

ACTUALIZACIÓN H2 2026:
PRINCIPALES TENDENCIAS
EN MATERIA DE FRAUDE

El Fraude en la Era de la Confianza Continua

Evaluación de riesgos cuando las identidades, las comunicaciones y las relaciones establecidas se ven comprometidas

TransUnion

CONTENIDOS

3 **Resumen Ejecutivo**

5 **Dentro del Panorama de la Confianza Global**

Las identidades sintéticas están redefiniendo la confianza

Las comunicaciones se han convertido en el nuevo campo de batalla contra el fraude

La inteligencia artificial permite a las redes criminales operar a escala industrial

23 **Perspectivas Regionales**

EE. UU.

América Latina

27 **Moldeando la Próxima Era de la Confianza Digital**

30 **Acerca de la Investigación**

Resumen Ejecutivo

Los líderes empresariales de todo el mundo estiman que sus organizaciones perdieron, en promedio, un 6,5% de sus ingresos debido al fraude durante el último año. Esas pérdidas son un síntoma de un problema mayor: el fraude está teniendo éxito porque la confianza se ha vuelto más fácil de explotar y más difícil de establecer. Y dado que la confianza es la base del crecimiento, las relaciones con los clientes, la eficiencia operativa y la reputación de la marca, el fraude ha pasado de ser un desafío operativo a convertirse en un riesgo estratégico para los negocios.

Durante años, la verificación de identidad sirvió como base de la confianza digital: establecer confianza en el momento de la incorporación, autenticar a los usuarios y aprobar transacciones. Esa base sigue siendo fundamental, pero ya no es suficiente.

La verificación de identidad por sí sola no puede asumir todo el peso de la prevención del fraude. El fraude explota cada vez más las identidades después de que se verifican, las comunicaciones después de que se envían y las relaciones después de que se establecen. La pregunta clave ya no es simplemente: "¿Es esta la persona correcta?", sino: "¿Se debe confiar en esta interacción?".

La prevención del fraude debe pasar de verificar la identidad en momentos aislados a evaluar la confianza de manera continua. Las organizaciones deben integrar señales de identidad, de dispositivos, de comportamiento, de comunicaciones y de red para crear una visión más completa del riesgo. La inteligencia conectada ayuda a las organizaciones a detectar el riesgo más temprano, tomar decisiones más precisas y reducir la fricción innecesaria para los clientes legítimos.

Este informe está dirigido a los líderes en materia de fraude, riesgo, identidad, autenticación, canales digitales y experiencia del cliente, quienes son responsables de proteger el crecimiento y la confianza de los clientes. Basándose en la inteligencia global de TransUnion, en investigaciones propias y en perspectivas de los mercados regionales, el informe explica hacia dónde se está dirigiendo el riesgo de fraude, por qué las estrategias tradicionales contra el fraude están perdiendo eficacia y qué capacidades deben priorizar las organizaciones para desarrollar una estrategia de confianza más resiliente a lo largo de todo el ciclo de vida del cliente.

La próxima era de la confianza digital va más allá de la prevención del fraude. Definirá la forma en que las organizaciones captan clientes, protegen las relaciones, reducen las fricciones y toman decisiones de riesgo con confianza. Las organizaciones que tengan éxito en la próxima década no solo detectarán el fraude de manera más eficaz, sino que establecerán la confianza de manera continua como base para un crecimiento sostenible.

Hay tres temas que definen la próxima era de la confianza digital:

La confianza ya no se establece una sola vez; se evalúa de manera continua.

El fraude surge cada vez más después de que se ha otorgado la confianza durante el proceso de incorporación, lo que exige que las organizaciones evalúen constantemente la identidad, el comportamiento y la intención a lo largo de todo el ciclo de vida del cliente.

El panorama de la prevención del fraude se extiende al ámbito de las comunicaciones.

La suplantación de marcas, las llamadas falsificadas y la ingeniería social influyen en la percepción y el comportamiento de los consumidores antes de que los controles tradicionales contra el fraude tengan la oportunidad de intervenir.

El fraude opera como un ecosistema conectado e industrializado.

La inteligencia artificial y la automatización permiten a las redes criminales crear y perfeccionar ataques más rápidamente, dirigirlos con precisión, personalizarlos de manera convincente y adaptarse rápidamente a las condiciones cambiantes.

Autores y Colaboradores

Autores



Brian Killeen

Vice President:
Product Management,
Fraud & Identity Solutions



Richard Tsai

Sr. Director:
Product Marketing,
Fraud & Identity Solutions

Colaboradores



Amritha Reddy

Sr. Director:
Africa Fraud & Identity Solutions



Glyn Cowlishaw

Director:
UK Fraud Solutions Specialists



Andrew Sigfrid

Sr. Director:
Canada Fraud & Identity Solutions



Manual Pineros

Director:
Spain Business Development



Anurag Anand

Director:
India Fraud & Identity Solutions



Miguel Rivera

Sr. Director:
Latin America Fraud & Identity Solutions



Anurag Varma

Director:
Asia Pacific Fraud & Identity Solutions



Wallace Massola

Sr. Advisor:
Brazil Head of Fraud & Identity Solutions

Dentro del Panorama de la Confianza Global



A medida que se vuelve más fácil aprovecharse de la confianza, las organizaciones tienen dificultades para mantenerse al día

El fraude se ha convertido en uno de los riesgos empresariales más importantes que enfrentan las organizaciones. A nivel mundial, el 6% de los líderes empresariales clasificaron el fraude entre los riesgos con mayor impacto potencial en los negocios, por delante de las violaciones de ciberseguridad, el cumplimiento normativo, la pérdida de clientes, los costos operativos y el riesgo reputacional. Lo que resulta aún más preocupante es que el 58% afirmó estar muy o extremadamente preocupado porque el fraude está evolucionando más rápido que la capacidad de sus organizaciones para detectarlo y prevenirlo.

Esto se debe a un cambio fundamental en la forma en que opera el fraude. Muchas de las amenazas de más rápido crecimiento están diseñadas no solo para robar dinero, sino para aprovecharse de la confianza. Se crean identidades sintéticas para que parezcan legítimas. Las estafas manipulan a los consumidores para que autoricen actividades fraudulentas. La inteligencia artificial permite que los ataques sean más adaptables, escalables y difíciles de detectar. Cada vez más, el fraude tiene éxito al aprovechar identidades, comunicaciones y relaciones de confianza.

El fraude es un riesgo estratégico que se esconde tras las pérdidas operativas

Muchas organizaciones siguen percibiendo el fraude principalmente como un problema financiero y operativo. Los datos sugieren algo más amplio. Si bien el 47% de los líderes empresariales afirmó que los costos operativos y las pérdidas financieras directas tuvieron un impacto significativo o grave en su negocio durante el último año, el 45% señaló la reputación de la marca y el 42% mencionó la capacidad de crecer o expandirse. El fraude influye cada vez más en la captación y la experiencia del cliente, así como en el desempeño empresarial a largo plazo.

Las organizaciones reconocen el riesgo, pero muchas siguen siendo las menos preparadas para las amenazas que están transformando el panorama del fraude. Más de la mitad de los líderes empresariales (53%) identificaron el fraude de identidad sintética como la amenaza para la que se sienten menos preparados para manejar, lo que la convierte en la mayor brecha de preparación identificada en esta investigación.

En conjunto, estos hallazgos apuntan a un cambio más amplio. El desafío al que se enfrentan las organizaciones ya no es simplemente detectar la actividad fraudulenta después de que ocurra. Se trata de comprender cómo se está explotando la confianza a través de las identidades, las comunicaciones y las interacciones con los clientes, para luego desarrollar las capacidades necesarias para responder.

Las secciones siguientes examinan tres fuerzas que impulsan este cambio: el aumento de las identidades sintéticas, el papel cada vez más importante de las comunicaciones en los ataques fraudulentos y la industrialización del fraude a través de la inteligencia artificial y la automatización.

Sobre los datos

A menos que se indique lo contrario, los datos citados a lo largo de este informe provienen de encuestas encargadas a empresas y consumidores, así como de información derivada de los datos propios de TransUnion sobre fraude, identidad, crédito e inteligencia de comunicaciones. Para obtener más detalles sobre la metodología, consulte la sección Acerca de la investigación.

Las identidades sintéticas están redefiniendo la confianza

En una era de identidades sintéticas y robo de identidad a gran escala, la identidad ya no es un punto de referencia confiable para la confianza. En todas las regiones, los estafadores parecen estar superando la capacidad de las organizaciones para distinguir las identidades genuinas de aquellas manipuladas o fabricadas.

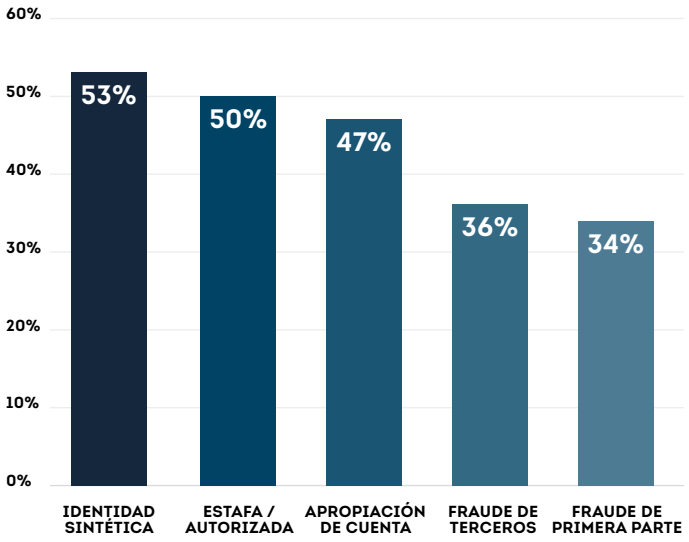
El fraude de identidad sintética está superando las capacidades de detección de las organizaciones

Las redes organizadas de fraude y los actores malintencionados están utilizando información de consumidores expuesta y la inteligencia artificial para crear identidades creíbles y documentos "deepfake" que pueden usarse para atacar a empresas de todos los sectores y mercados. A nivel global, el 18% de los líderes empresariales afirmó que el fraude de identidad sintética fue la principal causa de pérdidas por fraude para sus organizaciones durante el último año, y el 65% señaló que espera que sea el tipo de fraude que más aumente en sus negocios durante los próximos dos años.

A pesar de su impacto, el fraude de identidad sintética es el tipo de fraude que los líderes consideran que están menos preparados para manejar en la actualidad (véase la Figura 1). Una vez que las identidades sintéticas logran eludir los controles de fraude en el proceso de incorporación digital, las organizaciones se enfrentan al reto de detectarlas antes de incurrir en pérdidas por fraude o de enfrentar multas por incumplimiento normativo, sanciones o acciones legales.

Figura 1: El fraude de identidad sintética es la amenaza para la que las organizaciones se sienten menos preparadas para detener.

Porcentaje de líderes empresariales que afirmaron que sus organizaciones están menos preparadas para manejar cada tipo de fraude



Fuente: Encuesta sobre fraude empresarial de TransUnion, junio de 2026

65%

de los líderes empresariales esperan que el fraude de identidad sintética aumente en los próximos dos años

Fuente: Encuesta sobre fraude empresarial de TransUnion, junio de 2026

La exposición al fraude de identidad sintética parece ser más amplia de lo que muchas organizaciones creen

El fraude de identidad sintética es un problema global que afecta a todos los sectores. Está presente tanto en economías crediticias maduras como en mercados digitales emergentes. Si bien hay pocos informes sobre la exposición y las pérdidas a nivel mundial, la conciencia sobre el riesgo está creciendo, ya que muchas organizaciones confunden las pérdidas por fraude de identidad sintética con el fraude de primera o tercera parte.

Las observaciones regionales refuerzan el impacto comercial que señalaron los líderes. Por ejemplo, los líderes empresariales de Hong Kong, India, España y Estados Unidos se mostraron más propensos que el promedio a afirmar que el fraude de identidad sintética sería el tipo de fraude que más aumentaría en sus organizaciones en los próximos dos años. Los datos de Estados Unidos y Canadá, combinados con observaciones del Reino Unido y América Latina, sugieren que el fraude de identidad sintética podría estar más extendido de lo que indican los informes actuales. A medida que las organizaciones mejoran su capacidad para identificar actividades relacionadas con identidades sintéticas, muchas podrían descubrir que su nivel de exposición ha sido subestimado, lo que refuerza la necesidad de evaluar continuamente la confianza y la identidad de los usuarios más allá del proceso de vinculación o incorporación inicial.

Aumenta la concientización sobre el riesgo de fraude de identidad sintética

EE. UU.

