TransUnion

ACTUALIZACIÓN H1 2026: PRINCIPALES TENDENCIAS DE FRAUDE

LA SUPLANTACIÓN DE IDENTIDAD IMPULSA ATAQUES DE FRAUDE CADA VEZ MÁS COSTOSOS

Más de una cuarta parte de los consumidores afirmaron haber perdido dinero por fraude digital en el último año

Resumen ejecutivo

El fraude ha entrado en una nueva era en la que el principal campo de batalla es la identidad. Ha pasado de ser un gasto operativo a un riesgo estratégico para el negocio, con impacto en los ingresos, el crecimiento y la confianza del consumidor. Y los consumidores sienten esta presión: en 2025, los consumidores de Estados Unidos reportaron 99 mil millones de dólares en pérdidas por fraude digital, con un 16% de personas afectadas. A nivel global, surgió una paradoja para las organizaciones. Aunque las tasas de fraude digital disminuyeron al 3,8%, la gravedad y la sofisticación de los ataques basados en identidad se aceleraron, a medida que los delincuentes trasladaron sus acciones a etapas más tempranas para evitar la detección. Apropiación de cuenta, por ejemplo, aumentaron un 37%, hasta representar el 3,14% de sospecha de fraude digital en 2025.

Este cambio refleja una epidemia más amplia de suplantación de identidad. Los estafadores están explotando las filtraciones de datos, el phishing y la ingeniería social para pasar de ataques directos a compromisos de identidad más difíciles de detectar, identidades sintéticas y estafas basadas en consentimiento, con el fin de evadir los sistemas de detección de las empresas. Mientras tanto, los consumidores están exigiendo más protección que nunca: en todos los mercados, la seguridad de los datos personales es el principal factor que influye en dónde las personas eligen realizar transacciones.

La pregunta fundamental para las organizaciones no es cómo bloquear los ataques, sino si pueden verificar que una persona sea real, legítima y consistente a través de los distintos canales a lo largo del tiempo. Proteger el crecimiento ahora requiere un enfoque unificado de prevención del fraude centrado en la identidad. La resolución moderna de identidad, que integra inteligencia de dispositivos e inteligencia conductual con señales de riesgo impulsadas por inteligencia artificial, fortalece la confianza, reduce la fricción y ayuda a las empresas a mantenerse a la delantera frente a amenazas que evolucionan rápidamente.

PRINCIPALES HALLAZGOS

El fraude basado en la identidad afecta la confianza del consumidor y sus finanzas

26%
de los consumidores afirmaron haber perdido dinero a causa del fraude digital durante el último año.

77%
de los consumidores señalaron que la confianza en la seguridad de sus datos personales es el factor más importante a la hora de elegir con quién realizar transacciones en línea.

El riesgo de fraude persiste en todas las etapas del ciclo de vida del consumidor

8,3%
fue el porcentaje de sospechas de fraude digital en los intentos de creación de cuentas en 2025, lo que la convierte en la etapa de mayor riesgo en todo el ciclo de vida del consumidor.

37%
de incremento en la tasa de sospechas de fraude digital por apropiación de cuentas (ATO) entre 2024 y 2025.

Las identidades comprometidas aumentan el riesgo de sufrir ataques de fraude sofisticados

33%
de los consumidores que declararon haber sido víctimas de fraude digital afirmaron haber sufrido un ataque de phishing, el más frecuente de todos los tipos de estafa.

47%
de incremento en el volumen de filtración de datos en EE. UU. entre 2024 y 2025.

TransUnion

Acerca de la investigación

Este informe tiene como objetivo proporcionar a los responsables de fraude, riesgo, identidad y autenticación información actualizada para evaluar sus tácticas de prevención del fraude en el contexto de las tendencias globales de fraude y ajustar sus estrategias de prevención del fraude con confianza. Combina dos fuentes de información: conocimientos obtenidos de una encuesta global realizada a 12.730 consumidores en 18 países y regiones, y aquellos derivados de miles de millones de transacciones dentro de la red global de inteligencia propia de TransUnion. Cada enfoque aporta una parte distinta de la historia y, en conjunto, ofrecen una visión integral del panorama de amenazas actual, que evoluciona rápidamente.

Interpretación de los datos

Resultados de la encuesta a consumidores

Los hallazgos sobre los consumidores reflejan experiencias con el fraude digital (en línea, correo electrónico, llamadas telefónicas y mensajes de texto), así como actitudes y preferencias relacionadas con las experiencias digitales. Si bien a menudo coinciden con los patrones reales de ataque, siguen siendo interpretaciones personales. Utilícelos como indicadores de sentimiento, confianza, cambios de comportamiento y expectativas, y no como medidas transaccionales precisas.

Métricas de fraude digital

Todos los datos de fraude digital representan sospecha de fraude digital, basado en indicadores de riesgo de dispositivos utilizados por los clientes de TransUnion. Dado que las organizaciones ajustan continuamente sus controles y su apetito de riesgo, las tasas de fraude pueden variar a lo largo del tiempo o entre sectores y regiones. Los cambios pueden reflejar niveles de actividad, volúmenes de transacciones o umbrales de riesgo actualizados. Trate estas cifras como indicadores direccionales de la actividad de fraude digital.

Comparaciones geográficas: El fraude digital por geografía se basa en la ubicación del consumidor durante una transacción, no en el lugar donde opera una empresa. Los niveles regionales de fraude pueden variar según los umbrales de riesgo que las empresas apliquen a determinadas geografías o transacciones. Utilice estas comparaciones como indicadores direccionales, no como medidas absolutas de seguridad regional.

Referencias por sector: Las tasas de fraude digital a nivel sectorial representan el fraude cometido contra empresas de ese sector, no el fraude cometido por o contra consumidores de esa categoría de manera específica. Las diferencias entre sectores suelen reflejar la diversidad en sus tolerancias al riesgo, los recorridos del cliente y las estrategias de prevención del fraude.

TransUnion

Cómo aplicar estos conocimientos

Utilice este informe como una guía estratégica para:

- Comparar su entorno con las tendencias globales, regionales y del sector
- Identificar vulnerabilidades a lo largo del ciclo de vida del consumidor
- Evaluar el nivel de madurez de su ecosistema de fraude en la detección de ataques fraudulentos en evolución
- Alinear a las partes interesadas internas en torno a riesgos compartidos y expectativas del consumidor
- Fundamentar las decisiones de inversión en detección de fraude

Para más detalles, consulte la metodología completa de obtención de datos en la página 42.

Consideraciones sobre datos específicos de Estados Unidos

Filtraciones de datos: Los volúmenes de filtraciones se basan en información divulgada públicamente; la exposición real puede ser mayor. La Puntuación de Riesgo de Filtraciones (Breach Risk Score, BRS) mide qué tan fácilmente las credenciales expuestas pueden habilitar fraude de identidad.

Fraude en centros de atención telefónica: Las tasas de llamadas de alto riesgo están influenciadas por la forma en que cada institución configura sus umbrales de puntuación.

Exposición a identidades sintéticas: Las estimaciones de fraude sintético reflejan únicamente las categorías de crédito medidas por TransUnion; la exposición real puede ser mayor.

Disputas de informes crediticios: Estas métricas dependen de las disputas de informes crediticios en las que los consumidores declararon fraude en su contra y pueden fluctuar según las directrices y el comportamiento del consumidor.

TransUnion

Contenidos

¿Sus clientes son reales?

El futuro del fraude potenciado por la inteligencia artificial

Si la identidad es la nueva primera línea del fraude, la inteligencia artificial es la herramienta definitiva tanto para los estafadores como para quienes combaten el fraude. El fraude no está siendo reinventado por la inteligencia artificial; simplemente reduce la barrera de entrada y lo hace más fácil de escalar y más eficiente. Piénselo: una red de fraude que antes requería que 10 personas coordinaran solicitudes de crédito utilizando información de identidad alterada ahora puede ser ejecutada por una sola persona mediante identidades sintéticas generadas por inteligencia artificial y un agente de inteligencia artificial que completa formularios.

Ya se puede ver hacia dónde va esto. La inteligencia artificial hará que sea más difícil distinguir entre personas reales y estafadores en cada etapa del ciclo de vida del consumidor. Permitirá Apropiación de cuenta sin esfuerzo mediante credenciales de identidad comprometidas y fraude en nuevas cuentas utilizando identidades sintéticas o alteradas, deepfakes y biometría de prueba de vida. También facilitará que los estafadores suplanten a empleados de las organizaciones y falsifiquen sus canales digitales para perpetrar estafas contra los consumidores.

Para equilibrar el terreno, es necesario desarrollar un plan para combatir el fraude basado en la identidad, con la inteligencia artificial en el centro, con el fin de mejorar la detección sin añadir fricción innecesaria. La resolución de identidad es fundamental para respaldar las evaluaciones de riesgo a lo largo del tiempo, en todo el ciclo de vida y a través de los distintos canales. Considere incorporar detección impulsada por inteligencia artificial, habilitada por modelos de aprendizaje automático que aprovechen señales de riesgo diversas, incluida la inteligencia de dispositivos, la información conductual y los conocimientos de consorcio.

Ataque de Inyección
Los procesos de verificación remota de identidad son engañados mediante imágenes y videos alterados con inteligencia artificial que se introducen directamente en las verificaciones de prueba de vida.

Identidades sintéticas
La verificación de identidad es engañada mediante el uso de inteligencia artificial para combinar datos de identidad fabricados y reales, creando personas falsas que parecen legítimas.

Blanqueo de crédito
La puntuación de riesgo crediticio se ve socavada al mantener la solvencia de una identidad comprometida o sintética mediante el proceso de disputa de crédito, con el fin de ocultar cuentas y transacciones fraudulentas.

Deepfakes
Se logra superar la verificación de identidad o la autenticación para suplantar a una persona mediante documentos, rostros, voces o videos manipulados digitalmente con inteligencia artificial generativa.

Falsificación digital
Se inician ataques automatizados utilizando tecnología para asumir la identidad digital de una persona o entidad.

Suplantación
Se explota la confianza para engañar a consumidores o empleados mediante representaciones creíbles de la identidad corporativa o el uso de datos de consumidores comprometidos.

TransUnion

TENDENCIAS GLOBALES DE FRAUDE

Experiencias de fraude del consumidor

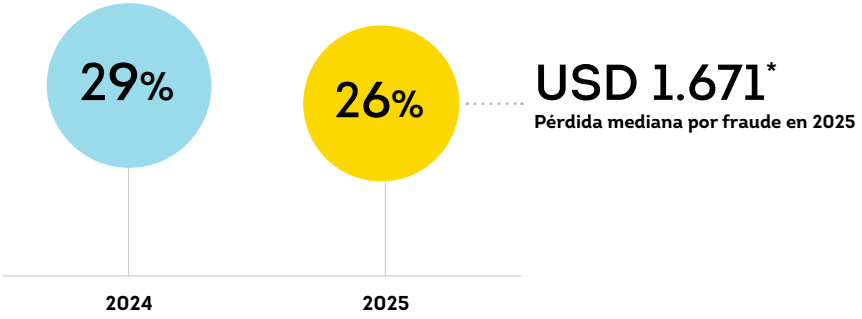
La generación Z es la más susceptible a pérdidas derivadas de esquemas de fraude basados en la confianza

Entre los consumidores encuestados en 18 países y regiones, el 26% afirmó haber perdido dinero a causa del fraude digital durante el último año, con una pérdida mediana de USD$1.671. Los consumidores más jóvenes tuvieron una mayor probabilidad de perder dinero por fraude que la población general; el 39% de la generación Z indicó haber perdido dinero debido al fraude digital en el último año, el porcentaje más alto entre todas las generaciones.

El uso generalizado de plataformas sociales, plataformas de videojuegos y criptomonedas puede desempeñar un papel en la mayor probabilidad de que la generación Z pierda dinero. Entre los tipos de fraude que la generación Z reportó haberles generado pérdidas, el fraude basado en la confianza encabezó la lista, incluidas las estafas de vendedores externos en sitios legítimos de comercio electrónico (27%) y las estafas de mulas de dinero (26%). Esto se compara con un 24% en ambos casos para el total de los consumidores, que también fue el porcentaje más alto. A corta distancia, el 23% de los consumidores en general reportó haber perdido dinero debido a estafas de vishing, es decir, llamadas telefónicas fraudulentas que inducen a los consumidores a revelar información personal, posiblemente como resultado de la suplantación de empresas legítimas u organizaciones gubernamentales.

Pérdidas por fraude reportadas por los consumidores

El porcentaje de consumidores en 18 países y regiones que afirmó haber perdido dinero a causa del fraude digital durante el último año y el monto mediano que reportaron haber perdido

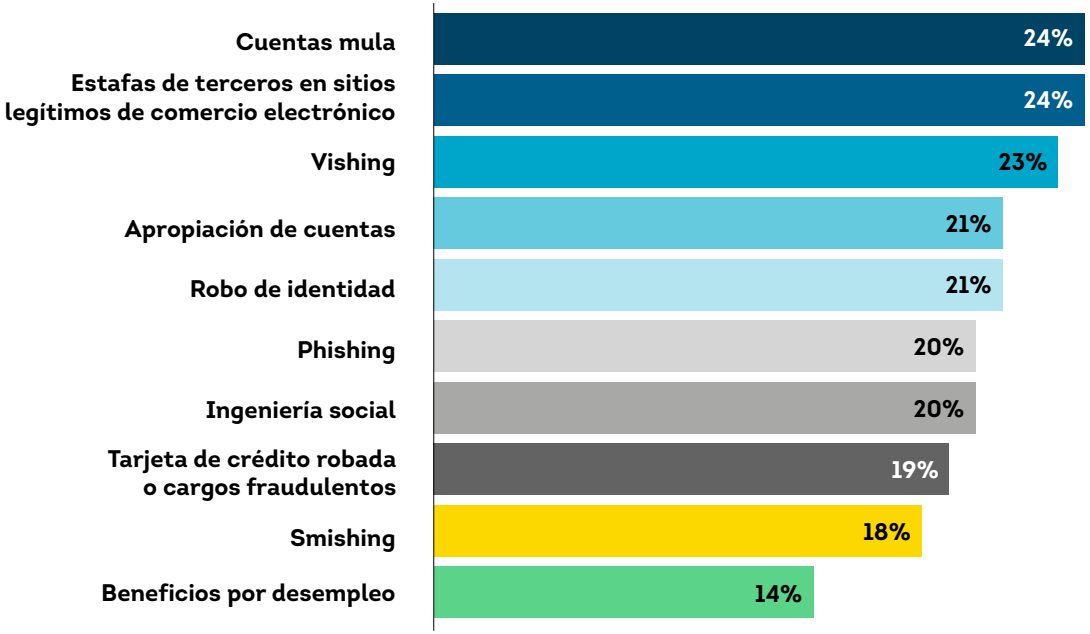


*Conversión a dólares basada en el tipo de cambio de moneda vigente al 29 de diciembre de 2025.

Fuente: Encuesta del consumidor de TransUnion

Esquemas más destacados de pérdida por fraude

Porcentaje de consumidores que reportaron haber perdido dinero a causa de estos esquemas, entre quienes indicaron haber perdido fondos por fraude digital durante el último año



Fuente: Encuesta del consumidor de TransUnion

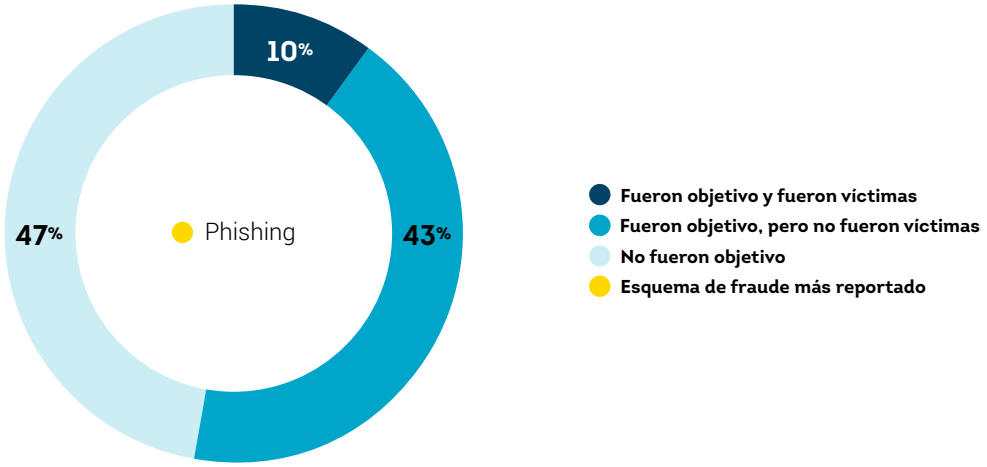
Los esquemas que exponen la identidad dominan el fraude reportado por los consumidores

Más de la mitad de los consumidores (53%), reportó haber sido objetivo de esquemas de fraude digital entre agosto y diciembre de 2025, y el 10% indicó haber sido víctima. Aun así, una proporción significativa (47%) de los encuestados, señaló no haber sido consciente de haber sido objetivo de fraude.

Entre quienes indicaron haber sido objetivo, los principales tipos de fraude reportados por los consumidores estuvieron orientados a exponer la identidad: phishing (33%), smishing (28%) y vishing (27%).

Consumidores objetivo de fraude

Porcentaje de consumidores que indicó que los estafadores los tuvieron como objetivo con intentos de fraude digital entre agosto y diciembre de 2025, y el esquema más frecuente mediante el cual reportaron haber sido atacados.



Fuente: Encuesta del consumidor de TransUnion

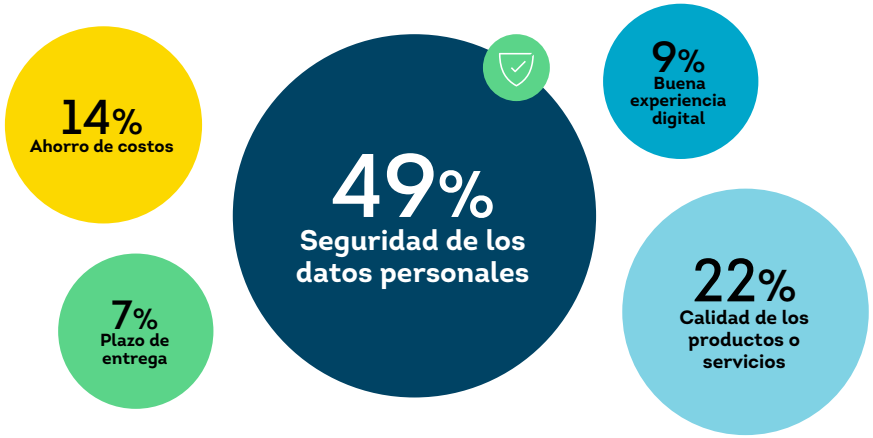
Las transacciones en línea seguras y fluidas impulsan la preferencia de marca de los consumidores

A medida que más consumidores dependen de los servicios digitales de las organizaciones, sus preferencias en materia de seguridad y protección resultan fundamentales para el crecimiento futuro del negocio. Más de un tercio de los consumidores, el 37%, indicó que realizó más de la mitad de sus transacciones minoristas y comerciales en línea, frente al 34% del año anterior, y el 39% afirmó que llevó a cabo más de la mitad de sus actividades de gestión de cuentas en línea, comparado con el 38% del año previo. De mayor relevancia para las marcas, aproximadamente la mitad de los hogares con altos ingresos reportó utilizar canales en línea para el comercio y la gestión de cuentas, con un 55% y un 50%, respectivamente.

