TransUnion

ACTUALIZACIÓN H2 2025: PRINCIPALES TENDENCIAS DE FRAUDE

LA IDENTIDAD DIGITAL ES UNA OPORTUNIDAD PARA MITIGAR EL IMPACTO DEL FRAUDE

Los líderes empresariales afirman que sus empresas perdieron un 18% más por fraudes en el último año

Introducción

El fraude está evolucionando rápidamente y los equipos de prevención de fraude luchan por mantener el ritmo. Un suministro interminable de datos de identidad comprometidos amenaza con desbordar los sistemas de detección de fraudes, lo que permite a los delincuentes atacar fácilmente todos los puntos de contacto con los clientes. Este fue el sombrío panorama de las tendencias de fraude de la primera mitad de 2025. El aumento del riesgo en la apertura de nuevas cuentas debido a identidades sintéticas, robadas y alteradas está exponiendo a su organización al fraude. Las estafas a los consumidores dirigidas al uso autorizado y el fraude por apropiación de cuentas han aumentado, lo que pone en riesgo a los clientes existentes y a su marca. Para adelantarse, necesita una imagen clara de la identidad, lo que le permitirá una mayor protección frente a los usuarios de riesgo y, al mismo tiempo, mejorar la experiencia de los clientes reales.

En la actualización H2 2025 del informe Principales Tendencias de Fraude, desde TransUnion®, reunimos las tendencias, los puntos de referencia y la experiencia en materia de identidad y fraude de toda nuestra red global. El informe ofrece información sobre los responsables de prevenir el fraude y garantizar la experiencia de los clientes para obtener mejores resultados empresariales. Utilice este informe para evaluar los programas actuales de prevención del fraude en el contexto del mercado en general. Comparta esta información en toda su organización con el objetivo de aumentar la satisfacción de los clientes, reducir el fraude y mejorar el rendimiento empresarial.

Todos los datos de este informe combinan información propia de la red de inteligencia global de TransUnion, una encuesta empresarial encargada específicamente en Canadá, Hong Kong, India, Filipinas, Reino Unido y Estados Unidos, y una encuesta a consumidores en 18 países y regiones de todo el mundo. El primer semestre o H1 abarca del 1 de enero al 30 de junio y el segundo semestre o H2, del 1 de julio al 31 de diciembre.

PRINCIPALES HALLAZGOS

El coste del fraude para las empresas se dispara

7.7%
de ingresos anuales perdidos de media debido al fraude en el último año, lo que representa USD534 billones entre 1200 líderes empresariales encuestados en 2025.

24%
de los líderes empresariales afirmaron que las estafas o los fraudes autorizados eran la principal causa de pérdidas por fraude, seguidos por un 20% que denunció la apropiación de cuentas o el fraude de identidad sintética.

Aumentan las apropiaciones de cuentas a corto y largo plazo

21%
Aumento del volumen de apropiaciones de cuentas digitales entre el primer semestre de 2024 y el primer semestre de 2025.

141%
Aumento en el volumen de apropiaciones de cuentas digitales entre el primer semestre de 2021 y el primer semestre de 2025.

La creación de la cuenta fue la etapa más arriesgada del ciclo de vida del consumidor

8.3%
de todos los intentos de creación de cuentas digitales en el primer semestre de 2025 fueron sospechosos de fraude, lo que lo convierte en la etapa de mayor riesgo en el ciclo de vida del consumidor.

26%
de aumento en la tasa de presuntos fraudes digitales por intentos de creación de cuentas desde el primer semestre de 2024 (cuando era del 6.6%) hasta el primer semestre de 2025.

Contenidos

TransUnion

Anatomía del Riesgo de Identidad Digital

Las identidades digitales de los consumidores, es decir, lo que utilizas para tomar innumerables decisiones comerciales cada día, son muy arriesgadas, algunos incluso dirían que poco fiables. ¿Por qué? Existe toda una industria dedicada al robo de identidades de consumidores que operan en la web alimentando los fraudes. Las tendencias de fraude en el primer semestre de 2025 lo confirmaron: accesos no autorizados de datos, estafas telefónicas de alta presión, engaños a los consumidores para obtener datos de identidad – y la lista continúa. Los delincuentes utilizan datos robados o recopilados para crear identidades con fines de explotación. Esto incluye la creación de perfiles sintéticos, el uso de deepfakes y la adquisición de credenciales para hacerse con el control de cuentas, aprovechando las vulnerabilidades a lo largo del ciclo de vida del consumidor. Dependiendo del éxito del ataque inicial, los estafadores pueden emplear ataques adicionales para superar la autenticación multifactorial, o utilizar tácticas como el cultivo de cuentas sintéticas o el lavado de crédito para resucitar perfiles de identidad solventes.

Durante el último año, hemos visto cómo esta cadena de suministro se ha especializado mucho. Los delincuentes han centrado sus hackeos y estafas en acceder a credenciales de alto valor para llevar a cabo planes de fraude específicos. A esto se suma la GenAI, la tecnología perfecta para potenciar los datos comprometidos y cometer fraudes, ya que permite crear identidades sintéticas, deepfakes y suplantaciones (de su organización o de la identidad de sus clientes) más creíbles.

El riesgo de identidad digital impulsado por los datos comprometidos de los consumidores

Adquisición

- Accesos no autorizados de datos
- Ataques de phishing
- Ataques de smishing
- Ataques de vishing
- Infecciones por malware
- Ingeniería social en centros de atención telefónica

Distribución

- Foros clandestinos
- Mercados de la web oscura

Preparación

- Creación de identidades sintéticas
- Prueba de credenciales
- Validación de credenciales
- Creación de deepfakes

Explotación

- Creación de nuevas cuentas
- Apropiación de cuentas
- Transacciones financieras
- Intercambio de SIM/apropiación de OTP

Refinamiento

- Lavado de crédito
- Cultivo de cuentas con identidades sintéticas
- Manipulación de perfiles

TENDENCIAS GLOBALES DE FRAUDE

Experiencias de fraude empresarial y al consumidor

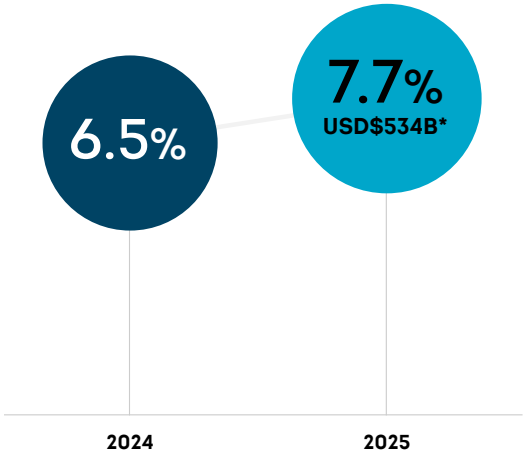
El costo del fraude aumentó a nivel mundial

Los líderes empresariales encuestados en Canadá, Hong Kong, India, Filipinas, Reino Unido y Estados Unidos informaron que sus empresas perdieron en promedio un 7.7% de sus ingresos en el último año debido al fraude, lo que supone un aumento con respecto al 6.5% registrado en 2024. Esto representa un total equivalente a USD$534 billones en pérdidas por fraude entre los 1200 líderes empresariales encuestados en 2025.

Casi una cuarta parte (24%) de los líderes empresariales citaron las estafas y los fraudes autorizados como la causa más destacada de las pérdidas por fraude, seguidas de la apropiación de cuentas y el fraude de identidad sintética (20% cada uno). Más líderes empresariales informaron haber sufrido más fraudes durante el último año. Cuando se les preguntó en qué medida habían aumentado los distintos tipos de fraude durante el último año, el 82% respondió que todos los tipos de fraude medidos se mantuvieron igual o aumentaron durante el último año (frente al 75% en 2024), y más del 40% informó de un aumento del fraude en todas las categorías.

Costo total del fraude

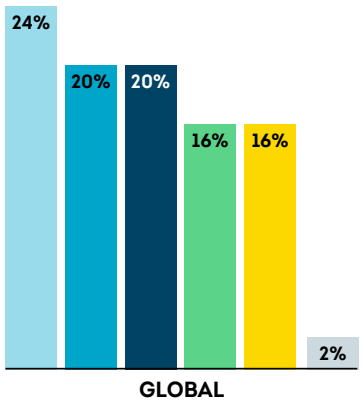
Los líderes empresariales indicaron el porcentaje de ingresos que sus empresas perdieron por fraude durante el último año y el importe total correspondiente entre los encuestados a nivel mundial.



*Conversión a USD basada en el valor de cambio de divisas del 16 de julio de 2025.
**No se muestra el total de 2024 debido a la diferencia en el número de empresas encuestadas a nivel mundial.

Fuente: Encuesta empresarial de TransUnion.

Causa más destacada de pérdidas por fraude



- **Estafa/fraude autorizado**
  Acción deshonesta destinada a engañar a una persona para que entregue algo de valor (por ejemplo, acceso a una cuenta, dinero, información).
- **Apropiación de cuentas**
  Personas no autorizadas que se apropian de la cuenta en línea de otra persona (por ejemplo, banca, redes sociales, correo electrónico) sin su permiso.
- **Fraude de identidad sintética**
  Uso de una combinación de información de identificación personal para fabricar una persona o entidad con el fin de cometer un acto deshonesto para obtener beneficios económicos o personales.
- **Fraude de primera mano**
  Falsificación de identidad o información con el fin de obtener beneficios económicos.
- **Fraude de tercera mano**
  Uso de una identidad robada para abrir una cuenta.
- **Otro**

Fuente: Encuesta empresarial de TransUnion

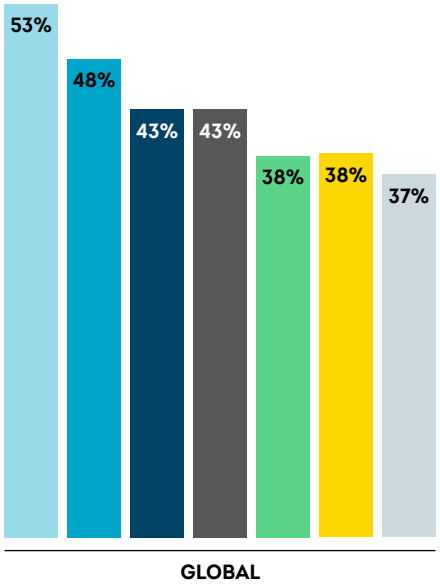
TransUnion

Las técnicas de prevención del fraude se basan en señales de identidad y dispositivos

Dado que el riesgo de estafas a los consumidores amenaza la integridad de la identidad, las organizaciones se basan en una combinación de datos, señales de riesgo, tecnología y herramientas para prevenir el fraude. Más de la mitad (53%) de los líderes empresariales encuestados clasificaron la verificación de identidad entre sus tres tecnologías principales para prevenir el fraude, seguidos por un 48% que clasificó la reputación de los dispositivos como la más eficaz.

Tecnología clasificada como la más eficaz para prevenir el fraude

Porcentaje de líderes empresariales que clasificaron estas tecnologías/ soluciones entre las tres más eficaces para prevenir el fraude.



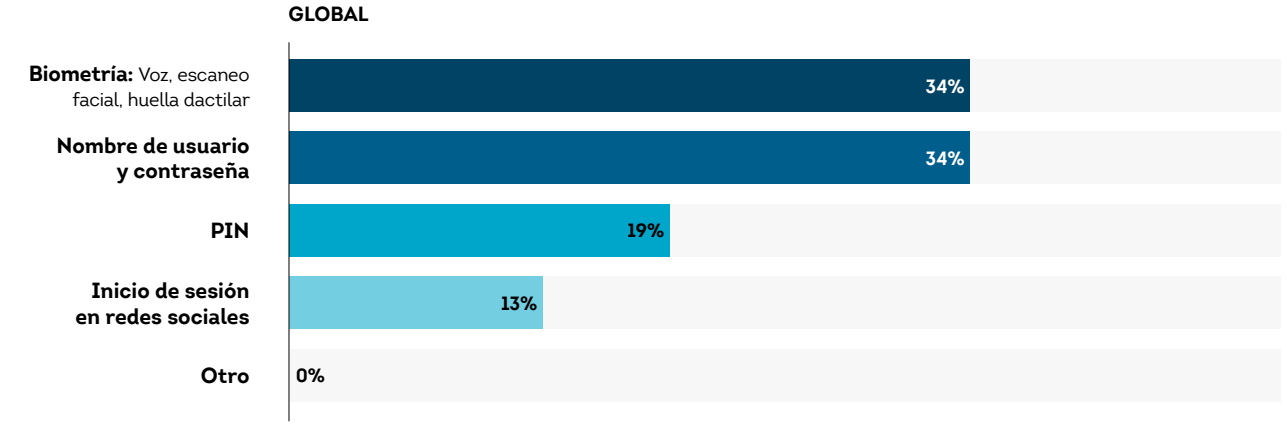
Fuente: Encuesta empresarial de TransUnion

La dependencia de las contraseñas para la autenticación de clientes está desapareciendo

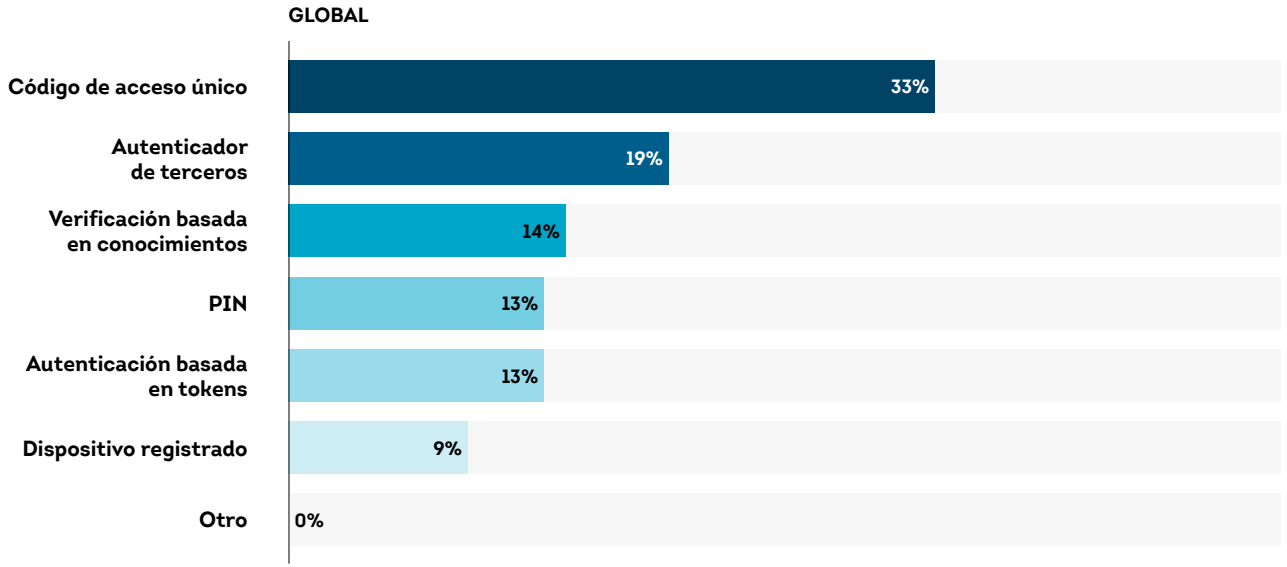
Las cuentas de usuario siguen estando amenazadas por las estafas a los consumidores y la suplantación de marcas. Las organizaciones parecen estar cambiando sus enfoques para incorporar un segundo factor en sus programas de autenticación como práctica habitual. Aunque más de un tercio (34%) de los líderes empresariales indicaron que utilizan nombres de usuario y contraseñas como método principal de autenticación de clientes, esto supone un descenso de cinco puntos porcentuales con respecto a 2024. Otro 34% informó que utiliza la biometría como método principal de autenticación de clientes, lo que supone un aumento de cinco puntos porcentuales con respecto a 2024.

