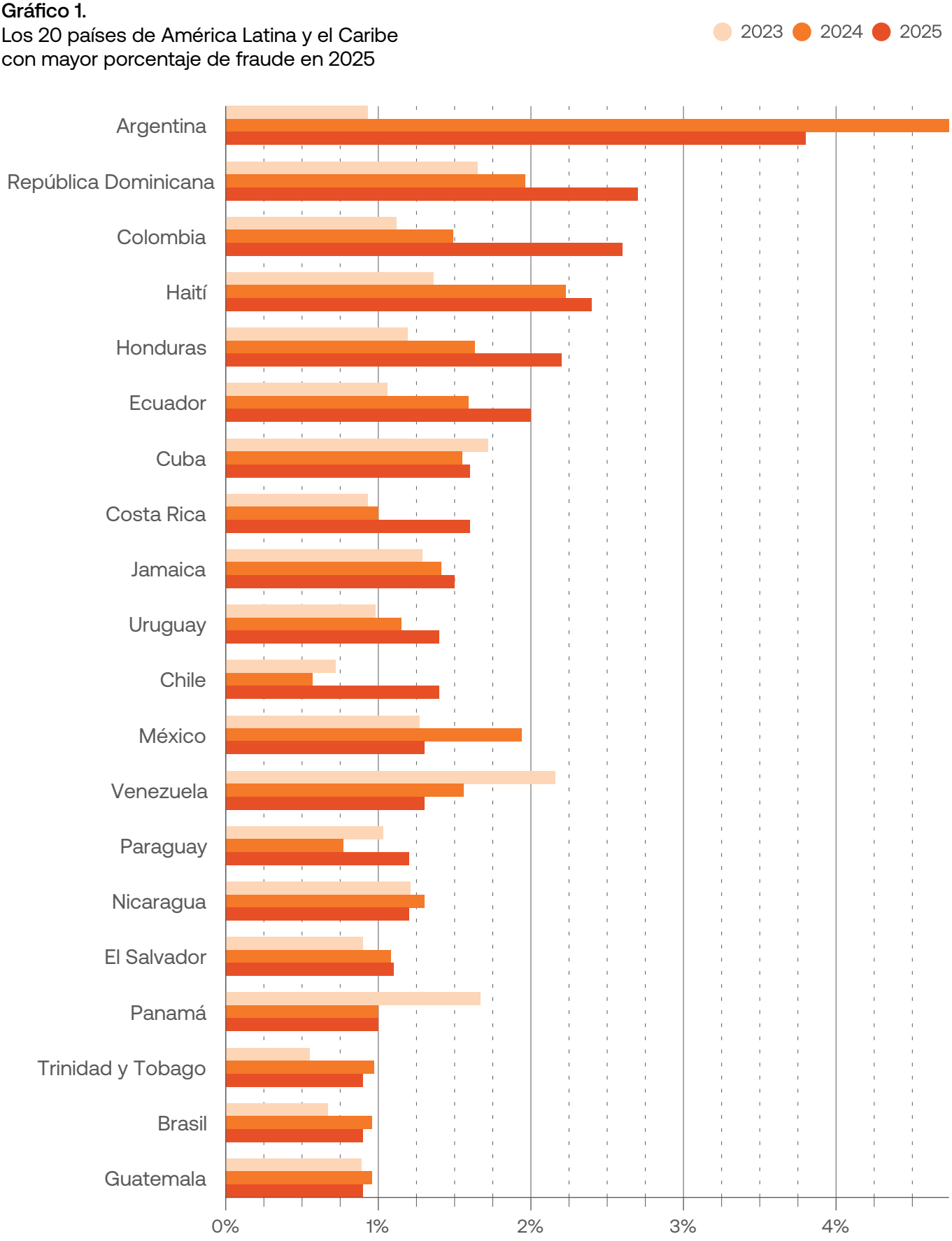
Las identidades editadas persisten, las identificaciones falsificadas son rechazadas.
El fraude con documentos de identidad editados aumentó ligeramente (+86 % interanual), estabilizándose en un 4,6 %, mientras que los documentos de identidad falsificados fueron perdiendo importancia hasta situarse en un 2,6 %, lo que indica que los estafadores prefieren la manipulación digital por sobre la falsificación de documentos físicos.

Los viejos trucos ya no funcionan.
Los intentos de bloqueo se han reducido casi a la mitad, lo que confirma que los errores básicos ya no pueden eludir los filtros antifraude.



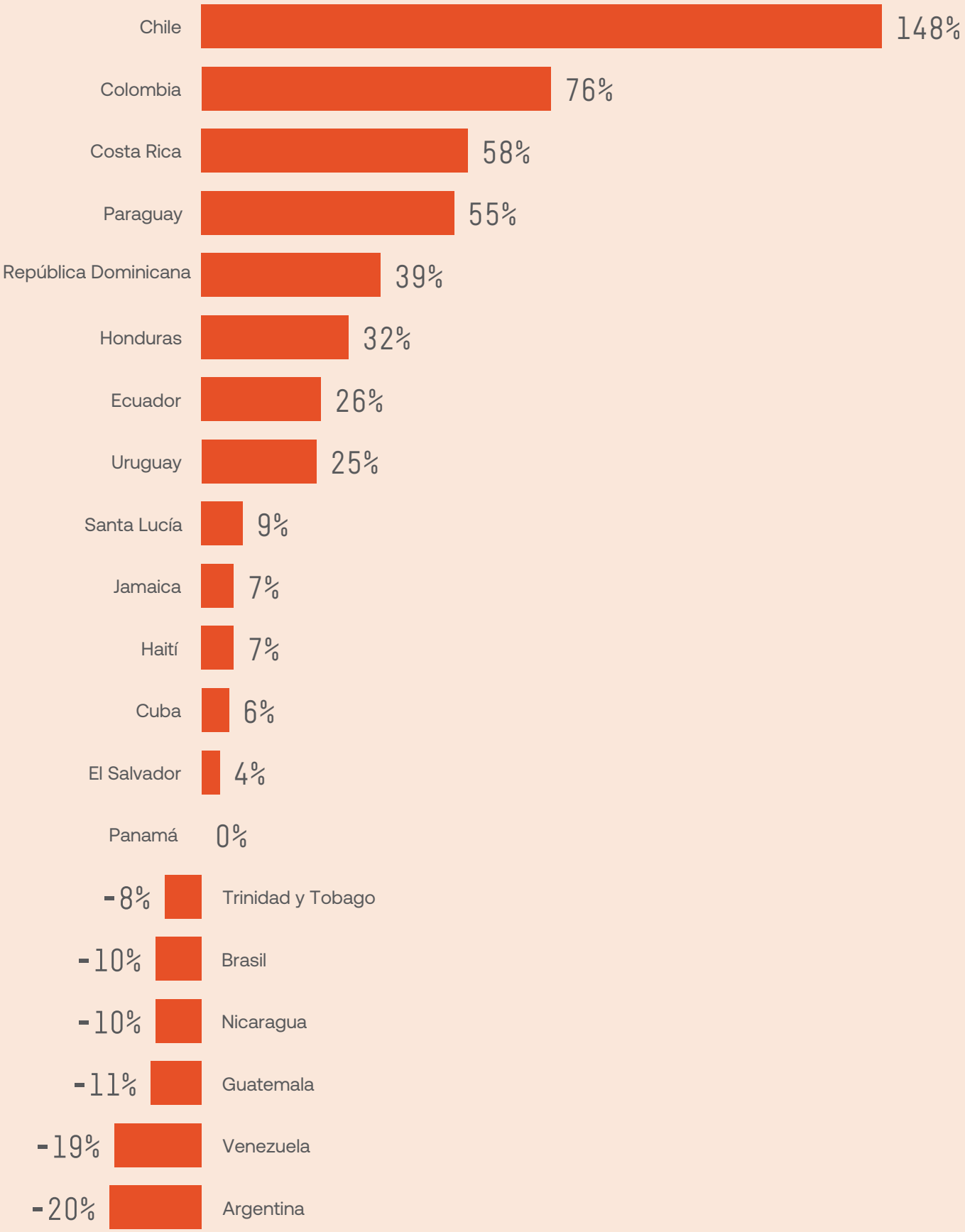
Nuevas señales de redes fraudulentas.
El fraude basado en plantillas aumentó (+56 % interanual) y los intentos de elusión de los controles de autenticidad se dispararon (+60 % interanual), lo que indica que las redes de fraude están investigando sistemáticamente los controles de autenticidad y reciclando plantillas de documentos en múltiples mercados.

Gráfico 1.
Los 20 países de América Latina y el Caribe con mayor porcentaje de fraude en 2025



en todas las verificaciones analizadas por país

Gráfico 2.
Los 20 países de América Latina y el Caribe con mayor procentaje de crecimiento de fraude interanual



Dinámica a nivel nacional

Los promedios regionales ocultan cifras nacionales sorprendentes:

Aumento de puntos de acceso

1 **Colombia** vio cómo su tasa de fraude subía hasta el 2,6 % (+76 % interanual), con un aumento de la actividad de deepfakes de más del 77 % interanual. Los estafadores se centran en los sectores de la banca digital y el comercio electrónico, que están creciendo rápidamente.

2 **República Dominicana** alcanzó el 2,7 % (+39 %) con una de las tasas de deepfakes más altas de la región (6 %).

3 **Honduras** (2,2 %, +32 %) y **Ecuador** (2,0 %, +26 %) tuvieron aumentos rápidos, impulsados por un KYC más débil en las carteras móviles.

4 **Chile** se destacó, con un aumento de casi el triple en los fraudes, hasta alcanzar el 1,4 % (+148 % interanual), lo que demuestra que los mercados más pequeños se están convirtiendo en campos de pruebas.

Estable pero bajo presión

1 **Brasil** (0,9 %, –10 % interanual) sigue manteniendo una de las tasas de fraude más bajas de la región, gracias a la sensatez de las leyes que previenen el blanqueo de capitales, a las normas cada vez más estrictas del Banco Central en materia de KYC y a la normativa de pagos de Pix, y a un fuerte enfoque en la supervisión de las transacciones en tiempo real. Sin embargo, las actividades relacionadas con las identidades falsas y sintéticas están aumentando, especialmente en la banca digital y las apuestas en línea, donde los atacantes aprovechan los perfiles generados por IA para eludir los controles de incorporación. Este cambio demuestra que, aunque Brasil ha logrado contener el fraude básico, está entrando en una nueva fase caracterizada por la suplantación de identidad mediante inteligencia artificial y la manipulación de múltiples cuentas.

2 **Haití** (2,4 %, +7 %) y **Jamaica** (1,5 %, + 7 %) siguen siendo mercados moderados, pero en crecimiento. Ambos están experimentando una aceleración en el uso de deepfakes, con un aumento del 250 % en los intentos de deepfakes registrados en Haití.

3 **Uruguay** (1,4 %, + 25 %) sigue teniendo una tasa relativamente baja, pero el 7 % de los solicitantes estaban vinculados a redes de fraude, una de las cifras más altas de América Latina.