Se estima que la exposición total de las entidades crediticias estadounidenses al riesgo de fraude de identidad sintética alcanzó los USD $2.4 mil millones a finales de junio de 2026. Los créditos para la compra de automóviles fueron los más afectados, con una exposición al riesgo sintético de USD $1.5 mil millones, mientras que otras líneas de crédito, incluidas las tarjetas bancarias y las líneas de crédito personales, mostraron niveles más bajos de exposición. En EE. UU., las pérdidas promedio por cancelaciones de cuentas debido al fraude de identidad sintética se duplicaron con creces entre el primer semestre de 2009 y el primer semestre de 2026. Una investigación propia de TransUnion indica que las organizaciones de servicios no financieros, como las de telecomunicaciones, también se enfrentan al riesgo de las identidades sintéticas.

CANADÁ

Según un estudio propio de TransUnion, el fraude sintético aumentó de manera constante en Canadá entre el tercer trimestre de 2021 y el cuarto trimestre de 2023, representando más del 14% de las pérdidas crediticias relacionadas con la incorporación de nuevos clientes, lo que pone de relieve el creciente desafío que supone identificar identidades falsas antes de que se establezcan en el ecosistema financiero.

REINO UNIDO

TransUnion descubrió que las instituciones del Reino Unido están identificando activamente un gran número de identidades sintéticas sospechosas en revisiones de prueba de concepto. Muchas de ellas están descubriendo que las pérdidas por fraude de identidad sintética se descartaron inicialmente como suplantación de identidad por parte de terceros o incumplimiento de pago por parte del titular.

AMÉRICA LATINA

Las preocupaciones relacionadas con las identidades sintéticas se asocian cada vez más con la incorporación digital y la obtención de crédito. Si bien muchos países latinoamericanos cuentan con registros civiles nacionales, TransUnion descubrió que estas medidas no están impidiendo la manipulación de identidades, la falsificación de documentos y el uso de inteligencia artificial para replicar documentos de identidad como licencias de conducir y pasaportes.

Las filtraciones de datos proporcionan material de base para un fraude de identidad sintética cada vez más sofisticado

Las filtraciones de datos alimentan continuamente la cadena de suministro del fraude basado en la identidad. Los ciberataques dirigidos a organizaciones con el fin de obtener información de identidad auténtica y credenciales están exponiendo a millones, si no miles de millones, de personas en todo el mundo a un posible fraude (véase la Figura 2). A medida que la inteligencia artificial permite ataques más rápidos y específicos, la amenaza que representan las identidades sintéticas para la confianza no hará más que acelerarse.

Los informes sobre filtraciones de datos en EE. UU. resaltan la magnitud de los datos de identidad a los que tienen acceso los estafadores para crear identidades sintéticas. Los números de Seguro Social quedaron expuestos en el 73% de las filtraciones de datos en EE. UU. durante el primer semestre de 2026, mientras que las licencias de conducir y las identificaciones estatales quedaron expuestas en el 34%. Los ciberdelincuentes también se enfocaron en información como historiales médicos (37% de las filtraciones en EE. UU.) y números de cuentas corrientes o de ahorro (34%). A medida que se dispone de más datos de identidad auténticos a través de las filtraciones, los estafadores tienen mayor capacidad para construir identidades sintéticas convincentes, lo que aumenta el desafío de distinguir a los consumidores legítimos de los falsos y refuerza la necesidad de una confianza continua durante el proceso de incorporación y más allá.

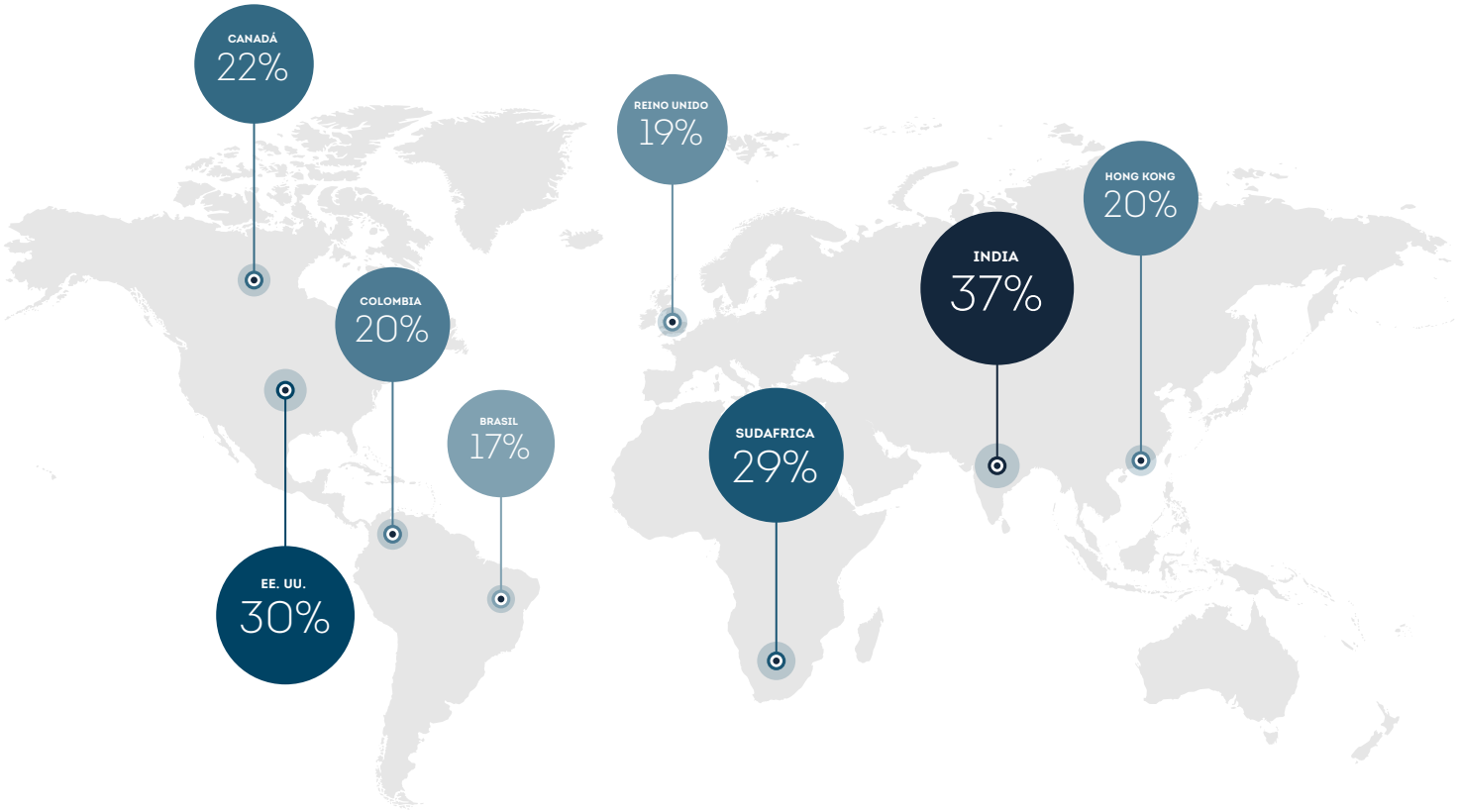
73%

Las violaciones de datos en EE. UU. expusieron números completos del Seguro Social en el primer semestre de 2026

Fuente: Red de inteligencia global de TransUnion

Figura 2: La brecha de datos continúan exponiendo la información personal de los consumidores a nivel mundial

Porcentaje de consumidores que indicaron que su información personal o los detalles de sus cuentas en línea quedaron expuestos en una filtración de datos durante un período reciente de tres meses



Fuente: Red de inteligencia global de TransUnion

El "lavado de crédito" en EE. UU. aumenta el riesgo de identidad de las identidades sintéticas después de que estas se revelan

Los delincuentes atacan procesos confiables para facilitar el fraude sintético. Una estrategia que emplean los estafadores para mantener las identidades sintéticas a lo largo del tiempo es el "lavado de crédito", un esquema que se aprovecha del proceso de disputa de crédito para eliminar información negativa legítima del historial crediticio mediante reclamaciones falsas de robo de identidad.

El "lavado de crédito" sdistorsiona la evaluación del riesgo crediticio al ocultar información negativa que normalmente alimenta los modelos de puntuación crediticia. Se ha demostrado que las cancelaciones de deuda de cartera (charge-offs) iniciadas por los consumidores están estrechamente relacionadas con esta práctica. En Estados Unidos, las supresiones de castigos cancelaciones de deuda de cartera iniciadas por los consumidores crecieron a una tasa de crecimiento anual compuesta (CAGR) del 29,2 % entre 2017 y 2026 (véase la Figura 3).

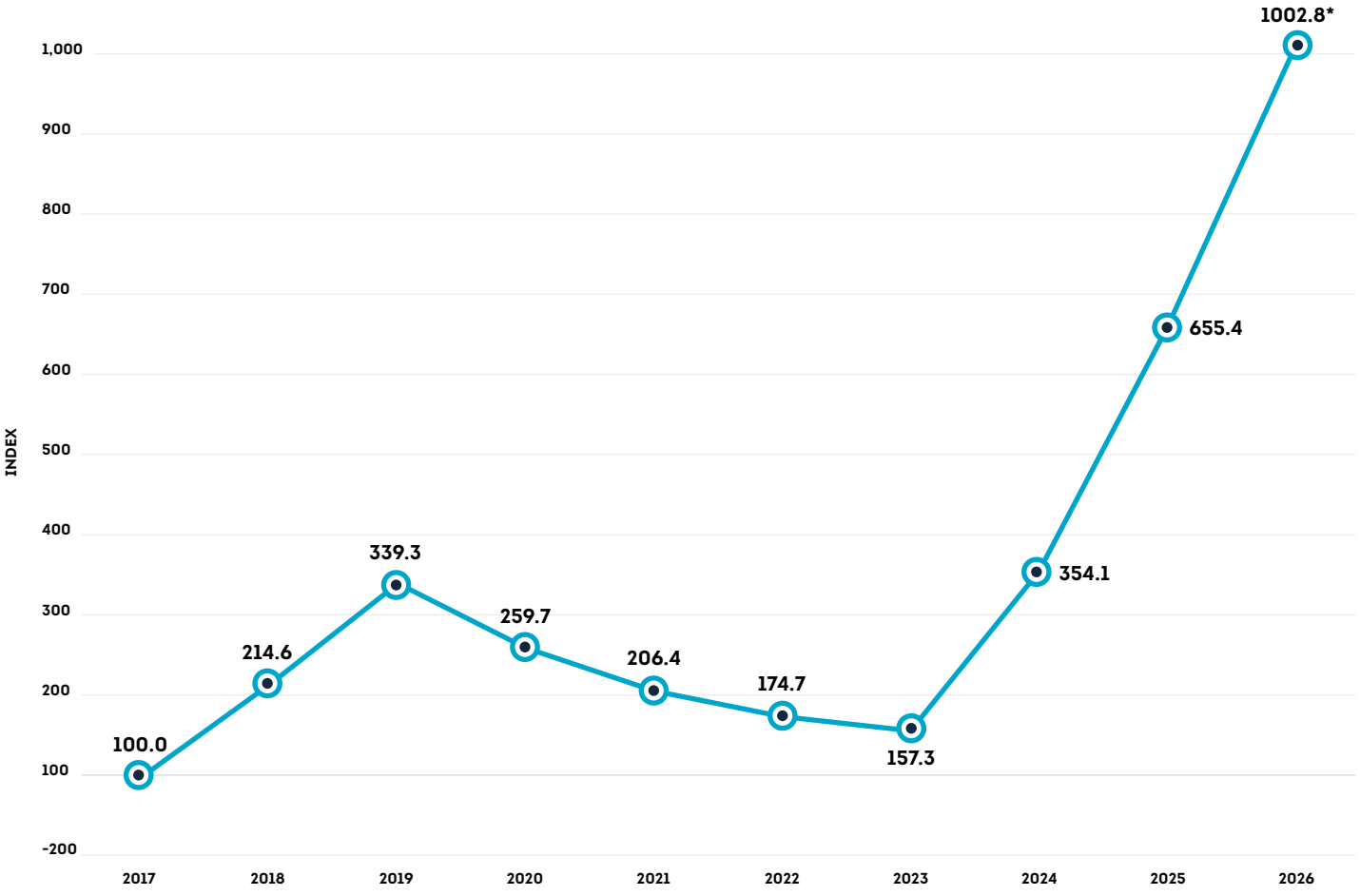
29.2%

Tasa de crecimiento anual compuesta de las reducciones en las bajas contables iniciadas por los consumidores de EE. UU. entre 2017 y 2026

Fuente: Red de inteligencia global de TransUnion

Figura 3: El rápido crecimiento de las supresiones de cuentas incobrables puede prolongar la vida útil de las identidades sintéticas

Crecimiento anual de las supresiones de cuentas incobrables iniciadas por los consumidores, indexado a 2017



**Proyección para 2026 basada en los datos reales del primer semestre de 2026.*
Fuente: Red de inteligencia global de TransUnion

El riesgo de identidad va mucho más allá de la creación de cuentas, convirtiéndose en un problema que abarca todo el ciclo de vida

Los ataques de fraude basados en la identidad suelen surgir antes de que las organizaciones cuenten con información suficiente para establecer confianza en los nuevos clientes. Si bien la creación de cuentas es un momento crítico para establecer confianza, la mayor parte de la exposición al fraude ocurre después de que ya se ha establecido la relación con el cliente.