En cuanto al segundo factor para la autenticación de clientes, los códigos de acceso de un solo uso (OTP) siguieron siendo los más populares: el 33% de los líderes empresariales indicaron que los utilizan, lo que supone un descenso con respecto al 35% de 2024. Las aplicaciones de autenticación de terceros quedaron en un distante segundo lugar, pero su uso declarado aumentó del 16% en 2024 al 19% en 2025.

Método principal utilizado para autenticar a los clientes



Método secundario utilizado para autenticar a los clientes



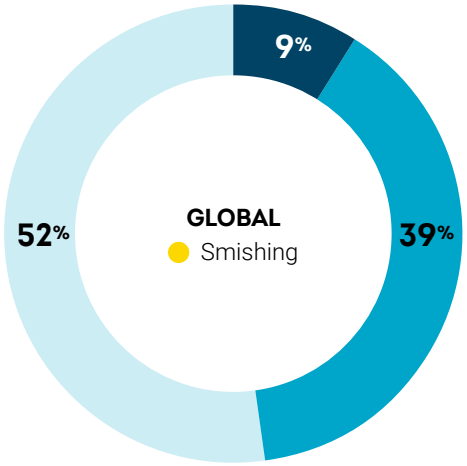
Fuente: Encuesta empresarial de TransUnion

Los consumidores denunciaron las estafas como el tipo de fraude más frecuente

Casi dos de cada cinco consumidores (39%) denunciaron haber sido víctimas de estafas por correo electrónico, Internet, teléfono o mensajes de texto entre febrero y mayo de 2025. Sin embargo, una parte significativa (52%) de la población afirmó no ser consciente de haber sido víctima de un fraude. Entre los que afirmaron haber sido víctimas, los principales tipos de fraude denunciados por los consumidores fueron el smishing (36%), el phishing (34%) y el vishing (33%).

Consumidores víctimas de fraude

Porcentaje de consumidores de 18 países y regiones que afirmaron haber sido víctimas de intentos de fraude por correo electrónico, Internet, llamadas telefónicas o mensajes de texto entre febrero y mayo de 2025, y el tipo de fraude más frecuente del que afirmaron haber sido víctimas.



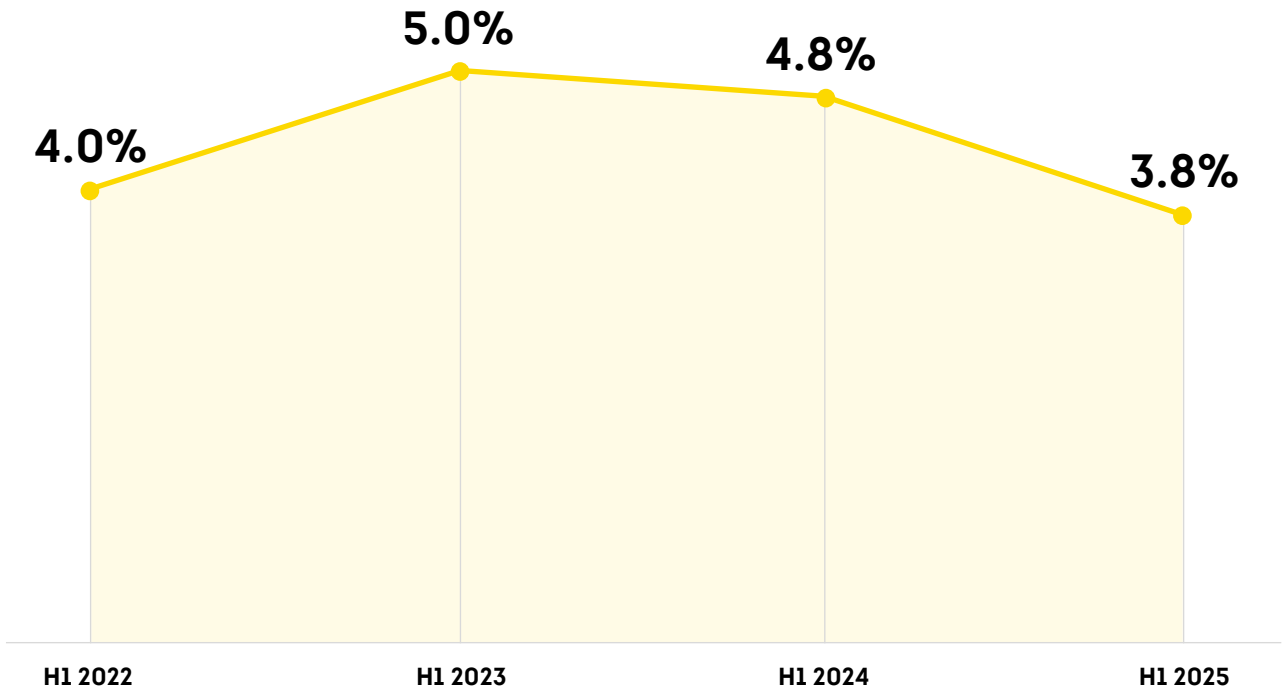
Fuente: Encuesta empresarial de TransUnion

Tendencias del Fraude Digital

Las tasas de fraude digital disminuyeron por segundo año consecutivo

Las tasas de fraude digital disminuyeron en la primera mitad del año. La tasa de presunto fraude digital a nivel mundial entre los clientes de soluciones antifraude de TransUnion cayó al 3.8% en el primer semestre de 2025, desde el 4.8% en el primer semestre de 2024 y el 5.0% en el primer semestre de 2023. Si bien las tasas de riesgo disminuyeron a nivel mundial, la República Dominicana (8.6%), India (8.4%) y Filipinas (4.4%) encabezaron la tasa mundial.

Tasa global de fraude digital sospechoso

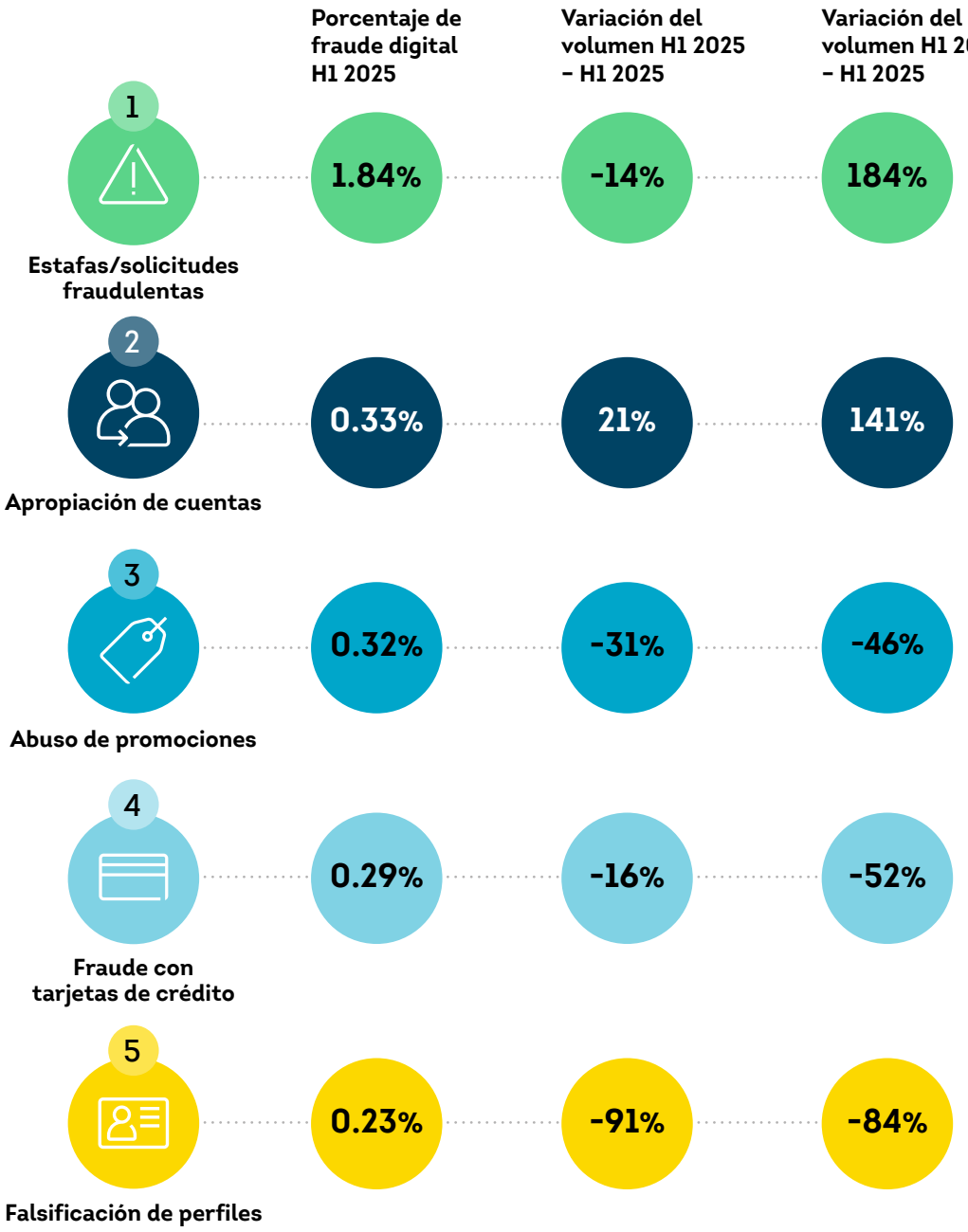


Fuente: Red de inteligencia global de TransUnion

El fraude por estafa/solicitud encabezó la lista de los tipos de fraude más comunes

Con un 1.8% de todos los tipos de fraude digital sospechoso denunciados a TransUnion por sus clientes en todo el mundo, el fraude por estafa/solicitud (una estafa destinada a engañar a una persona para que entregue algo de valor, es decir, acceso a una cuenta, dinero, información) fue el tipo de fraude digital más frecuente en el primer semestre de 2025. Sin embargo, la apropiación de cuentas (con un aumento del 21%) fue uno de los tipos de fraude digital que más creció en volumen entre el primer semestre de 2024 y el primer semestre de 2025. El fraude por estafa/solicitud (184%) fue el que más creció desde el primer semestre de 2021, según los clientes de TransUnion.

Principales tipos de fraude digital y su crecimiento a nivel global



Fuente: Red de inteligencia global de TransUnion

TransUnion

No es solo un juego de niños: los videojuegos registraron las tasas más altas de fraude digital

La industria de los videojuegos, que incluye los juegos en línea y para móviles, experimentó el mayor porcentaje (13.5%) de presuntos intentos de fraude digital a nivel mundial entre los sectores analizados en el primer semestre de 2025, lo que representa un aumento del 28% en la tasa y del 3% en el volumen de presuntos fraudes digitales en comparación con el primer semestre de 2024. El fraude por estafa/solicitud fue el tipo de fraude más denunciado por nuestros clientes de videojuegos.

Intentos de fraude digital a nivel mundial por sector

- **Índice de intentos de fraude sospechosos en el primer semestre de 2025**
- **Tipo de fraude más frecuente en el primer semestre de 2025**
- **Variación porcentual en el volumen de fraudes digitales sospechosos entre el primer semestre de 2024 y el primer semestre de 2025**

Videojuegos

H1 2025
13.5%
Estafador/solicitud

H1 2024 – H1 2025
+3%

Comunidades
(citas online, foros, etc.)

H1 2025
8.3%
Falsificación de perfiles

H1 2024 – H1 2025
-33%

Juegos
(apuestas en línea, póquer, etc.)

H1 2025
6.8%
Abuso de promociones

H1 2024 – H1 2025
+24%

Telecomunicaciones

H1 2025
4.4%
Estafadores/solicitudes

H1 2024 – H1 2025
+74%

Servicios financieros

H1 2025
3.3%
Apropiación de cuentas

H1 2024 – H1 2025
-20%

Comercio minorista

H1 2025
2.6%
Fraude con tarjetas de crédito

H1 2024 – H1 2025
-64%

Administración pública

H1 2025
2.3%
Fraude con tarjetas de crédito

H1 2024 – H1 2025
+52%

Logística

H1 2025
2.3%
Fraude en envíos

H1 2024 – H1 2025
-42%

Seguros

H1 2025
1.2%
Fraude en solicitudes de primera mano

H1 2024 – H1 2025
-47%

Viajes y ocio

H1 2025
0.2%
Fraude con tarjetas de crédito

H1 2024 – H1 2025
-56%

Fuente: Red de inteligencia global de TransUnion

El 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

Si analizamos el riesgo por etapas del ciclo de vida del consumidor, la creación de nuevas cuentas es motivo de especial preocupación, debido a que hay delincuentes que utilizan identidades sintéticas o robadas para abrir cuentas y cometer todo tipo de fraudes de primera mano. De todas las transacciones de creación de cuentas digitales a nivel mundial intentadas en el primer semestre de 2025 (que representan el 5% del volumen total de tráfico), TransUnion descubrió que el 8.3% eran sospechosas de fraude digital, lo que supone un aumento del 28% con respecto al primer semestre de 2024.

El riesgo de creación de cuentas dominó la mayoría de los sectores en el primer semestre de 2025, con la excepción de los servicios financieros, los seguros y la administración pública, donde las transacciones financieras eran las más arriesgadas. Las comunidades y las industrias del juego registraron las tasas más altas de presunto fraude digital durante la creación de cuentas entre los sectores analizados, con un 21.6% y un 20.0%, respectivamente.

Ejemplos de etapas del ciclo de vida del consumidor

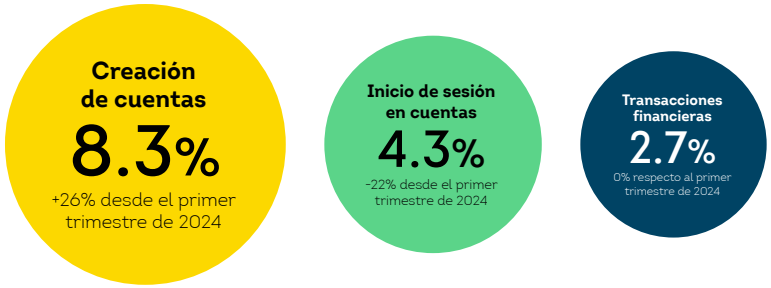
Creación de cuentas: registro de cuentas, inscripción y concesión de créditos.

Inicio de sesión en cuentas: inicio de sesión y eventos de inicio de sesión fallido.

Transacciones financieras: compras, retiradas y depósitos.