Mercados en declive

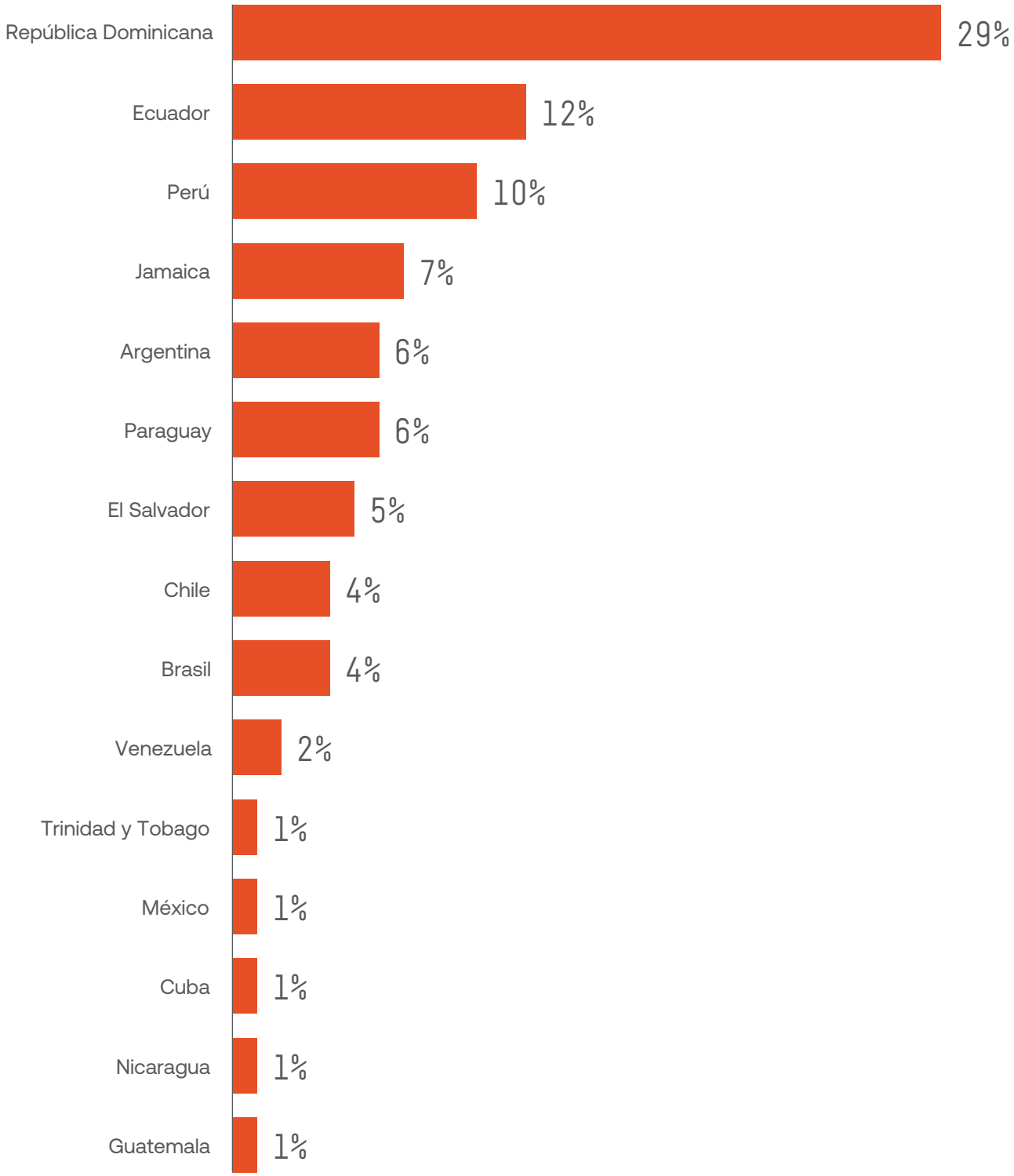
1 **Argentina** cayó al 3,8 % (–20 %) tras alcanzar su máximo en 2024, en parte debido al endurecimiento de la normativa en torno a la incorporación de tecnologías financieras. Sin embargo, los deepfakes siguieron aumentando un 66 % interanual, lo que demuestra que la sofisticación aumenta a pesar de la caída del volumen.

2 **México** cayó al 1,3 % (–32 %), pero registró uno de los mayores picos de deepfakes a nivel mundial (+484 % interanual), lo que indica que los atacantes están pasando del volumen a la calidad.

3 **Venezuela** descendió al 1,3 % (–19 %), mientras que los deepfakes casi se duplicaron (+99 % interanual).

4 En **Surinam**, el fraude se redujo al 0,4 % (–71 %), pero los deepfakes aumentaron más de un 400 %, lo que pone de relieve la paradoja: menos casos, pero ataques más sofisticados.

Gráfico 3.
Las 20 jurisdicciones con la mayor proporción de solicitantes aprobados involucrados en redes de fraude



Deepfakes en América Latina: calidad por sobre cantidad

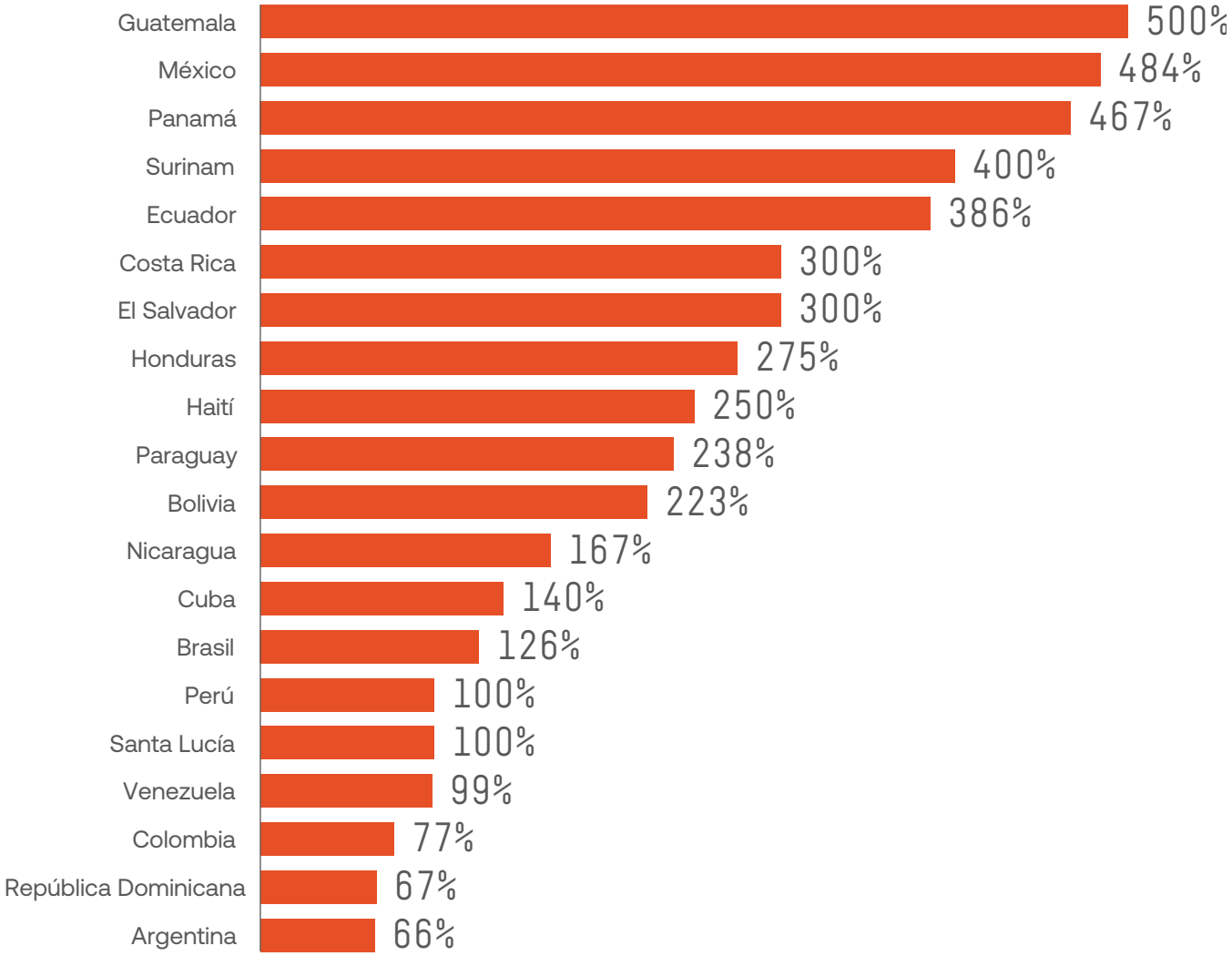
Los deepfakes se están extendiendo por Latinoamérica a una velocidad extraordinaria:

Aceleración de deepfakes: Brasil se sitúa en la mitad de la tabla (126 % de crecimiento interanual), mientras que países como Guatemala, México, Panamá y Surinam están experimentando un crecimiento exponencial (+400-500 %).

Costa Rica y El Salvador tuvieron un aumento significativo en la actividad de deepfakes, con tasas que se triplicaron o más, a pesar de que las tasas generales de fraude fueron relativamente bajas.

Surinam muestra la paradoja con mayor claridad: el fraude general se ha reducido drásticamente, pero los deepfakes se han cuadruplicado, lo que ilustra cómo la sofisticación aumenta incluso en mercados en declive.

Gráfico 4.
Los 20 países de América Latina con más crecimiento de deepfakes interanual (2025 respecto de 2024)



En toda la región, los deepfakes han pasado de ser herramientas novedosas a convertirse en instrumentos de fraude de gran precisión. Su función está pasando de la simple falsificación de videos a la infiltración completa en el ecosistema, combinando la imitación de la voz, el rostro y el comportamiento para eludir la verificación en varios niveles. Los datos confirman que la lucha de América Latina contra el fraude con IA no consiste en detener su propagación, sino en adelantarse a su evolución.

Por qué algunos países cayeron mientras que otros crecieron

El fraude aumentó más rápidamente en países con una rápida expansión de las empresas de tecnología financiera, pero dónde el cumplimiento de la ley es más laxo, como Colombia, la República Dominicana y Chile. Los estafadores se aprovechan de los ecosistemas de alto crecimiento que carecen de controles de incorporación coherentes, y con frecuencia reutilizan identidades sintéticas en diferentes plataformas.

Por el contrario, Argentina y México redujeron las tasas de fraude con una mayor presión legal, pero la proporción de deepfakes se disparó. Estos casos ponen de relieve la evolución fundamental en la sofisticación: está quedando atrás el fraude burdo y el fraude sofisticado permanece y es más peligroso en cada caso.

¿Qué se puede esperar?

Las perspectivas de América Latina se caracterizan por la polarización:

Algunos mercados seguirán sufriendo un aumento de las tasas de fraude, ya que los casos superan a los mecanismos de defensa. Otros mostrarán porcentajes a la baja, pero esas victorias se verán socavadas por el fraude impulsado por deepfakes, que es más difícil de detectar y más costoso cuando se pasa por alto.

En el año 2026, podemos esperar:

1 **Los deepfakes se generalizaran**
Además de las selfies, se extenderán a las comprobaciones de vida en video y e incluso a la imitación de voces para centros de atención telefónica.

2 **Las redes de fraude se están expandiendo**
Los intentos de fraude basados en plantillas y de elusión de la comprobación de vida están aumentando, lo que indica que hay redes organizadas que operan en distintos países.