Las expectativas de experiencias en línea seguras, protegidas y convenientes por parte de las marcas en las que los consumidores eligen gastar su dinero son elevadas. Más de la mitad de los consumidores, el 56%, afirmó que probablemente cambiaría de empresa para obtener una mejor experiencia digital. Cuando se les preguntó qué experiencias digitales harían que no regresaran a un sitio web, la respuesta principal fueron las preocupaciones por fraude, con un 65%.

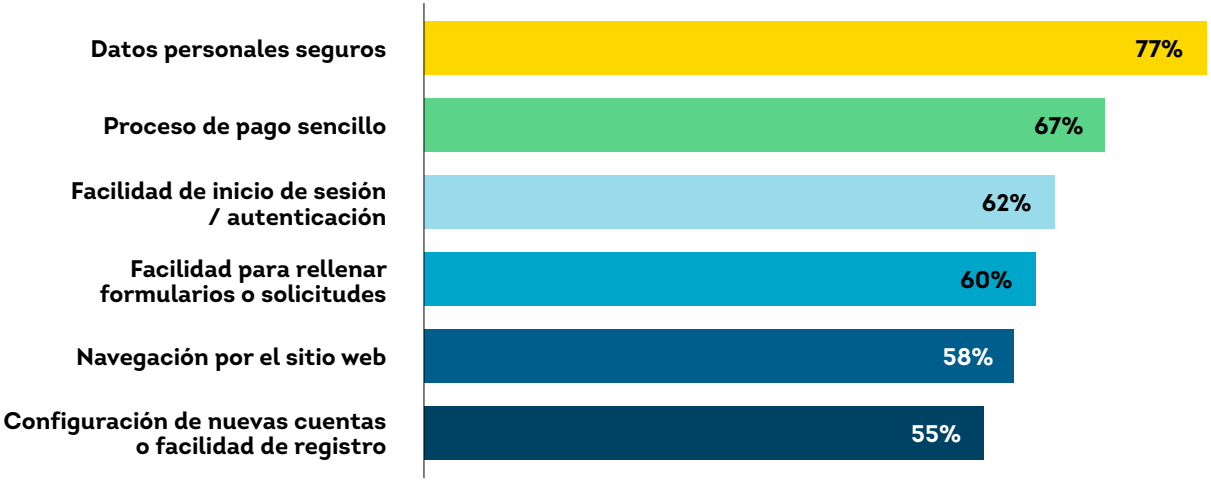
Para atraer a más clientes, las organizaciones necesitan demostrar confianza en lo que respecta a los datos del consumidor. Cerca de la mitad de los consumidores, el 49%, clasificó la seguridad de los datos personales como la expectativa o cualidad más importante en las empresas en línea preferidas. Además, más de tres cuartas partes, el 77%, indicaron que confiar en que sus datos personales no serán comprometidos es muy importante al elegir con quién realizar transacciones en línea. Ambas fueron las respuestas principales para sus respectivas preguntas.

Expectativas o cualidades valoradas en las empresas en línea preferidas
Respuesta principal seleccionada



Fuente: Encuesta del consumidor de TransUnion

Características consideradas importantes al elegir con quién realizar transacciones en línea
Porcentaje que respondió "Muy importante"



Fuente: Encuesta del consumidor de TransUnion

TransUnion

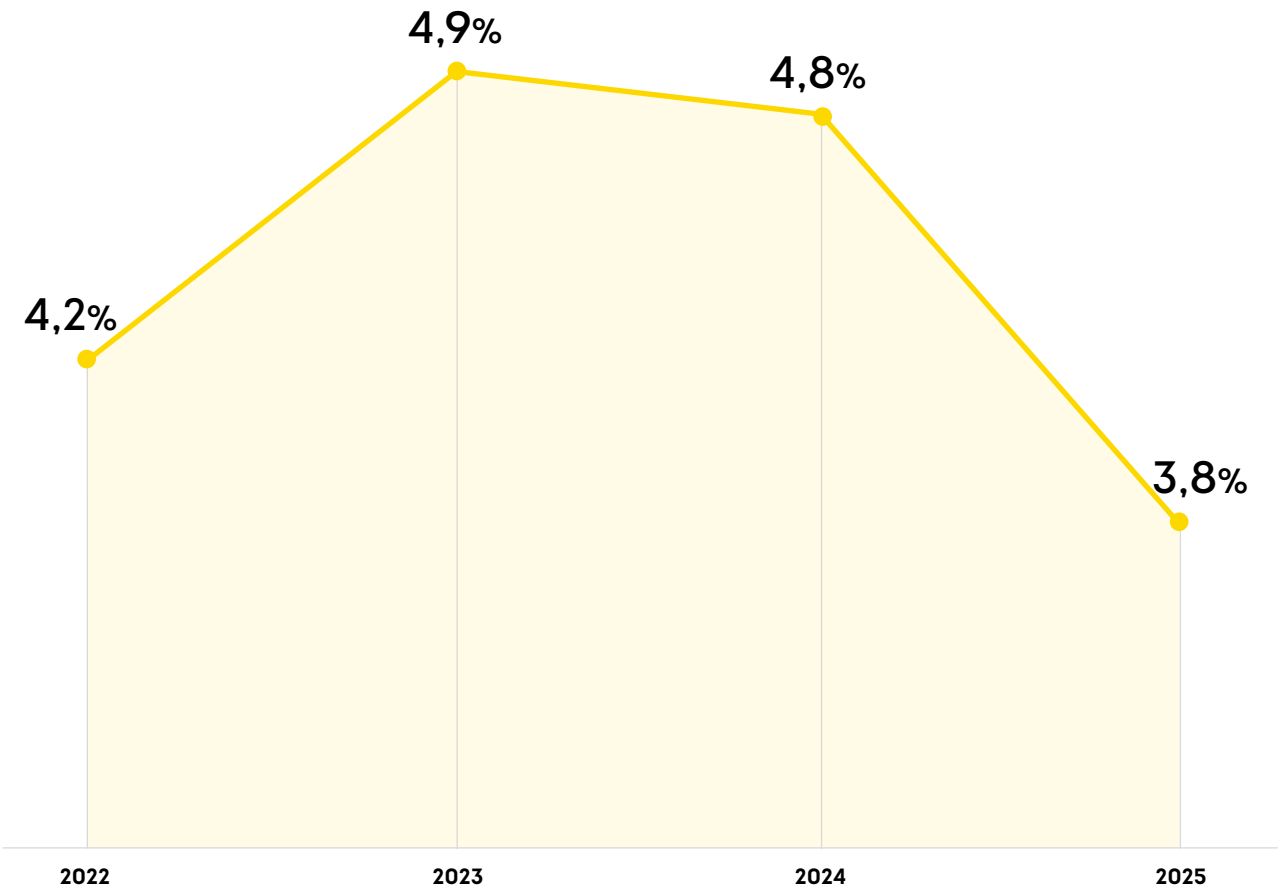
Tendencias de fraude digital

La tasa de sospecha de fraude digital es inferior en términos generales

La tasa de intentos de fraude digital a nivel global entre los clientes de TransUnion fue del 3,8% en 2025, la más baja en nuestro análisis desde 2022. ¿Qué hay detrás de esta tendencia? Es posible que las organizaciones estén reportando un porcentaje menor de fraude debido a un aumento en el volumen de transacciones digitales. Como resultado, sus sistemas de detección pueden estar configurados para identificar riesgos de fraude de mayor magnitud, permitiendo que más transacciones de riesgo medio continúen su curso. Los actores maliciosos también pueden estar socavando las herramientas existentes de detección y autenticación de fraude mediante el uso de credenciales de consumidores sintéticas, robadas o obtenidas mediante ingeniería social, para acceder a cuentas existentes o abrir nuevas. Asimismo, los delincuentes están evitando las herramientas de detección de fraude de las organizaciones al dirigirse con éxito directamente a los consumidores.

Aunque la tasa general disminuyó, las diferencias por región y sector cuentan una historia más matizada. Por ejemplo, a nivel regional, entre los países seleccionados analizados, Asia registró la tasa más alta de sospecha fraude digital con un 5,9%, mientras que Europa presentó la más baja, con un 2,1%.

Tasa de sospecha de fraude digital a nivel global



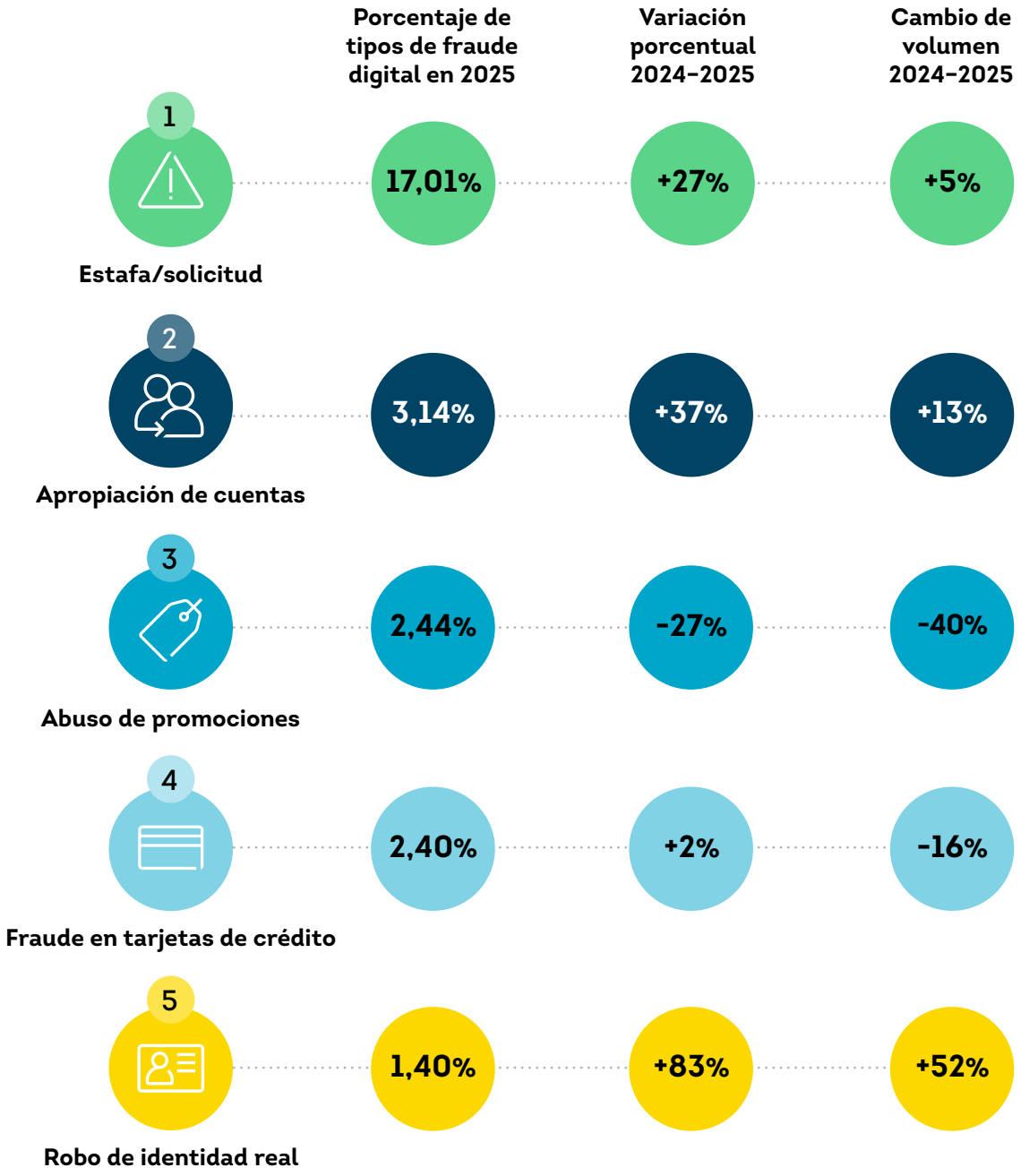
Fuente: Red global de inteligencia de TransUnion

Los ataques de apropiación de cuentas aumentan en frecuencia y volumen

Las cuentas de los consumidores continuaron siendo objeto de ataques, y la apropiación de cuentas representó el 3,14% del fraude digital reportado a TransUnion en 2025, frente al 2,3% en 2024. No solo la tasa creció un 37% en 2025, sino que el volumen de transacciones digitales reportadas como apropiación de cuentas también aumentó un 13%.

Con un 17,01% de toda la sospecha fraude digital reportado a TransUnion en 2025, el fraude de estafas de captación o solicitud, que promueve servicios y productos no autorizados, a menudo con el objetivo de robar credenciales de cuentas, volvió a ser el principal tipo de fraude digital, con un incremento del 27% desde 2024. La apropiación de cuentas y las estafas de captación o solicitud están estrechamente relacionadas, ya que estas estafas suelen derivar directa o indirectamente en intentos de apropiación de cuentas.

Principales tipos de fraude digital y su crecimiento



Fuente: Red global de inteligencia de TransUnion

Las industrias del entretenimiento son las más susceptibles al riesgo de fraude digital

La industria de los videojuegos registró el porcentaje más alto de intentos de fraude digital a nivel global en 2025 entre los sectores analizados, con un 12,8%, lo que representa un aumento del 7% en volumen frente a 2024. En segundo lugar, se ubicaron las comunidades, con un 8,1%. El principal tipo de fraude reportado por los clientes de TransUnion en estos sectores fue la estafa/solicitud.

¿Por qué los videojuegos son un objetivo atractivo para el fraude? No se trata principalmente de un problema relacionado con un adolescente de 14 años frente a una consola. De acuerdo con una encuesta global de la Entertainment Software Association, la edad promedio de los jugadores de videojuegos es de 41 años, y el segmento de mayor tamaño se encuentra entre los 25 y 36 años. Además, más de la mitad de los jugadores indicó que su dispositivo de juego preferido es el teléfono móvil. Con los nombres de usuario ficticios como norma en las plataformas de la economía de la atención, los estafadores encuentran un entorno ideal para interactuar con usuarios desprevenidos.

Los actores maliciosos aprovechan la alta interacción de los sitios orientados al entretenimiento y a lo social, incluidos los videojuegos y las comunidades, para crear perfiles de usuario falsos y dirigirse a los consumidores mediante estafas y solicitudes. En algunos casos, utilizan este método para defraudar directamente a los consumidores, pero con mayor frecuencia lo hacen para obtener información personal que posteriormente les permita perpetrar apropiación de cuentas o fraude de creación de nuevas cuentas.

Intentos de fraude digital por industria

- **Tasa de intentos de fraude en 2025**
- **Principal tipo de fraude en 2025**
- **Variación porcentual en el volumen de sospecha de fraude digital 2024–2025**

Videojuegos

2025
12,8%
Estafa/solicitud

2024-2025
+7%

Comunidades
(citas en línea, foros, etc.)

2025
8,1%
Estafa/solicitud

2024-2025
-36%

Apuestas
(apuestas deportivas en línea, póquer, etc.)

2025
7,7%
Abuso de promociones

2024-2025
+27%

Telecomunicaciones

2025
4,2%
Estafa/solicitud

2024-2025
+66%

Servicios financieros

2025
3,2%
Apropiación de cuentas

2024-2025
-21%

Comercio minorista

2025
2,8%
Apropiación de cuentas

2024-2025
-60%

Gobierno

2025
2,2%
Fraude con tarjeta de crédito

2024-2025
+28%

Logística

2025
1,6%
Fraude en envíos

2024-2025
-55%

Seguros

2025
1,3%
Intermediario fantasma sospechoso

2024-2025
-39%

Viajes y ocio

2025
0,2%
Fraude con tarjeta de crédito

2024-2025
-58%

Fuente: Red global de inteligencia de TransUnion

Fraude digital a lo largo del ciclo de vida del consumidor

La creación de cuentas es la etapa de mayor riesgo del ciclo de vida del consumidor

Los actores maliciosos que utilizan identidades alteradas, robadas, falsas o sintéticas se enfocaron en el proceso digital de creación de nuevas cuentas en 2025, con un 8,3% de todas estas transacciones identificadas como sospecha de fraude digital. Esta fue, por amplio margen, la etapa de mayor riesgo del ciclo de vida del consumidor, seguida del inicio de sesión en cuentas (4,3%).

La creación de cuentas fue la etapa más riesgosa del ciclo de vida del consumidor para la mayoría de las industrias analizadas en 2025, con excepción de servicios financieros, seguros, telecomunicaciones y gobierno, donde las transacciones financieras representaron el mayor riesgo. Las industrias de comunidades y comercio minorista registraron las tasas más altas de sospecha fraude digital durante la creación de cuentas entre los sectores analizados, con un 22,5% y un 22,3%, respectivamente.

Ejemplos de etapas del ciclo de vida del consumidor

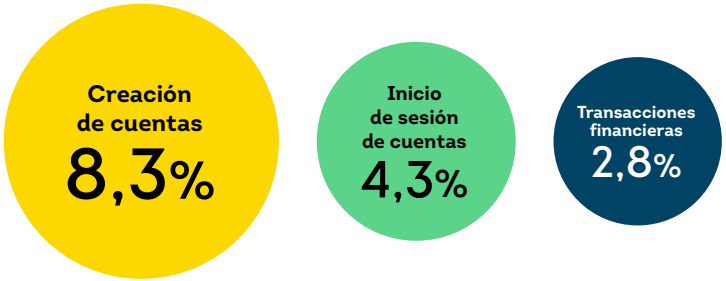
Creación de cuentas: registro de cuentas, procesos de inscripción y originación de préstamos

Inicio de sesión de cuentas: eventos de inicio de sesión y fallos de inicio de sesión

Transacciones financieras: compras, retiros y depósitos

Riesgo de fraude en el ciclo de vida digital del consumidor

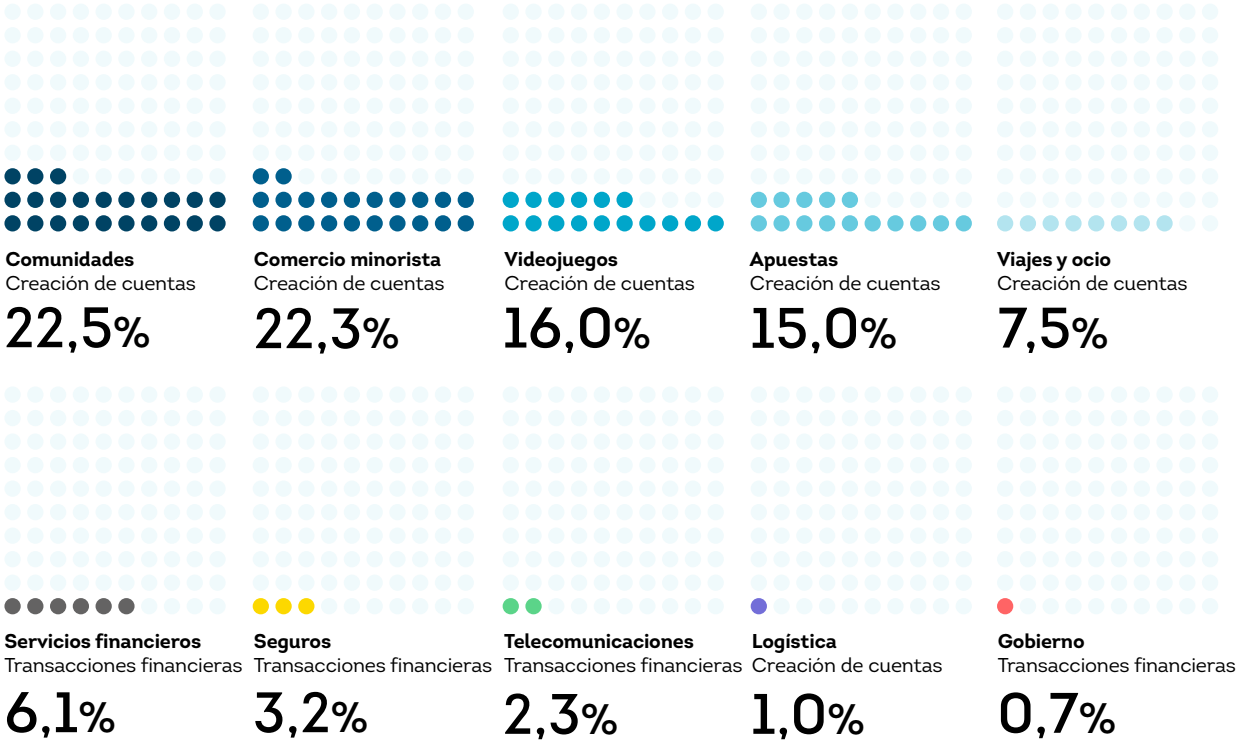
Porcentaje de cada tipo de transacción intentada identificada como sospecha fraude digital en 2025



Fuente: Red global de inteligencia de TransUnion

Riesgo de fraude en el ciclo de vida digital del consumidor por industria

Etapa del ciclo de vida del consumidor con la tasa más alta de sospecha de fraude digital por industria y el porcentaje correspondiente para esa etapa en 2025



Fuente: Red global de inteligencia de TransUnion

TransUnion

AMÉRICA LATINA

Panorama de América Latina

Gracias a las inversiones corporativas para mitigar el fraude, la tasa de intentos de fraude digital en los países de América Latina analizados disminuyó un 46% entre 2024 y 2025. Sin embargo, se siguió observando un alto porcentaje de transacciones digitales sospechosas durante las etapas de creación de cuentas e inicio de sesión. Los consumidores latinoamericanos que indicaron haber perdido dinero durante el último año a causa del fraude digital reportaron una pérdida mediana de USD$1.973. Esto representa un desafío significativo para sus finanzas personales e impacta su capacidad de continuar realizando transacciones con confianza.