Aparecen diferentes patrones de riesgo en las actividades de creación de cuentas, inicio de sesión y transacciones financieras, especialmente en el caso del fraude impulsado por IA. Por ejemplo, la IA puede ayudar a los estafadores a generar o modificar rápidamente identidades, credenciales e interacciones para atacar los controles más débiles a lo largo del ciclo de vida del cliente. Si bien la creación de cuentas suele presentar el mayor porcentaje de sospechas de fraude digital de todas las etapas del ciclo de vida (véase la Figura 4), el 81% de todas las sospechas de fraude digital en el primer semestre de 2026 ocurrió durante las interacciones continuas con los clientes (inicio de sesión en la cuenta y transacciones financieras).

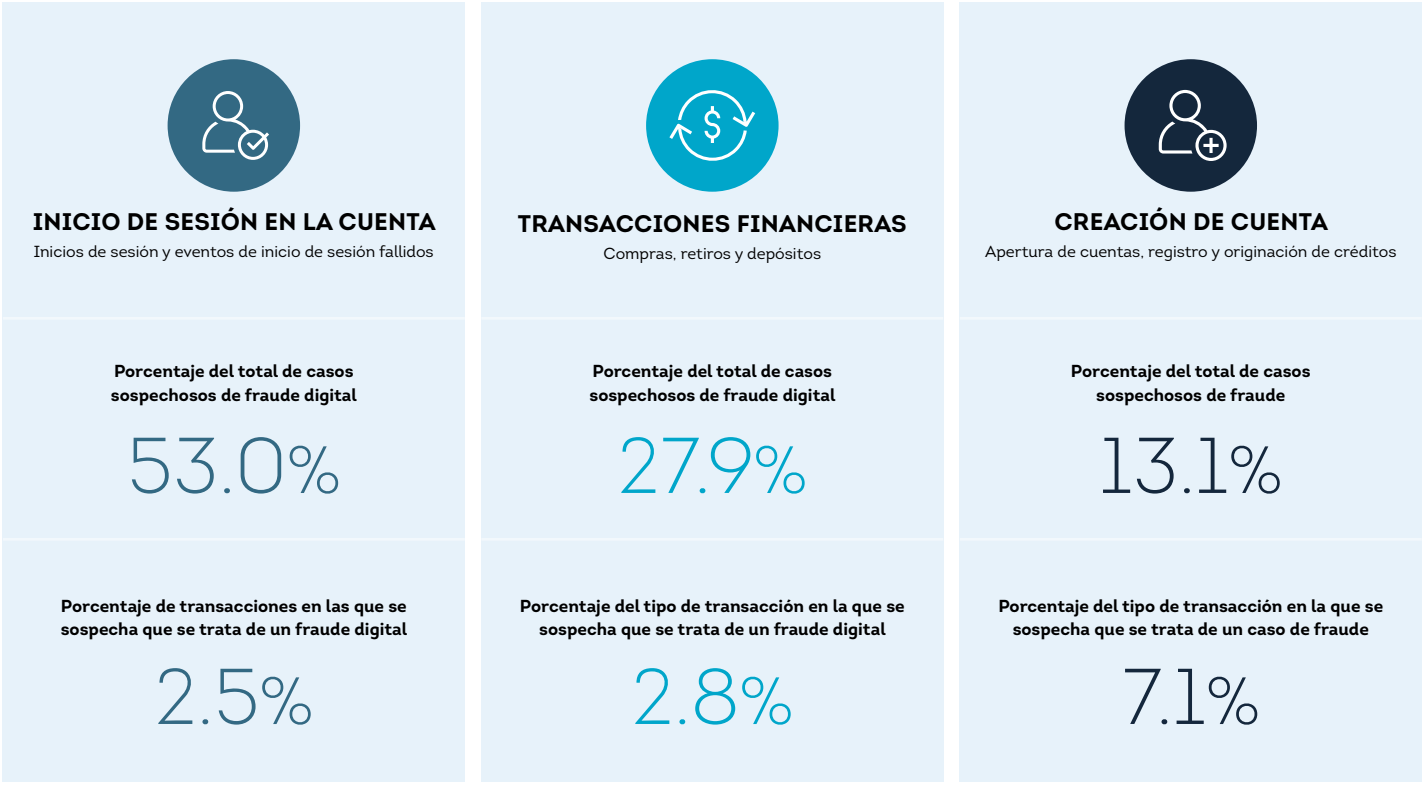
81%

de todos los casos sospechosos de fraude digital ocurrieron durante interacciones en curso con los clientes en el primer semestre de 2026

Fuente: Red de inteligencia global de TransUnion

Figura 4: La mayoría de los casos sospechosos de fraude digital ocurren después de la creación de la cuenta

Fraude digital en el ciclo de vida del cliente en el primer semestre de 2026



Fuente: Red de inteligencia global de TransUnion

El riesgo de identidad a lo largo del ciclo de vida del cliente representa una amenaza constante en todos los sectores

A medida que se expanden los ataques de fraude digital impulsados por la inteligencia artificial, los delincuentes buscan cada vez más explotar las defensas más débiles, moviéndose entre sectores y organizaciones en busca de los objetivos más fáciles. Por ejemplo, una sola identidad sintética puede utilizarse para obtener un préstamo de "compra ahora, paga después" (BNPL) en una tienda, abrir una cuenta de telefonía celular que incluya el alquiler de un teléfono, conseguir una tarjeta de crédito con un límite más alto en un banco y crear una cuenta de apuestas en línea.

Si bien la etapa del ciclo de vida en la que se concentra el riesgo varía según el sector y el modelo de negocio (véase la Figura 5), las organizaciones deben reconocer que cerrar las brechas en la verificación de identidad a lo largo del ciclo de vida del cliente es fundamental para reducir las pérdidas por fraude.

Por ejemplo:

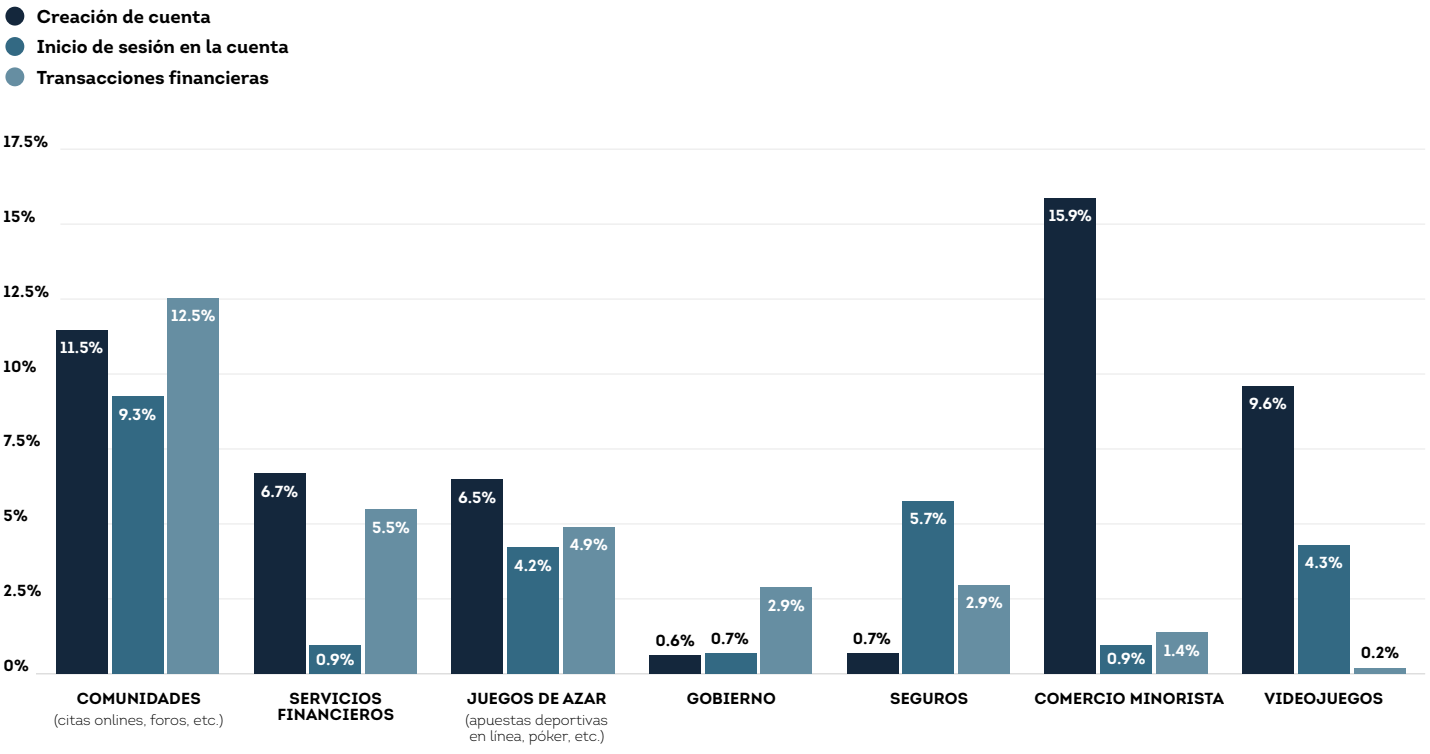
El sector minorista presenta un riesgo extremadamente alto de creación de cuentas debido al abuso de las promociones, ya que a menudo se requieren cuentas para obtener los descuentos anunciados. Sin embargo, en esta industria extremadamente competitiva se utiliza una verificación de identidad de baja fiabilidad para reducir al mínimo las dificultades para los clientes.

El sector de los servicios financieros presenta un riesgo elevado de creación de cuentas debido a la ganancia financiera inmediata que buscan los estafadores. Sin embargo, el riesgo de fraude asociado a las transacciones financieras (incluidos depósitos, retiros y pagos) es mayor que en la mayoría de los sectores, lo que indica que los desafíos relacionados con la verificación de identidad persisten mucho después de que se haya establecido la relación con el cliente.

El sector de gaming presenta un riesgo elevado en múltiples puntos de interacción. A pesar de la verificación de identidad de alta seguridad, los estafadores se enfocan en las cuentas nuevas para abusar de los bonos. Pero el riesgo persiste a lo largo de todo el ciclo de vida del cliente. Por ejemplo, puede surgir un riesgo de inicio de sesión cuando varias personas usan la misma cuenta, mientras que puede ocurrir un riesgo de transacción cuando un estafador usa una tarjeta de crédito robada para depositar fondos en una cuenta.

Figura 5: El riesgo de fraude se concentra en diferentes etapas del recorrido del cliente según el sector

Porcentaje de transacciones intentadas sospechosas de ser fraude digital, por etapa del recorrido del cliente, en sectores seleccionados durante el primer semestre de 2026



Fuente: Red de inteligencia global de TransUnion

ACCIONES RECOMENDADAS

Lo que esto significa para las organizaciones

La verificación de identidad ya no puede centrarse únicamente en el proceso de incorporación. A medida que el fraude de identidad sintética se vuelve más sofisticado y los estafadores se aprovechan de cuentas confiables a lo largo de todo el ciclo de vida del cliente, las organizaciones necesitan un enfoque más amplio para evaluar la confianza. Las siguientes acciones pueden ayudar a reducir la exposición al riesgo sin dejar de ofrecer experiencias de cliente fluidas.

1

Implementar la confianza continua, no una verificación única

La confianza en la identidad debe tratarse como un proceso empresarial continuo, en lugar de una decisión única en el momento de la incorporación. Las organizaciones deben reevaluar continuamente la confianza a medida que los comportamientos de los clientes, las credenciales y las señales de riesgo evolucionan a lo largo de la relación.

2

Adaptar la verificación de identidad a los riesgos cambiantes

Priorizar la inteligencia de identidad donde es más probable que cambie la confianza, no solo donde se establece inicialmente. Si bien la incorporación sigue siendo fundamental, las organizaciones deben fortalecer la verificación de identidad en los procesos de inicio de sesión, mantenimiento de cuentas, pagos y recuperación.

3

Conectar la inteligencia de identidad en todos los canales de servicio

Desviar la inversión de las herramientas de verificación aisladas hacia una inteligencia de identidad conectada que unifique las señales de identidad en todas las interacciones con los clientes para detectar el fraude en constante evolución, al tiempo que se reduce la fricción innecesaria para los clientes legítimos en todos los canales utilizados para atenderlos.