3 **Evolución a ecosistemas sintéticos**
Más fraudes basados en identidades generadas íntegramente por IA, no solo en identidades robadas.

4 **Mayor fragmentación normativa**
Algunos gobiernos (Argentina, México, Brasil) están endureciendo las normas de KYC, mientras que los mercados más pequeños siguen siendo vulnerables debido a los efectos colaterales del fraude procedente de países vecinos.

Jovanny Huerta,
Especialista en
Proyectos de seguridad
en inDrive (México)

"Para 2026, el fraude estará marcado sobre todo por el rápido avance de la inteligencia artificial. Los estafadores industrializarán los deepfakes, la clonación de voces y las identidades sintéticas, lo que hará que las estafas por suplantación de identidad, la ingeniería social y las apropiaciones de cuentas sean más convincentes y difíciles de detectar. La accesibilidad del "fraude como servicio" reducirá las barreras de entrada, lo que permitirá incluso a los actores menos cualificados lanzar ataques sofisticados a gran escala.

Al mismo tiempo, la expansión global de los sistemas de pago en tiempo real y los activos digitales creará un terreno fértil para el fraude de alta velocidad y gran impacto. Las transacciones instantáneas e irreversibles aumentarán los riesgos de estafas con pagos push autorizados y apropiaciones de cuentas, mientras que el continuo auge de las criptomonedas, los NFT y las plataformas DeFi dará lugar a estafas cada vez más complejas, como rug pulls (estafas de salida), vaciado de monederos y protocolos falsos. Los métodos de detección tradicionales tendrán dificultades para seguir el ritmo y la sofisticación de estos ataques.

Los mecanismos de defensa tendrán que evolucionar con la misma rapidez. La detección basada en inteligencia artificial, la biometría conductual y la verificación de identidad en varios niveles se convertirán en herramientas esenciales para contrarrestar las amenazas impulsadas por la inteligencia artificial. Las organizaciones deben combinar tecnología avanzada con una supervisión humana más estricta, marcos normativos y un enfoque de confianza cero. En resumen, 2026 marcará un punto de inflexión: el fraude será más rápido, más inteligente y más convincente que nunca, y solo aquellos que estén preparados para hacerle frente a la IA con IA podrán mantenerse a la vanguardia".

Desafíos globales, realidades locales

Conozca la situación de América Latina en la Encuesta sobre exposición al fraude 2025 de Sumsub.

Empresas

43 %

Las empresas de América Latina han sido víctimas de fraudes en 2025.

Consumidores

68 %

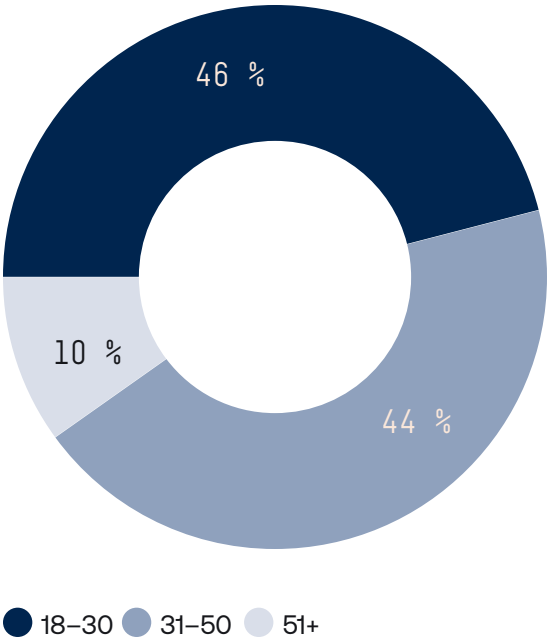
Los usuarios finales de América Latina han sido víctimas de fraude al menos una vez en 2025.

Hallazgos sobre fraude al consumidor en América Latina

Gráfico 5.

Observe más de cerca a nuestros consumidores con sede en América Latina, desde su edad hasta su situación laboral.

Edad



Situación laboral

73 %
Empleados de tiempo completo

11 %
Trabajadores independientes de tiempo completo/parcial

9 %
Empleados de tiempo parcial

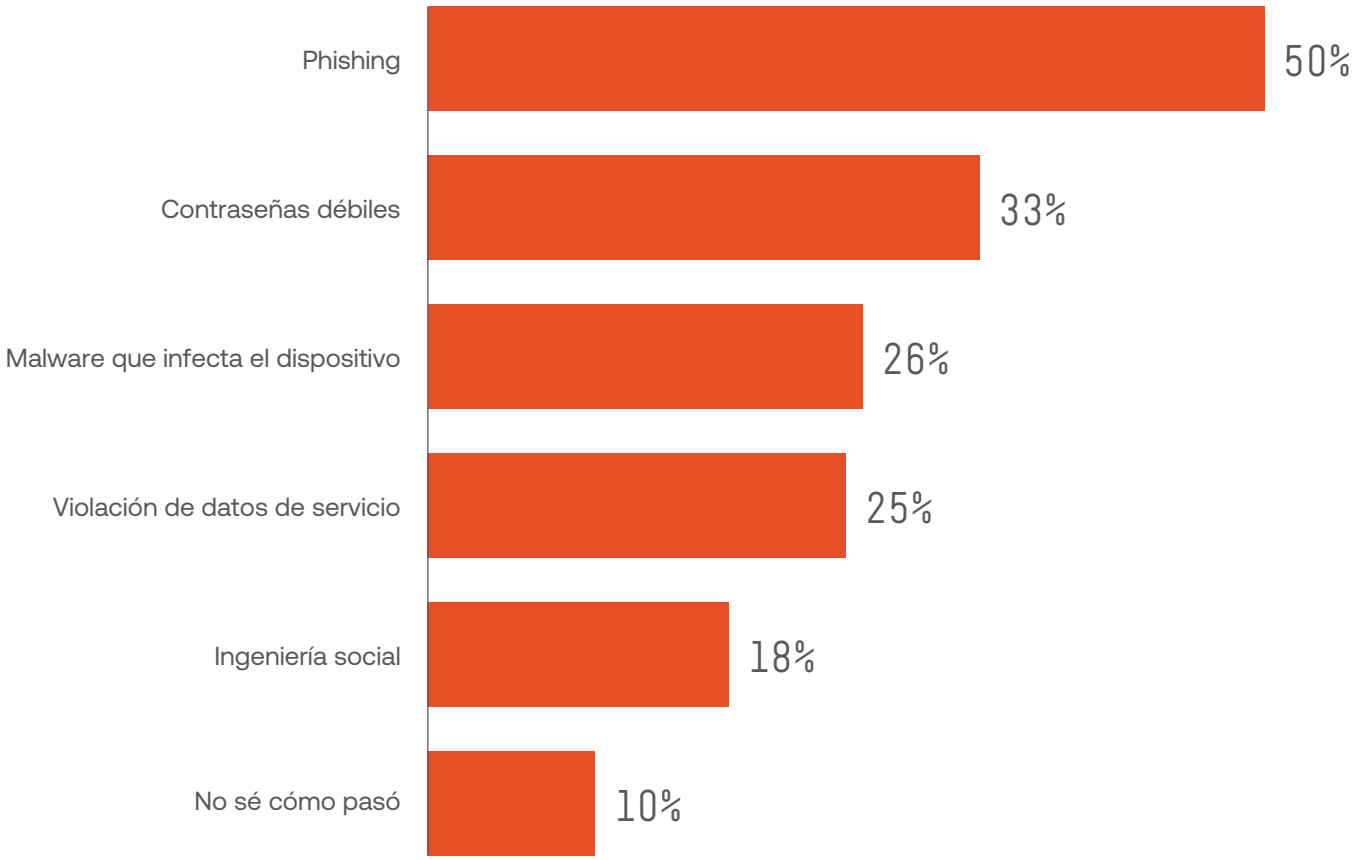
7 %
Desempleados temporalmente

Principales vectores de ataque

El phishing sigue siendo claramente el más importante: el 50 % de los incidentes comienzan con un mensaje engañoso.

Sin embargo, las contraseñas débiles (33 %) y el malware a nivel de dispositivo (26 %) siguen siendo puntos de entrada importantes y controlables por el usuario, mientras que las violaciones de datos de los servicios (25 %) indican que los atacantes aprovechan cada vez más las exposiciones de terceros tanto como los errores individuales. Un menor número de víctimas (10 %) desconoce el vector de la brecha, lo que indica una tendencia creciente hacia el sigilo y la automatización en los ataques.

Gráfico 6.
Pregunta:
¿Cuál cree que fue la causa del incidente de fraude?



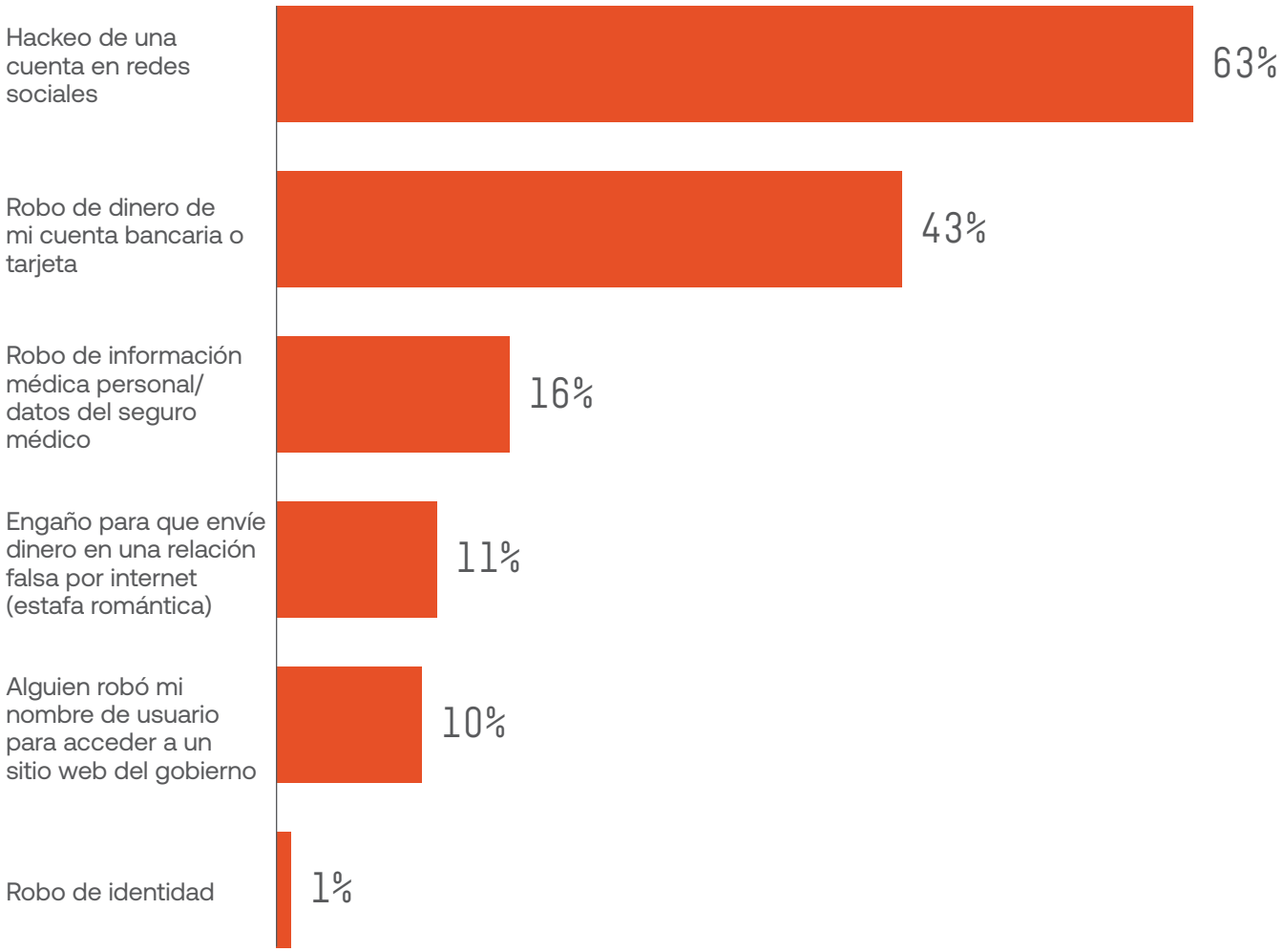
Encuesta sobre exposición al fraude de Sumsub 2025, América Latina: Consumidores

Principal resultado del fraude

Un sorprendente 63 % de los encuestados sufrió el hackeo de sus cuentas en redes sociales, y otro 10 % perdió el acceso a sus cuentas gubernamentales, ambos casos claros de apropiación de cuentas (ATO).