El vishing surgió como el esquema de fraude más reportado en América Latina. En este contexto, las estrategias de prevención del fraude deben seguir poniendo énfasis en la responsabilidad del consumidor en la protección de su información personal y credenciales. Esto debe lograrse mediante esfuerzos sostenidos de educación y concientización sobre el fraude dirigidos a los consumidores.

Las empresas deben continuar fortaleciendo e invirtiendo en sus programas de mitigación del fraude para garantizar que los consumidores puedan confiar en que sus datos personales están protegidos y se utilizan de manera adecuada. Este sigue siendo uno de los factores más importantes que los consumidores mencionaron al decidir con qué empresa realizar transacciones en línea.

Los datos de América Latina incluidos en esta sección combinan información propietaria sobre fraude digital de la red global de inteligencia de TransUnion en Brasil, Chile, Colombia, Costa Rica, República Dominicana, El Salvador, Guatemala, Honduras, México, Nicaragua y Puerto Rico, así como una encuesta a consumidores en Brasil, Chile, Colombia, República Dominicana, México y Puerto Rico.

PRINCIPALES HALLAZGOS

Los estafadores se enfocan en el vishing

41%
de los adultos en América Latina indicó haber sido objetivo de fraude digital entre agosto y diciembre de 2025.

27%
de los consumidores latinoamericanos que afirmó haber sido objetivo de fraude señaló el vishing como el esquema utilizado, lo que lo convierte en el esquema de fraude más común en la región.

Los estafadores persisten, presionando principalmente la creación de cuentas

5,7%
de los intentos de creación de cuentas digitales realizados cuando el consumidor se encontraba en América Latina en 2025 fue identificado como sospecha de fraude digital, lo que convierte a esta etapa en la más riesgosa del ciclo de vida del consumidor en la región.

83%
de los consumidores en América Latina indicó que es muy importante tener confianza en que sus datos personales no serán comprometidos al elegir con quién realizar transacciones en línea.

Digitalización continua y estafadores al acecho

37%
de los consumidores en América Latina afirmó que realiza la mayoría de sus actividades de gestión de cuentas en línea, dos puntos porcentuales más que el año anterior.

33%
de los encuestados de la generación Z en América Latina indicó haber perdido dinero a causa del fraude digital durante el último año, lo que los convierte en la generación con el porcentaje más alto, probablemente en correlación con su amplia presencia en línea.

TransUnion

Experiencias de fraude del consumidor

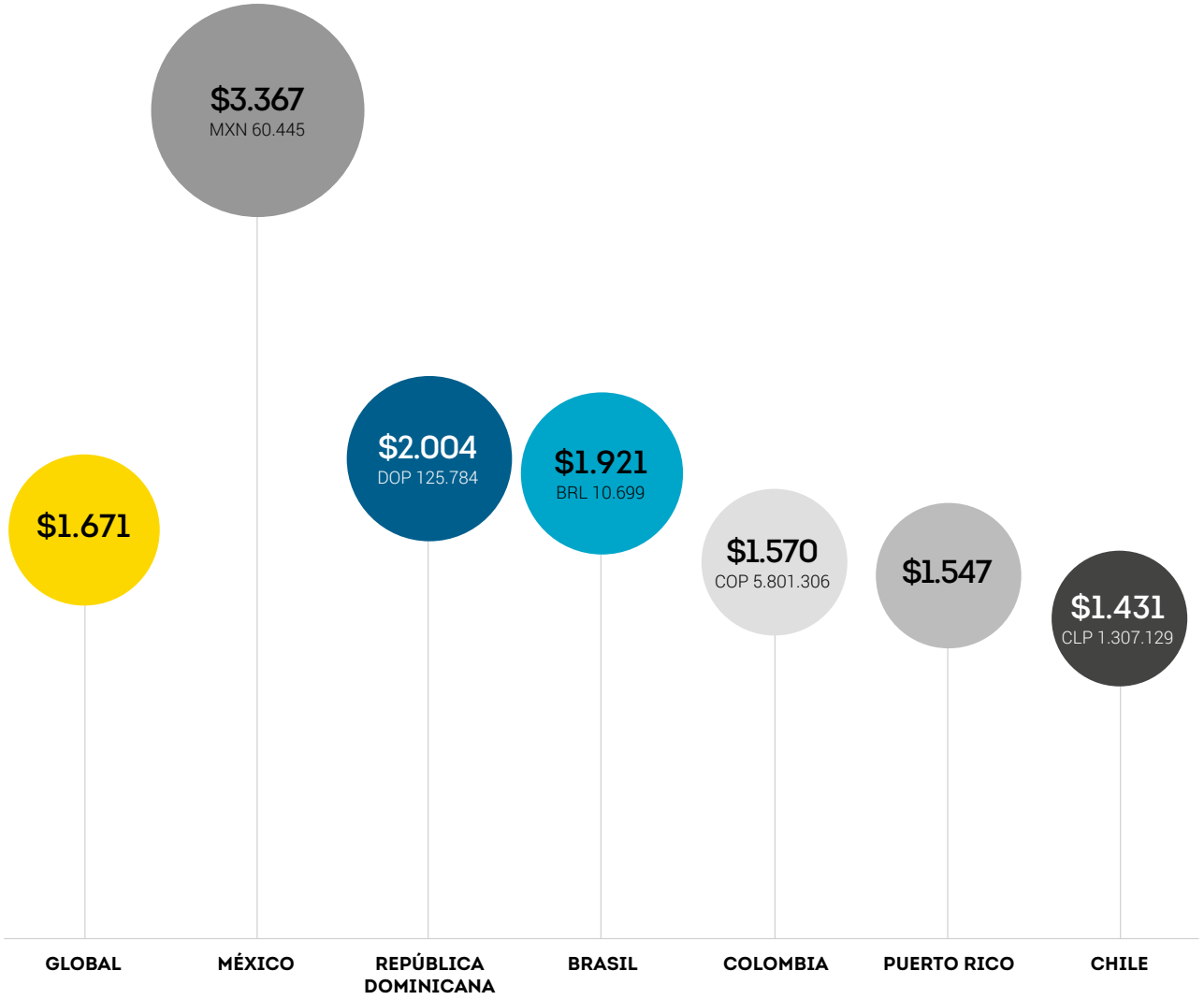
El impacto significativo del fraude en los consumidores

Con una pérdida mediana declarada de USD$1.973 por parte de los consumidores en América Latina que indicaron haber perdido dinero durante el último año debido al fraude digital, la región se sitúa por encima del promedio global y supera a países como Canadá y España. Estos costos tienen un impacto a largo plazo en los consumidores, ya que la recuperación financiera y crediticia suele requerir procesos de remediación extensos y graduales.

El vishing fue el esquema de fraude más reportado por los consumidores latinoamericanos que afirmaron haber perdido dinero durante el último año. Esto contrasta con lo reportado a nivel global, donde las estafas de terceros en sitios legítimos de comercio electrónico y los esquemas de cuentas mula se ubicaron como los más prevalentes. El vishing fue reportado por más de una cuarta parte de los consumidores en Brasil (32%), Chile (29%), República Dominicana (40%), México (37%) y Puerto Rico (42%), cifras significativamente superiores al promedio global del 23%.

Pérdidas por fraude denunciadas por los consumidores

Pérdida mediana por fraude reportada en dólares entre los consumidores que indicaron haber perdido fondos a causa del fraude digital durante el último año

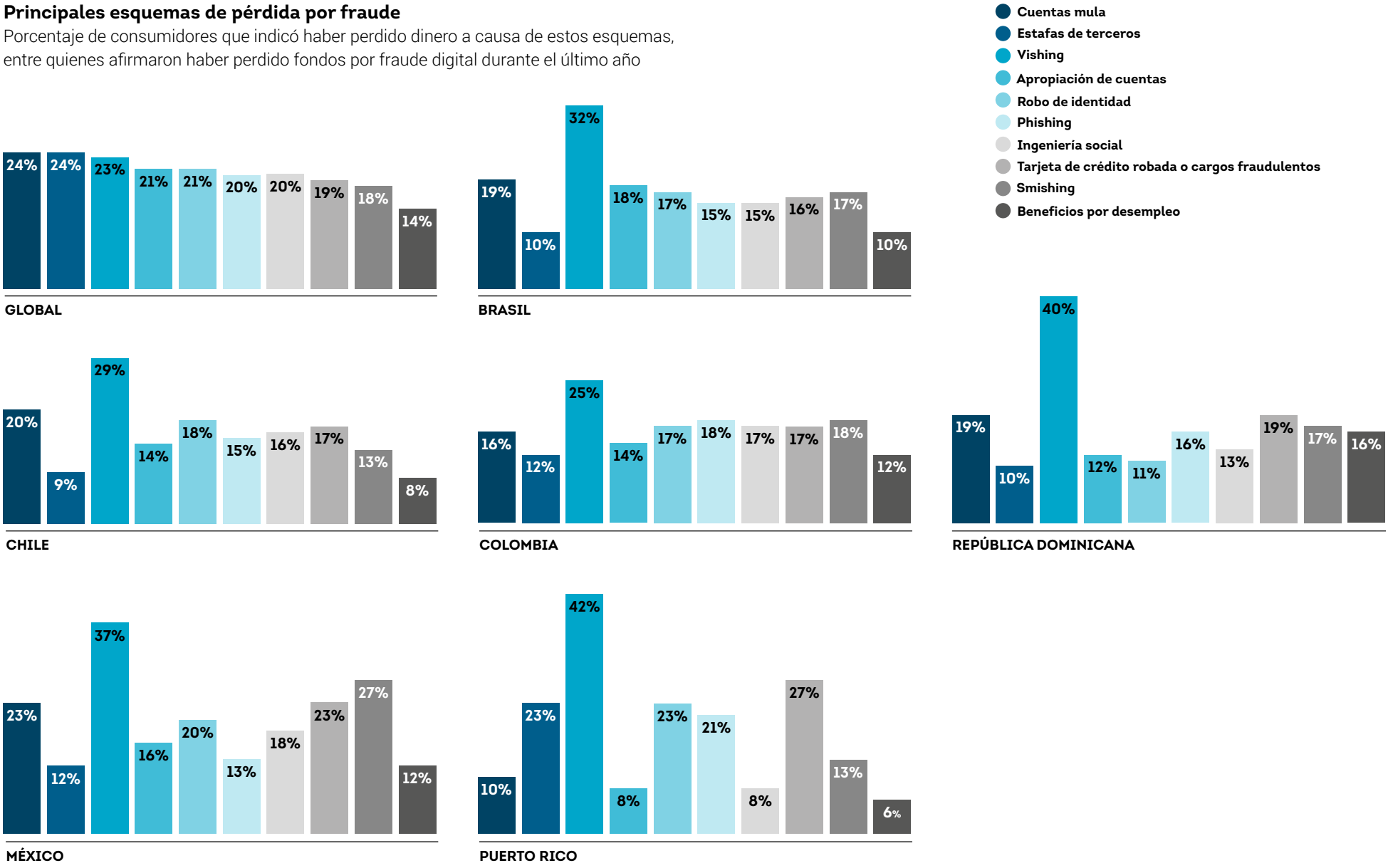


*Conversión a dólares basada en el tipo de cambio de moneda vigente al 29 de diciembre de 2025.
**El valor global corresponde al promedio mediano de los 18 países encuestados.

Fuente: Encuesta del consumidor de TransUnion

Principales esquemas de pérdida por fraude

Porcentaje de consumidores que indicó haber perdido dinero a causa de estos esquemas, entre quienes afirmaron haber perdido fondos por fraude digital durante el último año



Fuente: Encuesta del consumidor de TransUnion

Los estafadores continúan teniendo como objetivo a los consumidores, aunque muchos pueden no ser conscientes de ello

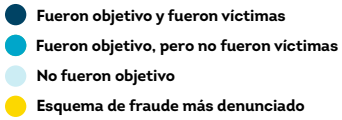
Si bien el 41% de los consumidores encuestados en América Latina indicó haber sido objetivo de un esquema de fraude digital en los últimos tres meses, una cifra inferior a la tasa global del 53%, una proporción significativa de la población puede no reconocer posibles intentos de fraude. Casi seis de cada diez consumidores, el 59%, afirmó no haber sido consciente de haber sido objetivo de fraude.

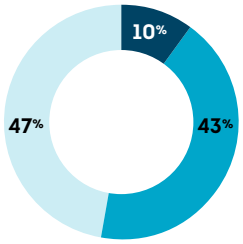
A nivel global, el phishing fue el esquema de fraude más denunciado entre quienes indicaron haber sido objetivo. En contraste, el vishing fue el esquema de fraude más denunciado por los consumidores que afirmaron haber sido objetivo en Brasil, Chile, Colombia y República Dominicana. El uso de tarjetas de crédito robadas o los cargos fraudulentos también tuvo una relevancia significativa en la región, donde los consumidores de México y Puerto Rico lo señalaron como el principal esquema de fraude.

Al considerar en conjunto a los países de América Latina incluidos en la encuesta, el vishing fue el esquema más denunciado. Para hacerle frente, las empresas deben enfocarse en promover mecanismos de protección centrados en el consumidor y en fortalecer la educación y concientización, con el fin de mitigar las vías que conducen a la apropiación de cuentas.

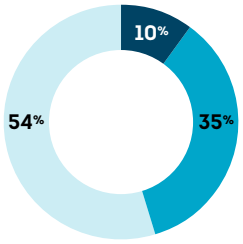
Consumidores objetivo de fraude

Porcentaje de consumidores que indicó que los estafadores los tuvieron como objetivo con intentos de fraude digital entre agosto y diciembre de 2025, y el esquema más frecuente mediante el cual señalaron haber sido atacados

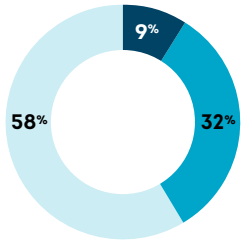




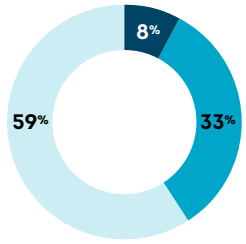
GLOBAL
Phishing



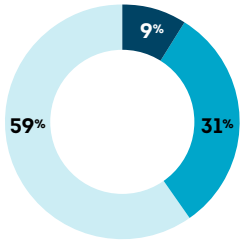
REPÚBLICA DOMINICANA
Vishing



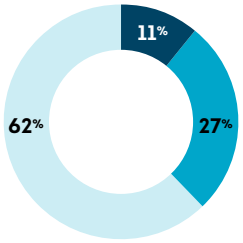
BRASIL
Vishing



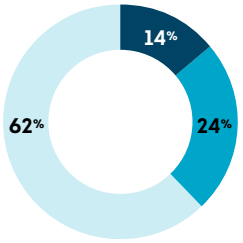
MÉXICO
Tarjeta de crédito robada o cargos fraudulentos



COLOMBIA
Vishing



CHILE
Vishing



PUERTO RICO
Tarjeta de crédito robada o cargos fraudulentos

Fuente: Encuesta del consumidor de TransUnion

La seguridad de los datos personales en línea es la principal expectativa del consumidor

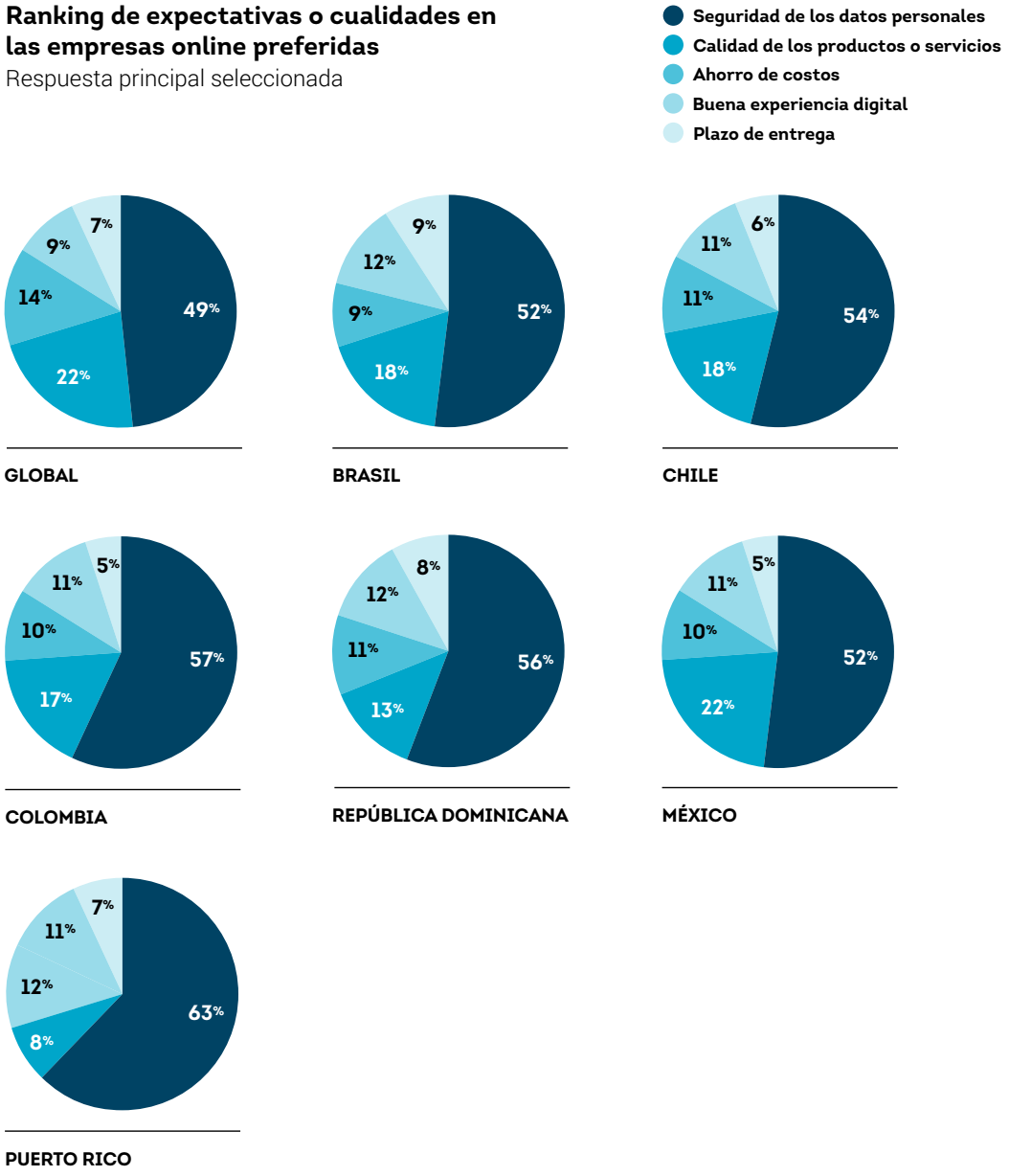
Los consumidores a nivel global tienen claras sus expectativas al realizar transacciones en línea. Cuando se les pidió clasificar las cualidades o expectativas que consideran al decidir con qué empresa en línea hacer negocios, la seguridad de sus datos personales ocupó el primer lugar para el 49%, mientras que la calidad de los productos y servicios fue la principal elección para el 22%.