Las comunicaciones se han convertido en el nuevo campo de batalla contra el fraude

El fraude comienza cada vez más antes de que se produzca el incidente tradicional de fraude, a través de la suplantación de identidad de marcas, la ingeniería social y la manipulación de la confianza. Los canales de comunicación se han convertido en una señal de fraude en las etapas iniciales, que a menudo influye en el comportamiento de los consumidores antes de que los controles tradicionales contra el fraude puedan intervenir.

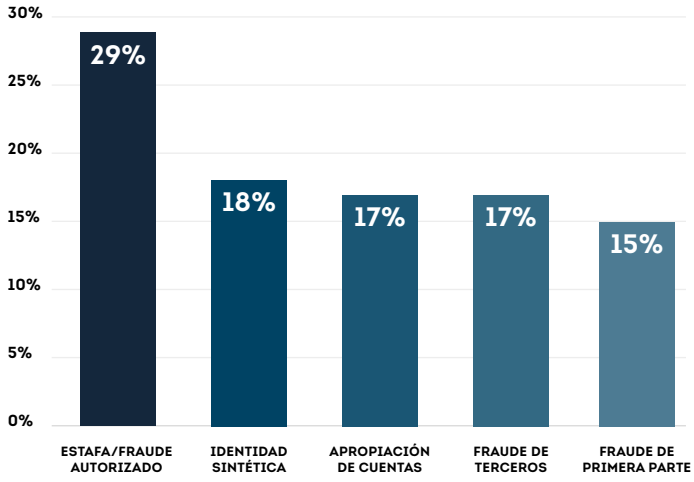
Las estafas se perfilan como la principal fuente de pérdidas por fraude y la de más rápido crecimiento

Las estafas se perfilan como la principal fuente de pérdidas por fraude y la de más rápido crecimiento. La mayoría de los consumidores que son blanco del fraude digital han recibido correos electrónicos, mensajes de texto y llamadas telefónicas fraudulentas. Pero el hecho de estar al tanto de ello no hace que estos ataques sean menos efectivos. Los líderes empresariales señalaron que las estafas y el fraude autorizado fueron la causa principal de las pérdidas por fraude en sus organizaciones durante el último año (véase la Figura 6).

Con estafas sofisticadas de suplantación de identidad impulsadas por inteligencia artificial, el riesgo no hace más que crecer. Casi la mitad (48%) de los líderes empresariales informó que las estafas y el fraude autorizado aumentaron en el último año (véase la Figura 7), lo que representa, con diferencia, el aumento más alto en comparación con otros tipos de fraude.

Figura 6: Las estafas y el fraude autorizado generan las mayores pérdidas para las organizaciones

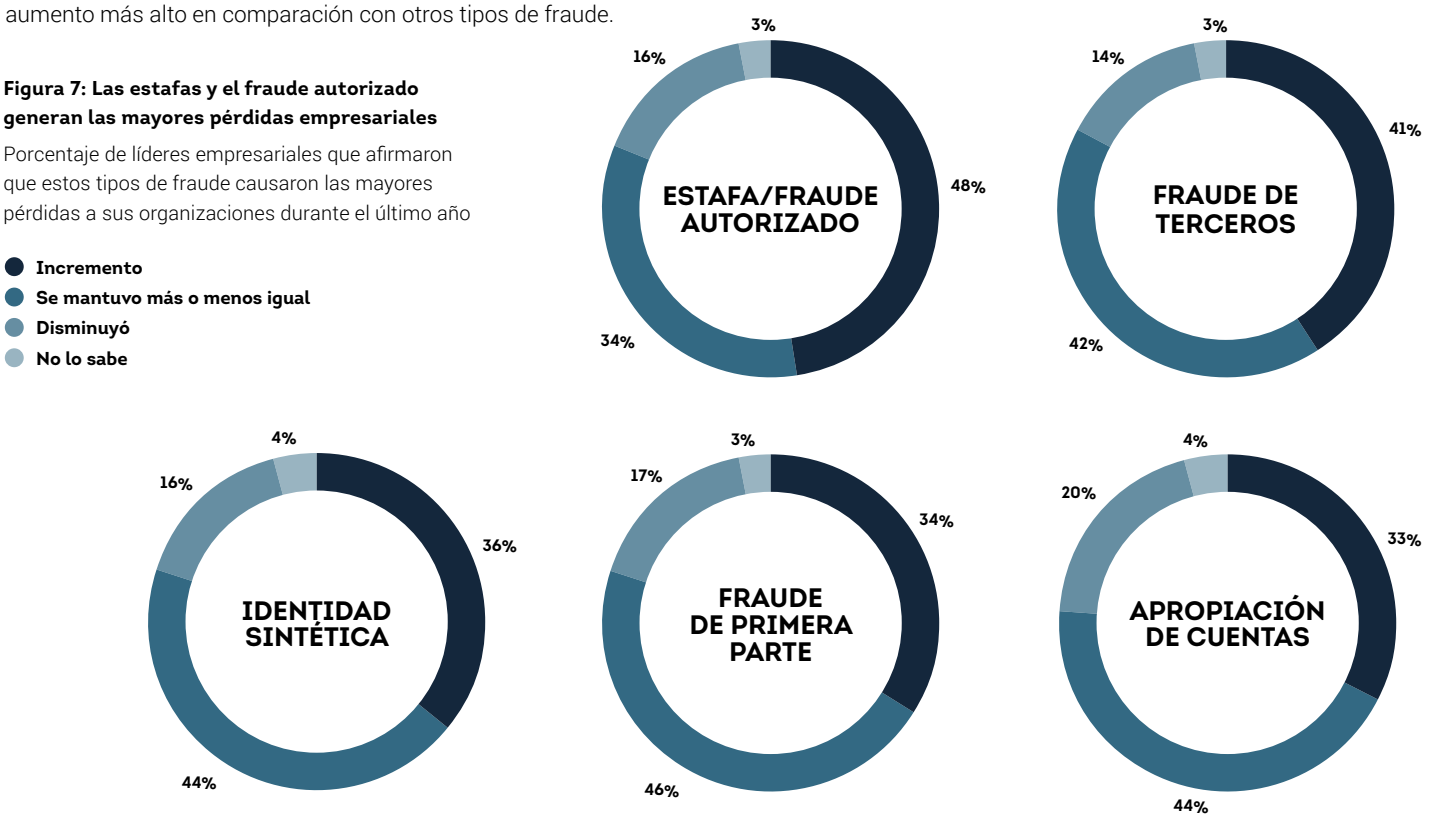
Porcentaje de líderes empresariales que afirmaron que estos tipos de fraude provocaron las mayores pérdidas para sus organizaciones durante el último año



Fuente: Encuesta sobre fraude empresarial de TransUnion, junio de 2026

Figura 7: Las estafas y el fraude autorizado generan las mayores pérdidas empresariales

Porcentaje de líderes empresariales que afirmaron que estos tipos de fraude causaron las mayores pérdidas a sus organizaciones durante el último año



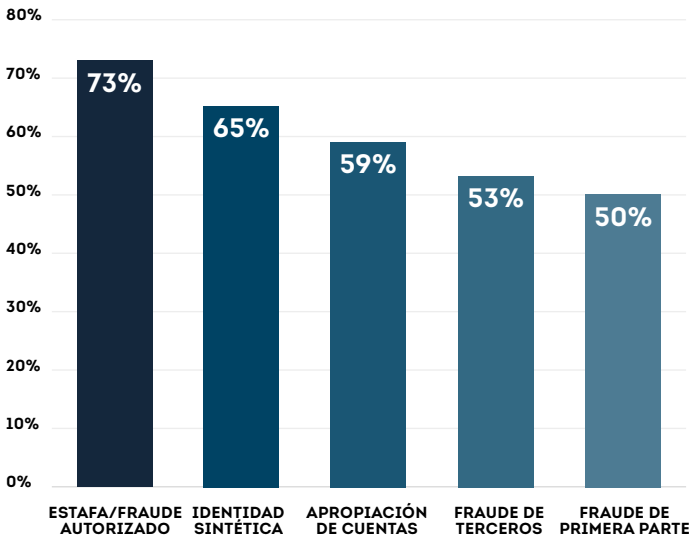
Fuente: Encuesta sobre fraude empresarial de TransUnion, junio de 2026

La suplantación de identidad corporativa es un indicador clave de futuros ataques de fraude

Las organizaciones deben considerar el riesgo de las comunicaciones como una señal de alerta temprana de fraude, que precede a ataques basados en la identidad, como la apropiación de cuentas (ATO), las estafas o el fraude autorizado y el fraude en cuentas nuevas. Si bien muchos ataques terminan en pérdidas financieras inmediatas para los consumidores, la mayoría da como resultado que los delincuentes logren recolectar datos para usarlos más adelante. Más de la mitad (56%) de las víctimas de estafas que revelaron información personal o financiera afirmaron no haber sufrido una pérdida económica.[1] Al mismo tiempo, las pérdidas de los consumidores por estafas disminuyeron drásticamente de un año a otro, lo que indica claramente que los estafadores se centran en robar información personal en lugar de buscar un robo monetario inmediato.[2] A pesar de la caída en las pérdidas por fraude a los consumidores el año pasado, las estafas o el fraude autorizado fueron el tipo de fraude que la mayoría de los líderes empresariales esperaban que creciera en los próximos dos años (véase la Figura 8).

Figura 8: Las organizaciones prevén que las estafas y el fraude autorizado crezcan más rápido que cualquier otro tipo de fraude

Porcentaje de los tres principales tipos de fraude que los líderes empresariales prevén que crecerán más en los próximos 24 meses



Fuente: Encuesta de TransUnion sobre fraude empresarial, junio de 2026

34%

De los consumidores que informaron haber sido víctimas de fraude digital, un porcentaje afirmó haber sufrido un ataque de smishing, más que cualquier otro tipo de estafa

Fuente: Encuesta Consumer Pulse de TransUnion; febrero, marzo, mayo, julio y agosto de 2026

Las comunicaciones confiables son una superficie de ataque común para las estafas de suplantación de identidad

Los consumidores esperan que las organizaciones hagan que las comunicaciones legítimas sean fáciles de verificar y que las comunicaciones fraudulentas sean fáciles de identificar. Los delincuentes se esfuerzan por socavar esa confianza, y la suplantación de identidad empresarial se ha convertido en una táctica muy extendida (véase la Figura 9). Aunque muchos hogares cuentan con múltiples dispositivos digitales, para la mayoría de las organizaciones a nivel mundial, especialmente aquellas en economías en desarrollo, las comunicaciones digitales salientes confiables se centran en el teléfono celular del consumidor. Sin embargo, las marcas no controlan la ruta hacia el dispositivo del cliente. Las vulnerabilidades en la interoperabilidad de las redes de telecomunicaciones convierten a los teléfonos celulares en objetivos principales para las estafas de suplantación de identidad que involucran llamadas y mensajes de texto falsificados.

Los estafadores aprovechan las vulnerabilidades en las redes telefónicas para ocultar sus identidades y falsificar los números de teléfono de empresas confiables, como bancos, proveedores de servicios de salud y aseguradoras. Al hacerse pasar por representantes legítimos, pueden engañar a los consumidores para que compartan códigos de acceso de un solo uso (OTP), "verifiquen" información personal, restablezcan las credenciales de sus cuentas o redirijan pagos como parte de esquemas de apropiación de cuentas.

La comunicación saliente confiable con los clientes es fundamental para mantener y fortalecer las relaciones comerciales. Las organizaciones suelen apoyarse en la educación para ayudar a proteger a los clientes contra el fraude, estableciendo políticas y canales claros sobre cuándo y por qué se pondrán en contacto con ellos, por ejemplo, mediante alertas de fraude. Sin embargo, dada la magnitud de las pérdidas ocasionadas por las estafas y el fraude autorizado, así como su crecimiento proyectado, las organizaciones deben adoptar mecanismos más robustos para proteger sus comunicaciones salientes con los clientes y reforzar la confianza en cada interacción.