La mitad de los encuestados se enfrentó a algún tipo de suplantación de identidad. Si bien el 43 % sufrió un robo financiero directo, estos ataques suelen comenzar con el compromiso de las credenciales.

Gráfico 7.
Pregunta:
¿Qué tipo de fraude de identidad sufrió?



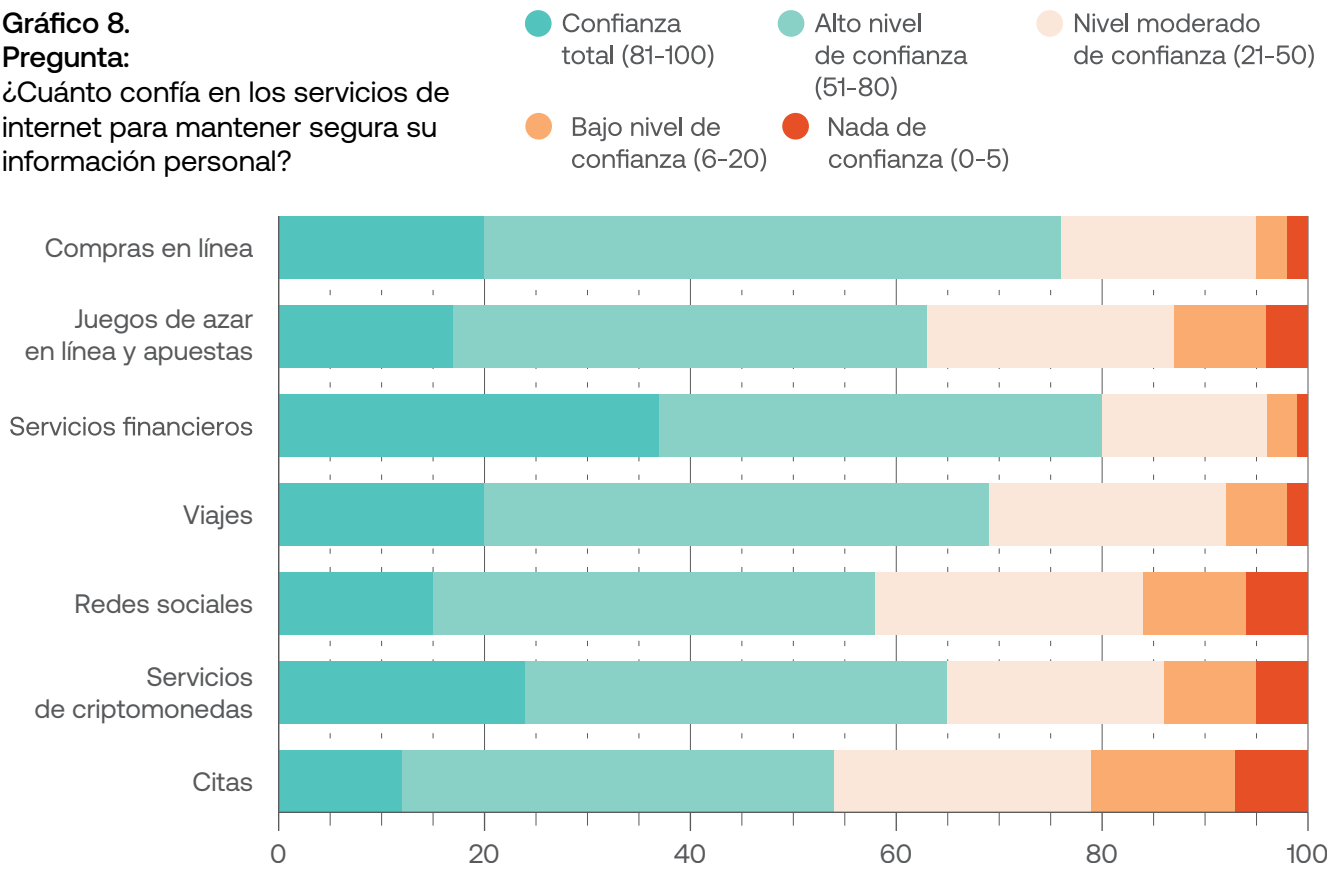
Encuesta sobre exposición al fraude de Sumsub 2025, América Latina: Consumidores

Confianza digital en América Latina

Los encuestados muestran la mayor confianza en los servicios financieros, con un 81 % que expresa una confianza alta o total, lo que confirma que los bancos siguen siendo los guardianes más fiables de los datos personales.

Las compras en línea (77 %) y las plataformas de viajes (70 %) mantienen niveles de confianza relativamente altos, probablemente debido a protecciones visibles, como métodos de pago seguros y políticas de reembolso claras. Por el contrario, las criptomonedas (66 %), las redes sociales (59 %) y las aplicaciones de citas (57 %) revelan un déficit de confianza importante, lo que refleja la preocupación de los usuarios por el uso indebido de los datos, las estafas y las garantías de privacidad débiles.

Gráfico 8.
Pregunta:
¿Cuánto confía en los servicios de internet para mantener segura su información personal?



Encuesta sobre exposición al fraude de Sumsub 2025, América Latina: Consumidores

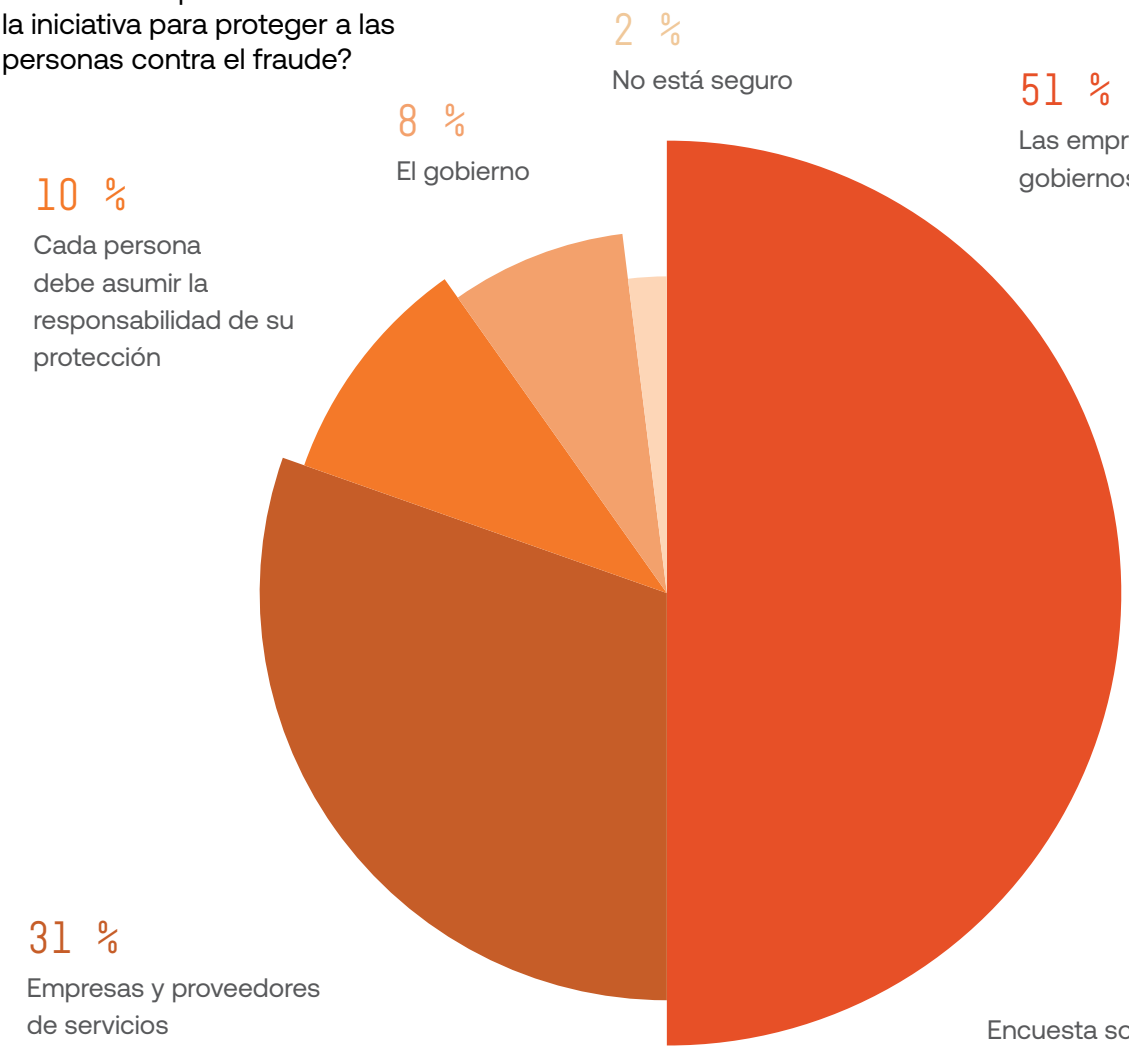
El 95 % de los encuestados elegiría un proveedor de servicios solo si este cuenta con medidas antifraude sólidas.

95%

Responsabilidad en la prevención del fraude

Más de la mitad de los encuestados (51 %) cree que la prevención del fraude debería ser una responsabilidad compartida entre las empresas y los gobiernos, lo que refleja las crecientes expectativas de protección de los sistemas, en lugar de limitarse a la vigilancia personal. Al mismo tiempo, el 31 % atribuye la responsabilidad principal a las empresas, lo que indica que los usuarios consideran que las plataformas y los proveedores de servicios son la primera línea de defensa, ya que son quienes disponen de las herramientas y los datos necesarios para detectar las amenazas de forma temprana.

Gráfico 9.
Pregunta:
¿Quién cree que debería tomar la iniciativa para proteger a las personas contra el fraude?