A pesar de la importancia que se atribuye a los plazos de entrega y a las experiencias digitales, los consumidores en América Latina están alineados con las expectativas globales; la seguridad de los datos personales se mantuvo como la cualidad principal en toda la región, particularmente en mercados como Puerto Rico y Colombia.

Cuando se les preguntó en qué medida consideran importantes ciertas características al elegir con quién realizar transacciones en línea, la confianza en que sus datos personales están protegidos volvió a posicionarse como la principal prioridad en los países de América Latina. Los consumidores en Puerto Rico señalaron que la confianza en que sus datos personales no serán comprometidos es muy importante (93%), el porcentaje más alto entre los países de América Latina, seguido por República Dominicana (86%). Un proceso de pago sencillo se ubicó como el segundo factor más importante para todos los países de América Latina encuestados, en consonancia con lo observado entre los consumidores a nivel global.

Ranking de expectativas o cualidades en las empresas online preferidas

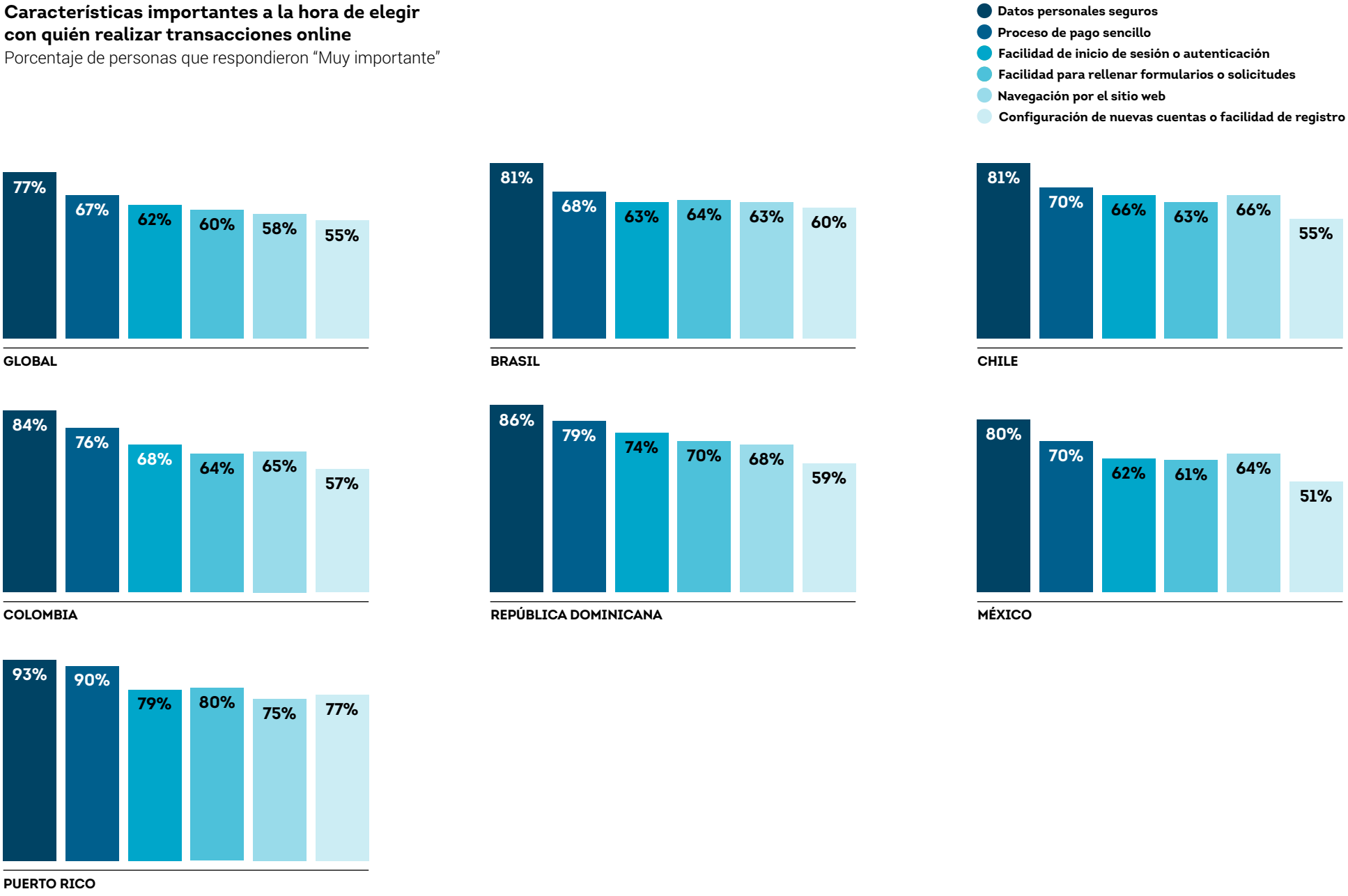
Respuesta principal seleccionada



Fuente: Encuesta del consumidor de TransUnion

Características importantes a la hora de elegir con quién realizar transacciones online

Porcentaje de personas que respondieron "Muy importante"



Fuente: Encuesta del consumidor de TransUnion

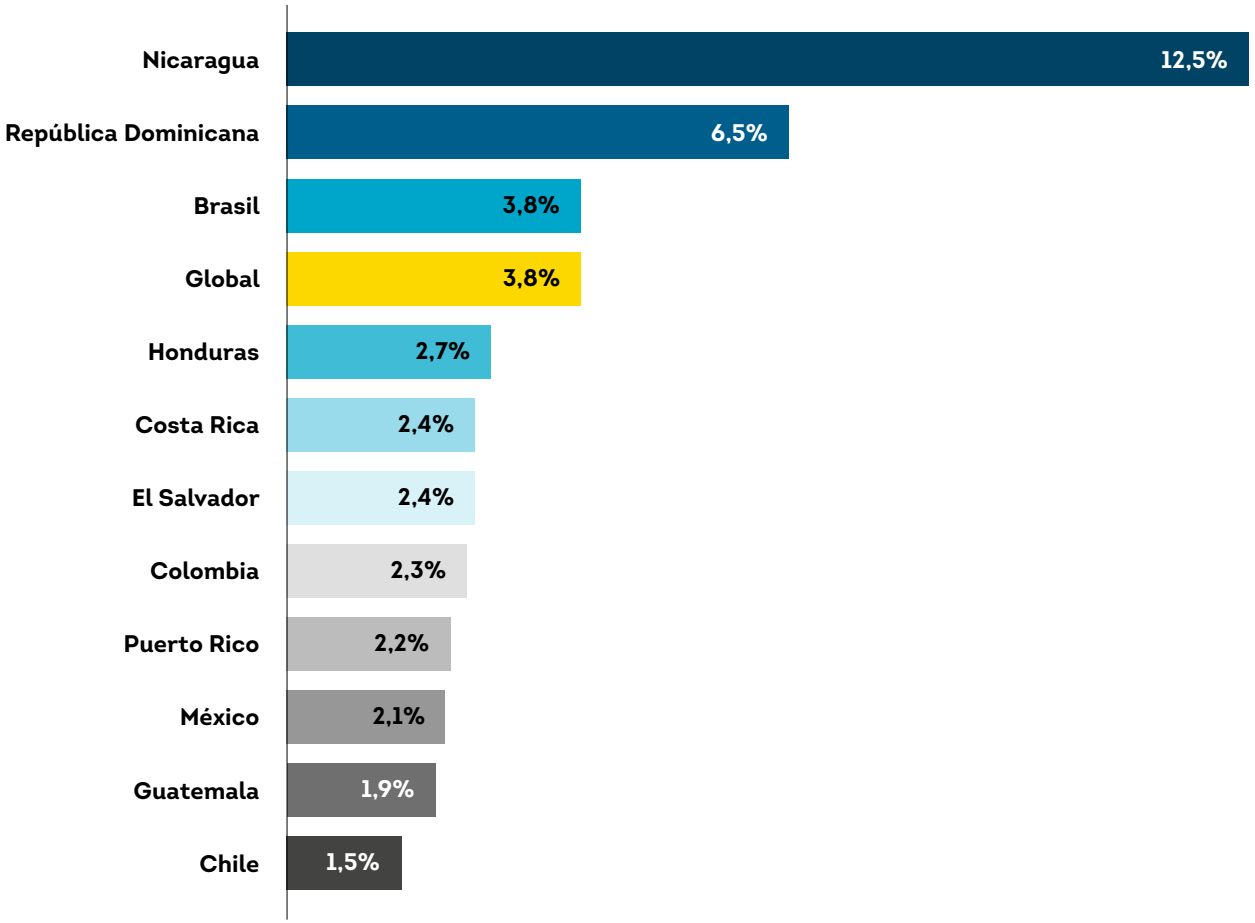
Tendencias de fraude digital

La sospecha de fraude digital se mantiene elevado en mercados clave de América Latina

La tasa global de intentos de fraude digital entre los clientes de TransUnion fue del 3,8% en 2025. Esto refleja la eficacia continua de las estrategias de prevención del fraude en los principales mercados. En los países de América Latina analizados, la tasa promedio se situó en el 2,7%, con variaciones relevantes entre países. Tres mercados, Brasil, República Dominicana y Nicaragua reportaron tasas por encima del promedio regional. Estos niveles elevados sugieren que los estafadores están más activos en estos mercados específicos, ya que las vulnerabilidades en estas ubicaciones podrían ser mayores que en otros países.

Todos los mercados evaluados en América Latina, con excepción de Nicaragua, reportaron una disminución interanual en los intentos de fraude digital, lo que pone de relieve la importancia y la eficacia de los esfuerzos coordinados de mitigación del fraude en estos países.

Tasa de sospecha de fraude digital en 2025



Fuente: Red global de inteligencia de TransUnion

Las industrias de gobierno y logística presentan la tasa más alta de sospecha de fraude digital en la mayoría de los países de América Latina

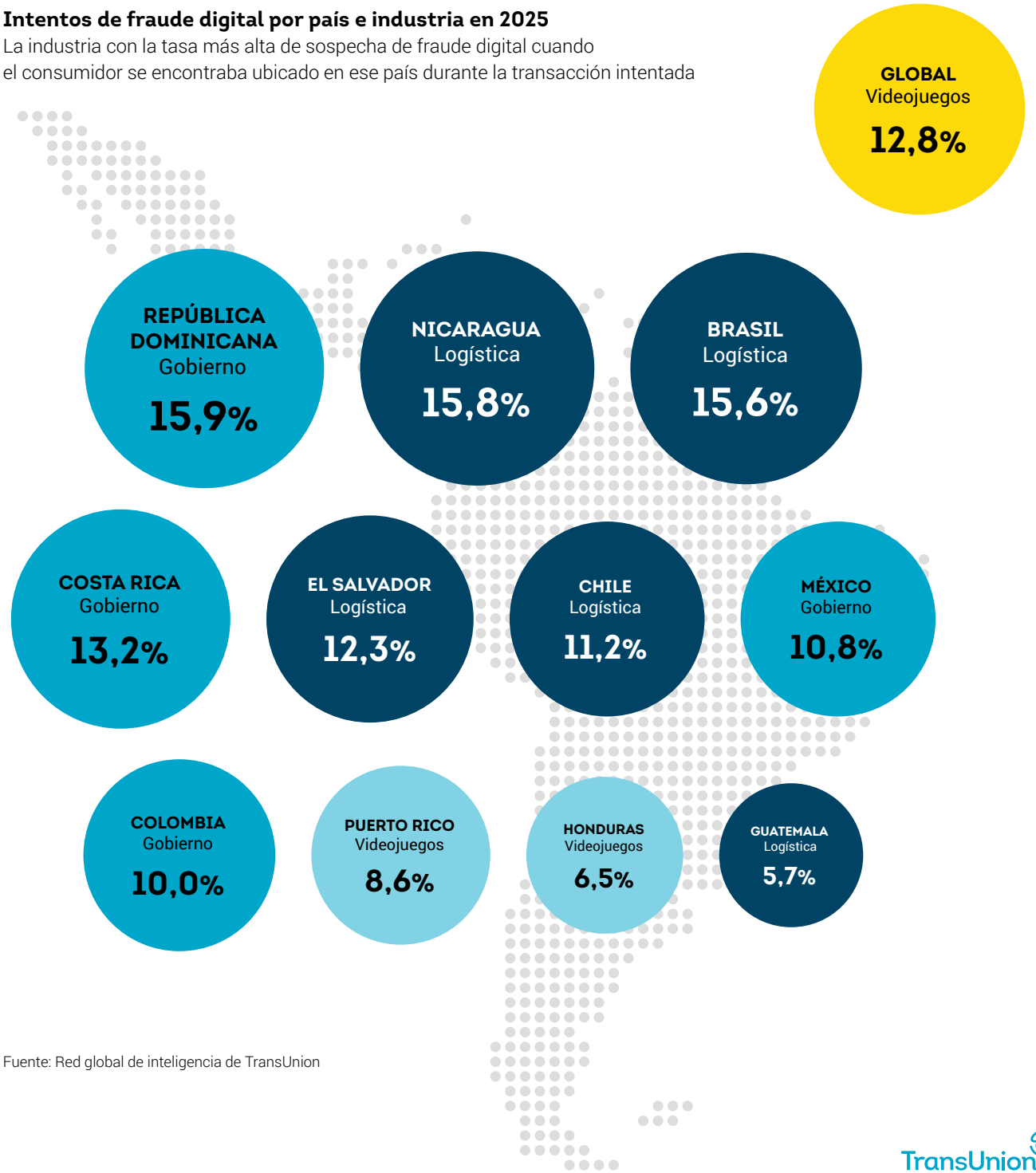
Entre las industrias analizadas a nivel global, el sector de los videojuegos registró el mayor porcentaje de intentos de fraude digital en 2025, con un 12,8%. El volumen de sospecha de fraude digital en este sector creció de forma significativa, un 7% entre 2024 y 2025, lo que subraya la creciente vulnerabilidad del sector frente a actividades fraudulentas.

En América Latina, distintas industrias dentro de mercados específicos mostraron tasas elevadas de fraude. Por ejemplo, en las transacciones intentadas en las que el consumidor se encontraba en Nicaragua, el sector de logística reportó la tasa más alta de sospecha de fraude digital entre todas las industrias analizadas, con un 15,8%.

En casi todos los mercados de la región, los sectores de gobierno y logística se consolidaron como aquellos con las tasas más altas de sospecha de fraude digital. Esta tendencia refleja los esfuerzos continuos de los estafadores por explotar sectores que gestionan datos personales sensibles y otro tipo de información, como direcciones o registros de compras. Estas cifras también ponen de relieve la necesidad de implementar estrategias de prevención del fraude específicas y focalizadas en estos sectores.

Intentos de fraude digital por país e industria en 2025

La industria con la tasa más alta de sospecha de fraude digital cuando el consumidor se encontraba ubicado en ese país durante la transacción intentada



Fuente: Red global de inteligencia de TransUnion

Las identidades de riesgo impactan todas las etapas del ciclo de vida del consumidor, especialmente la creación de cuentas

El porcentaje de intentos de transacciones digitales sospechosas durante la creación de cuentas representó el mayor crecimiento en el riesgo de fraude a lo largo del ciclo de vida digital del consumidor, con un incremento del 18% a nivel global entre 2024 y 2025. El inicio de sesión de cuentas también mostró un riesgo elevado en 2025, con una tasa de sospecha de fraude digital del 4,3%, superior a la tasa global del 3,8% para todos los intentos de transacciones digitales.

En los intentos de transacciones digitales en los que el consumidor se encontraba en los países seleccionados de América Latina, la creación de cuentas surgió como el tipo de transacción más atacado dentro del ciclo de vida digital del consumidor, con una tasa de sospecha de fraude digital del 5,7% en 2025. Nicaragua y la República Dominicana lideraron la región en riesgo de fraude digital durante la creación de cuentas, con tasas del 65,3% y del 15,8%, respectivamente, en 2025. La etapa de inicio de sesión de cuentas en El Salvador y México registró tasas de sospecha de fraude digital similares a las de creación de cuentas el año pasado.

En algunos mercados, como Brasil, el riesgo a lo largo del ciclo de vida se inclinó hacia las transacciones. En los intentos de transacciones digitales en los que el consumidor se encontraba en Brasil, la tasa de sospecha de fraude digital se ubicó por debajo del promedio global tanto en la creación de cuentas (3,7% frente a 8,3%) como en el inicio de sesión (2,6% frente a 4,3%), pero por encima del promedio global en las transacciones financieras (3,2% frente a 2,8%) en 2025.