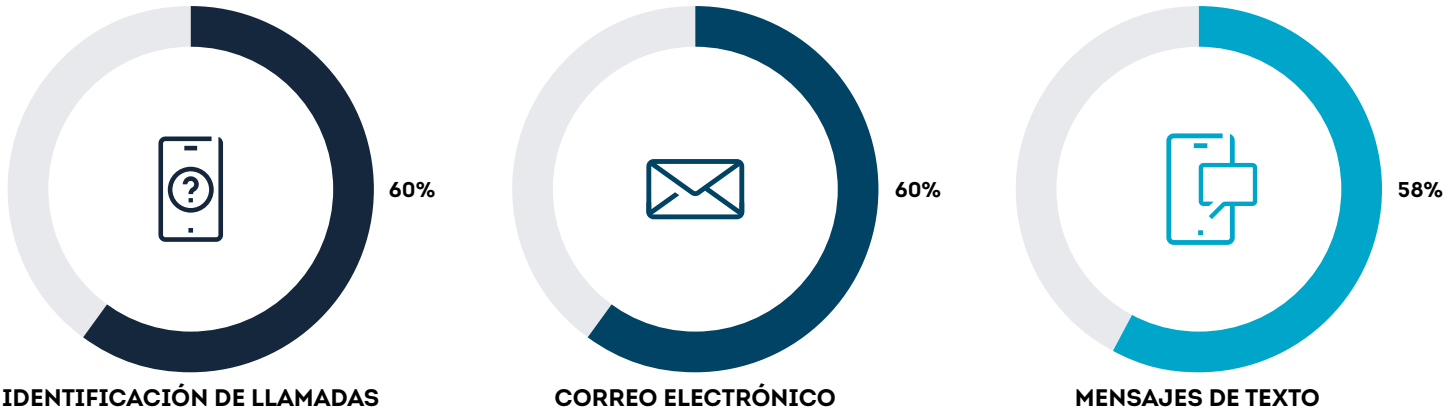
19.4%

de las llamadas salientes de empresas a consumidores realizadas a través de operadores de telefonía móvil de EE. UU. fueron falsificadas en el primer semestre de 2026

Fuente: Red de inteligencia global de TransUnion

Figura 9: La suplantación de marca está afectando a los clientes en todos los principales canales de comunicación

Porcentaje de líderes empresariales que afirmaron que los estafadores se hicieron pasar por sus organizaciones en estos canales durante el último año



Fuente: Encuesta sobre fraude empresarial de TransUnion, junio de 2026

ACCIONES RECOMENDADAS

Lo que esto significa para las organizaciones

Dado que el fraude se origina cada vez más a través de canales de comunicación confiables, las organizaciones deben ampliar su perspectiva sobre la prevención del fraude. El objetivo va más allá de simplemente autenticar a los usuarios o aprobar transacciones. Se trata de identificar la manipulación antes de que se vea comprometida la confianza. Esto requiere detectar el fraude más temprano mediante señales de riesgo en las comunicaciones relacionadas con la inteligencia de identidad, dispositivos y comportamiento, y utilizar esa inteligencia para proteger y restablecer la interacción confiable con los clientes.

1

Detectar el fraude más temprano mediante señales de riesgo en las comunicaciones

Utilice las señales de suplantación de identidad o spoofing de manera más temprana, creando oportunidades para frustrar el fraude antes de que se pongan a prueba los controles posteriores.

2

Conecte las señales de riesgo en las comunicaciones con la inteligencia de identidad

Incorpore señales de riesgo basadas en las comunicaciones junto con la inteligencia de identidad, dispositivos y comportamiento para crear una visión más dinámica y predictiva de la confianza del cliente.

3

Combata las estafas para restablecer la confianza y mejorar la interacción con el cliente

Invierta en capacidades que restablezcan la interacción de confianza más allá de los límites de la organización, bloqueen los intentos de los actores maliciosos de comprometer las credenciales y permitan respuestas coordinadas en todo el ecosistema de fraude más amplio.



La IA está permitiendo que las redes criminales operen a escala industrial

Las medidas tradicionales contra el fraude digital ya no abarcan todo el alcance de la amenaza, ya que las redes criminales aprovechan eficazmente la confianza para eludir o burlar los controles tradicionales. La IA ha transformado la economía fundamental del fraude. Permite a los estafadores automatizar actividades que históricamente requerían un esfuerzo humano significativo (por ejemplo, crear identidades y contenido, dirigir los ataques e interactuar con las víctimas), mejorando la precisión, la escala y la capacidad de adaptación de los ataques. Ha permitido a los delincuentes aumentar sus tasas de éxito en los ataques con una velocidad y escala sin precedentes, hasta el punto de industrializar toda la cadena de valor del fraude. De hecho, el 42% de los líderes empresariales afirmó que la creciente escala y/o sofisticación del fraude está ejerciendo una presión significativa o grave sobre sus organizaciones.

La cadena de valor del fraude se basa en la confianza que las organizaciones otorgan a las identidades digitales y que los consumidores depositan en las marcas (véase la Figura 10). Desde los procesos de generación de identidades hasta las inversiones a largo plazo en identidades sintéticas como activos de infraestructura, la IA está transformando la cadena de valor del fraude. Reduce el costo de ejecutar esquemas sofisticados y permite a los delincuentes explotar procesos comerciales legítimos en todos los sectores, robar activos y lavar las ganancias convirtiéndolas en activos difíciles de rastrear.

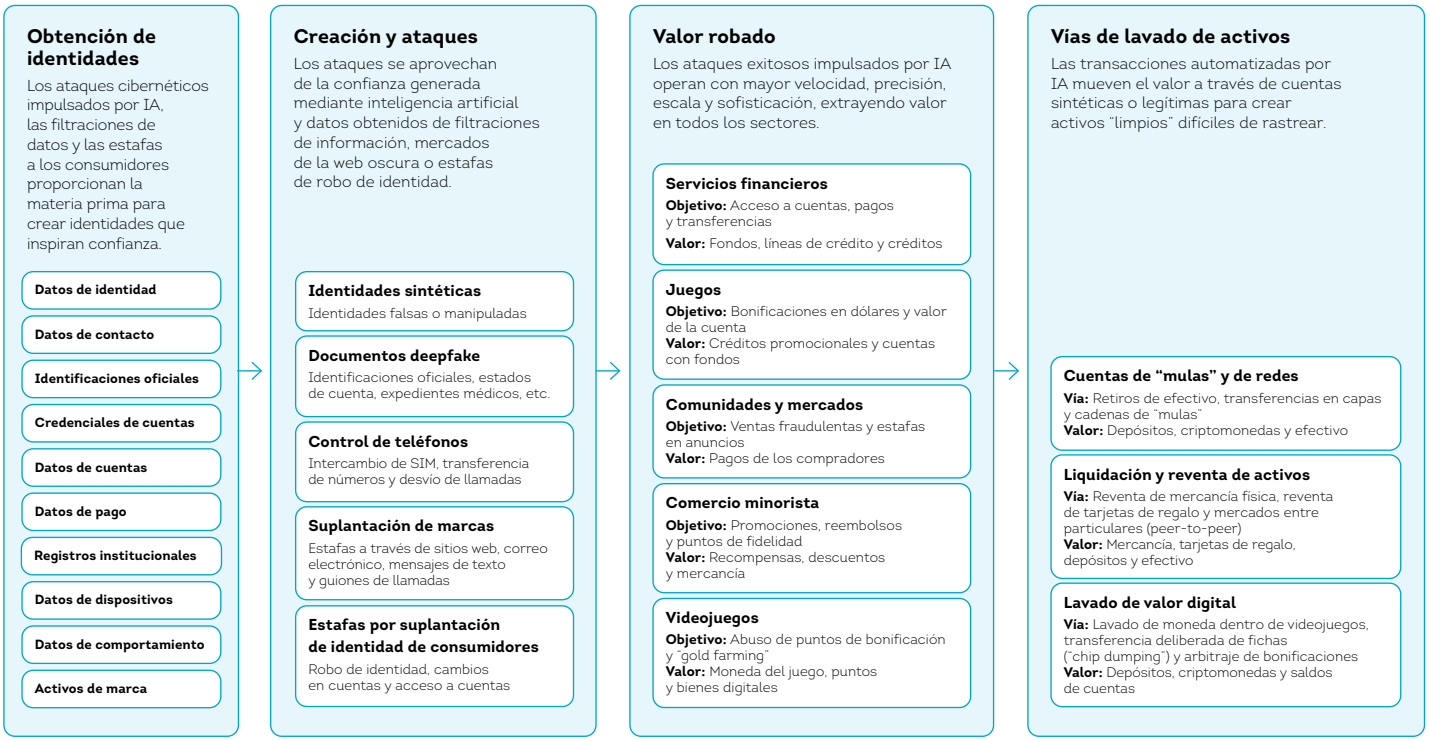
42%

Los líderes empresariales señalaron que el aumento en la magnitud y/o la sofisticación del fraude está ejerciendo una presión significativa o grave sobre sus organizaciones

Fuente: Encuesta sobre fraude empresarial de TransUnion, junio de 2026

Figura 10: Cómo el fraude industrializado convierte los datos de identidad en valor financiero

Ilustración de cómo la IA respalda cada etapa de la cadena de valor del fraude industrializado



Los estafadores se aprovechan de la confianza digital adaptándose a los entornos de prevención de fraudes

Las operaciones de fraude industrializadas se centran cada vez más en las interacciones digitales en las que se establece la confianza y, en última instancia, se puede obtener un beneficio. Sin embargo, los estafadores no atacan todos los pasos del ciclo de vida del cliente por igual (véase la Figura 11).

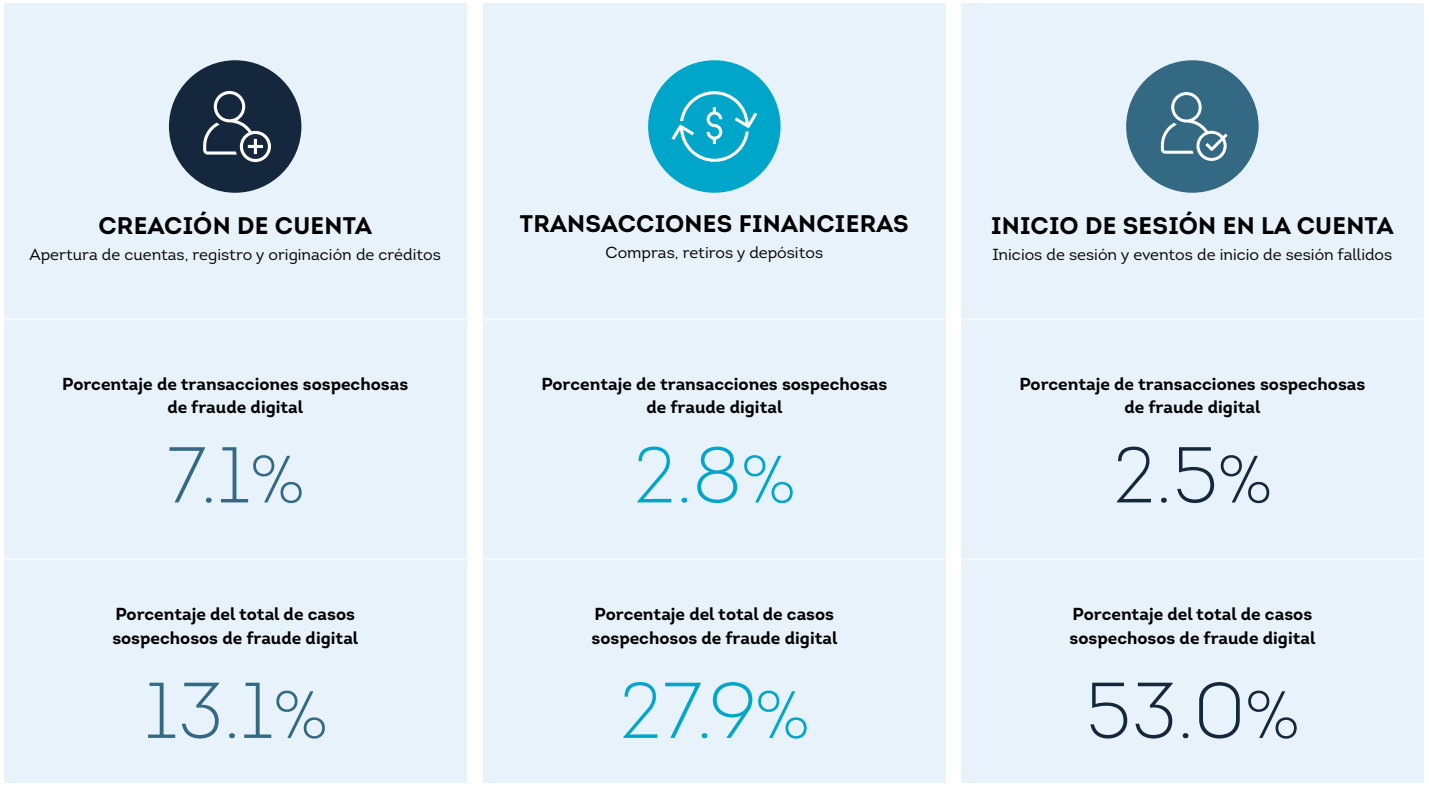
Las organizaciones han realizado importantes inversiones en controles sólidos de autenticación de clientes durante la última década, lo que ha hecho que los ataques simples basados en credenciales sean menos accesibles para los estafadores. Sin embargo, a medida que los controles de inicio de sesión han mejorado, los estafadores se han adaptado. Cada vez se enfocan más en flujos de trabajo de autenticación secundarios, como la recuperación de cuentas y las solicitudes de servicio, mediante ataques de tipo "adversario en el medio" (man-in-the-middle). La industrialización de la inteligencia artificial ha hecho que estos ataques sean más eficientes y escalables, reduciendo la necesidad de las campañas de ataque de gran volumen tradicionalmente asociadas con los flujos de trabajo de autenticación primarios.