Encuesta sobre exposición al fraude de Sumsub 2025, América Latina: Consumidores

Tarjetas virtuales como herramientas cotidianas

El uso de tarjetas virtuales/desechables está muy extendido en América Latina, ya que **casi 9 de cada 10 personas las utilizan y más de la mitad confía en ellas en forma habitual.**

El 87 % de los encuestados utiliza tarjetas desechables/virtuales al menos ocasionalmente, y el 58 % son usuarios habituales.

Pregunta:
¿Usa tarjetas desechables o virtuales para realizar pagos por internet?

Encuesta sobre exposición al fraude 2025 de Sumsub, América Latina: Consumidores

El reclutamiento de mulas de dinero se generaliza

El conocimiento sobre el blanqueo de dinero es relativamente alto, ya que casi **el 70 % de los encuestados** sabe algo del tema. Sin embargo, el 40 % admite que no entiende nada de lo que significa, lo que revela una brecha peligrosa entre el reconocimiento y la comprensión.

Es alarmante que casi 1 de cada 3 encuestados haya sido contactado directamente para mover fondos sospechosos, lo que confirma que el reclutamiento de mulas sigue siendo una amenaza activa y visible en la región.

Pregunta:
¿Ha oído hablar del "mulas de dinero", que consiste en permitir que alguien transfiera dinero robado a través de su cuenta bancaria?

Encuesta sobre exposición al fraude 2025 de Sumsub, América Latina: Consumidores

El 86 % de los encuestados están convencidos de que el fraude se está tornando cada vez más sofisticado y está impulsado por IA.

Lo que confirma que las empresas conocen los riesgos de los deepfakes, las falsificaciones impulsadas por IA y están buscando soluciones para prevenir el fraude.

86%

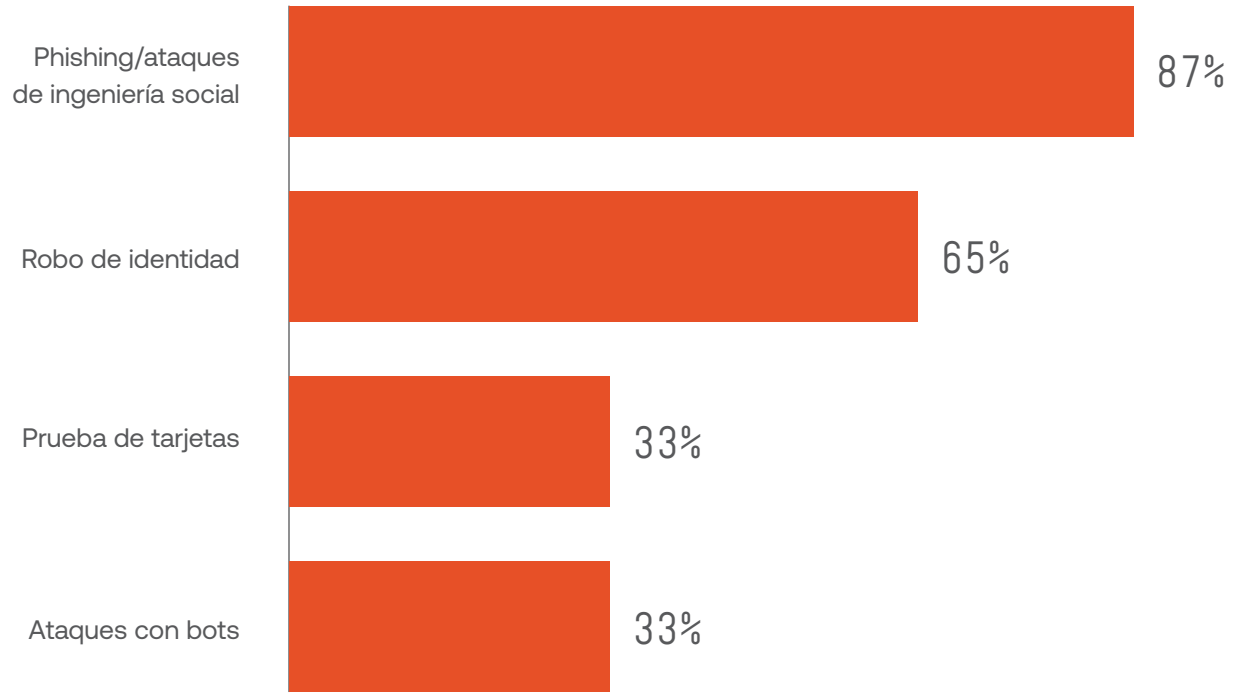
Hallazgos de fraude empresarial en América Latina

Los tres tipos de fraude más frecuentes a los que se enfrentan las empresas en América Latina

1 Phishing/ataques de ingeniería social (87 %)
2 Robo de identidad (65 %)
3 Pruebas con tarjetas y ataques de bots (33 % cada uno)

Al mismo tiempo, tuvieron que gestionar el fraude directo de sus clientes, que utilizaron identidades sintéticas y deepfakes (60 % y 55 %, respectivamente) y cometieron abusos en las solicitudes (52 %) y en las devoluciones (42 %).

Gráfico 10.
Pregunta:
¿Qué tipo de fraude de terceros tuvo que enfrentar su empresa?



Encuesta sobre exposición al fraude 2025 de Sumsub, América Latina: Empresas

Todas las empresas informan que los intentos de fraude organizado son cada vez más frecuentes.

Las consecuencias más importantes que las empresas han sufrido debido a los ataques de fraude:

1. Interrupción operativa
2. Pérdidas económicas
3. Daños a la reputación
4. Cancelación de clientes
5. Problemas con los inversores
6. Desconfianza/rotación de empleados
7. Problemas con los socios
8. Multas/sanciones
9. Cancelación de licencias

Cómo manejan las empresas el fraude

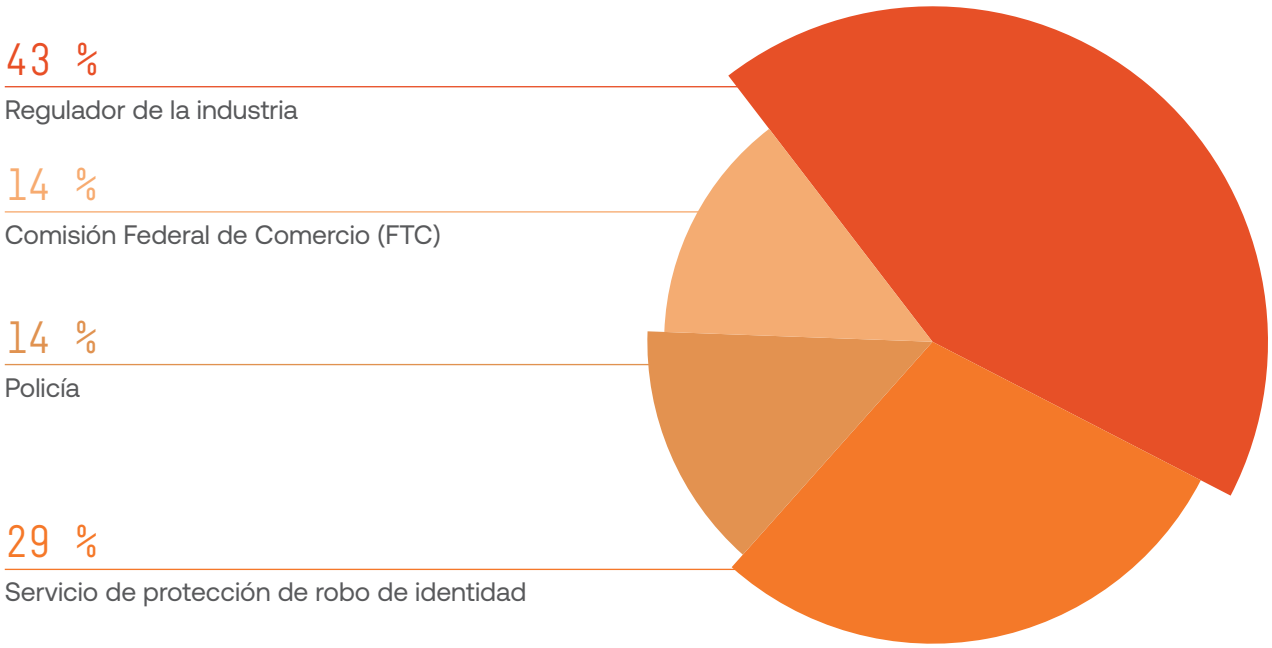
Un **abrumador 71 % de las empresas** confía en un modelo híbrido de prevención del fraude, que combina equipos internos con proveedores externos para lograr un equilibrio entre control, experiencia y escalabilidad. Sin embargo, un porcentaje igualmente elevado, el 71 %, sigue dependiendo de procesos manuales, lo que revela que la automatización y la coordinación siguen siendo carencias importantes en las operaciones contra el fraude.

Los datos revelan una paradoja: aunque las empresas reconocen la necesidad de la colaboración y la defensa por niveles, los flujos de trabajo manuales siguen ralentizando la detección y la respuesta.

Cuando se enfrenta a un fraude de identidad, la denuncia sigue siendo fragmentada. Menos de la mitad de las empresas (43 %) notifican a un organismo regulador del sector, mientras que son aún menos las que colaboran con las autoridades o con los socios financieros.

Solo el 14 % denuncia los incidentes a la policía o a un banco/institución financiera, y solo el 29 % recurre a servicios de protección contra el robo de identidad.

Gráfico 11.
Pregunta:
¿Su empresa denunció incidentes de fraude de identidad a las autoridades o instituciones?



Encuesta sobre exposición al fraude 2025 de Sumsub, América Latina: Empresas

Cuando se les pregunta por su apoyo a regulaciones más estrictas contra el fraude de identidad, la mayoría (el 57 % de las empresas) se muestra indecisa, lo que pone de manifiesto la fatiga regulatoria y la incertidumbre sobre cómo las nuevas exigencias de cumplimiento podrían afectar a las operaciones diarias.

Solo el 29 % expresa un apoyo claro, mientras que el 14 % se opone por completo a las normas más estrictas, lo que sugiere que las fricciones operativas y los costos de cumplimiento siguen siendo obstáculos importantes para una mayor armonización.

Alison Dorigão Palermo,
Experta en cumplimiento
normativo

"En Brasil y América Latina, ha aumentado considerablemente el fraude de identidad sintética, que combina datos reales y falsos, especialmente en los préstamos digitales y los monederos electrónicos. Los ataques de ingeniería social a través de WhatsApp y SMS son cada vez más habituales, ya que aprovechan los comportamientos prioritarios de los dispositivos móviles. Los estafadores se aprovechan de los sistemas de identificación fragmentados (múltiples identificaciones por persona en diferentes estados) lo que complica la verificación. Los organismos reguladores, como el Banco Central do Brasil, están endureciendo las obligaciones de KYC, mientras que la detección de anomalías basada en IA y la puntuación de riesgos en tiempo real están demostrando su eficacia para reducir el fraude sin afectar la experiencia del cliente. El spoofing biométrico y los deepfakes son preocupaciones emergentes que requieren sistemas de verificación avanzados y en varios niveles.