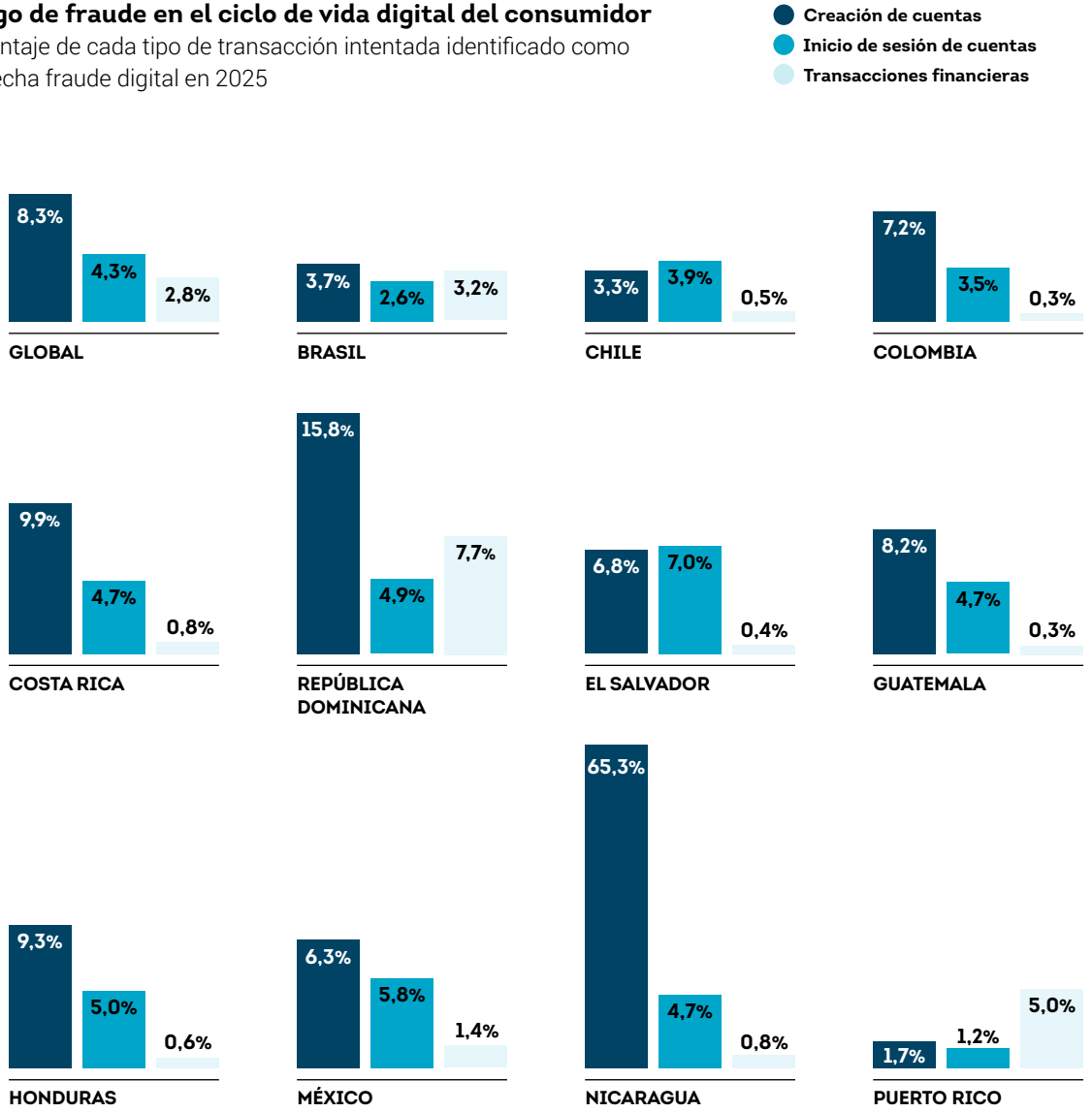
Ejemplos de etapas del ciclo de vida del consumidor

Creación de cuentas: Registro de cuentas, procesos de inscripción y originación de préstamos

Inicio de sesión de cuentas: Eventos de inicio de sesión y fallos de inicio de sesión

Transacciones financieras: compras, retiros y depósitos

Riesgo de fraude en el ciclo de vida digital del consumidor
Porcentaje de cada tipo de transacción intentada identificado como sospecha fraude digital en 2025



Fuente: Red global de inteligencia de TransUnion

NORTE AMÉRICA

Panorama de Estados Unidos

Los esquemas de fraude son cada vez más sofisticados y difíciles de detectar. Lo que empieza a hacerse evidente es la forma en que los delincuentes están trabajando para eludir las defensas. En 2025, los delincuentes parecieron explotar dos estrategias paralelas de fraude digital, ambas basadas en la instrumentalización de información de identidad del consumidor comprometida. En primer lugar, se dirigen a consumidores vulnerables mediante estafas cada vez más creíbles para obtener ganancias inmediatas, evitando por completo las defensas contra el fraude. En segundo lugar, roban información de identidad creíble a través de filtraciones de datos, estafas a consumidores y técnicas de ingeniería social dirigidas a agentes de centros de atención telefónica, con el objetivo de evadir los sistemas de autenticación o engañar a las herramientas de detección de fraude en la creación de nuevas cuentas.

En 2025, estas estrategias derivaron en pérdidas significativas para los consumidores por fraude relacionado con robo de identidad real y apropiación de cuentas. También revelaron una paradoja: una tasa general más baja de fraude digital junto con un aumento en la tasa de apropiación de cuentas, a medida que los estafadores se enfocaron en pagos de alto valor. La alta incidencia de estafa/solicitud reportada dentro de comunidades con credenciales, plataformas de comunidades o videojuegos indica que los actores maliciosos están creando sus propias cuentas. Además, las identidades sintéticas representan un problema significativo para cualquier organización, y en particular para los prestamistas, debido a la instrumentalización del lavado de crédito. Nada de esto será más sencillo en un entorno de fraude digital impulsado por inteligencia artificial, lo que exige un mayor enfoque en desenmascarar el fraude de identidad en todos los canales y en cada etapa del ciclo de vida del consumidor.

PRINCIPALES HALLAZGOS

Las estafas al consumidor generan grandes pérdidas por fraude

USD 2.307

Pérdida mediana denunciada durante el último año entre el 16% de los consumidores en Estados Unidos que indicaron haber perdido fondos por fraude digital en ese período.

29%

De los consumidores en Estados Unidos que afirmaron haber perdido dinero debido a cualquier tipo de fraude digital durante el último año, el 29% señaló robo de identidad real, solo por debajo de tarjetas de crédito robadas o cargos fraudulentos, con un 33%.

Las identidades comprometidas incrementan el riesgo de fraude futuro

78%

De las filtraciones de datos en Estados Unidos expusieron números completos de Seguro Social en 2025, la proporción más alta desde que comenzó la investigación de TransUnion en 2020.

39%

De los consumidores en Estados Unidos que indicaron haber sido objetivo de fraude digital entre agosto y diciembre de 2025 señalaron que el ataque fue una estafa de phishing, el tipo de fraude más denunciado.

El riesgo sofisticado de fraude de identidad se hace más evidente

13%

Aumento en las llamadas de alto riesgo recibidas en los centros de atención telefónica de clientes de TransUnion en Estados Unidos entre 2024 y 2025, incluido un aumento del 41% en las llamadas de alto riesgo provenientes de números móviles.

USD 2.6 billion

En exposición de prestamistas a identidades sintéticas en Estados Unidos para préstamos automotrices, tarjetas de crédito bancarias, tarjetas de crédito de comercios y préstamos personales sin garantía al cierre de 2025.

TransUnion

Experiencias de fraude del consumidor

El fraude basado en la identidad impulsa pérdidas significativas para los consumidores

El fraude al consumidor en Estados Unidos generó pérdidas significativas en 2025 que parecen estar estrechamente relacionadas con filtraciones de datos y estafas al consumidor, las cuales brindan a los delincuentes la identidad necesaria para perpetrar fraude. Casi uno de cada seis consumidores adultos en Estados Unidos, el 16%, indicó haber perdido dinero debido al fraude digital durante el último año, con una pérdida mediana denunciada de USD$ 2.307.

Extrapolado a la población adulta de Estados Unidos, estimada en 268,3 millones a julio de 2025 según la Oficina del Censo de Estados Unidos, esto representa una pérdida estimada de USD$ 99 mil millones por fraude digital en el último año.

Un tercio de los consumidores en Estados Unidos, el 33%, denunció que la causa de su pérdida fueron tarjetas de crédito robadas o cargos fraudulentos, seguido por robo de identidad real con el 29% y apropiación de cuentas con el 27%.

Pérdidas por fraude denunciadas por los consumidores

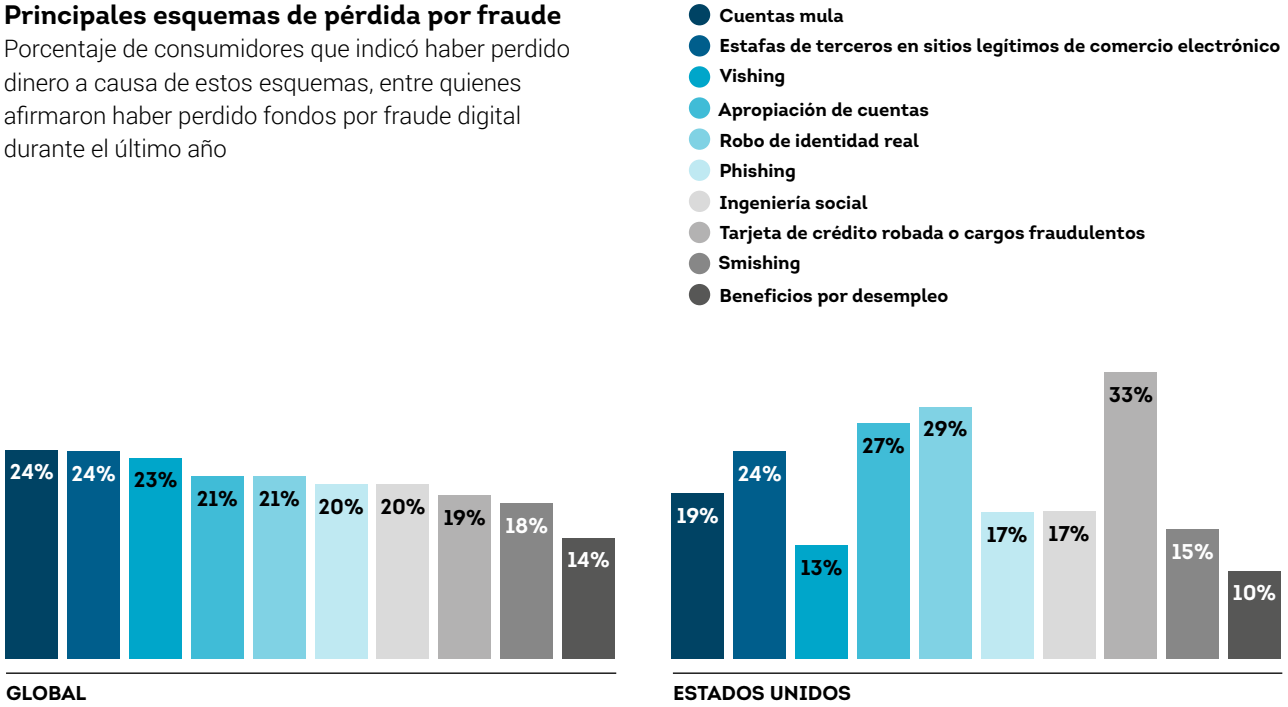
Pérdida mediana por fraude denunciada (USD$) entre los consumidores que indicaron haber perdido fondos por fraude digital durante el último año

*Conversión a USD$ basada en el tipo de cambio vigente al 29 de diciembre de 2025
**La cifra global corresponde al promedio de los 18 países encuestados

Fuente: Encuesta del consumidor de TransUnion

Principales esquemas de pérdida por fraude

Porcentaje de consumidores que indicó haber perdido dinero a causa de estos esquemas, entre quienes afirmaron haber perdido fondos por fraude digital durante el último año



Fuente: Encuesta del consumidor de TransUnion

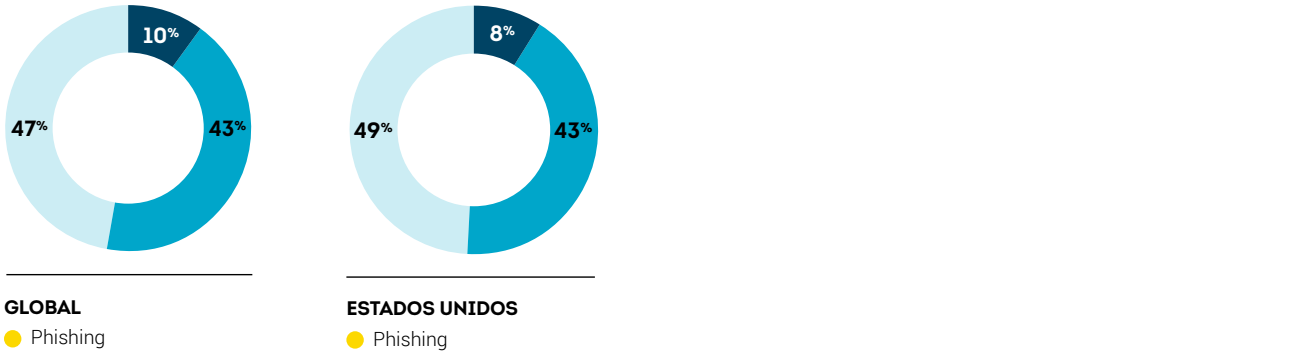
El phishing es el esquema de fraude más denunciado por los consumidores

Más de la mitad de los consumidores en Estados Unidos, el 51%, indicó haber sido objetivo de un esquema de fraude digital, y el 8% afirmó haber sido víctima entre agosto y diciembre de 2025. Sin embargo, una proporción significativa de la población no reconoció posibles intentos de fraude; el 49% señaló no haber sido consciente de haber sido objetivo de esquemas de fraude. Estas cifras se han mantenido consistentes durante los últimos dos años.

El phishing, que incluye correos electrónicos, sitios web, publicaciones en redes sociales, códigos QR fraudulentos y otros métodos diseñados para robar datos, fue la estafa más denunciada; el 39% de los consumidores en Estados Unidos indicó haber sido objetivo de este tipo de fraude. A este le siguió de cerca el smishing, que consiste en mensajes de texto fraudulentos destinados a engañar a las personas para que revelen información, con un 36%.

Consumidores objetivo de fraude

Porcentaje de consumidores que indicó que los estafadores los tuvieron como objetivo con intentos de fraude digital entre agosto y diciembre de 2025, así como el esquema más frecuente mediante el cual señalaron haber sido atacados



Fuente: Encuesta del consumidor de TransUnion

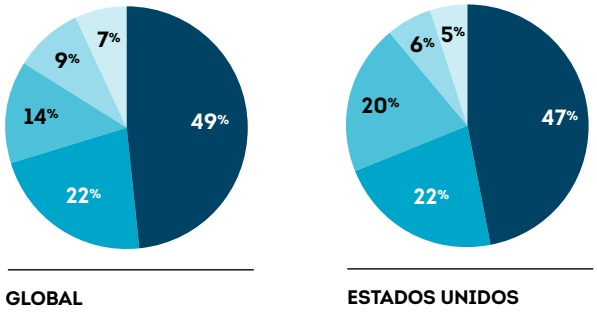
Los consumidores prefieren marcas que ofrecen experiencias digitales seguras y fluidas

Los consumidores estadounidenses ahora comprenden el riesgo del fraude empresarial en línea, pero la comodidad sigue siendo demasiado atractiva como para ignorarla. El 40% afirmó que realiza más de la mitad de sus transacciones en línea y el 75% indicó que gestiona más del 50% de la administración de sus cuentas de forma online. Sin embargo, con la adopción de los canales digitales, las personas esperan que las experiencias digitales de las marcas sean seguras y sencillas. Las expectativas son altas y los riesgos también. El 42% de los consumidores en Estados Unidos cambiaría de empresa para obtener una mejor experiencia digital y el 70% no volvería a un sitio si detecta cualquier riesgo de fraude.

Generar confianza es clave. Casi la mitad de los consumidores, el 47%, clasificó la seguridad de los datos personales como su principal expectativa de las empresas online y el 76% afirmó que la confianza en que sus datos personales están protegidos es muy importante al decidir con qué empresa hacer negocios. Además, el 44% señaló que las preocupaciones por fraude son la principal razón por la que abandonan un carrito de compra online, solo después de los costos de envío.

Ranking de expectativas o cualidades en las empresas online preferidas

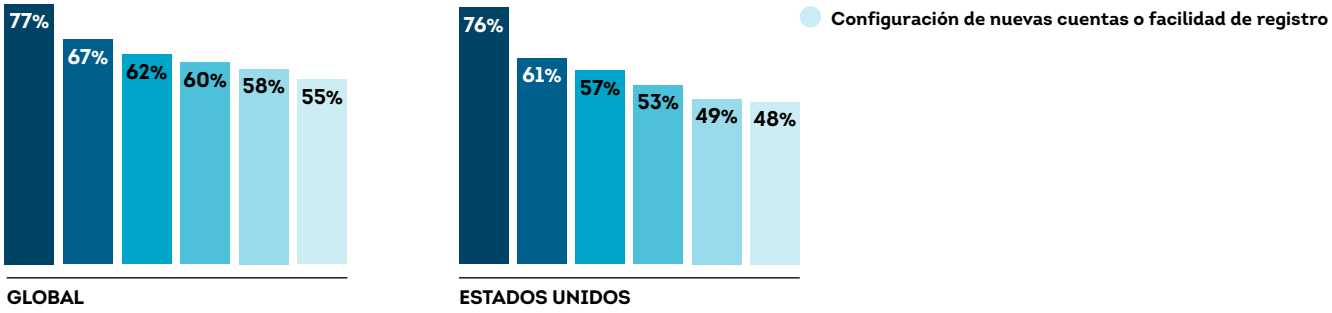
Respuesta principal seleccionada



Fuente: Encuesta del consumidor de TransUnion

Características importantes a la hora de elegir con quién realizar transacciones online

Porcentaje que respondió "Muy importante"



Fuente: Encuesta del consumidor de TransUnion

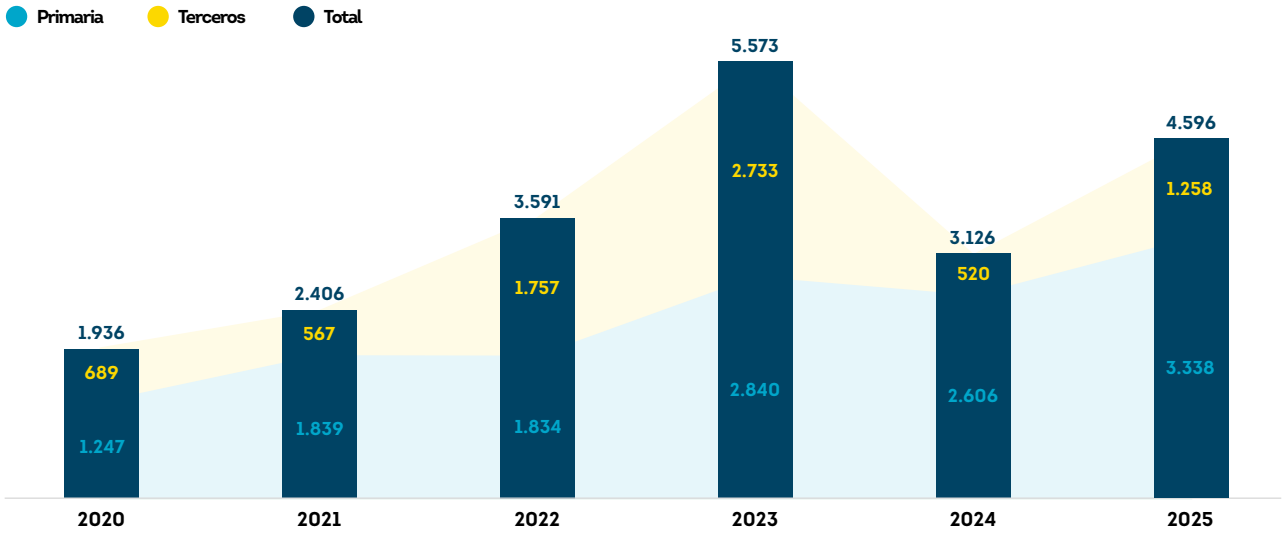
Tendencias de exposición de datos de identidad

La gravedad de las filtraciones de datos en Estados Unidos alcanza un nivel récord

Estados Unidos experimentó un aumento del 47% en el volumen de filtraciones de datos en 2025 en comparación con 2024. Los ataques parecieron enfocarse en datos que no están fácilmente disponibles en los mercados de la web oscura, para obtener credenciales de identidad que puedan utilizarse en esquemas de fraude.