El análisis de tres puntos específicos relacionados con la confianza digital pone de relieve los riesgos a los que se enfrentan las organizaciones:

- **La creación de cuentas** conlleva el mayor riesgo a pesar de que su volumen es relativamente menor
- **La actividad de transacciones** financieras conlleva el segundo mayor riesgo general, ya que representa el punto en el que se monetizan los ataques
- **El inicio de sesión** en las cuentas representa la mayor parte de la actividad, pero conlleva un riesgo comparativamente menor

Figura 11: La creación de cuentas conlleva el mayor riesgo de fraude, mientras que los inicios de sesión generan la mayor parte de la actividad fraudulenta

Fraude digital en el ciclo de vida del cliente en el primer semestre de 2026



Fuente: Red de inteligencia global de TransUnion

Por qué la creación de cuentas digitales sigue siendo un punto de contacto de alto riesgo

La creación de cuentas representa solo el 4,9% del volumen de transacciones, pero presenta la tasa más alta de sospechas de fraude, con un 7,1% (véase la Figura 12). La inteligencia artificial (IA) reduce el esfuerzo necesario para crear identidades sintéticas, completar formularios de solicitud, generar documentos "deepfake" y automatizar todo el proceso de incorporación. Si bien los estafadores abren cuentas principalmente para monetizar identidades robadas o sintéticas, también lo hacen para facilitar las vías de lavado de dinero, limpiando fondos ilícitos y ocultando sus identidades mientras realizan actividades ilegales. Algunas industrias no le dan importancia a una verificación rigurosa de la identidad al momento de la creación de cuentas porque esto obstaculiza las conversiones. Las organizaciones suelen establecer controles en la creación de cuentas en función del valor que se ofrece al consumidor. Por ejemplo, es probable que un minorista no le pida a un comprador que cree una cuenta para recibir un código de descuento del 10% a cambio de su dirección de correo electrónico. Si bien alinear el intercambio de valor con la fricción del cliente es una decisión comercial razonable, puede implicar depositar confianza en una identidad de riesgo destinada a actividades fraudulentas en el futuro

Para reducir este riesgo, es posible que las organizaciones deban adoptar controles de verificación de identidad similares a los de los sectores regulados, como el bancario, el crediticio y el de juegos de azar. Estas organizaciones deben aplicar medidas de cumplimiento normativo de "conozca a su cliente" (KYC) y contra el lavado de dinero (AML) a los flujos de trabajo de creación de cuentas, con el fin de ayudar a detener las actividades de lavado de dinero y reducir las vías para el fraude en etapas avanzadas de la cadena de valor. El fraude industrializado puede crear miles de cuentas nuevas utilizando identidades sintéticas o robadas que parecen legítimas. Si bien los procesos tradicionales validan los atributos de identidad individuales, a menudo se evalúan de manera aislada, pasando por alto las señales de confianza que pueden revelar redes criminales y redes de fraude.

Figura 12: Los sectores con menores medidas de garantía de identidad enfrentan un mayor riesgo de fraude en la creación de cuentas

Los cinco sectores con la tasa más alta de presuntos casos de fraude digital en la creación de cuentas durante el primer semestre de 2026

Industria	Intentos de creación de cuentas que se sospecha que son fraude digital	Método de verificación de identidad
TODAS LAS INDUSTRIAS	7.1%	
COMERCIO MINORISTA	15.9%	Verificación de identidad sencilla para que la creación de cuentas sea lo más sencilla posible
COMUNIDADES	11.5%	Verificación de identidad de leve a rigurosa para ayudar a proteger a los miembros de la comunidad, según el valor percibido del servicio
VIDEO GAMING	9.6%	Verificación de identidad sencilla para que la creación de cuentas sea lo más fluida posible
SERVICIOS FINANCIEROS	6.7%	Verificación rigurosa de la identidad para cumplir con los requisitos normativos y reducir el riesgo crediticio
JUEGOS DE AZAR	6.5%	Verificación rigurosa de la identidad para cumplir con los requisitos normativos y geográficos

Fuente: Red de inteligencia global de TransUnion

Los ataques de fraude optimizados para la monetización ponen de relieve el riesgo en las etapas finales del ciclo de vida

Si bien las transacciones financieras y el inicio de sesión en cuentas representan un riesgo similar en general, con la excepción de los seguros y los videojuegos, las transacciones financieras conllevan el mayor riesgo de fraude observado (véase la Figura 13). El fraude industrializado se optimiza para la monetización.

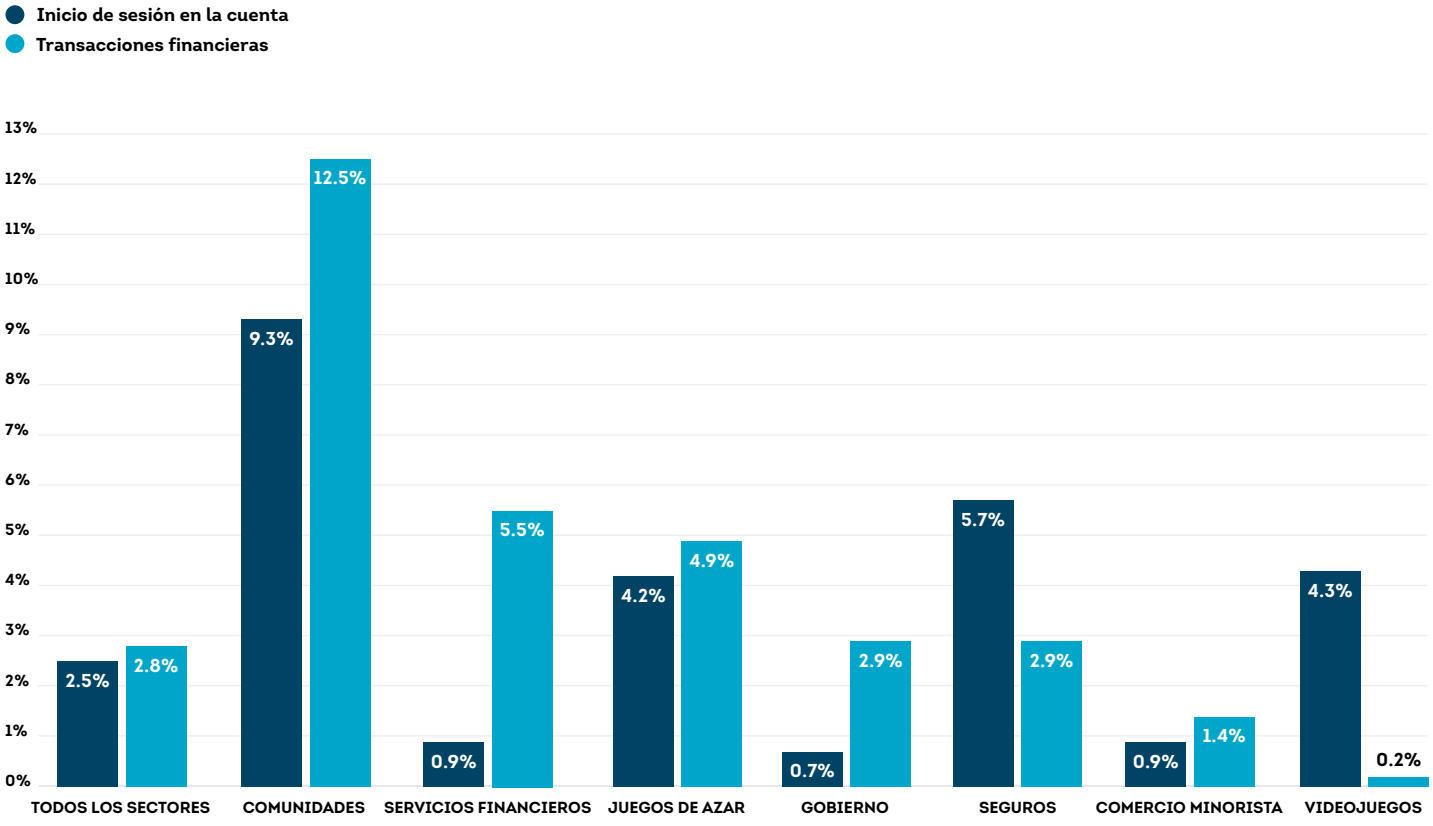
El riesgo en las transacciones financieras respalda esta realidad. La inteligencia artificial (IA) puede facilitar aún más la monetización al identificar objetivos, priorizar oportunidades y automatizar actividades diseñadas para extraer valor de cuentas ya establecidas y de sectores en los que las evaluaciones continuas de autenticación son menos rigurosas.

Si bien el sector de los servicios financieros ha realizado inversiones significativas en la autenticación de cuentas y el monitoreo de transacciones, la optimización excesiva de la experiencia del cliente puede dejar a las transacciones financieras en una posición vulnerable. Al mismo tiempo, tanto las comunidades como los videojuegos enfrentan un riesgo elevado tanto en las transacciones financieras como en el inicio de sesión en cuentas.

En el sector gaming, el riesgo de fraude es similar tanto en el inicio de sesión como en las transacciones financieras. Si bien la mayoría de las plataformas cuentan con reglas de geovallado que impiden a los usuarios acceder a sus cuentas en jurisdicciones donde los juegos de azar son ilegales, la ATO sigue siendo un problema debido a que los jugadores mantienen saldos en efectivo y de bonos. Aunque el sector de los juegos de azar sigue regulaciones contra el lavado de dinero similares a las de los servicios financieros, una industria basada en transacciones financieras de gran volumen será un blanco fácil. Las comunidades operan basándose en la confianza de sus miembros, a menudo con procesos de creación de cuentas menos restrictivos, lo que se traduce en un riesgo superior al promedio para el inicio de sesión y las transacciones. Estas plataformas brindan a las delincuentes oportunidades para actuar en cada etapa de la cadena de valor del fraude, dependiendo del modelo de negocio de la comunidad. Potenciadas por la inteligencia artificial, las comunidades son particularmente vulnerables a las cuentas sintéticas, la suplantación de identidad, las estafas en compras y la liquidación de activos.

Figura 13: El fraude en transacciones financieras a menudo iguala o supera el riesgo de fraude en el inicio de sesión

Porcentaje de cada tipo de transacción en la que se sospecha de fraude digital en sectores seleccionados durante el primer semestre de 2026



Fuente: Red de inteligencia global de TransUnion

ACCIONES RECOMENDADAS

Lo que esto significa para las organizaciones

El fraude industrializado está cambiando la dinámica económica de los ataques y la defensa. La inteligencia artificial permite a los estafadores probar, perfeccionar y ampliar sus ataques más rápido de lo que muchas organizaciones pueden adaptar sus controles. Como resultado, el riesgo se desplaza cada vez más hacia el punto más débil del ciclo de vida del cliente, en lugar de permanecer concentrado en una sola etapa.

El fraude se ha vuelto adaptativo e industrializado. Por lo tanto, la prevención del fraude debe volverse adaptativa e integrada. Las organizaciones que dependen de controles estáticos, señales inconexas y actualizaciones periódicas pueden tener dificultades para mantenerse al día con las amenazas que evolucionan rápidamente. En cambio, deben aprender continuamente de los patrones de fraude emergentes, integrar la inteligencia a lo largo de todo el ciclo de vida del cliente y automatizar las decisiones siempre que sea posible.

1 **Igualar la velocidad y la escala de los ataques impulsados por la IA**

Asuma que los ataques de fraude seguirán volviéndose más eficientes y construya defensas que puedan adaptarse a un ritmo similar.

2 **Modernizar la toma de decisiones con inteligencia adaptativa**

Complementar los controles tradicionales con inteligencia adaptativa que aprenda continuamente de las señales de fraude emergentes y las técnicas de ataque en constante evolución.

3 **Crear operaciones contra el fraude versátiles y ágiles**

Modernizar la detección de fraudes, pero también la investigación, la toma de decisiones y la respuesta. El éxito dependerá cada vez más de la combinación de datos confiables, análisis avanzados y automatización para proteger a los clientes, al tiempo que se mantienen experiencias sin fricciones.



Perspectivas Regionales



Resumen América Latina



La dinámica de la rápida adopción digital en América Latina expone a más consumidores y empresas al fraude. La transición de la región del efectivo a los pagos digitales está en constante evolución, y la confianza, la interoperabilidad y las condiciones específicas del mercado determinan dicha adopción.[3] El comercio centrado en los dispositivos móviles, los servicios financieros digitales y los pagos instantáneos están ampliando el acceso, lo que aumenta el número y la velocidad de las interacciones que las organizaciones deben proteger.