Riesgo de fraude en el ciclo de vida del consumidor digital

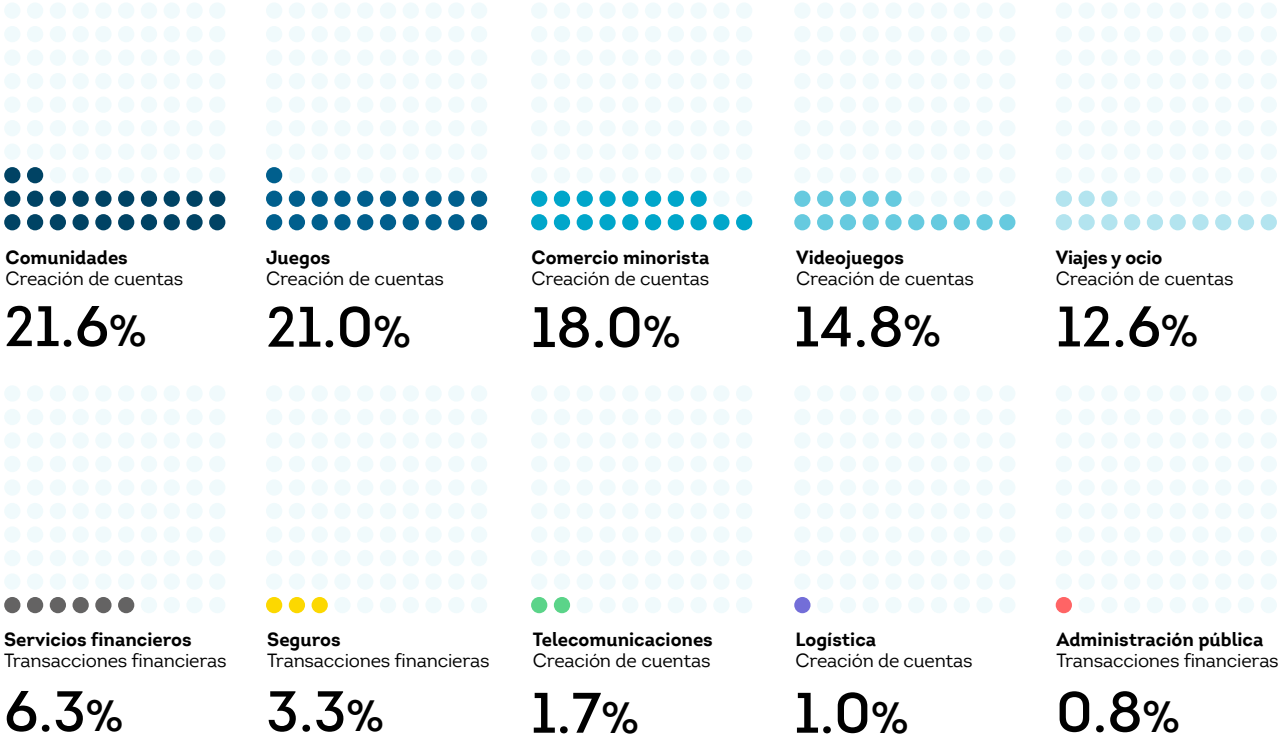
Porcentaje de cada tipo de transacción intentada que se sospecha que es fraude digital a nivel mundial en el primer semestre de 2025.



Fuente: Red de inteligencia global de TransUnion

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

Etapa del ciclo de vida del consumidor con la tasa más alta de sospecha de fraude digital por sector y porcentaje correspondiente en esa etapa a nivel mundial en el primer semestre de 2025.



Fuente: Red de inteligencia global de TransUnion

TransUnion

AMÉRICA LATINA

Panorama general de América Latina

Gracias a las inversiones que las empresas han realizado, y siguen realizando, en estrategias destinadas a establecer la identidad y mitigar el fraude en toda nuestra región, la tasa de intentos de fraude digital sospechosos ha disminuido en las transacciones en las que el consumidor se encontraba en todos los países latinoamericanos que analizamos, excepto en Puerto Rico, donde aumentó un pequeño 2% en la primera mitad del año en comparación con el mismo período de 2024. Sin embargo, se sigue observando un alto porcentaje de transacciones sospechosas en la creación de nuevas cuentas a través de canales digitales.

Los consumidores siguen siendo tanto objetivos como víctimas de diversos esquemas de fraude, y los latinoamericanos que encuestamos informaron que el smishing y el vishing son los más frecuentes. Por lo tanto, las estrategias de prevención del fraude deben seguir centrándose en el consumidor, haciendo hincapié en la protección de la información personal y las credenciales. Esto debe lograrse mediante campañas sostenidas de educación y sensibilización destinadas a mitigar esquemas como la apropiación de cuentas.

Los datos latinoamericanos de esta sección combinan información propia sobre el fraude digital procedente de la red de inteligencia global de TransUnion en Brasil, Chile, Colombia, Costa Rica, República Dominicana, El Salvador, Guatemala, Honduras, México, Nicaragua y Puerto Rico, y una encuesta a consumidores en Brasil, Chile, Colombia, República Dominicana y Guatemala.

PRINCIPALES HALLAZGOS

Objetivo a la vista: los consumidores siguen expuestos a estafas fraudulentas

34%
de los consumidores de los países latinoamericanos que participaron en nuestra encuesta afirmaron haber sido víctimas de estafas por correo electrónico, Internet, teléfono y mensajes de texto entre febrero y mayo de 2025, siendo Chile y Colombia los países con las tasas más altas.

34%
de los que afirmaron haber sido víctimas en Latinoamérica declararon haber sufrido ataques de vishing, lo que lo convierte en la estafa más citada en la región.

Intentos implacables: transacciones sospechosas sin cesar

11%
aumento en la tasa de presuntos fraudes digitales en intentos de transacciones financieras desde países latinoamericanos analizados en el primer semestre de 2025 en comparación con el primer semestre de 2024.

5%
de los intentos de creación de cuentas digitales desde países latinoamericanos analizados sospechosos de ser fraudes digitales en el primer semestre de 2025.

El coste sigue siendo elevado: los estafadores persisten en aprovechar las oportunidades

25%
de los ejecutivos empresariales encuestados informó de que sus empresas perdieron el equivalente al 10% o más de sus ingresos en el último año.

42%
de los ejecutivos empresariales encuestados creía que los ataques de apropiación de cuentas comienzan en línea, seguidos por un 20% que indicaba que comienzan con aplicaciones móviles.

Experiencias de fraude al consumidor

Los estafadores se dirigen a los consumidores a través de sus canales preferidos.

Los estafadores se dirigen a los consumidores a través de sus canales preferidos. Si bien más de un tercio (34%) de los consumidores encuestados en América Latina informaron haber sido víctimas de un fraude por correo electrónico, Internet, llamada telefónica o mensaje de texto en los últimos tres meses (por debajo de la tasa global del 48%), es posible que una parte significativa de la población no reconozca un posible fraude: el 66% afirmó no saber que había sido víctima de un fraude.

Entre los que afirmaron haber sido víctimas, el vishing (34%) y el smishing (31%) fueron los principales tipos de fraude que los consumidores declararon haber sufrido en los últimos tres meses.

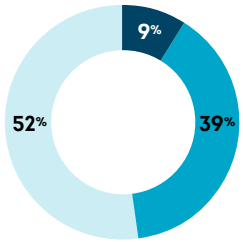
Aunque los delincuentes atacan en cualquier momento y a través de cualquier canal, parecen centrarse en los canales más populares. En Chile y Colombia, donde las suscripciones a teléfonos móviles son más elevadas que en otros países de América Latina,1 el vector de ataque más común declarado por los consumidores fue el vishing.

Grupo del Banco Mundial: Suscripciones de telefonía móvil (por cada 100 personas) – Colombia, Chile, República Dominicana, Brasil y Guatemala | Datos

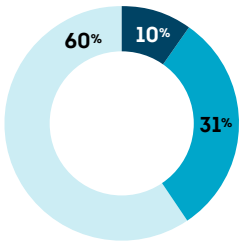
Consumidores víctimas de fraude

Porcentaje de consumidores que afirmaron haber sido víctimas de intentos de fraude por correo electrónico, Internet, llamadas telefónicas o mensajes de texto entre febrero y mayo de 2025, y la estafa más frecuente de la que informaron haber sido víctimas.

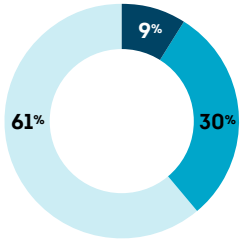
- **Víctimas de estafa**
- **Víctimas de estafa, pero no de fraude**
- **No víctimas de estafa**
- **Estafa más denunciada**



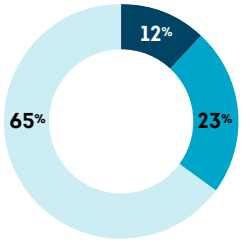
GLOBAL
- Smishing



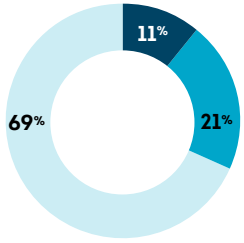
CHILE
- Vishing



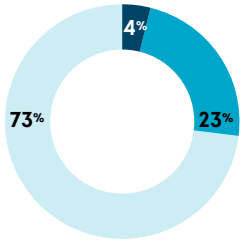
COLOMBIA (TIE)
- Smishing
- Vishing



GUATEMALA (TIE)
- Dinero/tarjeta regalo
- Estafas de vendedores externos en sitios web legítimos



REPÚBLICA DOMINICANA (TIE)
- Dinero/tarjeta regalo
- Estafas de vendedores externos en sitios web legítimos



BRASIL
- Vishing

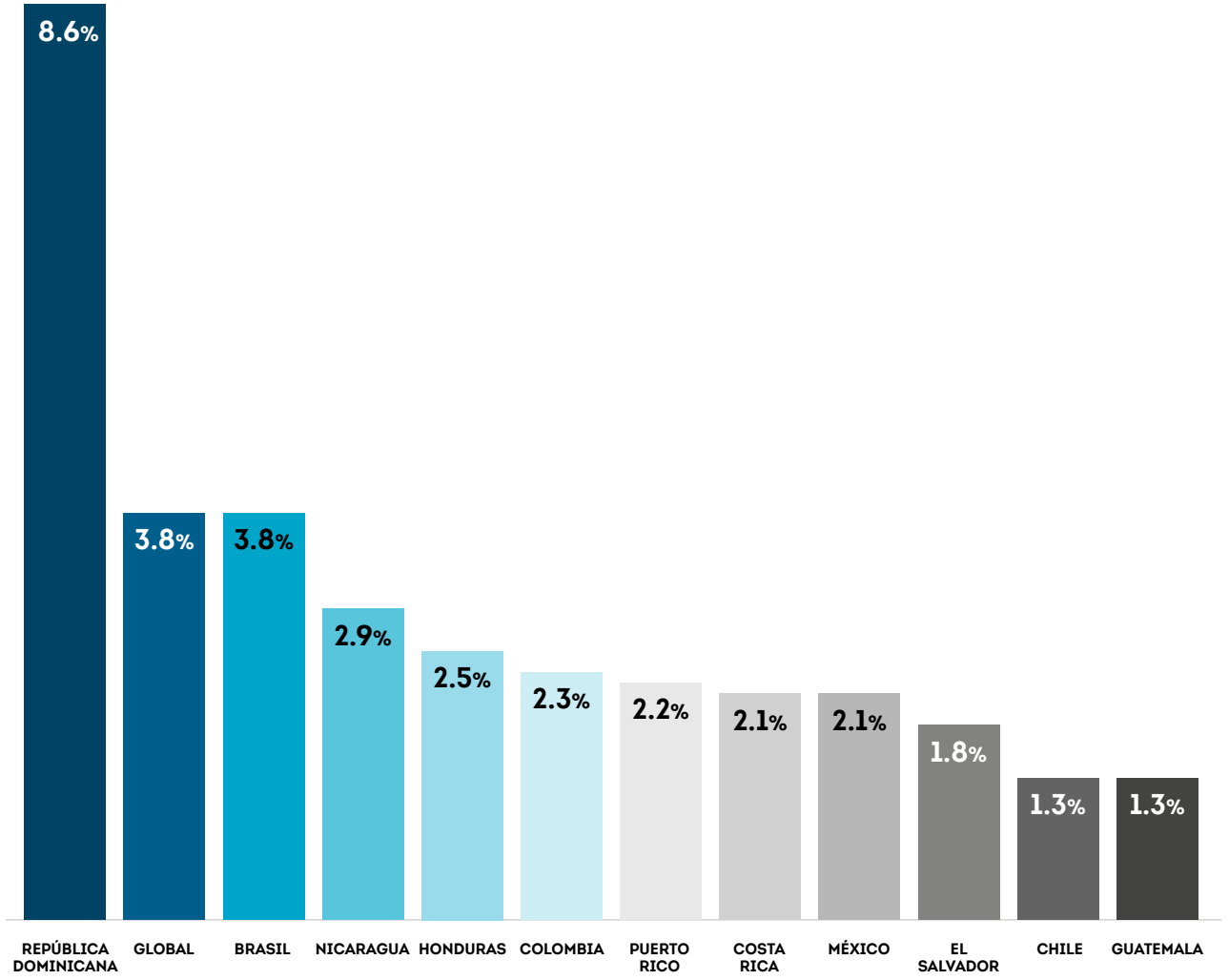
Fuente: Encuesta a consumidores de TransUnion

Tendencias de fraude digital

Las tasas de presunto fraude digital se estabilizaron, siendo más altas en los principales mercados latinoamericanos

La tasa global de presuntos intentos de fraude digital entre los clientes de TransUnion se mantuvo por debajo del 5% en el primer semestre de 2025, registrando un 3.8%. Esto refleja la eficacia continuada de las estrategias de prevención del fraude en los principales mercados. En los mercados latinoamericanos que analizamos, tres mercados (Brasil, República Dominicana y Nicaragua) registraron tasas superiores al promedio regional del 2.8%, lo que pone de relieve la necesidad de intensificar los esfuerzos de mitigación del fraude en estas zonas geográficas. Estos niveles elevados sugieren que los estafadores se están centrando activamente en mercados específicos en los que aún pueden existir vulnerabilidades.

Tasa de sospechas de fraude digital
H1 2025



Fuente: Red de inteligencia global de TransUnion

Ciertos sectores son blanco de los estafadores en algunos países

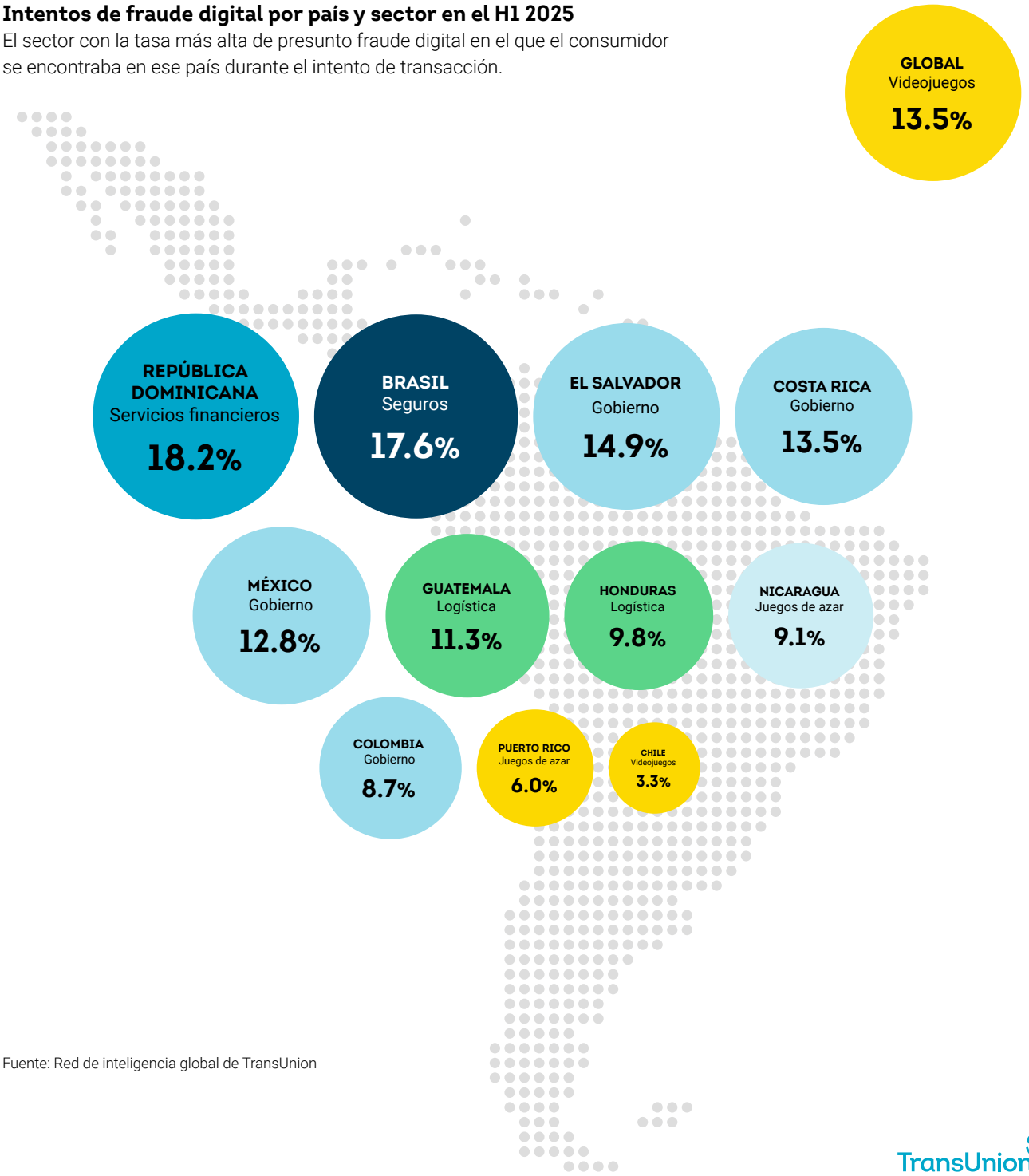
Entre las industrias analizadas a nivel mundial, el sector de los videojuegos registró el mayor porcentaje de presuntos intentos de fraude digital en el primer semestre de 2025, alcanzando el 13.5%. Esto representa un aumento significativo del 28% en volumen en comparación con el mismo período de 2024, lo que pone de relieve la creciente vulnerabilidad de este sector a las actividades fraudulentas.