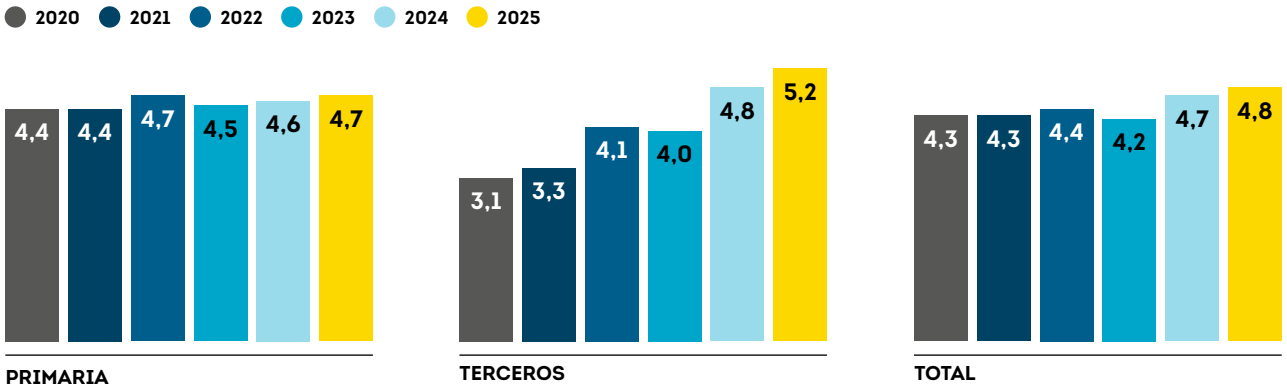
Los delincuentes se enfocaron en credenciales de alto riesgo, incluidos los números completos de Seguro Social, que impulsan la gravedad promedio de una filtración al afectar directamente la capacidad de una organización para responder de manera eficaz, según lo medido por el Breach Risk Score de TruEmpower™ de TransUnion, un indicador líder del riesgo futuro de fraude. Esta fue la gravedad más alta desde que comenzó nuestro análisis en 2020. Las filtraciones de datos de terceros implican ataques a organizaciones que prestan servicios comerciales a las marcas y fueron significativamente más riesgosas que aquellas dirigidas a organizaciones primarias.

Volumen de filtraciones de datos en Estados Unidos



Fuente: Red global de inteligencia de TransUnion

Puntaje promedio de riesgo de filtración para filtraciones de datos en Estados Unidos



Fuente: Red global de inteligencia de TransUnion

Una filtración de datos primaria representa un ataque directo a una organización. Una filtración de datos de terceros, también conocida como ataque a la cadena de suministro, a la cadena de valor o filtración por puerta trasera, ocurre cuando un atacante accede a la red de una entidad a través de proveedores o suministradores externos, por ejemplo, procesamiento de nómina o facturación médica.

TransUnion

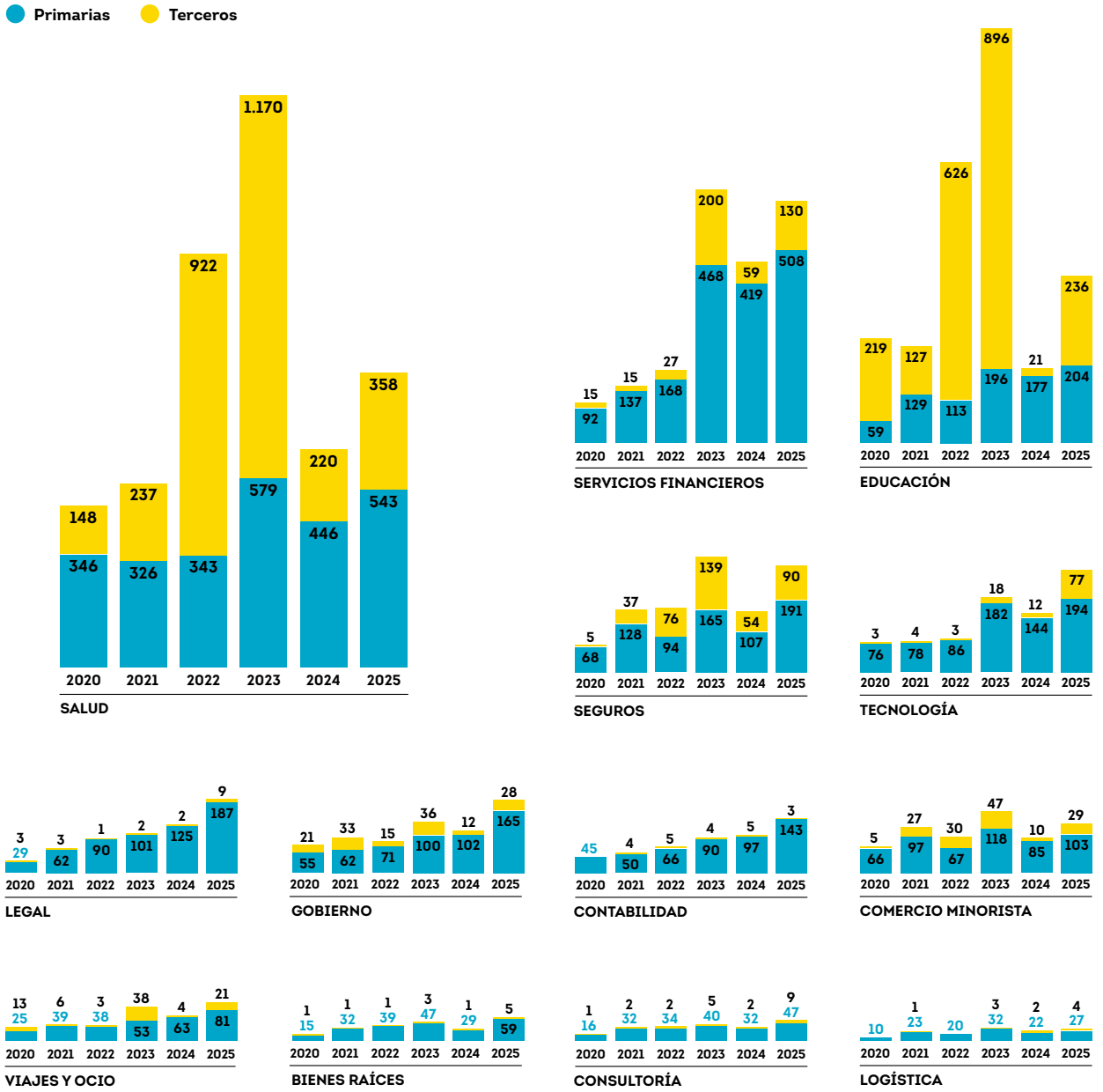
La industria de la salud continúa siendo la más afectada por filtraciones de datos

La industria de la salud continuó registrando el mayor número de filtraciones de datos en 2025, seguida por los servicios financieros. Mientras tanto, los sectores de salud y contabilidad se posicionaron como aquellos con los Puntajes de Riesgo de Filtración más altos (BRS, por sus siglas en inglés) de 5,1.

Tanto los ataques directos como los indirectos en el sector salud se enfocaron en credenciales de identidad de alto valor, incluidos los números completos de Seguridad Social, historiales médicos, números de pago e información de contacto, todos ellos fundamentales para perpetrar estafas al consumidor y verificar datos previamente comprometidos.

Más del 84% de las filtraciones en cada uno de los cuatro sectores con mayor BRS — salud, contabilidad, legal y viajes y ocio, fueron causadas por ciberataques, en contraste con otros tipos de filtraciones como errores de sistemas o fallas humanas. En cambio, los sectores de servicios financieros y gobierno experimentaron una proporción de filtraciones impulsadas por ciberataques inferior al promedio.

Volumen de filtraciones de datos en Estados Unidos



Fuente: Red global de inteligencia de TransUnion

Los delincuentes se enfocan en credenciales de alto valor para la apropiación de cuentas y el fraude en nuevas cuentas

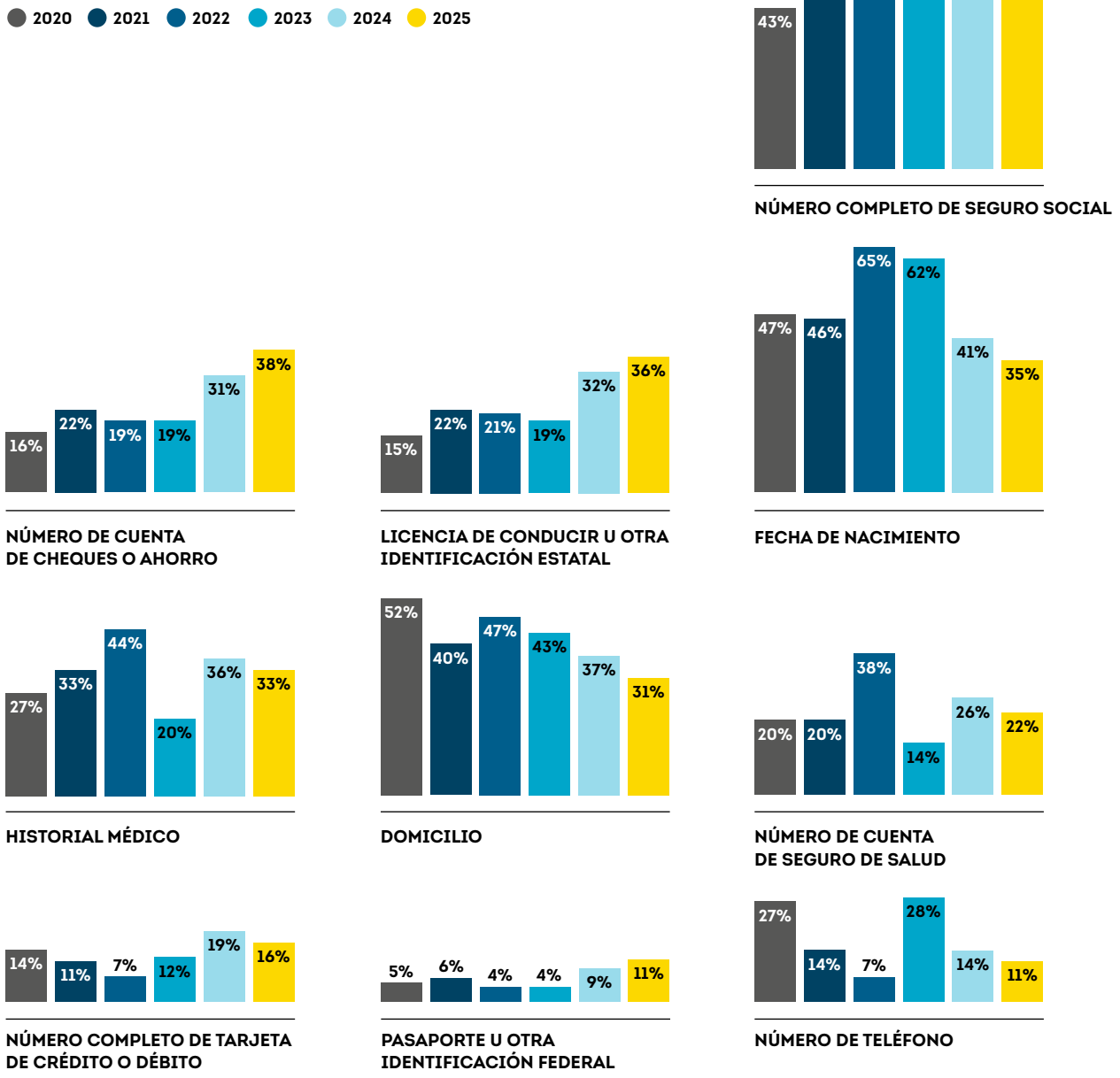
Los números completos de Seguro Social estuvieron expuestos en el 78% de las filtraciones de datos en 2025, manteniéndose como la credencial más buscada desde 2021 y registrando un aumento de 10 puntos porcentuales frente a 2024. Esta es una credencial clave para perpetrar fraude en la creación de nuevas cuentas, apropiación de cuentas, devoluciones de impuestos y fraude en beneficios gubernamentales.

En 2025, por primera vez desde que comenzó nuestro análisis en 2020, la exposición de números de cuentas de cheques y ahorro se posicionó como la segunda credencial de identidad más expuesta, presente en el 38% de las filtraciones de datos en general y en el 41% de las filtraciones de terceros. La exposición de estas cuentas de depósito creció de forma significativa, con un aumento acumulado del 138% en los últimos seis años y un incremento del 356% en filtraciones de terceros.

A medida que los delincuentes continúan aprovechando inteligencia artificial generativa, deepfakes y otras técnicas avanzadas para evadir controles de autenticación, la exposición de credenciales de identificación emitidas por el gobierno siguió aumentando. La exposición de licencias de conducir y otras identificaciones estatales creció un 140% en los últimos seis años, mientras que la exposición de pasaportes aumentó un 120% en el mismo periodo. Los historiales médicos, incluidos diagnósticos e información de profesionales de la salud, estuvieron presentes en el 33% de las filtraciones de datos a nivel general, lo que representa un incremento interanual del 22% y un aumento del 400% en las filtraciones de terceros.

Las 10 principales credenciales de identidad expuestas en filtraciones de datos en Estados Unidos

Porcentaje de credenciales expuestas en una filtración de datos



Fuente: Red global de inteligencia de TransUnion

TransUnion

Tendencias de fraude digital

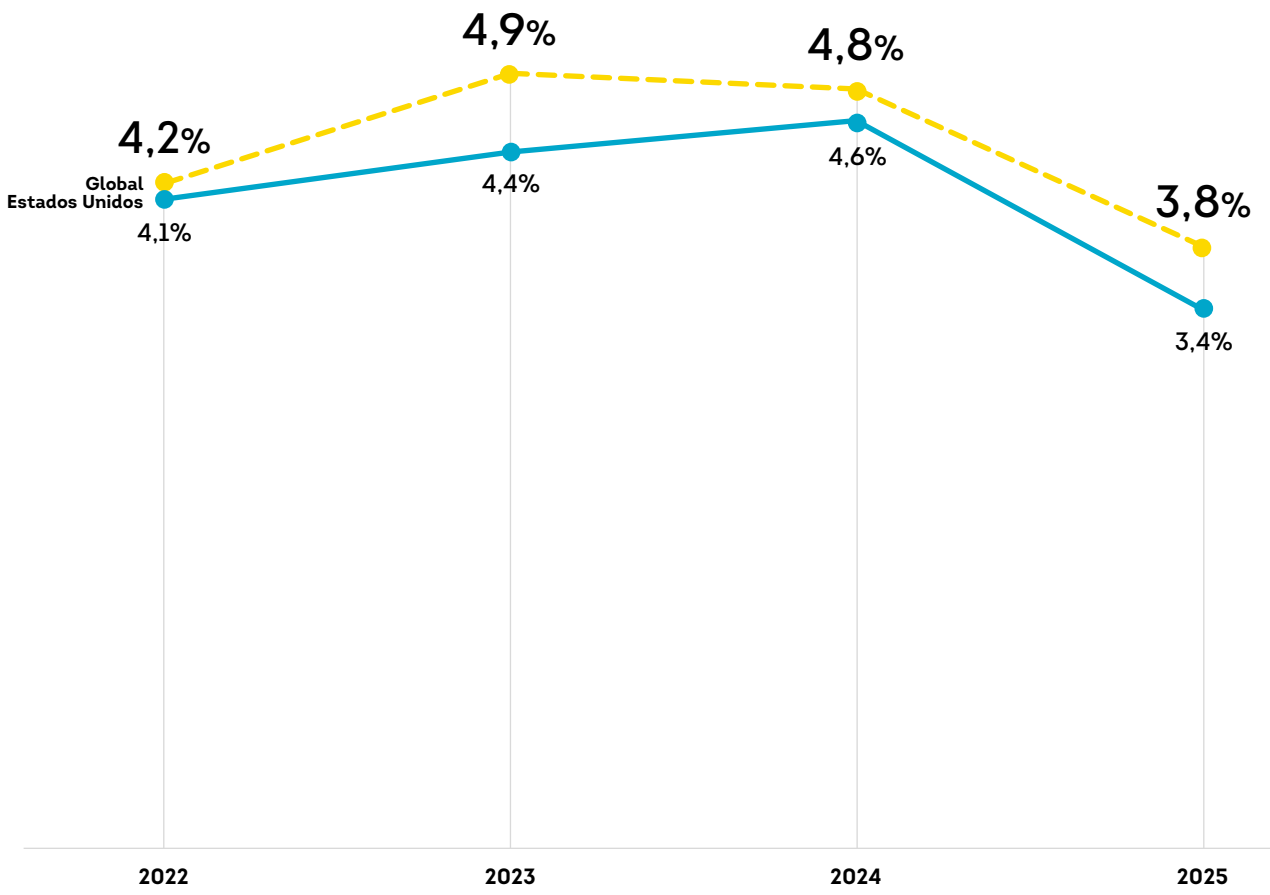
La tasa de sospecha de fraude digital disminuye mientras los ataques se vuelven más sofisticados

La tasa de sospecha de fraude digital en los intentos de transacciones en los que el consumidor se encontraba en Estados Unidos disminuyó un 26% en 2025 en comparación con 2024. La tasa se redujo al 3,4% en 2025, ligeramente por debajo del promedio global del 3,8%.

Los delincuentes tienden a concentrar los ataques de fraude en los objetivos más fáciles, al mismo tiempo que utilizan herramientas de inteligencia artificial para superar sistemas de detección de fraude obsoletos o fragmentados. Las tendencias de riesgo de fraude digital parecen reflejar este comportamiento, ya que los estafadores evitan intentar eludir directamente sistemas de autenticación multifactor más robustos y, en su lugar, recurren a estafas de phishing y vishing impulsadas por inteligencia artificial generativa, dirigidas a los consumidores.

Obtener acceso a las credenciales de inicio de sesión de los consumidores fortalece la capacidad de los estafadores para perpetrar con éxito la apropiación de cuentas, utilizando técnicas para sortear códigos de acceso de un solo uso y aprovechar métodos de autenticación secundaria. Esto da lugar a pérdidas promedio más elevadas, particularmente prevalentes en Estados Unidos. Además, el robo de información de identidad personal suele derivar en el uso de técnicas basadas en inteligencia artificial generativa, como identidades sintéticas o credenciales de identidad deepfake, lo que puede estar ocultando ataques de fraude sofisticados durante la apertura de nuevas cuentas, sin generar alertas hasta que las pérdidas se materializan días o incluso meses después.