La tasa de sospechas de fraude digital en América Latina fue casi tres veces superior al promedio mundial. Y al igual que las tendencias globales, el volumen de riesgo de fraude digital en América Latina fue mayor en el momento del inicio de sesión en las cuentas. Muchas organizaciones, especialmente las instituciones financieras, le dan gran importancia a la verificación de identidad al momento de la creación de la cuenta; sin embargo, el riesgo de identidad va más allá de la incorporación y requiere una evaluación continua a lo largo de todo el ciclo de vida del cliente.

Si bien la manipulación de identidades impulsada por la inteligencia artificial y el fraude de identidades sintéticas apuntan a un fraude cada vez más industrializado, las tendencias más marcadas en América Latina son el riesgo de identidad a lo largo del ciclo de vida, el riesgo de confianza derivado de las comunicaciones y el cambio de la verificación de identidad a la inteligencia de prevención de fraude de extremo a extremo. A medida que crece la participación digital, el riesgo de fraude se extiende a la creación de cuentas, el inicio de sesión, las comunicaciones y los pagos.

PUNTOS CLAVE

Hoy en día, la confianza digital se gana o se pierde a través de la comunicación

33%

de los consumidores latinoamericanos que afirmaron haber sido víctimas recientemente de fraude digital reportaron haber sido objeto de phishing, lo que lo convierte en la estafa digital más denunciada por los consumidores en la región

Las organizaciones deben pasar de la verificación a la inteligencia contra el fraude de principio a fin

10.4%

de las transacciones de servicios financieros con clientes latinoamericanos fueron objeto de sospechas de fraude digital en el primer semestre de 2026, lo que la convierte en la industria de mayor riesgo de la región

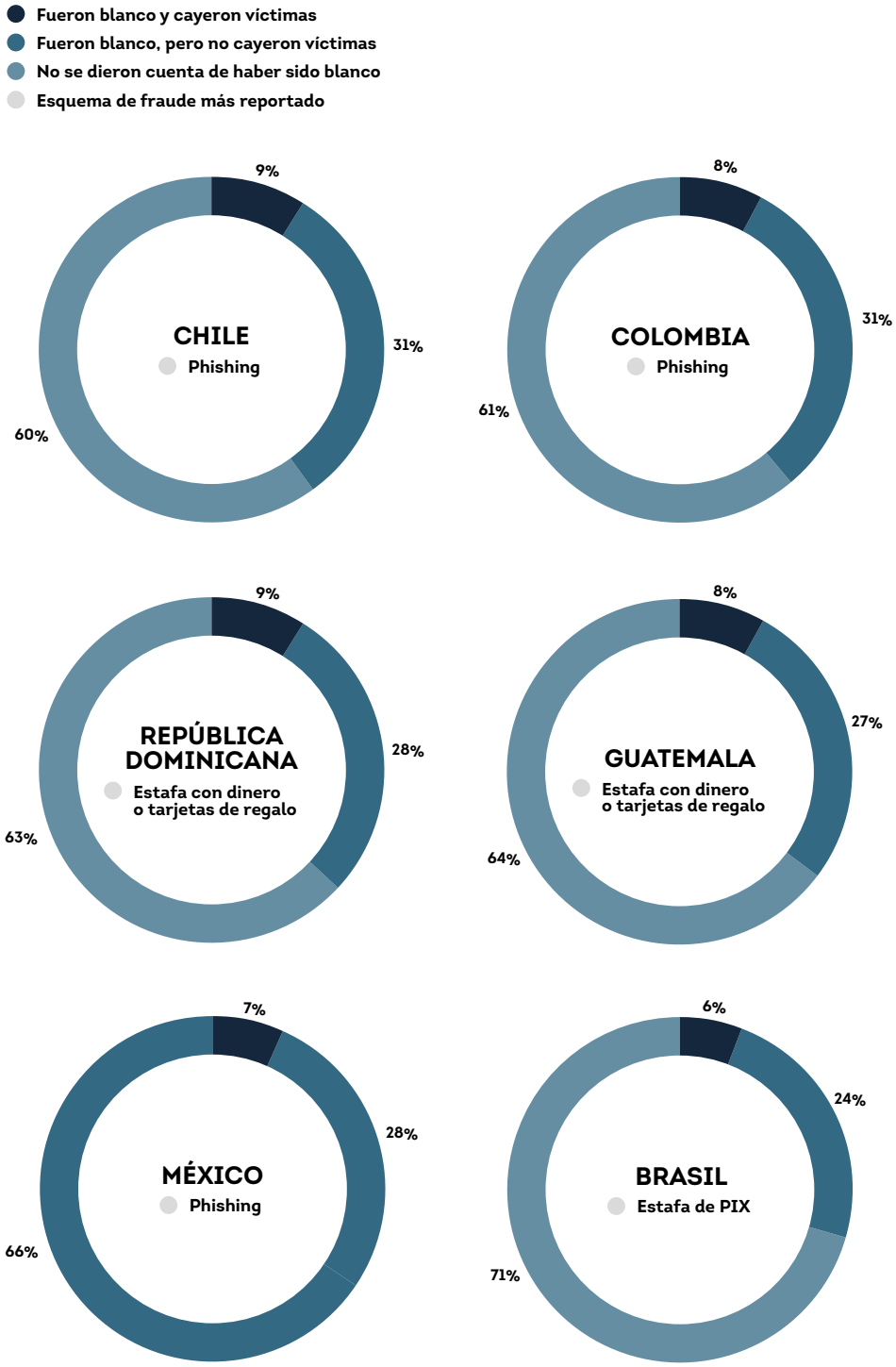
Los estafadores se aprovechan de las relaciones comerciales que priorizan los dispositivos móviles

Los canales de comunicación móvil son fundamentales en la forma en que el fraude llega a los consumidores en América Latina. Entre los consumidores que indicaron haber sido blanco de estafadores mediante fraude digital en un período reciente de tres meses, el "vishing" fue la estafa más reportada por los consumidores en los países latinoamericanos encuestados (véase la Figura 14). Esto concuerda con una tendencia más amplia hacia la ingeniería social, en la que los estafadores utilizan la urgencia, la suplantación de identidad y canales de comunicación familiares para persuadir a los consumidores de que actúen.

La exposición de los consumidores fue significativa en América Latina, destacando Chile y la República Dominicana, donde el 9% de los consumidores en esos mercados afirmó haber sido víctima de fraude digital. La implicación para las organizaciones es clara: la confianza no puede protegerse únicamente dentro de una aplicación o un sitio web. Los controles contra el fraude, las comunicaciones con los clientes y la educación deben funcionar de manera integrada a través de llamadas, mensajes de texto y correo electrónico, con una verificación reforzada cuando una solicitud, un dispositivo o un patrón de pago se desvíe del comportamiento esperado.

Figura 14: El fraude telefónico se convirtió en la estafa más reportada en gran parte de América Latina

Porcentaje de consumidores que afirmaron haber sido blanco de estafadores mediante esquemas de fraude en línea, por correo electrónico, por teléfono o por mensajes de texto en un período reciente de tres meses, y el esquema de fraude más reportado



Fuente: Estudio Consumer Pulse de TransUnion, julio de 2026

Los servicios financieros destacan el riesgo en la economía de los pagos digitales

El cambio de verificar la identidad en un momento específico a comprender el riesgo a lo largo de todo el recorrido del cliente es especialmente importante en los servicios financieros. El sector registró una tasa de sospechas de fraude digital del 10,4% entre los clientes latinoamericanos en el primer semestre de 2026, la más alta de los sectores analizados en la región (véase la Figura 15). Esa presión va en aumento a medida que los pagos digitales y el acceso a las cuentas se vuelven cada vez más fundamentales para la actividad financiera cotidiana.

La tecnología aumenta el costo de una prevención del fraude fragmentada

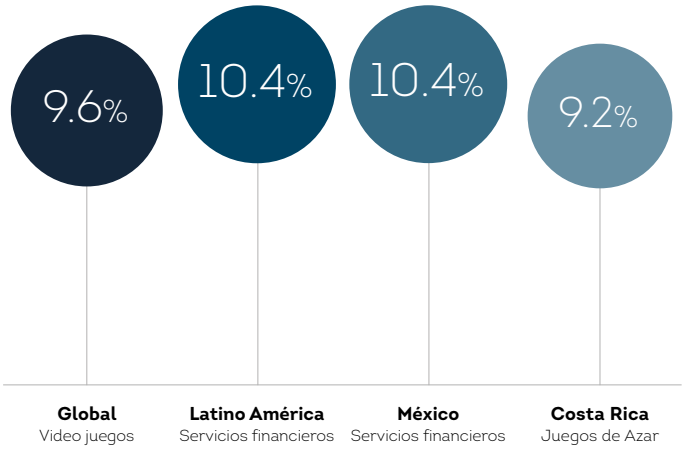
La presión del fraude está aumentando a medida que el entorno tecnológico se vuelve más complejo. En general, el 70% de los líderes empresariales de Brasil clasificaron el riesgo de fraude como el más alto entre sus tres principales riesgos de impacto en los negocios, en comparación con el 61% de referencia global (véase la Figura 16). Las preocupaciones por las violaciones de la ciberseguridad también ocuparon un lugar destacado en Brasil.

En lo que respecta a la lucha contra el fraude, las nuevas tecnologías podrían estar complicando la situación; el 80% de los profesionales del sector comercial a nivel mundial mencionaron la eficacia de los datos y la tecnología como desafíos que afectan la prevención del fraude.[4] El problema no es simplemente la falta de herramientas. Los datos desconectados, la calidad irregular de la señal y los controles que operan de manera aislada pueden ralentizar las decisiones o generar fricciones innecesarias con los consumidores sin mejorar la detección.

A medida que la inteligencia artificial y la automatización facilitan la ampliación de los ataques, las empresas necesitan un modelo operativo integrado que combine tecnología con gobernanza, equipos calificados, intercambio de inteligencia y resultados de decisiones medibles. Pero las estrategias efectivas también deben reflejar las realidades locales. Los canales de pago, la madurez digital, la regulación, el comportamiento de los clientes y las tácticas de fraude difieren entre los distintos mercados. El éxito depende de convertir un volumen creciente de señales en acciones más rápidas y precisas.

Figura 15: El sector de servicios financieros enfrenta el mayor riesgo de fraude digital en América Latina

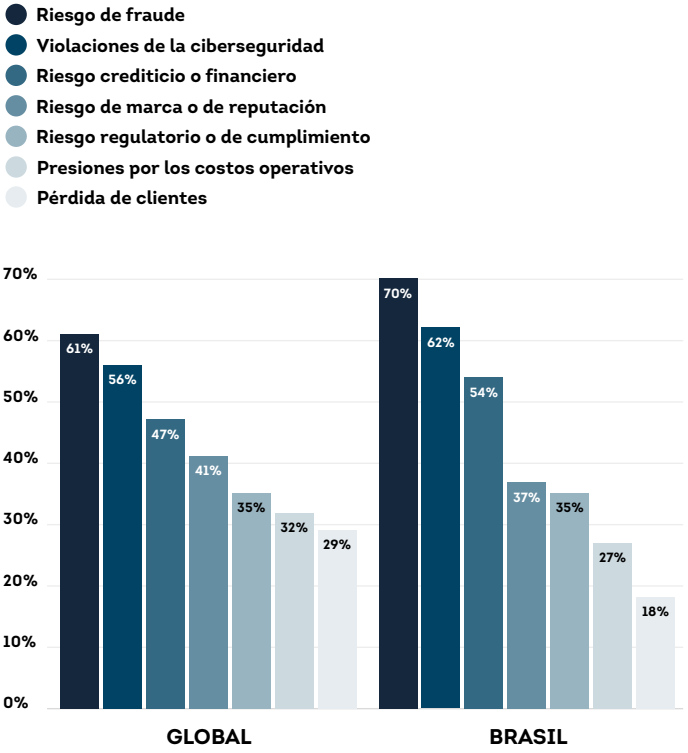
Industria con la tasa más alta de sospecha de fraude digital en la región y su tasa correspondiente durante el primer semestre de 2026 (H1 2026)



Fuente: Red de inteligencia global de TransUnion

Figura 16: El fraude se ha convertido en uno de los principales riesgos empresariales en Brasil

Porcentaje de líderes empresariales que incluyeron estos riesgos entre sus tres principales en cuanto a impacto potencial en el negocio



Fuente: Encuesta sobre fraude empresarial de TransUnion, junio de 2026

Moldeando la Próxima Era de la Confianza Digital

En todas las regiones analizadas en este informe se observa el mismo patrón: el fraude se está volviendo cada vez más interconectado, cada vez más adaptable y más difícil de contener dentro de los límites organizacionales tradicionales. La inteligencia artificial, las redes de fraude industrializadas, los ecosistemas digitales en expansión y las expectativas regulatorias en constante evolución están cambiando no solo la forma en que se comete el fraude, sino también la forma en que se debe establecer y mantener la confianza misma. A medida que el fraude se extiende a través de identidades, dispositivos, comunicaciones, organizaciones y canales, ninguna señal o control por sí solo será suficiente. La próxima etapa de la prevención del fraude se definirá por la forma en que las organizaciones establezcan la confianza en ecosistemas completos de clientes, en lugar de hacerlo solo en transacciones aisladas. Exploramos hacia dónde podría llevar al mercado el cambio hacia el establecimiento de una confianza continua en ecosistemas completos de consumidores.