En 2026, el mercado brasileño y latinoamericano de verificación de identidad dependerá cada vez más de la biometría basada en la inteligencia artificial (reconocimiento facial, detección de vida y análisis del comportamiento) para reducir el fraude y acelerar la incorporación de nuevos clientes. Un desafío fundamental en América Latina sigue siendo la ausencia de un sistema de identificación unificado, a diferencia de la UE, donde los documentos estandarizados simplifican la verificación. En Brasil, los ciudadanos pueden tener hasta cinco documentos de identidad diferentes (ese es mi caso, por ejemplo), y si cada estado emitiera los suyos propios, esta cifra podría ascender a 30, lo que complicaría los procesos de KYC y CDD. Las iniciativas de banca abierta e identidad digital serán de ayuda, pero la interoperabilidad regional y la verificación segura y auditable siguen siendo esenciales. Las identificaciones descentralizadas basadas en blockchain pueden ganar terreno como identificaciones verificables y que cumplen con la normativa de privacidad, especialmente para las poblaciones con acceso limitado a servicios bancarios, mientras que los reguladores impulsan el cumplimiento automatizado y supervisado continuamente de \ la normativa FRAML."

Predicciones para el futuro

1 Los encuestados prevén un aumento drástico del fraude por suplantación de identidad, y el **71 % prevé un aumento de los robos** de identidad relacionados con las continuas violaciones de datos.

2 Las tecnologías emergentes son una gran preocupación: **el 57 % espera que los deepfakes y las falsificaciones generadas por IA se conviertan en herramientas fundamentales para los estafadores,** mientras que casi la mitad prevé que se utilicen identidades sintéticas para evadir los controles de KYC y de incorporación.

3 Al mismo tiempo, el endurecimiento de las regulaciones por parte de los gobiernos (57 %) y el refuerzo de la ciberseguridad por parte de las empresas (43 %) demuestran que ambos sectores se están preparando para esta evolución, aunque solo el 29 % cree que los ataques impulsados por la IA o la delincuencia digital organizada serán predominantes, lo que sugiere que se está subestimando la rapidez con la que avanza la innovación en materia de fraude.

Estudios regionales de casos de fraude en detalle

Los siguientes estudios de casos prácticos destacan incidentes de fraude reales que ocurrieron en América Latina y el Caribe en 2025.

1 **Ex presidentes latinoamericanos condenados en importantes casos de corrupción**

En marzo de 2025, se dictaron sentencias históricas contra antiguos jefes de Estado. En Colombia, el expresidente Álvaro Uribe fue condenado por soborno y fraude procesal, convirtiéndose en el primer expresidente colombiano en ser declarado culpable en un juicio. En Perú, Ollanta Humala fue condenado a 15 años de prisión por blanquear más de 3 millones de dólares estadounidenses procedentes de sobornos de Odebrecht. Estas sentencias forman parte de un ajuste de cuentas regional más amplio, en el que otros antiguos líderes de Brasil, Ecuador, El Salvador, Guatemala y Panamá también se enfrentan a condenas o acusaciones por corrupción y fraude a gran escala.

2 **Los fundadores de OmegaPro acusados de una estafa piramidal global con criptomonedas por valor de 650 millones de dólares estadounidenses.**

En julio de 2025, los fiscales estadounidenses hicieron públicas las acusaciones contra los operadores de OmegaPro, una estafa global de inversión con criptomonedas y divisas que defraudó a los inversores en más de 650 millones de dólares. Con la promesa de obtener un rendimiento del 300 % en 16 meses, el plan pagaba a los primeros inversores con los fondos de las nuevas víctimas, mientras que sus fundadores vivían lujosamente e incluso proyectaban su logotipo en el Burj Khalifa de Dubái para parecer legítimos. Descrito por las autoridades como una "traición planificada con precisión", el caso pone de relieve la magnitud internacional del fraude en materia de inversiones y la creciente cooperación transfronteriza para enjuiciar a sus autores.

3 **Los escándalos de fraude del sector público expuestos en toda América Latina**

En mayo de 2025, algunas investigaciones dieron a conocer la importante corrupción dentro de instituciones públicas de América Latina. En Chile, las investigaciones sobre el caso "Fraude de los Carabineros" sacaron a la luz una trama de malversación de fondos llevada a cabo durante años por altos mandos de la policía, en la que se desviaron millones de fondos públicos (un escándalo conocido como "Verde Austral"). En México, el caso Zaragoza sacó a la luz redes de lavado de dinero que usaban empresas fantasma y plataformas de criptomonedas para mover fondos ilícitos a través de bancos y casas de cambio no reguladas. Aunque algunas investigaciones comenzaron antes, los procesos judiciales y las nuevas acusaciones de 2025 demuestran los continuos esfuerzos por combatir la corrupción sistémica en la región.

Cambios normativos que redefinen la protección de la identidad

A medida que las operaciones fraudulentas se vuelven más sofisticadas, los países de América Latina están reforzando sus regulaciones contra el lavado de dinero, la corrupción y las finanzas digitales para aumentar la resiliencia regional. A continuación se presentan algunas de las últimas novedades en América Latina y el Caribe.

Argentina

La Ley 27.739 reforma la ley fundamental contra el lavado de dinero.
En marzo de 2024, Argentina reformó su marco normativo principal contra el lavado de dinero (Ley 25.246) promulgó la Ley 27.739, que elevó el umbral monetario para juzgar los delitos de lavado de dinero a 150 salarios mínimos (SMVM) a fin de compensar la inflación. La ley amplió el alcance de las entidades obligadas para incluir a abogados, contadores, notarios, proveedores de servicios de activos virtuales (VASP) y custodios y eliminó a otras, como las organizaciones sin fines de lucro. También creó un Registro Centralizado de Titulares Finales Beneficiarios e introdujo nuevas definiciones para "activos virtuales", "acto terrorista", "UBO", "enfoque basado en el riesgo" y "transacciones inusuales".

Decreto Presidencial 891/2024 – reducción de las entidades obligadas.
En octubre de 2024, el decreto refinó aún más el alcance de las obligaciones de información al excluir a los agentes de aduanas y a las empresas dedicadas a la compra y venta de vehículos, maquinaria agrícola, embarcaciones, yates y aeronaves.

Resolución de la CNV 1058/2025: registro dedicado a los VASP.
Autorizada por la Ley 27.739, la Comisión Nacional de Valores (CNV) estableció un registro específico para los VASP mediante la Resolución 1058/2025, sometiendo a los proveedores de servicios de activos virtuales (VASP) a una supervisión regulatoria formal.

Resolución 078/2025 de la UIF: nuevos umbrales de información.
En 2025, la Unidad de Inteligencia Financiera elevó los umbrales de información para las transacciones inmobiliarias (750 SMVM) y de vehículos (50 millones de pesos, ajustados semestralmente). También exigía la elaboración de perfiles de clientes para las adquisiciones de vehículos que superaran los 115 millones de pesos anuales y exigía que se informen los depósitos en efectivo o las transacciones en divisas iguales o superiores a 40 SMVM.

Brasil

Apuestas en línea.
Además del marco anterior (Ley n.º 14.790/2023 y Ordenanzas 1.143/2024 y 722/2024), Brasil publicó la Ordenanza 817/2025, que describe 13 proyectos prioritarios para 2025-26 en el marco del SPA/MF, lo que supone una transición de la concesión de licencias a la supervisión continua, la integración de la lucha contra el fraude y el refuerzo de la lucha contra el blanqueo de capitales. El mercado regulado de apuestas en línea se puso en marcha el 1 de enero de 2025, exigiendo a los operadores la implementación de procedimientos KYC con reconocimiento facial, así como la supervisión continua de la actividad de los apostantes. En octubre de 2025, el Ministerio emitió la Ordenanza Nº 2117/2025, por la que se puso en marcha el sistema SIGPA en colaboración con SERPRO, con el objetivo de verificar si las personas tienen prohibido apostar debido a su condición de beneficiarias de programas de asistencia social.

Resolución Nº 475/2025 del Banco Central: Registro de restricciones voluntarias.
Emitida en mayo de 2025 y vigente desde diciembre de 2025, esta resolución creó un registro en el que las personas pueden solicitar voluntariamente que se les restrinja la posibilidad de celebrar nuevos contratos financieros. Las instituciones financieras deben consultar el registro antes de abrir cuentas o añadir nuevos titulares, reforzando así la prevención del fraude y el cumplimiento de las normas KYC.

Resolución del Banco Central Nº 498/2025: Medidas de seguridad para Pix

Tras una serie de fallos de seguridad en la plataforma Pix, el Banco Central emitió la Resolución Nº 498 en septiembre de 2025. La medida introdujo límites a las transacciones electrónicas de fondos y a las transacciones Pix realizadas por instituciones de pago no autorizadas y aquellas que utilizan proveedores de servicios informáticos para conectarse al sistema financiero. Los proveedores de TI también deben tener un capital mínimo de 15 millones, implementar controles internos y cumplir con las normas obligatorias de ciberseguridad.

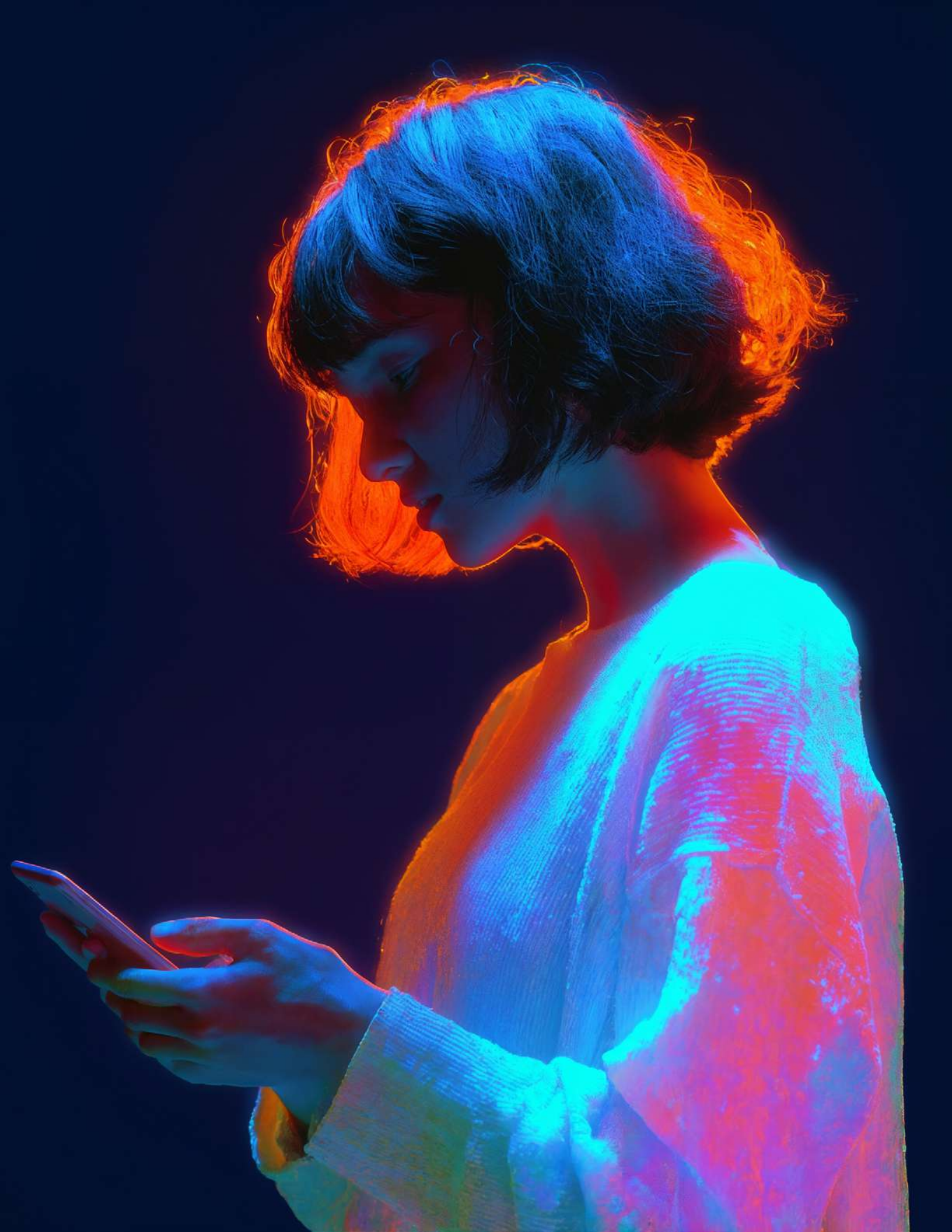
México

Enmiendas a la CNBV para prevenir el fraude.