En América Latina, algunas industrias específicas dentro de mercados individuales también mostraron elevadas tasas de fraude. Por ejemplo, en las transacciones en las que el consumidor se encontraba en la República Dominicana, el sector de los servicios financieros registró la tasa más alta (18.2%) de presuntos fraudes digitales entre las industrias analizadas en el primer semestre de 2025. En Brasil, el sector de los seguros lideró la lista con una tasa del 17.6%. Estas cifras ponen de relieve la necesidad de estrategias específicas de prevención del fraude dentro de estos sectores verticales.

En muchos otros países analizados de la región, el sector gubernamental registró la tasa más alta, con un aumento medio del 80% en comparación con el primer semestre de 2024 en América Latina. Esta tendencia refleja los continuos esfuerzos de los estafadores por explotar los sectores que manejan datos personales sensibles.

Intentos de fraude digital por país y sector en el H1 2025

El sector con la tasa más alta de presunto fraude digital en el que el consumidor se encontraba en ese país durante el intento de transacción.



Fuente: Red de inteligencia global de TransUnion

Las identidades de riesgo afectan a todas las etapas del ciclo de vida del consumidor

El fraude basado en la identidad, impulsado por la gran cantidad de identidades expuestas y por ciberdelincuentes cada vez más sofisticados, sigue creciendo. Los delincuentes tienen la capacidad de atacar en todas partes, al mismo tiempo.

La creación de cuentas fue la que experimentó un mayor crecimiento en el riesgo de fraude a lo largo del ciclo de vida del consumidor digital, con un aumento del 26% a nivel mundial entre el primer semestre de 2024 y el primer semestre de 2025. En las transacciones en las que el consumidor se encontraba en América Latina, la creación de cuentas se reveló como el tipo de transacción digital más arriesgado, con un 5% de esos tipos de transacciones sospechosas de ser intentos de fraude digital. La creación de cuentas también fue el tipo de transacción más arriesgado en el ciclo de vida del consumidor, con una tasa global del 8.3%.

Costa Rica y la República Dominicana lideraron la región entre los países analizados en cuanto al riesgo de fraude en la creación de cuentas, con tasas del 10.6% y el 14.2%, respectivamente. Estas tendencias ponen de relieve la creciente necesidad de contar con estrategias sólidas de verificación de identidad y prevención del fraude en las primeras etapas de la interacción digital.

Ejemplos de etapas del ciclo de vida del consumidor

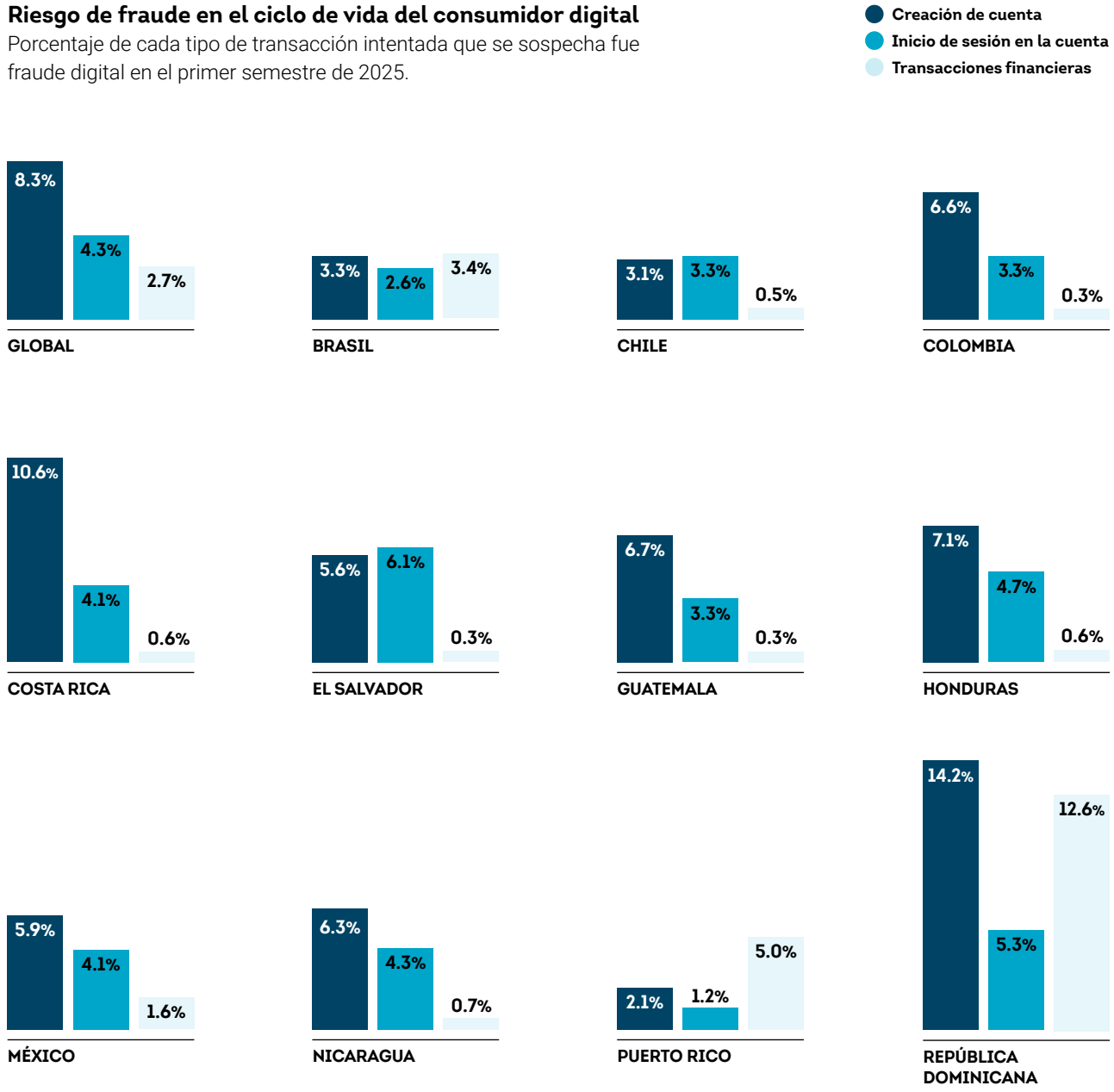
Creación de cuentas: registro de cuentas, inscripción y concesión de préstamos

Inicio de sesión en cuentas: inicio de sesión y eventos de inicio de sesión fallido

Transacciones financieras: compras, retiradas y depósitos

Riesgo de fraude en el ciclo de vida del consumidor digital

Porcentaje de cada tipo de transacción intentada que se sospecha fue fraude digital en el primer semestre de 2025.



Fuente: Red de inteligencia global de TransUnion

NORTE AMÉRICA

Panorama general de Estados Unidos

Las estafas son cada vez más sofisticadas, y Estados Unidos es un entorno muy atractivo para los delincuentes. Los líderes en prevención del fraude de Estados Unidos reconocen el riesgo y la urgencia de reforzar sus defensas para mantenerse al día, ya que cada vez más negocios se realizan en línea. No es una tarea fácil. Las identidades comprometidas por los constantes accesos no autorizados de datos y las estafas a los consumidores aumentan el riesgo a lo largo del ciclo de vida del consumidor. En la primera mitad de 2025, este problema se manifestó de muchas maneras. Los líderes empresariales estadounidenses identificaron el fraude por apropiación de cuentas (ATO) como la principal causa de las pérdidas por fraude. Dadas las estafas de robo de identidad a las que se enfrentan los consumidores, junto con su preferencia por métodos de autenticación de cuentas más vulnerables, las cuentas de los clientes serán el principal objetivo de los ataques.

Al mismo tiempo, la creación de cuentas era la etapa más arriesgada del ciclo de vida del consumidor digital, y no es de extrañar. Con el uso de herramientas GenAI, los estafadores pueden crear identidades sintéticas creíbles. Estas identidades, completas con documentos falsificados, historiales crediticios legítimos y cuentas online manipuladas, son difíciles de distinguir de las personas reales. Dada la cantidad de datos de consumidores que se obtienen a partir de los accesos no autorizados de datos y estafas a consumidores en Estados Unidos., cada vez es más difícil ver claramente el riesgo de la identidad digital.

PRINCIPALES HALLAZGOS

Aumenta el coste del fraude para las organizaciones

9.8%
de ingresos equivalentes perdidos de media debido al fraude, un 46% más que en 2024, lo que representa USD$114 billones en pérdidas por fraude durante el último año entre los 200 líderes empresariales encuestados en Estados Unidos.

USD$2.7 billones
en exposición de los prestamistas a identidades sintéticas sospechosas para préstamos para automóviles, tarjetas de crédito bancarias, tarjetas de crédito minoristas y préstamos personales sin garantía en Estados Unidos.

La cadena de suministro de identidades robadas alimenta un fraude más sofisticado

77%
de los accesos no autorizados de datos en Estados Unidos incluyeron el número completo de la Seguridad Social en el primer semestre de 2025, lo que supone un aumento del 8% con respecto al primer semestre de 2024 y un máximo histórico desde que TransUnion comenzó a informar sobre ello en 2020.

51%
de los consumidores estadounidenses denunció haber sido objeto de fraudes por correo electrónico, Internet, llamadas telefónicas y mensajes de texto, principalmente phishing, smishing y vishing diseñados para robar credenciales de identidad, entre febrero y mayo de 2025.

La creación de cuentas supuso el mayor riesgo de fraude en todo el ciclo de vida del consumidor

4.2%
de todos los intentos de creación de cuentas digitales en Estados Unidos fueron sospechosos de fraude digital; esta fue la etapa de mayor riesgo en el ciclo de vida del consumidor, y superior a la tasa global de sospecha de fraude digital del 3.5% para todas las transacciones en Estados Unidos.

47%
de los líderes empresariales estadounidenses encuestados identificaron los nuevos tipos de fraude en cuentas nuevas (identidad propia, de terceros y sintética) como las principales fuentes de pérdidas por fraude en el último año.

Experiencias de fraude empresarial y al consumidor

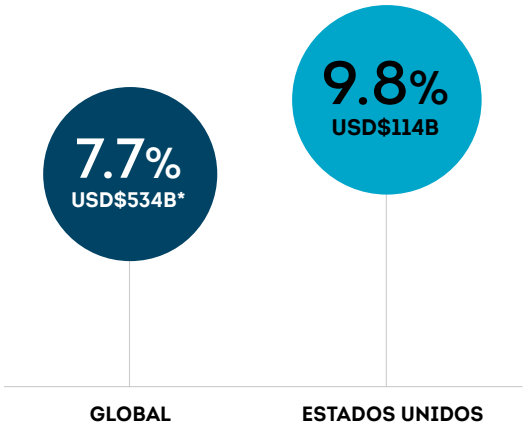
El coste del fraude aumenta

Reducir la exposición a las pérdidas por fraude es una función clave de los responsables de riesgos de fraude. Sus homólogos encuestados en Estados Unidos informaron de que sus empresas perdieron (de media) el equivalente al 9.8% de sus ingresos debido al fraude durante el último año. Esto supone un aumento del 46% con respecto a 2024. Los responsables estadounidenses también informaron de que las pérdidas por fraude como porcentaje de los ingresos eran un 27% superiores a la media mundial del 7.7%. En Estados Unidos, eso representa un total de USD$114 billones en pérdidas por fraude entre los 200 responsables empresariales encuestados.

Casi un tercio (31%) de los líderes empresariales estadounidenses citaron el ATO como la causa más destacada de las pérdidas por fraude notificadas, seguido del fraude de identidad sintética (24%) y la estafa/fraude autorizado (23%).

Coste total del fraude

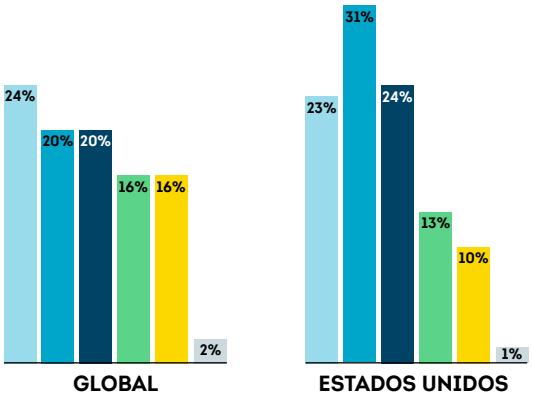
Los líderes empresariales indicaron el porcentaje de ingresos que sus empresas perdieron por fraude durante el último año y el importe monetario total correspondiente.



*Conversión a USD basada en el tipo de cambio del 16 de julio de 2025.

Fuente: Encuesta empresarial de TransUnion.