Tasa de sospecha fraude digital



Fuente: Red global de inteligencia de TransUnion

TransUnion

La industria de comunidades registró el mayor riesgo de fraude digital

La industria de comunidades, que incluye propiedades web y aplicaciones como sitios de citas en línea y foros de discusión, experimentó la tasa más alta de sospecha de fraude digital en intentos de transacción en los que el consumidor se encontraba en Estados Unidos en 2025, con un 11,7%. Esto representa un aumento del 15% frente a 2024 y un crecimiento del 7% en el volumen de fraude digital sospechoso entre ambos períodos.

Otras industrias orientadas al entretenimiento también registraron tasas de fraude superiores al promedio. La industria del gaming, que incluye sitios y aplicaciones de apuestas en línea, continuó registrando intentos de fraude digital sospechoso en casi 1 de cada 10 transacciones, con un 9,8%. Los videojuegos representaron el 8,3% de los intentos de fraude digital sospechoso en 2025. Cabe destacar que la industria gubernamental registró el mayor aumento interanual en el número de intentos de fraude digital sospechoso, con un crecimiento del 19%, el más alto entre todas las industrias analizadas.

Intentos de fraude digital desde Estados Unidos por industria

- **Tasa de sospecha de fraude digital 2025**
- **Variación porcentual del volumen de fraude digital sospechoso 2024-2025**

Comunidades
(citas en línea, foros, etc.)

2025
11,7%

2024-2025
+7%

Juegos de azar
(apuestas deportivas en línea, póker, etc.)

2025
9,8%

2024-2025
0%

Videojuegos

2025
8,3%

2024-2025
-32%

Comercio minorista

2025
3,8%

2024-2025
-41%

Servicios financieros

2025
3,2%

2024-2025
-23%

Logística

2025
1,6%

2024-2025
-70%

Gobierno

2025
0,8%

2024-2025
+19%

Seguros

2025
0,5%

2024-2025
-19%

Telecomunicaciones

2025
0,4%

2024-2025
-22%

Viajes y ocio

2025
0,2%

2024-2025
-47%

Fuente: Red global de inteligencia de TransUnion

El riesgo de fraude digital impacta todas las etapas del ciclo de vida del consumidor

Todas las etapas del ciclo de vida del consumidor presentaron niveles similares de riesgo de fraude digital en Estados Unidos. En 2025, la creación de cuentas fue ligeramente más riesgosa que el inicio de sesión y las transacciones financieras. Los intentos de creación de cuentas registraron la tasa más alta de sospecha de fraude digital en el ciclo de vida del consumidor para transacciones en las que el usuario se encontraba en Estados Unidos en 2025, aunque fue sustancialmente inferior al 8,3% observado a nivel global. El inicio de sesión y las transacciones financieras, con tasas del 3,6% y 3,3% respectivamente, mostraron niveles similares de riesgo en Estados Unidos en 2025.

El riesgo de fraude digital en la creación de cuentas estuvo impulsado por industrias específicas. El 35,2% de los intentos de creación de cuentas en telecomunicaciones, el 28,1% en comercio minorista y el 21,3% en comunidades realizados desde Estados Unidos fueron identificados como fraude digital en 2025. Al mismo tiempo, el sector de seguros registró el mayor riesgo en inicio de sesión de cuentas, con el 42,7% de los intentos de inicio de sesión desde Estados Unidos identificados como fraude digital.

Ejemplos de etapas del ciclo de vida del consumidor

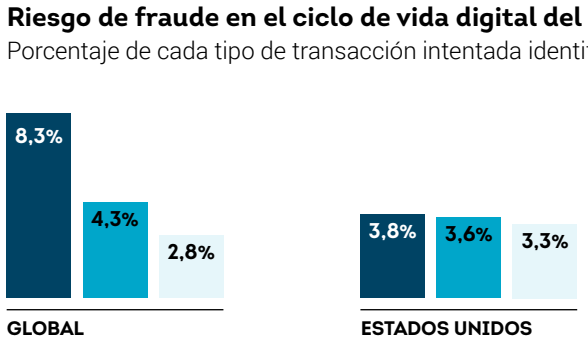
Creación de cuentas: registro de cuentas, procesos de inscripción y originación de préstamos

Inicio de sesión de cuentas: eventos de inicio de sesión y fallos de inicio de sesión

Transacciones financieras: compras, retiros y depósitos

Riesgo de fraude en el ciclo de vida digital del consumidor

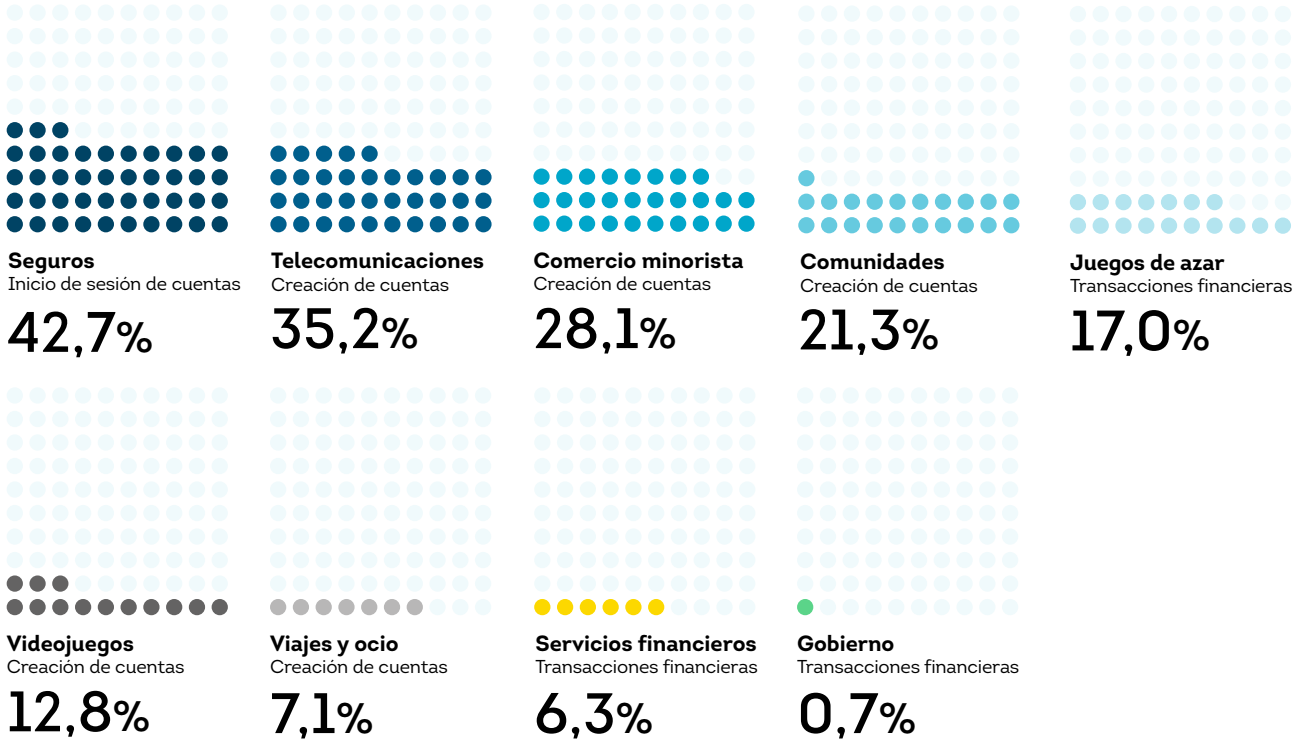
Porcentaje de cada tipo de transacción intentada identificado como fraude digital en 2025



Fuente: Red global de inteligencia de TransUnion

Riesgo de fraude en el ciclo de vida digital del consumidor por industria

La etapa del ciclo de vida del consumidor con la tasa más alta de sospecha de fraude digital desde Estados Unidos por industria y el porcentaje correspondiente en 2025



Fuente: Red global de inteligencia de TransUnion

TransUnion

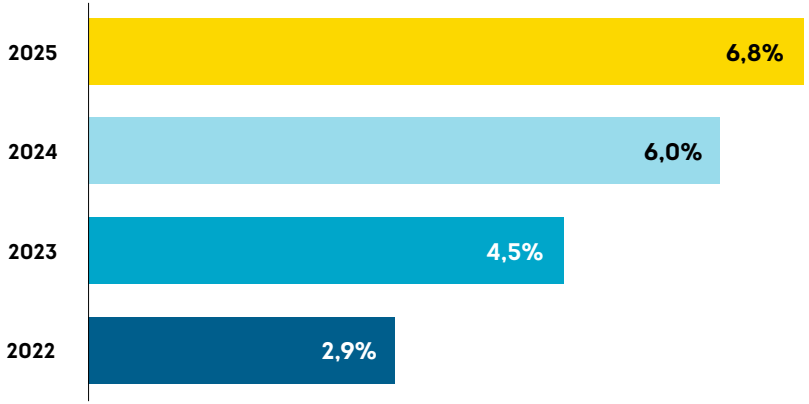
Tendencias de fraude en centros de atención telefónica

Las llamadas de alto riesgo a los centros de atención continúan en aumento

Las organizaciones dependen cada vez más de centros de atención telefónica a medida que los consumidores multicanal los utilizan con mayor frecuencia. Los centros de atención siguen siendo un objetivo clave para los delincuentes, que buscan facilitar la apropiación de cuentas mediante ingeniería social, engañando a los agentes para que revelen datos del cliente o modifiquen los detalles de la cuenta.

Al medir el riesgo de las llamadas entrantes a los centros de atención de Estados Unidos, TransUnion documentó un incremento del 13%, hasta alcanzar el 6,8%, en el porcentaje de llamadas de alto riesgo entre 2024 y 2025. Las llamadas de alto riesgo son aquellas que obtienen una puntuación de 0 o 100. Las llamadas telefónicas de mayor riesgo aumentaron en tres de los cuatro canales monitoreados durante ese período.

Llamadas de alto riesgo hacia centros de atención en Estados Unidos



Fuente: Red global de inteligencia de TransUnion

El riesgo de las llamadas entrantes desde móviles aumenta en los centros de atención

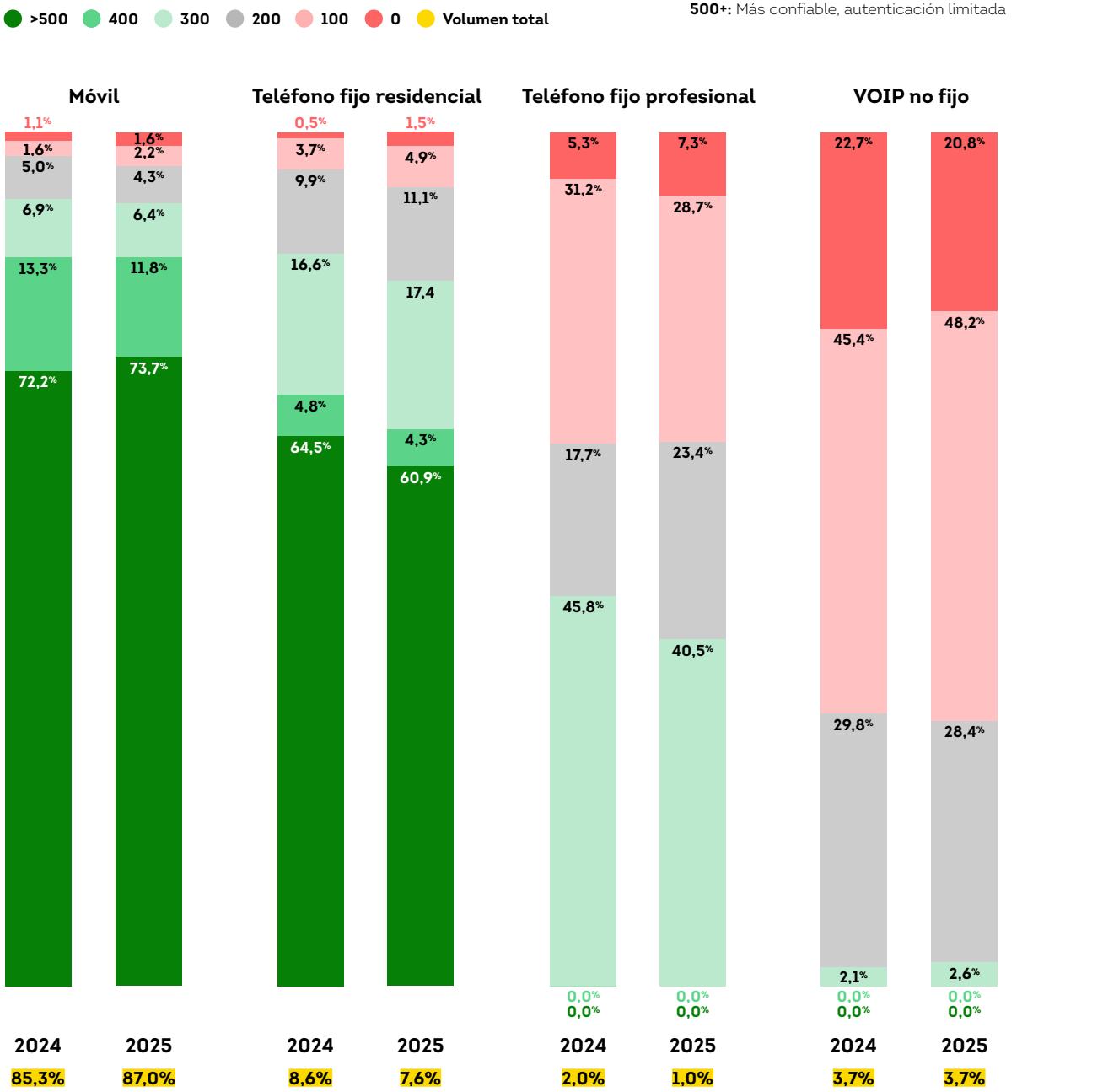
La gran mayoría de las llamadas, el 87%, recibidas por los centros de atención telefónica de Estados Unidos de TransUnion en 2025 provinieron de teléfonos móviles y fueron más riesgosas que en 2024. Tan solo el 3,8% de las llamadas móviles fueron identificadas como de mayor riesgo de fraude, lo que representa un aumento del 41% frente al 2,7% registrado en 2024.

El canal más riesgoso para los centros de atención fue la VoIP no fija, un tipo de número telefónico que no está asociado a un dispositivo físico. Si bien este canal representó solo el 3,7% del volumen total de llamadas, el 69% de estas llamadas fue identificado como de alto riesgo de fraude en 2025.

Riesgos en los Centros de Atención Telefónica de Estados Unidos por canal y por volumen total

Niveles de puntuación de riesgo de llamadas

0 & 100: Más alto, autenticación reforzada
200-400: Funcionamiento habitual con autenticación
500+: Más confiable, autenticación limitada



Fuente: Red global de inteligencia de TransUnion

Tendencias de identidades sintéticas y lavado de crédito

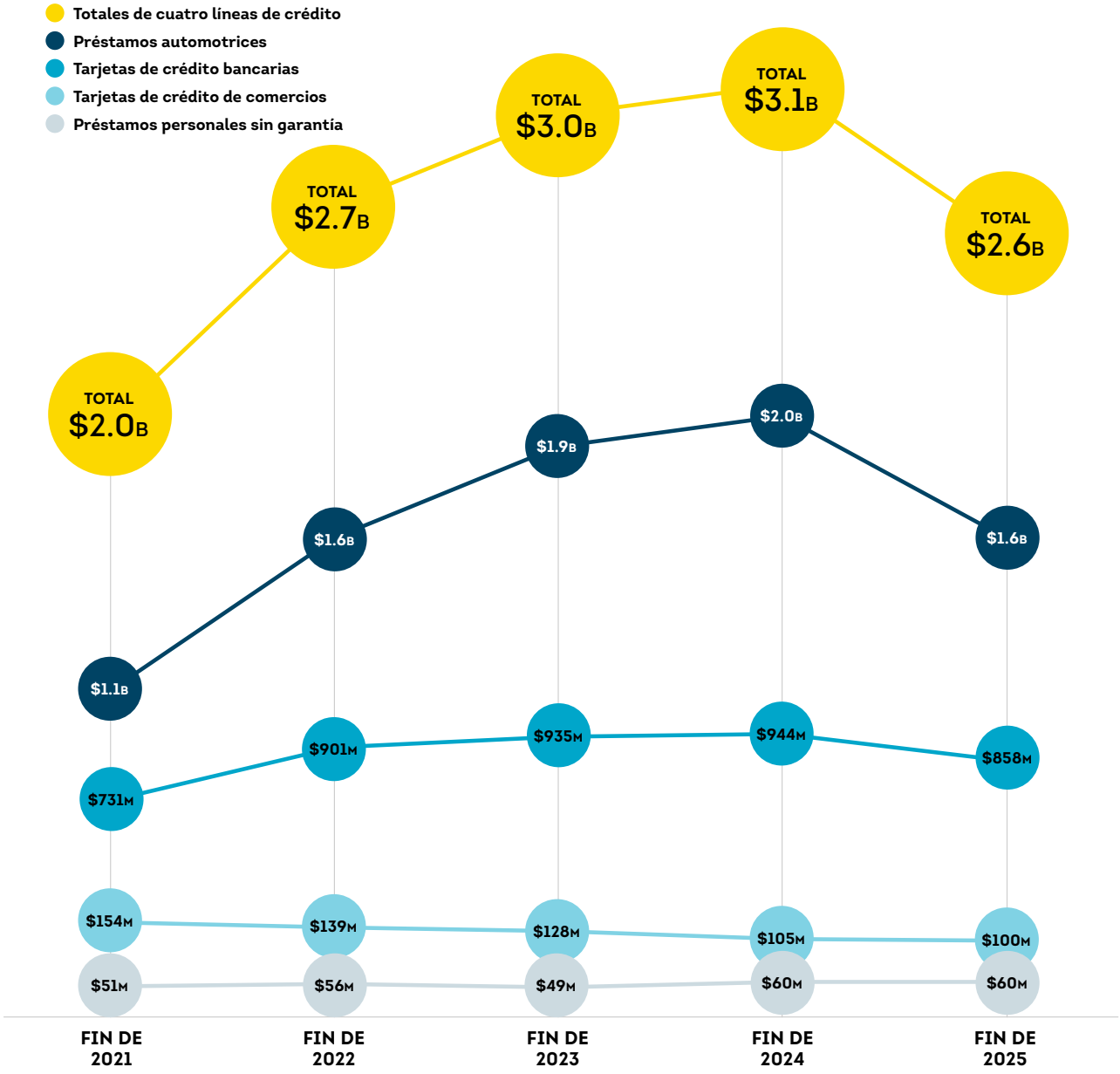
La exposición a identidades sintéticas en el otorgamiento de crédito se mantiene persistentemente alta

Las identidades sintéticas continúan siendo un enfoque de alto riesgo para las organizaciones en los procesos de creación de nuevas cuentas, impulsadas por credenciales comprometidas y por el uso prolongado de inteligencia artificial generativa. Según los datos globales de crédito al consumidor de TransUnion, la exposición total a identidades sintéticas entre las cuentas abiertas por prestamistas de Estados Unidos para préstamos automotrices, tarjetas de crédito bancarias, tarjetas de crédito de comercios y préstamos personales sin garantía alcanzó USD$ 2.600 millones en pérdidas potenciales al cierre de 2025.