En junio de 2024, la Comisión Nacional Bancaria y de Valores (CNBV) introdujo nuevas obligaciones en las "Disposiciones generales aplicables a las instituciones de crédito" para mejorar la prevención del fraude y la seguridad de los usuarios. Una medida clave fue la creación del "Plan de gestión para la prevención del fraude", que exige a las instituciones abordar el robo de identidad, las violaciones de datos y el fraude electrónico. La reforma también introdujo el concepto de "importe transaccional del usuario", un umbral —establecido por los usuarios o estimado por las instituciones— para supervisar las transacciones inusuales o potencialmente fraudulentas en los canales de banca en línea y móvil.

AML/CFT reformas a LFPIORPI.

En julio de 2025, México promulgó una importante reforma a la Ley Federal para la Prevención e Identificación de Operaciones con Recursos Ilícitos (LFPIORPI). Las actualizaciones clave incluyen definiciones formales de personas políticamente expuestas (PEP), beneficiarios efectivos y representantes de cumplimiento; la clasificación de los desarrollos inmobiliarias como actividad vulnerable; la supervisión, auditorías y revisiones automatizadas obligatorias para las entidades que realizan actividades vulnerables; y la revisión de los umbrales de notificación para tarjetas prepago, notarios, corredores y activos virtuales.



Anastasia Shvechkova,
Directora de ventas para
América de Sumsub

"América Latina está pasando más rápido que cualquier otra región de las estafas escandalosas y poco calificadas al fraude sofisticado impulsado por la inteligencia artificial. Nuestros datos de 2025 lo muestran claramente: el fraude relacionado con inconsistencias entre la selfie de un usuario y la imagen de su documento de identidad predomina (esa categoría casi se triplicó), porque los deepfakes ahora entran en lo que antes eran simples casos de discrepancia. Los datos sintéticos también están aumentando, con un fuerte crecimiento de los datos personales falsos, ya que los delincuentes crean identidades digitales completas en lugar de robarlas.

Los patrones nacionales cuentan la misma historia de polarización. México redujo el fraude en general, pero los deepfakes se dispararon, lo que demuestra que el volumen puede disminuir mientras que la sofisticación aumenta. Colombia, República Dominicana, Honduras, Ecuador y Chile tuvieron un crecimiento rápido, ya que las carteras móviles y el comercio electrónico superaron al KYC constante, lo que los convirtió en objetivos principales para las redes internacionales. Mientras tanto, incluso en los lugares donde el fraude disminuyó, como en Argentina, Venezuela, Suriname, seguimos observando un crecimiento de los deepfakes de tres y cuatro dígitos. Brasil sigue siendo el mercado más grande e influyente de la región, con casi el 39 % de todos los deepfakes detectados en América Latina. Esto es la Evolución de la sofisticación en acción en América Latina.

La señal operativa es igual de importante: los intentos basados en plantillas y de elusión de la verificación de vida están aumentando, y muchas empresas siguen dependiendo de las revisiones manuales incluso cuando adoptan modelos híbridos. El camino a seguir no es generar más fricciones, sino aplicar capas más inteligentes (lógica documental, actividad multimodal, telemetría de dispositivos y análisis de comportamiento), además de compartir información regional para que una falsificación detectada en un mercado no pueda reaparecer en otro. Si alineamos esas piezas, América Latina puede convertir el fraude industrializado en defensa industrializada."

Prevención de

Cómo debemos responder

Fraude

Cómo diseñar una estrategia de prevención de fraude ganadora

El fraude en 2026 ha entrado en la era de la evolución de la sofisticación. Aunque es posible que el porcentaje mundial de intentos de fraude esté disminuyendo, cada ataque exitoso está más calculado, es más dañino y es más difícil de detectar. Los deepfakes, las identidades sintéticas y los abusos cuidadosamente orquestados tras el proceso KYC están sustituyendo a las burdas falsificaciones de documentos y las estafas de copiar y pegar.

La gran mayoría de los usuarios finales (aproximadamente el 89 %) prefiere los servicios en línea que implementan medidas estrictas de verificación y antifraude.

Encuesta sobre exposición al fraude de Sumsub 2025: Consumidores

Para las empresas, esto significa que hay mucho más en juego: cada caso que se pase por alto puede provocar mayores pérdidas económicas, daños a la reputación y un mayor escrutinio regulatorio.

Para prosperar en este entorno, las estrategias de prevención del fraude deben evolucionar. Una estrategia "ganadora" no se basa en un único control o solución rápida. Se basa en defensas por niveles, impulsadas por la inteligencia, que se adaptan tan rápido como innovan los estafadores.

¿Qué hace efectiva una estrategia de prevención de fraude?

Verificación por niveles

Una sola comprobación ya no resulta efectiva. Combine la verificación de documentos, la biometría, la huella digital del dispositivo y las señales de comportamiento en diferentes puntos de contacto. Los usuarios genuinos pasan sin problemas, mientras que los estafadores se encuentran con múltiples barreras adaptativas.

Detección de fraudes con IA

El aprendizaje automático elimina el ruido de los datos de gran volumen. Utilice la inteligencia artificial para minimizar los falsos positivos, identificar patrones sospechosos y analizar anomalías en todas las regiones y sectores en tiempo real. El objetivo: decisiones más rápidas y precisas que se adapten a las necesidades.

Análisis conductual

Las comprobaciones de identidad estáticas se detienen en el momento de la incorporación, pero el fraude no. Supervise las señales de comportamiento, como la cadencia de escritura, el flujo de navegación o los patrones de transacción inusuales, para identificar los fraudes que eluden las defensas tradicionales.

Intercambio global de inteligencia

El fraude no tiene fronteras. Proteja su ecosistema aprovechando los datos del mercado, las listas de vigilancia compartidas y las redes de inteligencia para mejorar su seguridad. La capacidad de aprender de los ataques perpetrados en otros lugares significa detectar las amenazas antes de que golpeen su plataforma.

Andrew Novoselsky,
CPO de Sumsub

"Estamos viendo al auge de lo que denominamos el 'banco de trabajo de cumplimiento normativo unificado', un entorno único en el que convergen la gestión de casos, la evaluación de riesgos y la detección de fraudes.

Esto no es solamente una evolución técnica sino operativa. Los reguladores están demandando transparencia y los clientes están demandando confianza. El cumplimiento de la normativa y la prevención del fraude ya no pueden operar en forma aislada. En 2026, los responsables del cumplimiento normativo necesitarán conjuntos de herramientas nativas de IA para lograr ambos objetivos."

¿Está preparado para 2026?

Lista de verificación para la preparación contra el fraude

Para empresas

Evalúe su organización en estos seis ámbitos fundamentales. Sea honesto en su puntuación para identificar los puntos ciegos antes de que lo hagan los estafadores.

Gobiernos y estrategias

- [ ] Política de prevención del fraude revisada y actualizada en los últimos 12 meses
- [ ] La necesidad de evitar los riesgos de fraude está definida, documentada y aprobada por la dirección
- [ ] Roles y responsabilidades claros asignados para la prevención del fraude en todos los equipos
- [ ] Evaluación anual del riesgo de fraude realizada y medidas adoptadas
- [ ] Revisión independiente de la resistencia al fraude realizada en los últimos 12-18 meses

Verificación por niveles y KYC

- Comprobaciones en varios niveles (Identificación, biometría, dispositivos, conducta) integrados desde la incorporación
- Verificación de la titularidad real y autenticidad de la identidad para todas las cuentas
- Programas de supervisión y reverificación continuas están establecidos
- Se aplican controles reforzados para usuarios o regiones de alto riesgo
- La identificación de PEP, las sanciones y la detección de medios adversos se realizan de forma automatizada y continua

Monitoreo de transacciones y comportamiento

- El sistema de supervisión de transacciones está operativo y se examina periódicamente
- Modelos de IA implementados para detectar anomalías en tiempo real
- Análisis del comportamiento (por ejemplo, pulsaciones de teclas, flujo de sesiones) implementados para flujos de alto riesgo
- Alertas clasificadas, investigadas y documentadas con resultados claros
- Procedimientos de escalamiento y notificación están claramente definidos

Respuesta e investigación de incidentes

- [ ] Compendio documentado de incidentes de fraude con rutas de escalamiento claras
- [ ] Todas las investigaciones se registran en un sistema de administración central de casos
- [ ] Tiempo medio de investigación comparado y revisado
- [ ] Las lecciones aprendidas de incidentes anteriores se documentan y se divulgan a los equipos
- [ ] Procesos de notificación a la UIF y al regulador probados y validados

Entrenamiento y conciencia

- [ ] Personal de todas las funciones (atención al público, fraude, cumplimiento normativo, productos) es entrenado anualmente
- [ ] El entrenamiento incluye la evolución de amenazas como las deepfakes y las estafas con IA
- [ ] Los nuevos empleados completan la formación inicial sobre concienciación contra el fraude en el plazo de 30 días
- [ ] Las actualizaciones se publican cuando hay nuevos vectores de fraude
- [ ] Se realizan simulacros de fraude para comprobar la preparación

Supervisión de proveedores y tecnología	☐ Las herramientas de fraude de terceros se prueban periódicamente para comprobar el desempeño y la adaptabilidad
	☐ Las responsabilidades de los proveedores en materia de prevención del fraude están definidas claramente en contratos
	☐ Los servicios externalizados (por ejemplo, verificación, supervisión) se auditan en forma independiente
	☐ Integración de datos entre fraude, cumplimiento y sistemas de productos verificados
	☐ Hoja de ruta tecnológica alineada con los objetivos de prevención del fraude (IA, biometría, cadenas de bloques)

Evaluación de su preparación

Anote 1 punto por cada pregunta que responda "Sí". Calcule el total para conocer su exposición actual y nivel de madurez.

28–32	Gran capacidad de recuperación. Mantenerse, probar regularmente y continuar optimizando.
23–27	Base sólida. Abordar las deficiencias identificadas antes de que se conviertan en vulnerabilidades.
18–22	En riesgo. Los estafadores podrían aprovechar las debilidades, así que priorice las soluciones inmediatas.
<18	Alta exposición. Actúe en forma urgente para actualizar las herramientas, la dirección y los procesos.