Causa más destacada de las pérdidas por fraude



- **Estafa/fraude autorizado**
  Acción deshonesta destinada a engañar a una persona para que entregue algo de valor (por ejemplo, acceso a una cuenta, dinero, información).
- **Apropiación de cuentas**
  Personas no autorizadas que se apropian de la cuenta en línea de otra persona (por ejemplo, banca, redes sociales, correo electrónico) sin su permiso.
- **Fraude de identidad sintética**
  Uso de una combinación de información de identificación personal para fabricar una persona o entidad con el fin de cometer un acto deshonesto para obtener beneficios económicos o personales.
- **Fraude de primera mano**
  Falsificación de identidad o información con el fin de obtener beneficios económicos.
- **Fraude de tercera mano**
  Uso de una identidad robada para abrir una cuenta.
- **Otro**

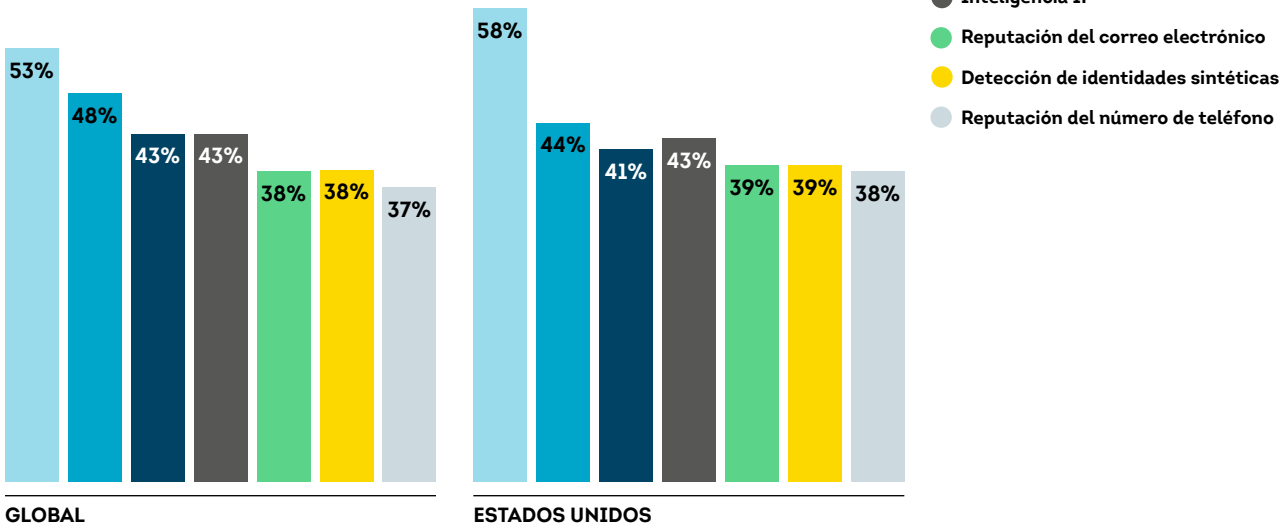
Fuente: Encuesta empresarial de TransUnion

La verificación de identidad se sitúa como la tecnología más eficaz para combatir el fraude

La verificación de identidad sigue siendo la piedra angular de la tecnología de prevención del fraude en Estados Unidos. Más de la mitad (58%) de los líderes empresariales estadounidenses encuestados situaron la verificación de identidad entre las tres tecnologías más eficaces para prevenir el fraude. Tras la verificación de identidad, la reputación de los dispositivos (44%), la inteligencia IP (43%) y la biometría conductual (41%) se situaron como las más eficaces.

Tecnología clasificada como la más eficaz para prevenir el fraude

Porcentaje de líderes empresariales que clasificaron estas tecnologías/ soluciones entre las tres más eficaces para prevenir el fraude.



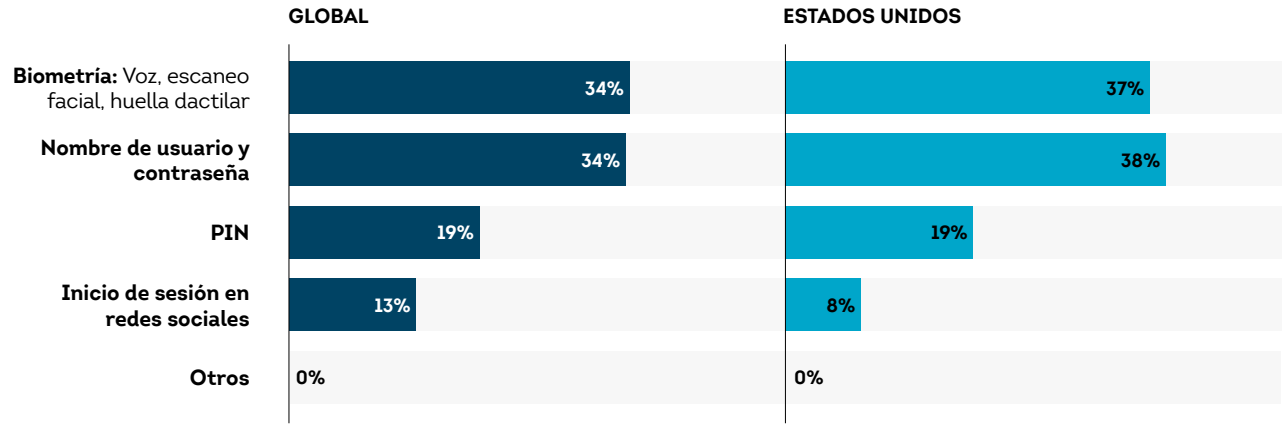
Fuente: Encuesta empresarial de TransUnion

La biometría alcanza a las contraseñas como método principal de autenticación

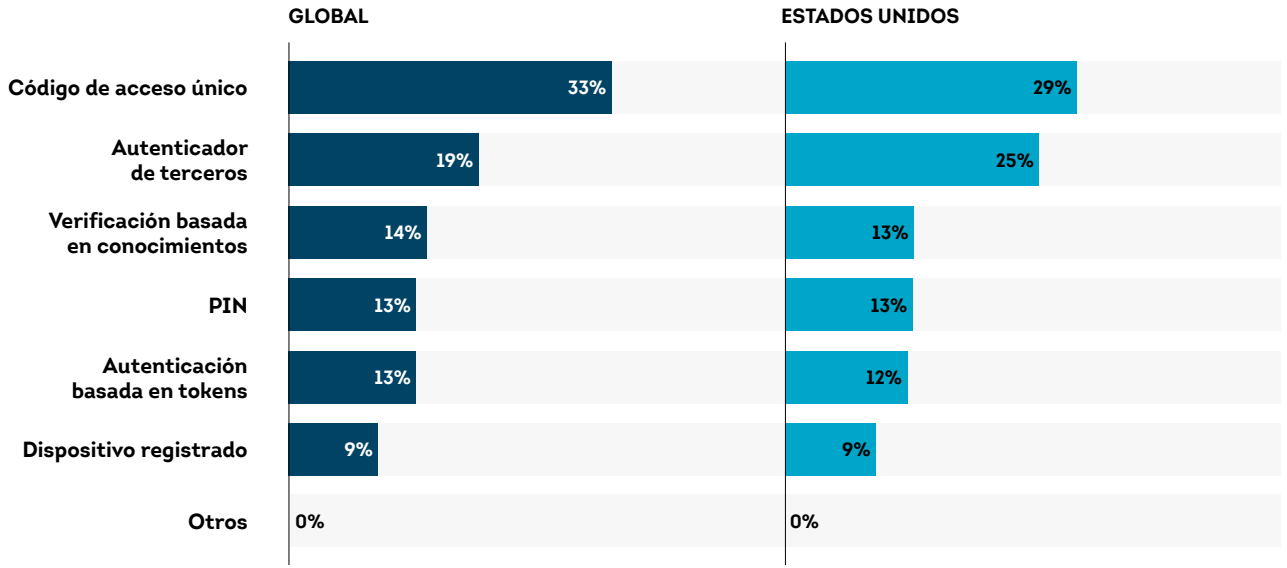
Las credenciales de los usuarios siguen estando amenazadas por las estafas a los consumidores y los accesos no autorizados de datos. No es de extrañar que los líderes empresariales estadounidenses hayan señalado el ATO como la principal causa de las pérdidas por fraude. Para frenar esta tendencia, los líderes empresariales estadounidenses parecen estar abandonando la autenticación mediante nombre de usuario y contraseña para incorporar la verificación biométrica en sus programas de autenticación. Aunque más de un tercio (38%) de los líderes empresariales estadounidenses afirman que siguen utilizando nombres de usuario y contraseñas como método principal de autenticación de clientes, esta cifra supone un descenso del 14% con respecto a 2024. Otro 37% afirmó utilizar la biometría como método principal de autenticación de clientes, lo que supone un aumento del 42% con respecto a 2024.

Los códigos de acceso de un solo uso siguieron siendo el segundo factor más popular para la autenticación de clientes, con un 29% de los líderes empresariales estadounidenses indicando que los utilizan, lo que supone un descenso con respecto al 35% de 2024. Las aplicaciones de autenticación de terceros (el segundo factor más popular para la autenticación de clientes, según los líderes empresariales estadounidenses) aumentaron su uso declarado del 20% en 2024 al 25% en 2025.

Principal método utilizado para autenticar a los clientes



Método secundario utilizado para autenticar a los clientes



Fuente: Encuesta empresarial de TransUnion

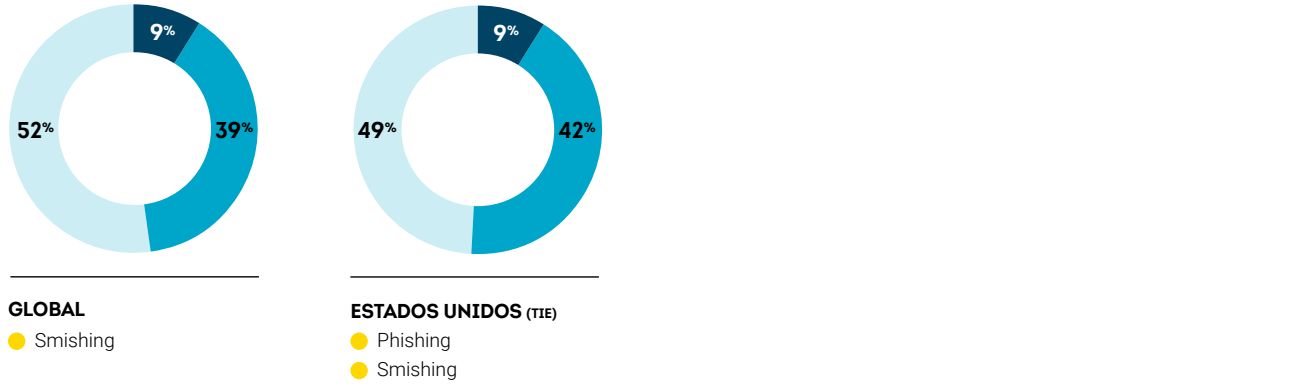
El phishing y el smishing empataron como los fraudes más comunes denunciados por los consumidores

Más de la mitad (51%) de los consumidores estadounidenses denunciaron haber sido víctimas de un fraude por correo electrónico, internet, llamada telefónica o mensaje de texto, y el 9% afirmó haberlo sufrido entre febrero y mayo de 2025. Sin embargo, una parte significativa de la población no reconoció el posible fraude: el 49% afirmó no ser consciente de haber sido víctima de un fraude.

El phishing (correos electrónicos, sitios web, publicaciones en redes sociales, códigos QR, etc. fraudulentos destinados a robar datos) y el smishing (mensajes de texto fraudulentos destinados a engañar a alguien para que revele datos) fueron denunciados por el 46% de los consumidores estadounidenses que afirmaron haber sido víctimas de fraude, lo que los convierte en los principales tipos de fraude que han sufrido.

Consumidores víctimas de fraude

Porcentaje de consumidores que afirmaron haber sido víctimas de intentos de fraude por correo electrónico, Internet, teléfono o mensajes de texto entre febrero y mayo de 2025, y el tipo de fraude más frecuente del que afirmaron haber sido víctimas.



Fuente: Encuesta a consumidores de TransUnion

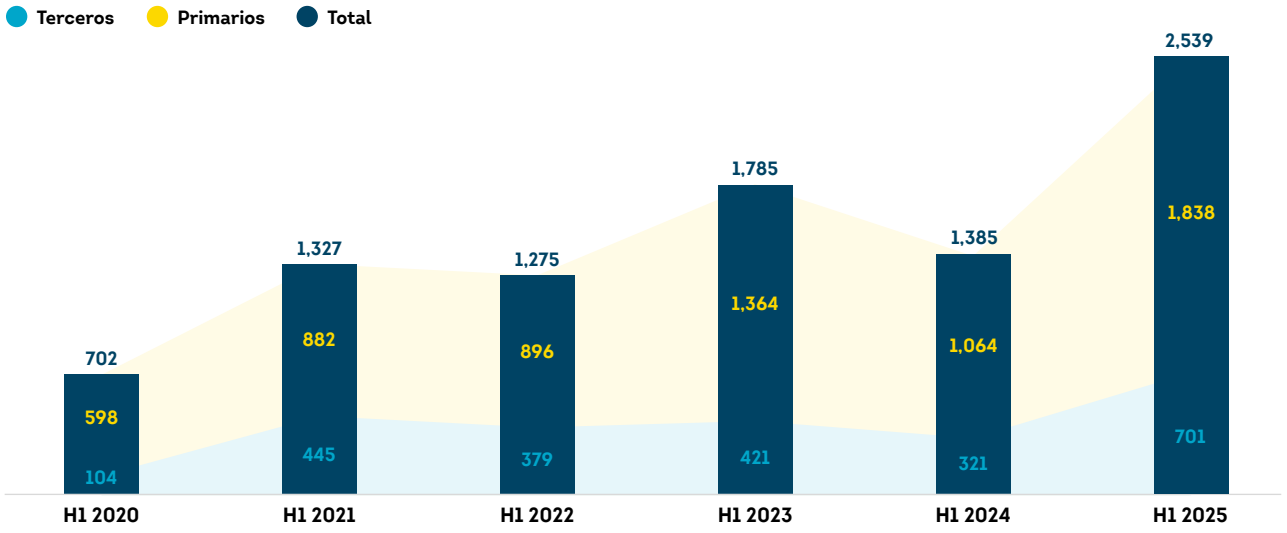
Tendencias en la exposición de datos de identidad

El número y la gravedad de accesos no autorizados de datos en Estados Unidos alcanzan niveles récord

Los delincuentes siguen cambiando sus ataques frente a los accesos no autorizados de datos para recopilar credenciales de alta calidad. Con ataques más frecuentes dirigidos a menos personas por incidente, Estados Unidos experimentó un aumento del 83% en el volumen de accesos no autorizados de datos en la primera mitad de 2025 en comparación con el mismo periodo de 2024, y el nivel más alto durante el periodo medido. Sin embargo, el número medio de personas afectadas por cada acceso no autorizado de datos se redujo a 301 en el primer semestre de 2025, en comparación con las 616 del mismo periodo de 2024, y por debajo del máximo de seis años de 5278 registrado en 2022. Estos ataques pueden buscar datos que no están fácilmente disponibles para los delincuentes que utilizan el mercado de datos de la web oscura para obtener datos de identidad con fines fraudulentos. También concuerda con las estafas de fraude al consumidor que se denuncian con frecuencia, como el smishing, el phishing y el vishing.

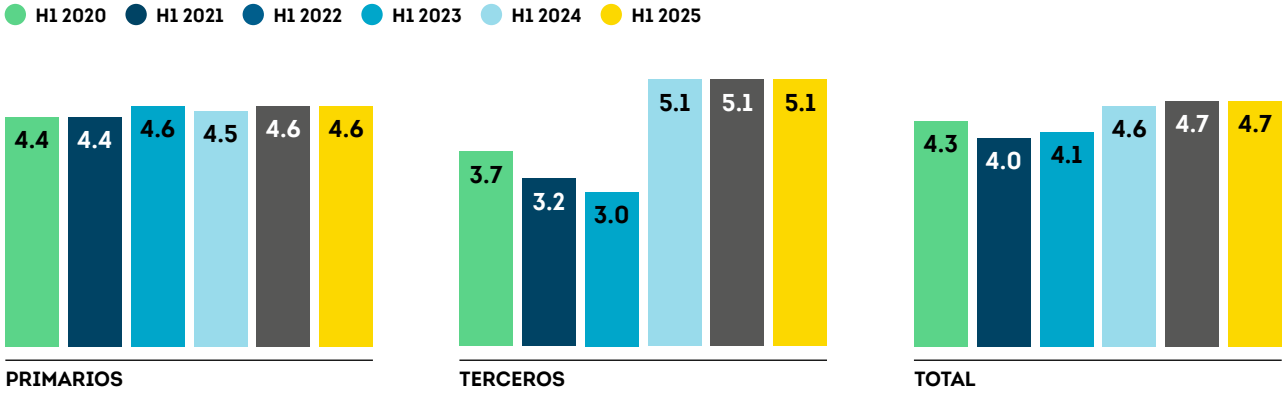
Debido a que se dirigen a credenciales de alto riesgo, como los números de la Seguridad Social, la gravedad media de los accesos no autorizados de datos (la capacidad de esta acción para permitir el fraude de identidad), medida por el TransUnion TruEmpower™ Breach Risk Score (BRS), un indicador adelantado de fraude futuro se mantuvo en el nivel más alto en el periodo examinado. Los accesos no autorizados de seguridad de terceros que implicaban ataques a organizaciones que prestan servicios comerciales a marcas siguieron siendo significativamente más riesgosas que las dirigidas a organizaciones orientadas al consumidor.