La construcción de cuentas de crédito para establecer un historial personal creíble sigue siendo una táctica central de las identidades sintéticas, ya que les otorga legitimidad y hace que los perfiles fabricados sean difíciles de detectar. A medida que la inteligencia artificial generativa facilita la creación de documentos deepfake realistas y de identidades sintéticas escalables, los delincuentes están expandiéndose más allá de los servicios financieros. El aumento de la exposición a identidades sintéticas entre los prestamistas puede señalar un desplazamiento en el uso de este tipo de fraude hacia industrias menos preparadas, como educación, fintech, gobierno, salud, comercio minorista y telecomunicaciones, ampliando la superficie de ataque para el fraude con identidades sintéticas.

Riesgo de identidades sintéticas para prestamistas en Estados Unidos 2021–2025

Exposición crediticia total en USD a identidades sintéticas a las que tienen acceso los prestamistas de Estados Unidos en préstamos automotrices, tarjetas de crédito bancarias, tarjetas de crédito de comercios y préstamos personales sin garantíacards, retail credit cards and unsecured personal loans



Fuente: Red global de inteligencia de TransUnion

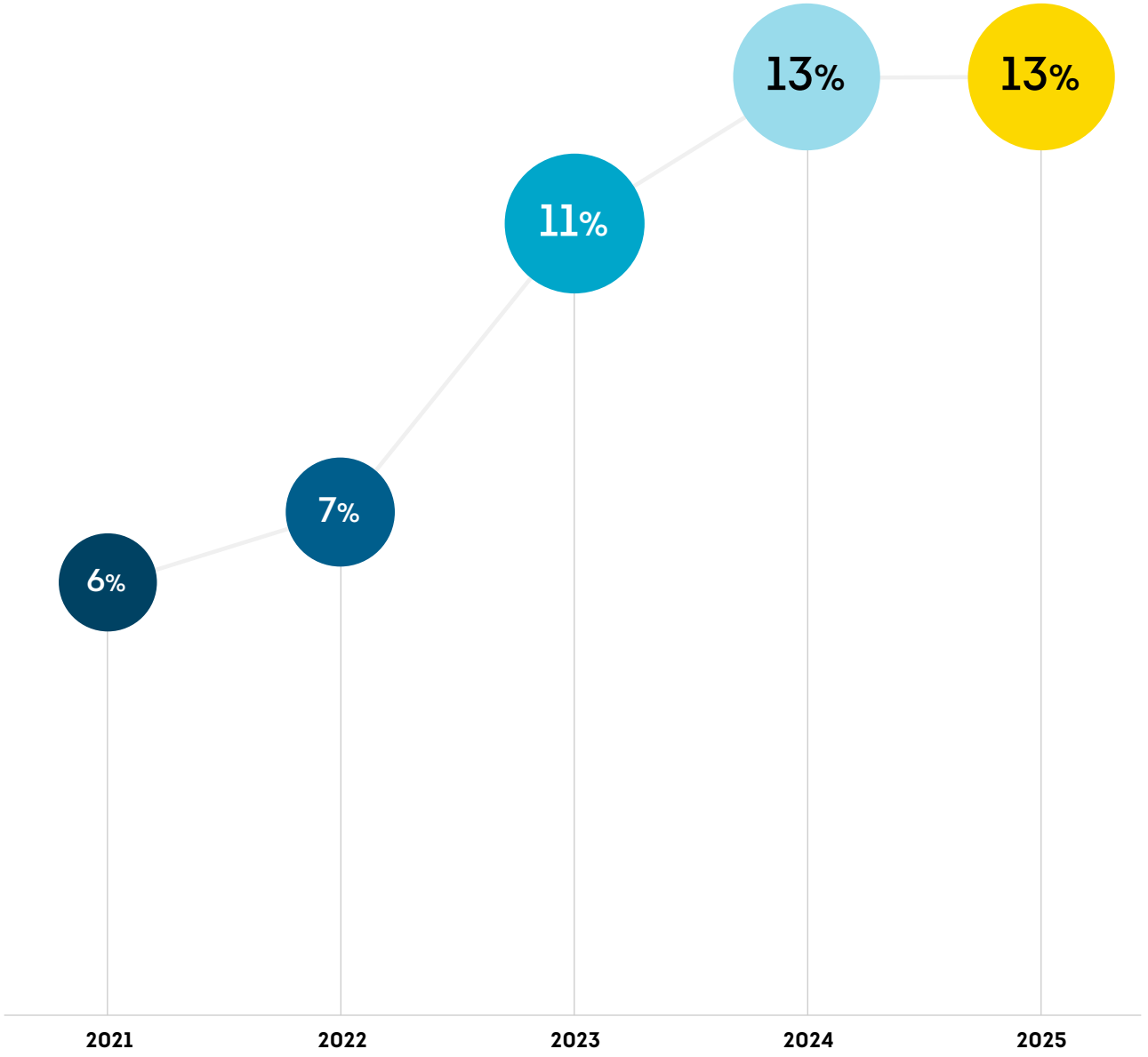
El lavado de crédito da nueva vida a identidades de riesgo

Los delincuentes refuerzan identidades sintéticas alteradas mediante historiales crediticios construidos de forma legítima, lo que dificulta distinguirlas de personas reales. Una vez detectadas, pueden abandonarlas o intentar reutilizarlas, y es ahí donde entra en juego el lavado de crédito.

El lavado de crédito es un esquema de manipulación crediticia que consiste en eliminar información negativa legítima de un historial crediticio mediante la presentación de una denuncia falsa de robo de identidad. Estas disputas falsas de informes crediticios pueden realizarse contra cuentas abiertas usando identidades de consumidores robadas o identidades sintéticas, o bien contra transacciones no autorizadas en la cuenta crediticia legítima de un consumidor.

Los consumidores en Estados Unidos, o sus representantes autorizados, tienen el derecho legal de disputar información incorrecta en sus informes crediticios, y TransUnion sigue un proceso de resolución de disputas altamente regulado. En 2025, las disputas de informes crediticios de consumidores en Estados Unidos que denunciaban fraude representaron el 13% del total de disputas, sin cambios frente a 2024.

Disputas de informes crediticios de consumidores en Estados Unidos que denuncian fraude como porcentaje del total de disputas



Fuente: Red global de inteligencia de TransUnion

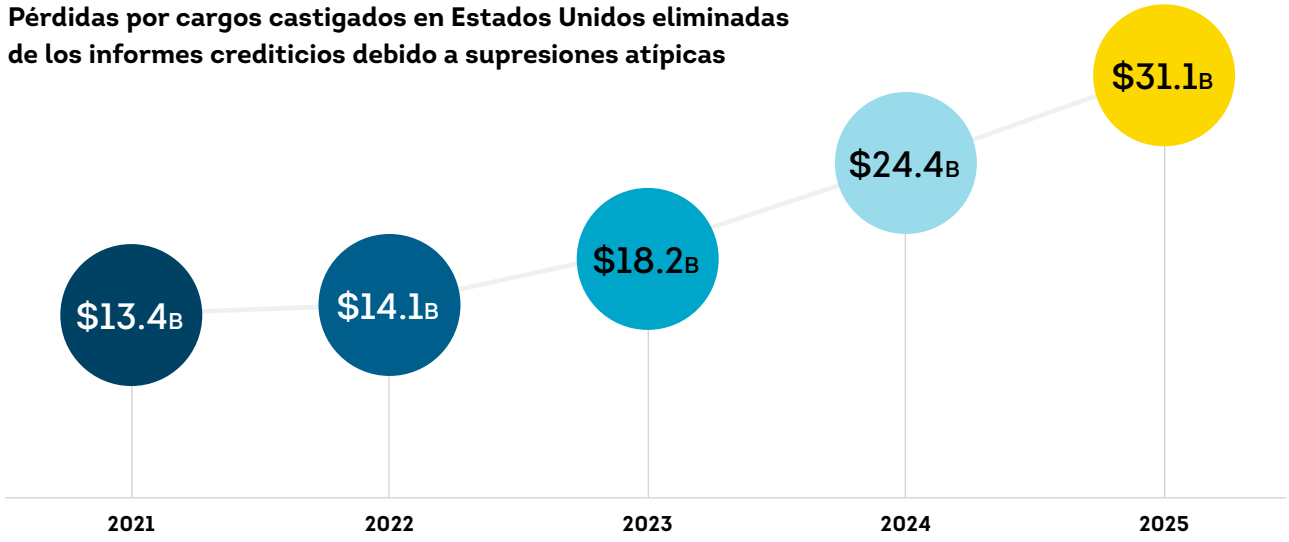
El crecimiento atípico de cargos castigados suprimidos ilustra el riesgo del lavado de crédito

Si una deuda permanece impaga durante un período prolongado, las instituciones financieras generalmente la dan de baja, en un proceso conocido como castigo de cargo. Las pérdidas por cargos castigados representan un tipo de riesgo crediticio. Al mismo tiempo, los cargos castigados suelen aparecer como información negativa en el informe crediticio de una persona, afectando su puntaje de crédito. Sin embargo, cuando el registro negativo, ya sea un préstamo, una cuenta crediticia o una transacción, se disputa exitosamente por un consumidor como fraude, el resultado sigue siendo una pérdida por cargo castigado, pero el elemento se elimina de los modelos de calificación crediticia como si nunca hubiera ocurrido, lo que se conoce como ¨supresión atípica¨.

Las supresiones atípicas pueden ser reportadas a las agencias de crédito por instituciones financieras o directamente por consumidores mediante el proceso de disputa crediticia. Si bien esta es una herramienta importante para que los consumidores se protejan del fraude, también puede ser utilizada por delincuentes para reciclar identidades y perpetrar fraude mediante lavado de crédito.

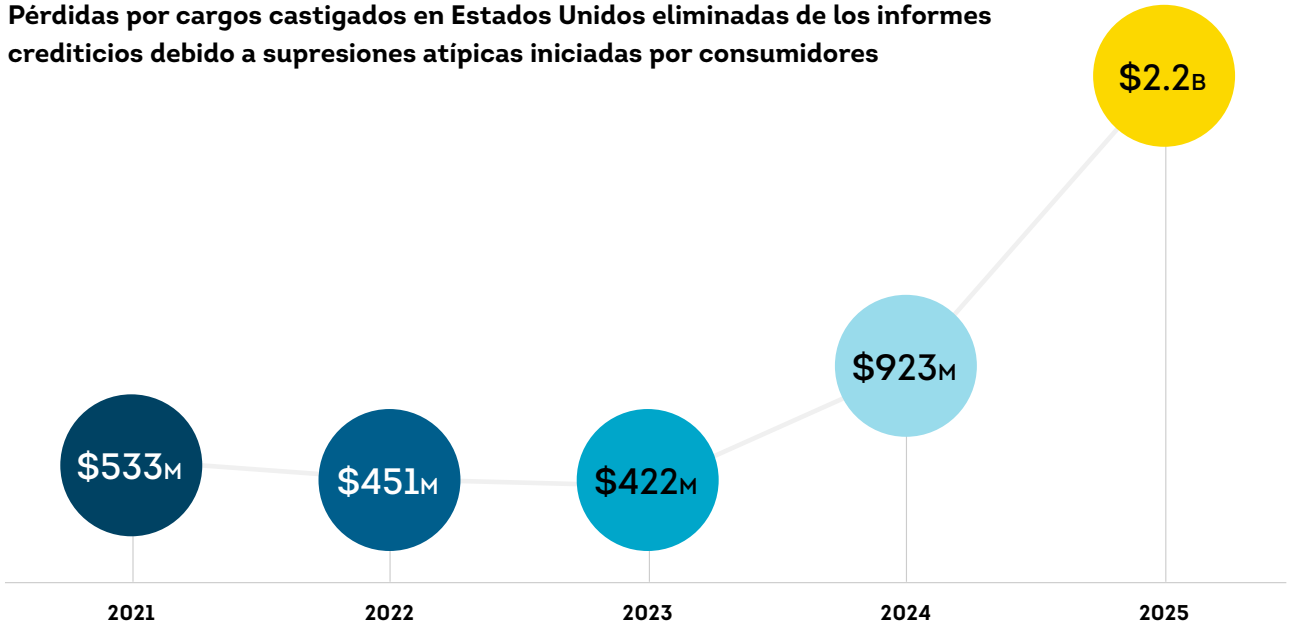
La magnitud del lavado de crédito ha sido significativa, especialmente entre las supresiones iniciadas por consumidores. Las pérdidas por cargos castigados eliminadas de los informes crediticios en Estados Unidos debido a cualquier tipo de supresión atípica crecieron un 28% entre 2024 y 2025, superando los USD$ 31 mil millones al cierre de 2025. Las supresiones atípicas iniciadas por consumidores representaron cerca del 90% de todas las supresiones de cargos castigados al cierre de 2025, con un aumento del 138% frente a finales de 2024, superando por primera vez los USD$ 2.000 millones.

Pérdidas por cargos castigados en Estados Unidos eliminadas de los informes crediticios debido a supresiones atípicas



Fuente: Red global de inteligencia de TransUnion

Pérdidas por cargos castigados en Estados Unidos eliminadas de los informes crediticios debido a supresiones atípicas iniciadas por consumidores



Fuente: Red global de inteligencia de TransUnion

Conclusiones

El fraude se está convirtiendo en un desafío cada vez mayor para organizaciones de todos los tamaños e industrias. A medida que avanzamos hacia 2026 y más allá, los riesgos continuarán creciendo a medida que los estafadores trabajen para evadir las defensas. Las filtraciones de datos y las estafas seguirán comprometiendo identidades, lo que hace esencial proteger tanto a la organización como a los consumidores. La realidad es que es necesario generar confianza en los consumidores sin comprometer, al mismo tiempo, una experiencia sin fricciones para el cliente.

Con los riesgos de identidad presentes a lo largo de todo el ciclo de vida del consumidor, invertir en una detección de fraude más inteligente ya no es un valor agregado, sino una necesidad. Esto implica adoptar un enfoque holístico e interempresarial para la prevención del fraude. Los sistemas fragmentados son más fáciles de explotar para los estafadores, por lo que es fundamental derribar silos y fortalecer cada capa de defensa. Desde la verificación de identidad y la autenticación hasta el monitoreo de sesiones, cada capa debe ser más inteligente, adaptable y estar respaldada por mejores señales y modelos de evaluación.

La IA debe estar en el centro de esta evolución. A medida que las estrategias de fraude se vuelven más sofisticadas y centradas en reducir la identidad fragmentada mediante analítica avanzada, mejores señales de riesgo y tecnología integrada, las organizaciones no solo podrán detectar mejor el fraude, sino también reducir riesgos innecesarios para los consumidores, manteniendo al mismo tiempo experiencias fluidas y seguras. TransUnion puede asociarse con usted para demostrar cómo aplicar los aprendizajes derivados de 20 años de uso exitoso de inteligencia artificial para generar información integrada y basada en datos para sus clientes.

Metodología de obtención de datos

Este informe combina datos propietarios de la red global de inteligencia de TransUnion y una encuesta a consumidores especialmente comisionada.

Centro de atención telefónica

Los hallazgos relacionados con centros de atención telefónica de TransUnion se basaron principalmente en datos de instituciones financieras grandes y pequeñas ubicadas en Estados Unidos. La tasa o el porcentaje de llamadas de alto riesgo se determinó a partir de la evaluación de múltiples factores de riesgo.

Disputas de informes crediticios de consumidores

Los hallazgos de TransUnion sobre disputas de informes crediticios de consumidores se basaron en datos de informes crediticios de consumidores de Estados Unidos, territorios estadounidenses y protectorados. La base de datos crediticia de consumidores de TransUnion se obtiene de más de 50 años de datos de crédito del consumidor y contiene información crediticia de aproximadamente 400 millones de consumidores.

Encuesta a consumidores

Esta encuesta en línea se llevó a cabo del 20 de noviembre al 9 de diciembre de 2025 en Brasil (1.000 encuestados), Canadá (999), Chile (499), Colombia (653), República Dominicana (415), Hong Kong (China) (1.000), India (950), Kenia (495), México (500), Namibia (308), Filipinas (821), Puerto Rico (218), Ruanda (308), Sudáfrica (1.000), España (999), Reino Unido (1.000) y Zambia (365), en asociación con terceros independientes. Los adultos de 18 años o más participaron mediante el uso de dispositivos de escritorio, móviles y tabletas. Las preguntas de la encuesta se administraron en chino (Hong Kong), inglés, francés (Canadá), portugués (Brasil) y español (Colombia, República Dominicana, México, Puerto Rico y España). Para garantizar una representación equilibrada entre los grupos demográficos, la encuesta incluyó cuotas para balancear las respuestas por edad, género e ingreso. Tenga en cuenta que algunos porcentajes de los gráficos pueden no sumar 100% debido al redondeo o a la aceptación de múltiples respuestas.

Filtraciones de datos

TransUnion obtiene datos propietarios sobre filtraciones de datos en asociación con el Identity Theft Resource Center (ITRC). El ITRC rastrea eventos de exposición pública de datos desde múltiples fuentes, incluidas comunicaciones de fiscales generales estatales, comunicados de prensa de entidades afectadas, empresas de ciberseguridad y otros actores del sector. TransUnion amplía estos datos mediante un proceso que calcula el nivel de riesgo de cada filtración, proporciona medidas accionables para los consumidores y asigna un Puntaje de Riesgo de Filtración, o BRS. El BRS se basa en la cantidad y gravedad de las credenciales particulares de identidad que se determinó que fueron expuestas. El rango del BRS va de 1 a 10, donde 1 representa el menor nivel de riesgo y 10 el más alto.

Fraude digital

TransUnion utiliza inteligencia proveniente de miles de millones de transacciones originadas en más de 40.000 sitios web y aplicaciones. Los intentos de fraude digital reflejan aquellos en los que los clientes de TransUnion determinaron la presencia de una o más de las siguientes condiciones según indicadores de riesgo del dispositivo: 1) denegación en tiempo real de debido a factores de fraude, 2) denegación en tiempo real por violaciones a políticas corporativas, 3) fraude confirmado tras una investigación del cliente o 4) violación de políticas corporativas tras una investigación del cliente. Los análisis por país examinaron transacciones en las que el consumidor sospechado de fraude se encontraba ubicado en un país específico durante la transacción. Las estadísticas globales representan todos los países a nivel mundial y no únicamente los países y regiones seleccionados.

Fraude con identidades sintéticas

Los hallazgos de TransUnion sobre fraude con identidades sintéticas se basaron en datos de informes crediticios de consumidores de Estados Unidos, territorios estadounidenses y protectorados. Sus datos crediticios de consumidores se obtienen rutinariamente de más de 50 años de información crediticia y contienen datos de aproximadamente 400 millones de consumidores. El análisis de fraude con identidades sintéticas abarcó toda la actividad registrada de consumidores en Estados Unidos entre el 1 de enero de 2009 y el 31 de diciembre de 2025. Las mediciones de exposición del prestamista se basaron en la fórmula propietaria de TransUnion para capturar la pérdida potencial total en riesgo para los prestamistas.

Acerca de TransUnion TruValidate

TruValidate organiza información de identidad, dispositivos y comportamiento para ayudar a las organizaciones a interactuar con confianza y seguridad con los consumidores en todos los canales y en cada etapa del recorrido del cliente, mejorando las conversiones, reduciendo las pérdidas por fraude y ofreciendo experiencias de usuario mejoradas y con la fricción correcta.

transunion.mx/solucion/truvalidate

TransUnion