Lista de verificación para la preparación contra el fraude

Para consumidores

Complete esta autoevaluación para saber si está preparado para hacer frente a la nueva ola de sofisticados fraudes impulsados por la inteligencia artificial, o si está dejando sus datos, su identidad y sus finanzas en una situación vulnerable.

Concienciación y mentalidad

- [ ] Manténgase alerta ante los nuevos tipos de estafas (por ejemplo, deepfakes, estafas de inversión o de entrega).
- [ ] Lea regularmente actualizaciones de fuentes fiables, como su banco, su proveedor de telecomunicaciones o la autoridad nacional contra el fraude.
- [ ] Piense dos veces antes de compartir su información personal en internet o hacer clic en enlaces desconocidos.
- [ ] Considere las ofertas "demasiado buenas para ser verdad" como señales de alerta, no como oportunidades.

Protección de identidad y cuentas

- Use contraseñas únicas y seguras para todas las cuentas importantes.
- Habilite la autenticación de dos factores (2FA) o las claves de acceso siempre que sea posible.
- Revise su configuración de privacidad en las redes sociales y limite lo que publica.
- Sepa cómo congelar o bloquear su cuenta si le roban su documento de identidad o su teléfono.
- No debe compartir información personal ni contraseñas con nadie.

Seguridad de dispositivos y redes

- Su teléfono, computadora portátil y aplicaciones están configuradas para actualizarse en forma automática.
- Solo debe descargar las aplicaciones de tiendas oficiales.
- Use un antivirus o herramientas de protección integradas y haga un análisis regular en busca de amenazas.
- Evite usar redes públicas de Wi-Fi para transacciones sensibles (o use un VPN si es necesario).
- Haga un respaldo seguro de la información importante para casos de pérdidas o cibersecuestro de datos.

Pagos y transacciones seguros

- Compruebe dos veces las solicitudes de pago, incluso si parecen provenir de alguien que conoce y en quien confía.
- Verifique los sitios web y los vendedores antes de introducir los datos de su tarjeta (busque HTTPS y opiniones fiables).
- Use métodos de pago seguros como tarjetas de crédito o monederos digitales que ofrecen protección para el comprador.
- Controle sus resúmenes de cuenta bancaria y de tarjetas semanalmente para detectar cargos inusuales.
- Sepa cómo informar una transacción sospechosa rápidamente a su banco.

Respuesta a estafas

- Conozca los canales oficiales para denunciar estos casos (por ejemplo, Action Fraud en el Reino Unido, FTC en los Estados Unidos, etc.).
- No responda ni reenvíe correos electrónicos, llamadas o mensajes de texto sospechosos: denúncielos y elimínelos.
- Si ha sido víctima de una estafa, actúe rápidamente: póngase en contacto con su banco, cambie sus contraseñas y avise a las plataformas correspondientes.
- Hable abiertamente sobre las estafas con sus familiares y amigos para ayudarles a estar alerta también.

Alfabetización digital y concienciación sobre la IA

- Entienda que la IA puede crear falsificaciones convincentes: voces, imágenes e identidades.
- Cuestione las videollamadas inesperadas, las notas de voz o los mensajes que lo presionan para que actúes rápidamente.
- Verifique las identidades a través de canales secundarios (llame a la persona o confirme directamente).
- Manténgase informado sobre las nuevas tácticas de fraude impulsadas por la inteligencia artificial a partir de fuentes de seguridad fiables.

Evaluación de su preparación

Anote 1 punto por cada pregunta que responda "Sí". Calcule el total para conocer su exposición actual y nivel de madurez.

26-30	Gran capacidad de recuperación. Tiene conocimientos digitales y es proactivo. Manténgase al tanto de las nuevas tendencias en estafas.
20-25	Base sólida. Tiene un buen desempeño, pero podría reforzar sus hábitos, especialmente en lo que respecta a las estafas basadas en la inteligencia artificial y la privacidad de los datos.
14-19	En riesgo. Tiene buenas intenciones, pero hay lagunas importantes que lo dejan expuesto. Revise la lista de verificación y actúe ya mismo.
<14	Alta exposición. Tiene las defensas bajas. Aprenda lo básico, actualice sus dispositivos y pida consejos a organizaciones fiables.

Cómo Sumsub puede ayudar

La primera solución auténtica para la prevención del fraude, reforzada por nuestro motor KYC líder en el mercado

La prevención del fraude ya no consiste solo en atrapar a los malos actores, sino en crear sistemas que se adapten más rápido de lo que los estafadores pueden innovar. Ahí es donde entra en juego Sumsub.

1.5B+
de identidades han enriquecido nuestro sistema de prevención del fraude

Como pioneros en el mercado de la comprobación de identidad, hemos verificado más de 1500 millones de identidades en todo el mundo, lo que nos ha proporcionado una visibilidad sin igual de las tendencias de fraude en diversos sectores y regiones. Cada interacción enriquece nuestro sistema con datos únicos sobre patrones de fraude, lo que agudiza nuestra capacidad para distinguir a los usuarios genuinos de las amenazas sofisticadas.

Más de 23 mil
muestras de fraude analizadas diariamente

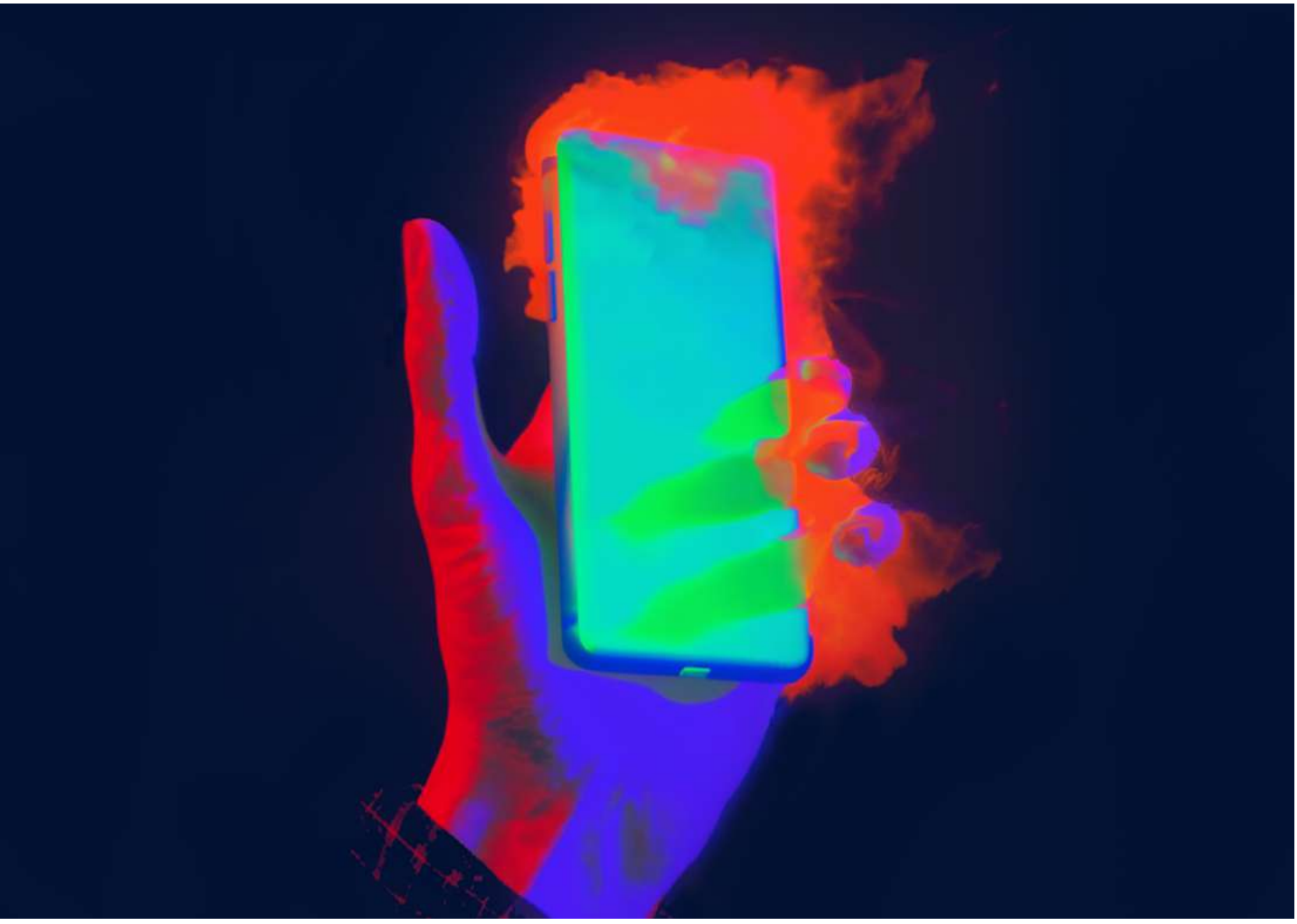
Nuestra plataforma analiza más de 23 000 muestras de fraude al día y aprovecha una base de datos global de más de 2,3 millones de estafadores conocidos, asegurando que nuestras tecnologías de detección evolucionan en tiempo real. ¿Cuál es el resultado? Prevención casi total de intentos de fraude, con muchos menos falsos positivos que ralentizan el negocio.

Más de 2.3 mill de
estafadores conocidos en nuestra base de datos exclusiva

Al combinar nuestro motor KYC con supervisión basada en IA, análisis de comportamiento y detección de redes de fraude, Sumsub ofrece una defensa unificada contra el robo de cuentas, la creación de cuentas múltiples, el fraude en los pagos y los nuevos ataques basados en deepfakes, todo ello a través de una única integración perfecta.

Con Sumsub, las empresas pueden:

1. Bloquear los intentos de fraude antes de que afecten los ingresos o la reputación
2. Automatizar las revisiones manuales para bajar los costos operativos
3. Obtener una visión completa del riesgo del usuario con el manejo de casos centralizado
4. Estar preparadas para las auditorías y cumplir con las normativas internacionales



INTERPOL

"En el último año, INTERPOL ha observado un aumento en el uso de la IA en diversos tipos de fraude. En concreto, los delincuentes utilizan cada vez más videos y audios generados por IA para suplantar la identidad de personas de confianza con el fin de engañar a sus víctimas. El aumento de la disponibilidad de herramientas de deepfake ha democratizado e industrializado el fraude impulsado por la inteligencia artificial, lo que ha llevado a su uso no solo en fraudes sofisticados, sino también en phishing, vishing y clonación de voz. Por lo tanto, la superficie de ataque de las organizaciones y los individuos se ha ampliado para incluir canales que antes eran fiables, como los basados en voz, video e identidad.

De cara al futuro, el fraude basado en la inteligencia artificial será cada vez más sofisticado y accesible. Las herramientas de detección de medios sintéticos están mejorando, pero los sectores público y privado deben colaborar para crear soluciones eficaces. Estas soluciones también requerirán un enfoque integral y holístico, como la detección mediante IA combinada con rigurosos controles de identidad, el uso de canales de autenticación secundarios y una mayor adaptación legal y normativa.

INTERPOL se dedica a ayudar a los países miembros a combatir el fraude impulsado por la inteligencia artificial mediante la colaboración con las fuerzas del orden y el sector privado en el desarrollo de enfoques innovadores."

¿Le gustaría mantener todo el ciclo de vida del usuario libre de fraude?

Agende una demostración →