Volumen de accesos no autorizados de datos en Estados Unidos



Fuente: Red de inteligencia global de TransUnion

Puntuación media de riesgo de accesos no autorizados de datos en Estados Unidos



Fuente: Red de inteligencia global de TransUnion

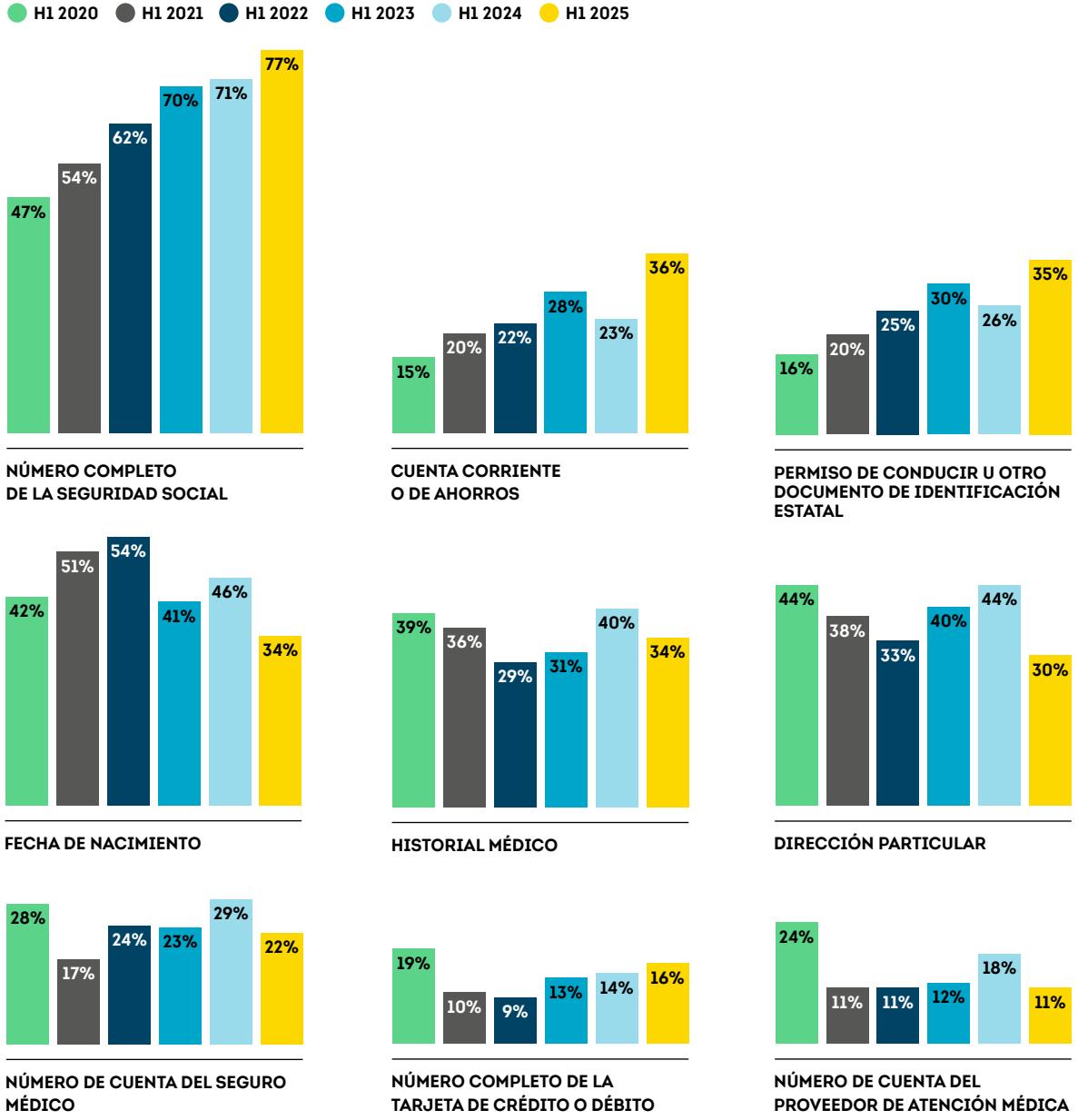
Un acceso no autorizado de datos primarios representa un ataque directo a una organización. Mientras que un acceso no autorizado de datos de terceros, también conocido como ataque a la cadena de suministro, ataque a la cadena de valor, se produce cuando un atacante accede a la red de una entidad a través de proveedores o distribuidores externos, por ejemplo, el procesamiento de nóminas o la facturación médica.

Credenciales de identidad de alto valor priorizadas por los delincuentes

En la primera mitad de 2025, los delincuentes parecían centrarse en credenciales de alto valor para cometer fraudes y estafas a los consumidores en el futuro. TransUnion descubrió que los números completos de la Seguridad Social quedaron expuestos en el 77% de los accesos no autorizados de datos en Estados Unidos durante el primer semestre de 2025 (un aumento del 8% con respecto al primer semestre de 2024 y el punto más alto de esta investigación), lo que podría facilitar el fraude de identidad para crear nuevas cuentas, obtener reembolsos fiscales y prestaciones gubernamentales, entre otros. La exposición de datos de cuentas corrientes y de ahorro mostró un crecimiento significativo, pasando del 23% en el primer semestre de 2024 al 36%, lo que podría dar lugar a más fraudes ATO o ACH/pagos. La exposición de datos de permisos de conducir también aumentó del 26% en el primer semestre de 2024 al 35% en el primer semestre de 2025, lo que podría alimentar los deepfakes de documentos de identificación generados por IA.

Las 10 credenciales de identidad más expuestas en los accesos no autorizados de datos en Estados Unidos en el primer semestre de 2025

Porcentaje de credenciales expuestas en un acceso no autorizado de datos



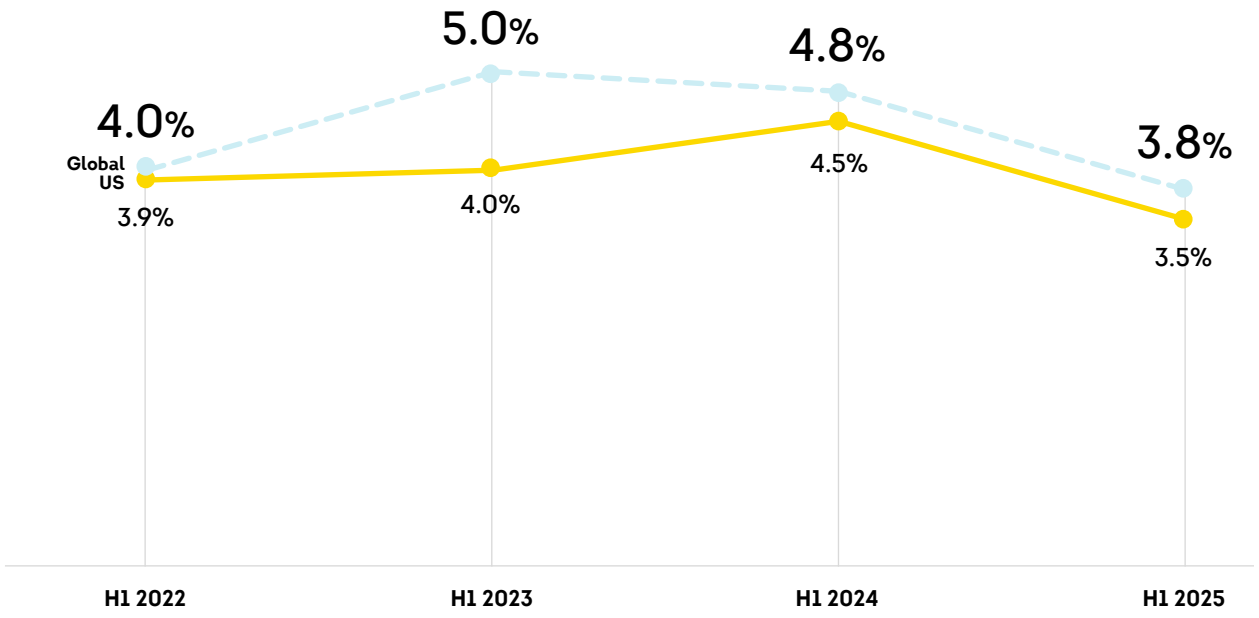
Fuente: Red de inteligencia global de TransUnion

Tendencias del Fraude Digital

La tasa de sospechas de fraude digital desciende

El riesgo de fraude digital en Estados Unidos cayó en la primera mitad del año por primera vez en tres años en el primer semestre de 2025. La tasa de sospechas de fraude digital en transacciones intentadas en las que el consumidor se encontraba en Estados Unidos cayó al 3.5% en el primer semestre de 2025, tras alcanzar un máximo del 4.5% en el primer semestre de 2024. Esta cifra fue ligeramente inferior a la media mundial del 3.8% en el primer semestre de 2025. Es muy probable que la caída de la tasa de fraude digital se deba a una combinación de factores, como el aumento del uso de la autenticación multifactorial por parte de las organizaciones para frustrar los ataques de ATO y el mayor recelo de los consumidores hacia las estafas de phishing, vishing y smishing. Al mismo tiempo, las identidades comprometidas están propiciando ataques de fraude cada vez más sofisticados que seguirán representando un riesgo para su organización.

Tasa de presuntos fraudes digitales



Fuente: Red de inteligencia global de TransUnion

El sector de las comunidades experimentó el mayor riesgo de fraude digital

El sector de las comunidades, que incluye propiedades web como foros en línea y sitios de citas, experimentó el mayor porcentaje (13.7%) de presuntos fraudes digitales en transacciones intentadas en las que el consumidor se encontraba en Estados Unidos en el primer semestre de 2025. Esto representa un aumento del 139% en el volumen de presuntos fraudes digitales entre el primer semestre de 2022 y el primer semestre de 2025, y del 64% entre el primer semestre de 2024 y el primer semestre de 2025. Los usuarios de las comunidades en línea confían en que las organizaciones les proporcionen confianza y seguridad, protegiéndoles de los vendedores y otras estafas mientras utilizan sus plataformas. Quizás no sea sorprendente que los clientes de las comunidades de TransUnion informaran de la falsificación de perfiles y las estafas/solicitudes como los tipos más frecuentes de fraude digital que presenciaron en el primer semestre de 2025 a nivel mundial, lo que ilustra el valor de estas plataformas para los estafadores.

Intentos de fraude desde Estados Unidos por industria

- **Tasa de intentos de fraude sospechosos en el primer semestre de 2025**
- **Variación porcentual en el volumen de fraudes digitales sospechosos entre el primer semestre de 2024 y el primer semestre de 2025**

Comunidades
(citas online, foros, etc.)

H1 2025
13.7%

H1 2024-H1 2025
+64%

Juegos de azar
(apuestas en línea, póquer, etc.)

H1 2025
9.6%

H1 2024-H1 2025
-10%

Videojuegos

H1 2025
8.3%

H1 2024-H1 2025
-38%

Comercio minorista

H1 2025
3.5%

H1 2024-H1 2025
-46%

Servicios financieros

H1 2025
3.4%

H1 2024-H1 2025
-18%

Logística

H1 2025
1.9%

H1 2024-H1 2025
-70%

Administración pública

H1 2025
0.9%

H1 2024-H1 2025
+49%

Seguros

H1 2025
0.4%

H1 2024-H1 2025
-40%

Telecomunicaciones

H1 2025
0.4%

H1 2024-H1 2025
-32%

Viajes y ocio

H1 2025
0.2%

H1 2024-H1 2025
-35%

Fuente: Red de inteligencia global de TransUnion

Tendencias del Fraude en los Centros de Atención Telefónica

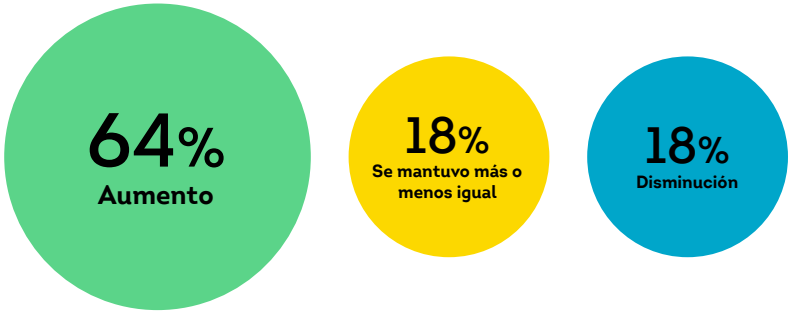
Las llamadas entrantes son arriesgadas debido al papel fundamental que desempeñan los centros de llamadas en la experiencia del cliente, ya que representan un punto de contacto de gran confianza para los consumidores. Entre los líderes empresariales estadounidenses encuestados, el 64% indicó que los estafadores aumentaron sus ataques a los centros de llamadas en el último año, frente al 44% en 2024. Más de la mitad de los líderes empresariales encuestados informaron de un aumento de las tácticas delictivas dirigidas a los centros de atención telefónica, incluidas las llamadas en las que se suplantaba la identidad de los consumidores y el uso de servicios de llamadas virtuales e información de identidad robada para superar las preguntas de autenticación basadas en el conocimiento.

Aumento de las llamadas de alto riesgo a los centros de atención telefónica

TransUnion documentó un ligero aumento (hasta el 6.1%) en el porcentaje de llamadas de alto riesgo a los centros de atención telefónica de Estados Unidos entre el primer semestre de 2024 y el primer semestre de 2025. Las llamadas telefónicas de mayor riesgo aumentaron durante ese periodo en la mitad de los canales medidos.

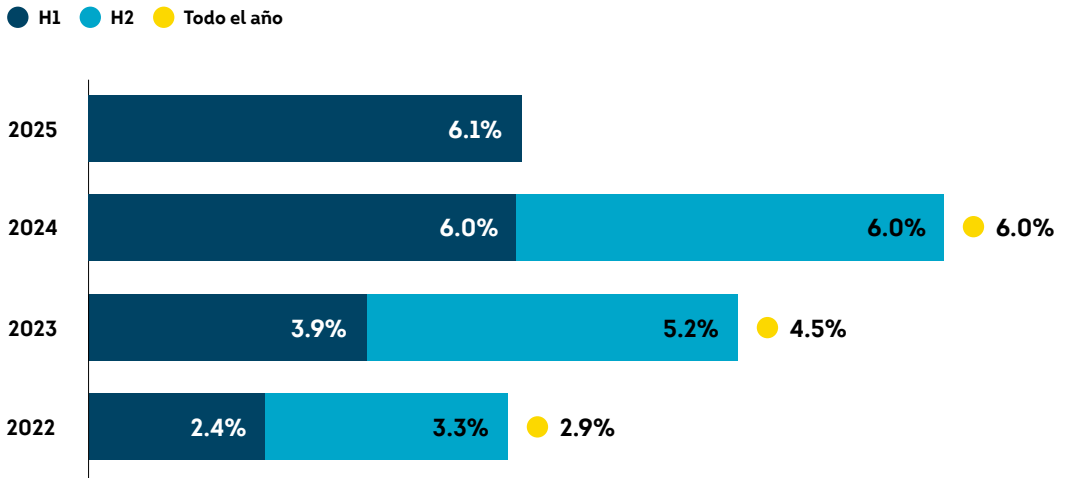
Aumento de la frecuencia de los ataques fraudulentos a los centros de atención telefónica

Cambio en la frecuencia de los ataques fraudulentos a los centros de atención telefónica durante el último año, según los directivos empresariales que afirmaron tener un conocimiento muy alto o extremadamente alto de las actividades fraudulentas en sus centros de atención telefónica.



Fuente: Encuesta empresarial de TransUnion

Llamadas de alto riesgo a centros de atención telefónica



Fuente: Red de inteligencia global de TransUnion

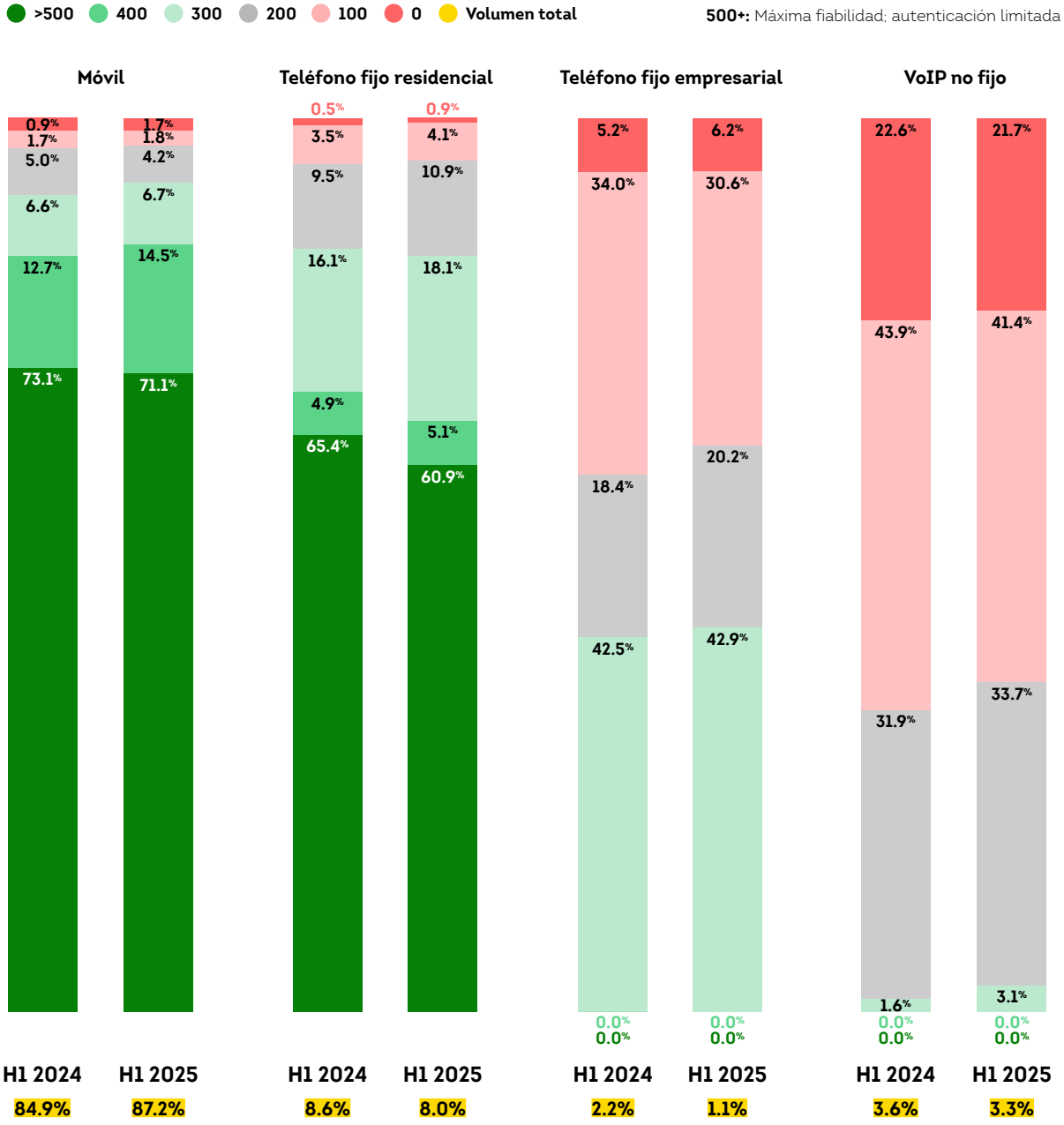
Aumentó el riesgo de las llamadas móviles; las llamadas virtuales siguieron siendo las más arriesgadas

TransUnion documentó que la gran mayoría (87.2%) de las llamadas recibidas por sus clientes de centros de atención telefónica de Estados Unidos en el primer semestre de 2025 procedían de teléfonos móviles, y estas llamadas son cada vez más arriesgadas. Aunque solo el 3.5% de las llamadas móviles se identificaron como de mayor riesgo de fraude, esto supone un aumento del 35% con respecto al 2.6% del primer semestre de 2024. El canal más arriesgado para el centro de atención telefónica fue el protocolo de voz sobre Internet (VoIP) no fijo, un número de teléfono que no está asociado a un dispositivo físico. Aunque ese canal solo representó el 3.3% del volumen total de llamadas, el 63.1% de esas llamadas se identificaron como de alto riesgo de fraude en el primer semestre de 2025.

Riesgo de los centros de llamadas de Estados Unidos por canal y volumen total

Niveles de puntuación de riesgo de las llamadas

0–100: Máximo; autenticación reforzada
200–400: Actividad normal con autenticación
500+: Máxima fiabilidad; autenticación limitada



Fuente: Red de inteligencia global de TransUnion

TransUnion

Las identidades de riesgo afectan a todas las etapas del ciclo de vida del consumidor

No todas las interacciones digitales con los clientes suponen el mismo riesgo para las organizaciones. En el primer semestre de 2025, la creación de cuentas presentó un riesgo especial tanto en Estados Unidos como a nivel mundial. Los intentos de creación de cuentas tuvieron la tasa más alta (4.2%) de presunto fraude digital en el ciclo de vida del consumidor para las transacciones en las que el usuario se encontraba en Estados Unidos en el primer semestre de 2025, aunque considerablemente inferior al 8.3% a nivel mundial. Los inicios de sesión en cuentas (un problema importante para los gestores de fraude de Estados Unidos, que señalan el ATO como la mayor fuente de pérdidas por fraude) fueron los segundos más riesgosos en el ciclo de vida del consumidor, con una tasa de sospecha de fraude digital del 3.8% para las transacciones en las que el usuario se encontraba en Estados Unidos en el primer semestre de 2025.

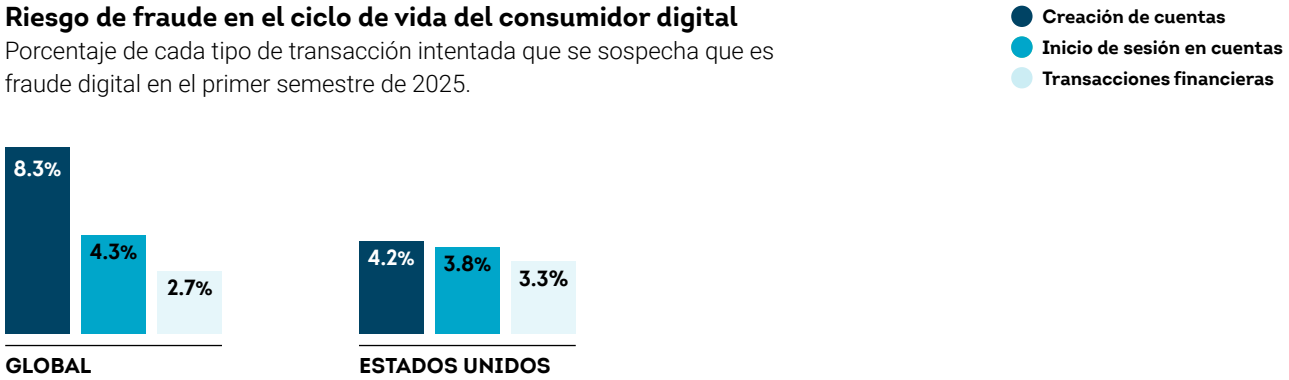
El riesgo digital de la creación de cuentas está impulsado por sectores específicos en Estados Unidos; el 37.8% de las transacciones de creación de cuentas en telecomunicaciones, el 24.6% en comercio minorista y el 22.9% en comunidades de Estados Unidos fueron sospechosas de fraude digital en el primer semestre de 2025. Al mismo tiempo, los seguros tuvieron el mayor riesgo de inicio de sesión en cuentas, con un 29.7% de las transacciones de inicio de sesión desde Estados Unidos sospechosas de fraude digital.

Ejemplos de etapas del ciclo de vida del consumidor

Creación de cuentas: registro de cuentas, inscripción y apertura de préstamos
Inicio de sesión en cuentas: inicio de sesión y eventos de inicio de sesión fallido
Transacciones financieras: compras, retiradas y depósitos

Riesgo de fraude en el ciclo de vida del consumidor digital

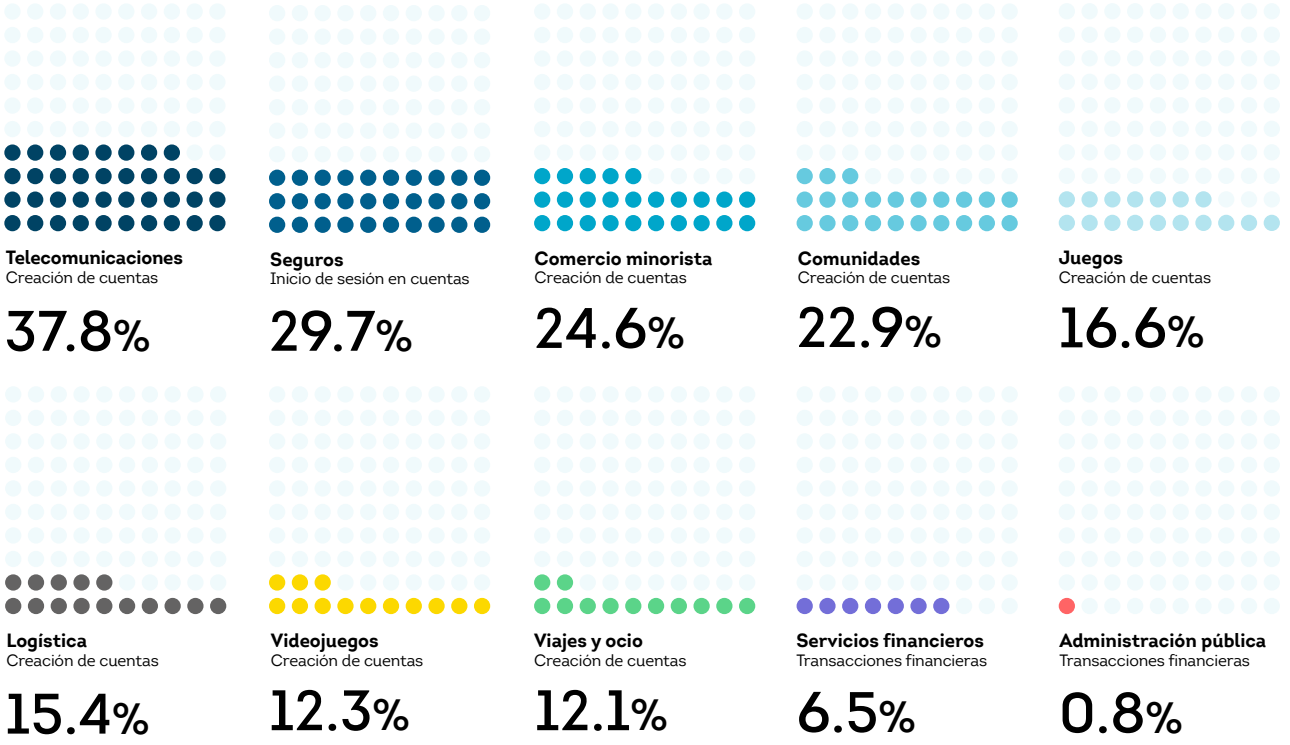
Porcentaje de cada tipo de transacción intentada que se sospecha que es fraude digital en el primer semestre de 2025.



Fuente: Red de inteligencia global de TransUnion

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

Etapa del ciclo de vida del consumidor con la tasa más alta de sospecha de fraude digital por sector y el porcentaje correspondiente en esa etapa en Estados Unidos en 2024.



Fuente: Red de inteligencia global de TransUnion

Los préstamos con identidad sintética pusieron de manifiesto el riesgo de apertura de nuevas cuentas

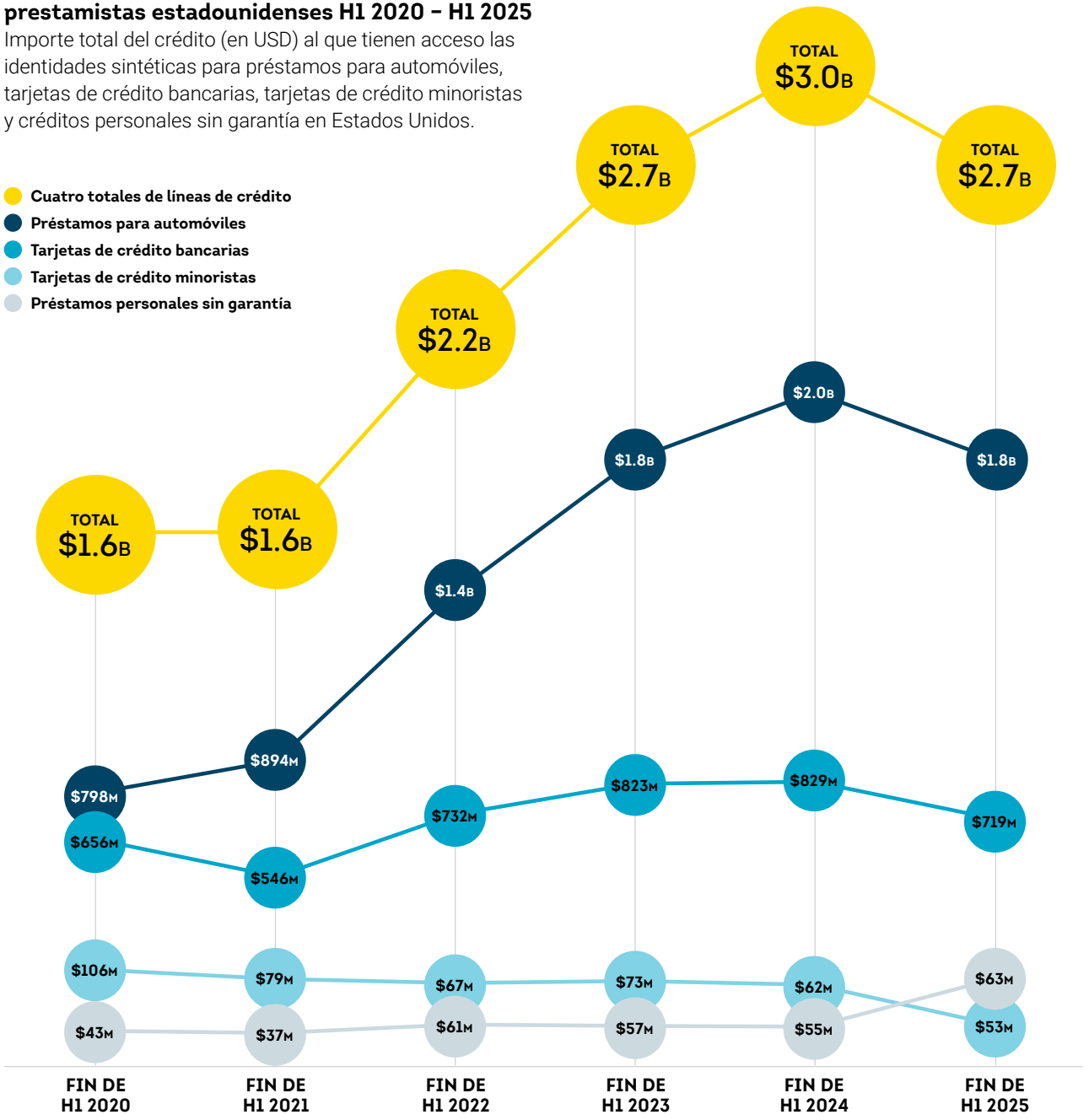
Con una gran cantidad de credenciales de identidad robadas combinadas con GenAI, el fraude de identidad sintética es una amenaza persistente. Casi una cuarta parte (24%) de los líderes empresariales estadounidenses encuestados por TransUnion afirmaron que el fraude de identidad sintética era la principal fuente de pérdidas por fraude para sus organizaciones.

Según los datos de crédito al consumo de TransUnion, la exposición total a identidades sintéticas entre las cuentas abiertas por prestamistas estadounidenses para préstamos de automóviles, tarjetas de crédito bancarias, tarjetas de crédito minoristas y préstamos personales sin garantía era de USD$27 billones en pérdidas potenciales al final del primer semestre de 2025.

El uso de cuentas de crédito para crear un historial personal creíble es una táctica clave para las identidades sintéticas, una técnica de respaldo de identidad muy eficaz, lo que las hace difíciles de detectar. Con el crecimiento de las herramientas de GenAI para crear documentos deepfake realistas e identidades sintéticas a gran escala, los delincuentes tienen los medios para cometer fraudes sintéticos en otros sectores como el comercio minorista, el comercio electrónico, la sanidad, la administración pública, las telecomunicaciones, la tecnología financiera y la educación.

Riesgo de identidad sintética para los prestamistas estadounidenses H1 2020 – H1 2025

Importe total del crédito (en USD) al que tienen acceso las identidades sintéticas para préstamos para automóviles, tarjetas de crédito bancarias, tarjetas de crédito minoristas y créditos personales sin garantía en Estados Unidos.



Fuente: Red de inteligencia global de TransUnion

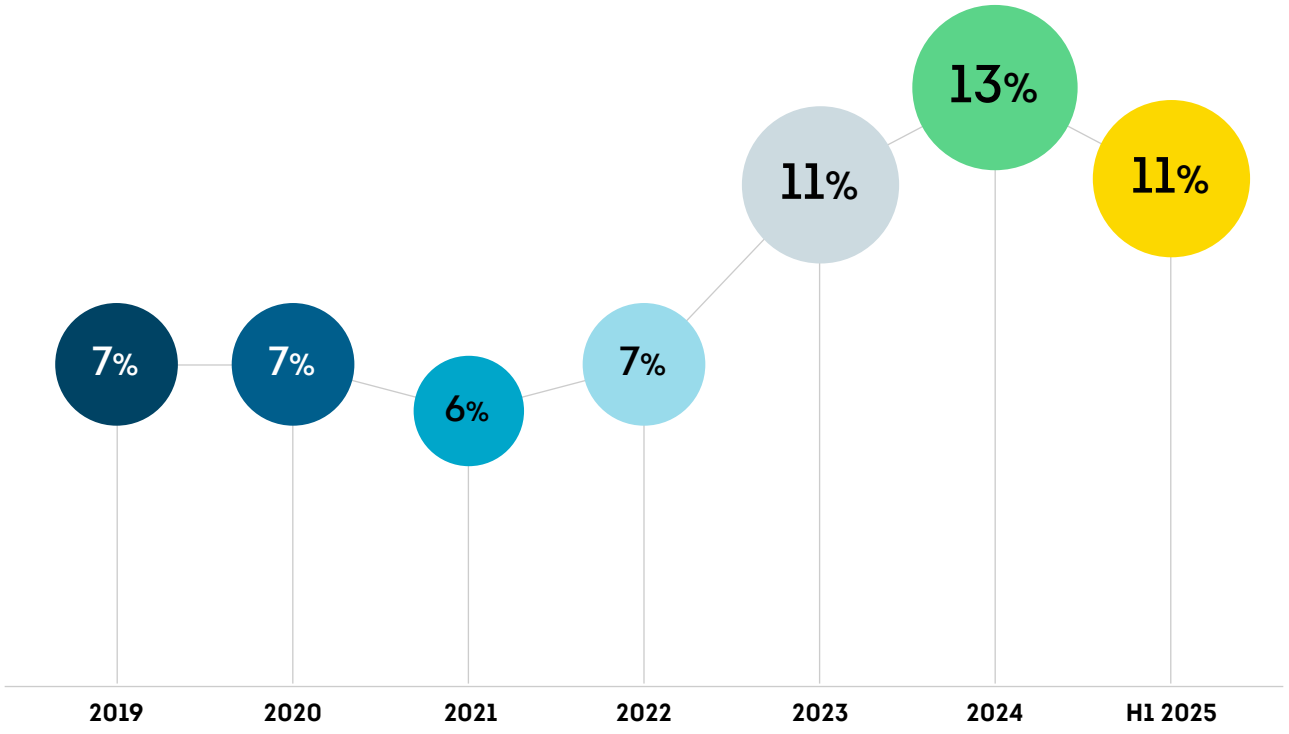
TransUnion

El lavado de crédito aumenta el riesgo de fraude en cuentas nuevas

A medida que evoluciona el fraude de identidad, los delincuentes que cometen fraude en primera o tercera persona pueden intentar reciclar una identidad mediante el lavado de crédito, una estafa de manipulación de crédito para borrar la información negativa del historial crediticio de una identidad mediante una denuncia falsa de fraude de identidad. Estas disputas falsas de informes crediticios podrían realizarse contra cuentas abiertas con una identidad de consumidor robada o una identidad sintética, o contra transacciones no autorizadas en la cuenta de crédito legítima de un consumidor.

Los consumidores de Estados Unidos (o sus representantes autorizados) tienen el derecho legal de disputar los datos inexactos de sus informes crediticios, y TransUnion sigue un proceso de resolución de disputas altamente regulado. En el primer semestre de 2025, las disputas sobre informes crediticios de consumidores en Estados Unidos que alegaban fraude representaron el 11% de todas las disputas, manteniéndose cerca del máximo durante el período de análisis del 13% en todo 2024.

Disputas sobre informes de crédito de consumidores estadounidenses que alegan fraude como porcentaje del total de disputas



Fuente: Red de inteligencia global de TransUnion

Conclusión

No importa en qué parte del mundo te encuentres, el aumento del riesgo de fraude y las pérdidas monetarias son preocupaciones crecientes para las organizaciones de todos los tamaños y en todas las industrias. Para el resto de 2025 y más allá, las amenazas para los consumidores y las organizaciones continuarán, ya que los accesos no autorizados de datos y las estafas conducirán a más identidades y credenciales comprometidas. Proteger a tu organización y a tus clientes no es negociable. Debes asumir una postura de seguridad en la que todos los datos de identidad y credenciales presentados a tu organización se consideren comprometidos. A medida que el riesgo de identidad digital aumenta en todo el ciclo de vida del consumidor, la inversión en una detección de fraude más inteligente —resolviendo la identidad de manera más efectiva— es imprescindible.

Debes priorizar un enfoque empresarial integral para la prevención del fraude con el fin de superar los sistemas fragmentados que son más vulnerables a la explotación. Al mismo tiempo, debes reforzar cada capa de tus defensas, especialmente debido a la amenaza del vector de IA. Cada capa existente —verificación de identidad, verificación de documentos, autenticación, monitoreo de sesiones, etc.— necesita señales de riesgo aumentadas, aplicando una mejor puntuación de riesgos y revisando tus estrategias de fraude para que sean adaptativas a las amenazas en evolución. Emplea estrategias encaminadas a reducir la fragmentación de la identidad del consumidor mediante mejores datos y señales de riesgo, análisis avanzados y tecnología integrada. Reducir los datos de identidad inconsistentes y aislados te permitirá detectar posibles fraudes de manera más efectiva, minimizar la fricción innecesaria para los clientes y evitar gastos adicionales por falsos positivos.

Metodología de obtención de datos

Este informe combina datos propietarios de la red de inteligencia global de TransUnion y encuestas comerciales y de consumidores especialmente encargadas.

Encuesta empresarial:

Esta encuesta en línea se realizó en Canadá (200 encuestados), Hong Kong (200), India (200), Filipinas (200), Reino Unido (200) y Estados Unidos (200) del 29 de mayo al 6 de junio de 2025, por TransUnion en asociación con el proveedor de investigación externo Dynata. La encuesta tuvo como objetivo a personas con roles gerenciales responsables del riesgo y/o fraude en empresas cuyo principal grupo de clientes fueran consumidores, y con un ingreso anual mínimo de CAD$300M en Canadá, HK$200M en Hong Kong, 1B en India, 1B en Filipinas, £200M en Reino Unido y USD$200M en Estados Unidos. Los encuestados participaron mediante un método de panel de investigación en línea utilizando una combinación de dispositivos de escritorio, móviles y tabletas. Tenga en cuenta que algunos porcentajes del gráfico pueden no sumar 100% debido a redondeos o a que se aceptaron múltiples respuestas.

Centro de atención telefónica:

Los hallazgos sobre centros de atención telefónica de TransUnion se basaron predominantemente en datos de instituciones financieras grandes y pequeñas con sede en Estados Unidos. La tasa o porcentaje de llamadas de alto riesgo se determinó mediante la evaluación de múltiples factores de riesgo.

Disputas de informes de crédito al consumidor:

Los hallazgos de disputas de informes de crédito al consumidor de TransUnion se basaron en datos de crédito al consumidor de Estados Unidos provenientes de estados, territorios, protectorados y bases militares estadounidenses y en el extranjero. Normalmente se obtiene de más de 50 años de datos de crédito al consumidor y contiene información crediticia sobre aproximadamente 400 millones de consumidores.

Encuesta a consumidores

Esta encuesta en línea se realizó entre el 5 y el 25 de mayo de 2025 en Botsuana (251 encuestados), Brasil (949), Canadá (982), Chile (888), Colombia (933), República Dominicana (601), Guatemala (478), Hong Kong (968), India (999), Kenia (433), Namibia (291), Filipinas (943), Ruanda (345), Sudáfrica (922), España (957), Reino Unido (1000), Estados Unidos (2998) y Zambia (325) por TransUnion en colaboración con la empresa de investigación independiente Dynata. Se encuestó a adultos mayores de 18 años utilizando un método de panel de investigación en línea a través de una combinación de dispositivos de escritorio, móviles y tabletas. Las preguntas de la encuesta se realizaron en chino (Hong Kong), inglés, francés (Canadá), portugués (Brasil) y español (Colombia, República Dominicana, Guatemala y España). Para garantizar la representatividad de la metodología de obtención de datos en toda la población residente, la encuesta incluyó cuotas para equilibrar las respuestas entre los principales grupos demográficos, como la edad, el género y los ingresos. Tenga en cuenta que algunos porcentajes de los gráficos pueden no sumar el 100% debido al redondeo o a que se aceptaron múltiples respuestas.

Filtraciones de datos

TransUnion obtiene su información exclusiva sobre accesos no autorizados de datos, en colaboración con el Centro de Recursos contra el Robo de Identidad (ITRC). El personal del ITRC realiza un seguimiento de todos los casos de exposición de datos denunciados públicamente en Estados Unidos a partir de fuentes que incluyen fiscales generales estatales, comunicados de prensa de entidades afectadas, bufetes de abogados, expertos en ciberseguridad y más. TransUnion amplía los datos del ITRC con un proceso que calcula los principales riesgos de cada acceso no autorizado de datos, las medidas adecuadas que pueden tomar los consumidores y la puntuación de riesgo de acceso no autorizado (BRS por sus siglas en inglés – Breach Risk Score). La BRS se basa en la cantidad y la gravedad de las credenciales de identidad específicas que la entidad afectada ha determinado que han sido expuestas. De entre 60 posibles opciones de credenciales de identidad, cada acceso no autorizado de datos se analiza mediante el perfil de amenazas de identidad TruEmpower de TransUnion para generar una puntuación y un patrón de riesgo, así como las medidas recomendadas para los consumidores. La BRS utiliza una escala del 1 al 10, en la que 1 representa la menor gravedad y 10 la mayor gravedad.

Fraude digital

TransUnion utiliza inteligencia derivada de miles de millones de transacciones provenientes de más de 40,000 sitios web y aplicaciones. La tasa o el porcentaje de intentos sospechosos de fraude digital refleja aquellos casos que los clientes de TransUnion determinaron que cumplían con una de las siguientes condiciones: 1) denegación en tiempo real debido a indicadores de fraude, 2) denegación en tiempo real por violaciones de políticas corporativas, 3) determinación de fraude tras una investigación del cliente, o violación de políticas corporativas identificada tras una investigación del cliente, 4) comparados con el total de transacciones evaluadas.Los análisis por país y región examinaron transacciones en las que el consumidor o el presunto estafador se encontraba en un país o región específicos al momento de realizar la transacción. Las estadísticas globales representan todos los países del mundo y no solo los países o regiones seleccionados.

Fraude sintético

Las conclusiones de TransUnion sobre el fraude sintético se basaron en datos de crédito de consumidores estadounidenses procedentes de estados, territorios, protectorados y bases militares estadounidenses y en el extranjero. Se obtienen de forma rutinaria a partir de más de 50 años de datos de crédito de consumidores y contienen información crediticia sobre aproximadamente 400 millones de consumidores. El análisis del fraude sintético abarca la actividad crediticia estadounidense registrada entre el 1 de enero de 2009 y el 30 de junio de 2025. Las medidas de exposición de los prestamistas se basaron en la fórmula patentada de TransUnion para capturar la pérdida total potencial en riesgo para los prestamistas.

ACERCA DE TRANSUNION

TransUnion es una compañía global de información con más de 13.000 colaboradores operando en más de 30 países. Hacemos posible la confianza al garantizar que cada persona esté representada de manera confiable en el mercado; logramos esto a través de una visión Tru™ de cada individuo: una perspectiva accionable de los consumidores, gestionada con cuidado. Gracias a nuestras adquisiciones e inversiones en tecnología, hemos desarrollado soluciones innovadoras que van más allá de nuestra sólida base en crédito, abarcando áreas como marketing, fraude, riesgo y analítica avanzada. Como resultado, los consumidores y las empresas pueden realizar transacciones con confianza y alcanzar grandes logros. A esto lo llamamos Información para el Bien® – y se traduce en oportunidades económicas, experiencias excepcionales y empoderamiento personal para millones de personas en todo el mundo.

Combine una potente detección de fraude con análisis avanzados para proteger su organización y sus clientes. **Conozca hoy la Solución de Prevención de Fraude de TransUnion.**

TransUnion