1

Los consumidores se protegen de los riesgos digitales con aplicaciones de seguridad específicas

La próxima generación de protección de identidad se basará en escudos digitales impulsados por inteligencia artificial que ayudarán a los consumidores a determinar si pueden confiar en una interacción antes de actuar.

Señales del mercado

Las aplicaciones móviles para consumidores ya evalúan la identidad de quien llama, la reputación de las empresas, las etiquetas de estafas y los mensajes verificados.

Cómo prepararse

Piensa más allá del monitoreo de identidad y la corrección posterior a los incidentes, y enfócate en una protección proactiva del consumidor que detecte la manipulación a tiempo y les ayude a evitar acciones irreversibles.

2

El nombre de usuario comenzará a desaparecer

Las claves de acceso, los dispositivos de confianza, las carteras digitales y las credenciales reutilizables harán que los inicios de sesión tradicionales sean menos visibles y menos centrales.

Señales del mercado

Las claves de acceso están disponibles en los principales ecosistemas tecnológicos. Las carteras digitales y los sistemas nacionales de identidad, como Apple Wallet, la Cartera de Identidad Digital de la UE, Aadhaar y Singpass, siguen expandiéndose.

Cómo prepararse

Diseña la autenticación en torno a una identidad establecida de manera continua en todos los dispositivos, credenciales e interacciones, en lugar de basarla en un solo inicio de sesión.

3

La defensa contra el fraude se convierte en una red, no en un producto

La inteligencia colectiva revelará relaciones, patrones y amenazas que ninguna organización puede identificar por sí sola.

Señales del mercado

Las redes de intercambio de datos, como Cifas[5], Stop Scams UK[6] y el Centro Antifraude de Singapur[7], demuestran este cambio. Las regulaciones de EE. UU. también respaldan el intercambio de información[8].

Cómo prepararse

Determina en qué aspectos la inteligencia de consorcios, la colaboración que preserva la privacidad y las alianzas intersectoriales pueden fortalecer las defensas propias.

4

Demostrar la identidad ya no será suficiente para generar confianza digital

La verificación de la identidad seguirá siendo esencial, pero no garantizará que una interacción sea confiable.

Señales del mercado

El aumento de las estafas y los fraudes autorizados pone de manifiesto los límites de la verificación de identidad por sí sola.

Cómo prepararse

Integre la verificación de identidad con la inteligencia de dispositivos, comportamiento, comunicaciones y redes a lo largo de todo el ciclo de vida del cliente. No se limite a preguntar: "¿Es esta la persona correcta?", sino también: "¿Se puede confiar en esta interacción? "

5

La inteligencia contra el fraude adoptará un lenguaje operativo común

El sector adoptará formas más consistentes de describir las tácticas, técnicas y comportamientos relacionados con el fraude.

Señales del mercado

El Marco de Lucha contra el Fraude de MITRE ofrece una taxonomía basada en el comportamiento para los autores de fraudes financieros.[9]

Cómo prepararse

Alinear las clasificaciones de fraude con los marcos emergentes y desarrollar arquitecturas de datos que respalden una inteligencia contra el fraude interoperable y legible por máquina.

El futuro conectado de la prevención del fraude

La lección más importante que nos deja el panorama global del fraude no es que el fraude se haya vuelto más sofisticado, sino que la confianza se ha vuelto más valiosa.

Durante décadas, las organizaciones trataron la confianza como un evento puntual que se establecía durante el proceso de incorporación, la autenticación o la aprobación de una transacción. Ese modelo está cada vez más desconectado de cómo opera el fraude digital hoy en día.

El fraude ahora se aprovecha de las identidades después de que se verifican, de las comunicaciones después de que se envían y de las relaciones después de que se establecen. Las organizaciones ya no pueden separar la experiencia del cliente, la gestión de riesgos y la prevención del fraude en disciplinas independientes. Se han convertido en componentes interconectados de un mismo desafío: determinar si se puede confiar en una interacción digital.

Las organizaciones que tengan éxito no serán necesariamente aquellas que detecten la mayor cantidad de fraudes. Serán aquellas que generen mayor confianza en los clientes, eliminen las fricciones innecesarias y tomen mejores decisiones a través de la inteligencia conectada.

En la próxima era del comercio digital, la confianza ya no será un control. Será un activo. Y, cada vez más, será una ventaja competitiva.

1,2 Javelin Group, Estudio de Fraude de Identidad 2026: La ilusión del progreso, abril de 2026.
3 Banco Interamericano de Desarrollo (BID), Más allá del efectivo: La revolución de los pagos digitales en América Latina y el Caribe, septiembre de 2025.
4 Merchant Risk Council, Encuesta Global de Pagos Electrónicos y Fraude 2026, marzo de 2026.
5 Cifas.
6 Stop Scams UK.
7 Centro Antiestafas de Singapur.
8 Red para el Control de Delitos Financieros (FinCEN) del Departamento del Tesoro de Estados Unidos, Hoja informativa de la Ley USA PATRIOT, Sección 314(b), 12 de junio de 2026.
9 Centro para la Defensa Informada sobre Amenazas del MITRE, Marco de Fraude Fight, abril de 2026.



Acerca de la Investigación

Este informe combina los resultados de encuestas encargadas a empresas y consumidores con información derivada de la inteligencia propia de TransUnion en materia de fraude, identidad, crédito y comunicaciones.

Encuesta sobre fraude empresarial

Los resultados de la encuesta empresarial que se presentan en este informe se basan en las respuestas de 1,600 responsables de la toma de decisiones en materia de fraude y riesgo en grandes organizaciones orientadas al consumidor de Brasil, Canadá, Hong Kong, India, Filipinas, España, el Reino Unido y los Estados Unidos. La encuesta fue realizada en línea del 5 al 12 de junio de 2026 por TransUnion, en colaboración con el proveedor externo de investigación Dynata. Los encuestados tenían responsabilidades gerenciales en materia de fraude y/o riesgo y representaban a organizaciones con ingresos anuales superiores a 300 millones de reales brasileños (BRL) en Brasil, 300 millones de dólares canadienses (CAD) en Canadá, 200 millones de dólares de Hong Kong (HKD) en Hong Kong, 1 mil millones de rupias indias (INR) en la India, 1 mil millones de pesos filipinos (PHP) en Filipinas, 150 millones de euros (EUR) en España, 200 millones de libras esterlinas (GBP) en el Reino Unido y 200 millones de dólares estadounidenses (USD) en Estados Unidos. La encuesta se llevó a cabo a través de un panel de investigación en línea y se completó en computadoras de escritorio, dispositivos móviles y tabletas. Es posible que los porcentajes no sumen el 100% debido al redondeo, ya que algunas preguntas permitían respuestas múltiples o se excluyeron las respuestas “no sé” y “ninguna de las anteriores”.

Encuesta del Consumer pulse

Los resultados de la encuesta a consumidores que se presentan en este informe se basan en las respuestas de más de 13 500 adultos mayores de 18 años en 19 mercados de todo el mundo. La encuesta fue realizada por TransUnion en colaboración con Dynata, una empresa externa de investigación, mediante un panel de investigación en línea. El trabajo de campo se llevó a cabo entre el 10 de febrero y el 7 de agosto de 2026 en Botsuana, Brasil, Canadá, Chile, Colombia, la República Dominicana, Guatemala, Hong Kong, India, Kenia, México, Namibia, Filipinas, Ruanda, Sudáfrica, España, el Reino Unido, Estados Unidos y Zambia. Los encuestados completaron la encuesta a través de computadoras de escritorio, dispositivos móviles y tabletas. Las preguntas de la encuesta se presentaron en chino (Hong Kong), inglés, francés (Canadá), portugués (Brasil) y español (Colombia, República Dominicana, Guatemala y España). Para garantizar que los resultados fueran representativos, se utilizaron cuotas para equilibrar las respuestas según características demográficas clave, como la edad, el género y los ingresos. Es posible que los porcentajes no sumen el 100% debido al redondeo o a que algunas preguntas permitían respuestas múltiples.

Filtraciones de datos

Los hallazgos sobre fugas de datos que se presentan en este informe provienen de la base de datos propia de TransUnion sobre fugas de datos, la cual se mantiene en colaboración con el Centro de Recursos contra el Robo de Identidad (ITRC). La base de datos da seguimiento a los incidentes de exposición de datos en EE. UU. que se han reportado públicamente, utilizando información de fuentes que incluyen a los fiscales generales estatales, divulgaciones de organizaciones, bufetes de abogados y expertos en ciberseguridad. Cada fuga se evalúa mediante el Perfil de Amenazas de Identidad TruEmpower™ de TransUnion, el cual analiza las credenciales de identidad expuestas, las características de la fuga y el riesgo asociado para el consumidor. A las filtraciones se les asigna una puntuación de gravedad en una escala del 1 al 10, donde 1 representa el nivel más bajo de riesgo y 10, el más alto. Los porcentajes reportados de datos de identidad expuestos se calculan únicamente a partir de las filtraciones en las que se reveló información de credenciales comprometidas y no representan todas las filtraciones de datos reportadas. Los datos sobre violaciones de seguridad son una de las múltiples señales de riesgo que se utilizan en la creación de la Puntuación de Seguridad de Identidad de TransUnion, la cual ayuda a evaluar el perfil general de riesgo de identidad de una persona y a priorizar las medidas de protección recomendadas.

Fraude digital

Los hallazgos sobre fraude digital que se presentan en este informe provienen de la información de TransUnion, que abarca miles de millones de transacciones en más de 40,000 sitios web y aplicaciones en todo el mundo. La tasa de sospecha de fraude digital representa el porcentaje de transacciones identificadas por los clientes de TransUnion como fraudulentas o que violan la política de la organización. Esto incluye transacciones rechazadas en tiempo real debido a indicadores de fraude o violaciones de políticas, así como transacciones confirmadas posteriormente mediante investigaciones de clientes o usuarios. Los análisis por país y región se basan en transacciones asociadas con clientes que operan en el mercado correspondiente. Los resultados globales reflejan la actividad de transacciones en todos los países representados dentro de la red de TransUnion y no se limitan a los mercados destacados en este informe. Al analizar el volumen de transacciones por etapa del recorrido del cliente, se excluyeron las transacciones clasificadas como “otras”. Como resultado, es posible que los porcentajes de las distintas etapas del recorrido del cliente no sumen el 100%.

Llamadas salientes

Los hallazgos sobre llamadas salientes que se presentan en este informe provienen de datos de operadores de telefonía celular relacionados con llamadas a consumidores de EE. UU. en las que los estafadores se hicieron pasar por instituciones financieras legítimas.

La tasa de llamadas falsificadas reportada refleja los casos en los que se falsificó la información de identidad de la persona que llamaba para que pareciera que las llamadas provenían de una institución financiera de confianza.

Dado que los operadores de telefonía celular pueden intentar volver a conectar las llamadas fallidas varias veces, los volúmenes y las tasas de llamadas falsificadas reportados pueden estar ligeramente elevados.

Fraude sintético

Los hallazgos sobre el fraude sintético en este informe se derivan principalmente de la base de datos de crédito de consumidores de TransUnion en EE. UU., la cual contiene información crediticia de aproximadamente 400 millones de consumidores en todos los estados, territorios e instalaciones militares de EE. UU., tanto en el país como en el extranjero.

La base de datos incorpora más de 50 años de historial crediticio de los consumidores. Los análisis de fraude sintético incluyeron la actividad crediticia en EE. UU. registrada entre el 1 de enero de 2009 y el 30 de junio de 2026.

Las estimaciones de la exposición de los prestamistas se calcularon utilizando la metodología propia de TransUnion, diseñada para cuantificar las pérdidas potenciales de los prestamistas asociados con el fraude de identidad sintético.

ACERCA DE TRANSUNION (NYSE: TRU)

TransUnion es una empresa global de información y análisis con más de 13.000 colaboradores que opera en más de 30 países. Hacemos posible la confianza al garantizar que cada persona esté representada de manera confiable en el mercado. Lo logramos mediante un perfil Tru™ de cada persona: una visión práctica de los consumidores, gestionada con cuidado. A través de nuestras adquisiciones e inversiones en tecnología, hemos desarrollado soluciones innovadoras que van más allá de nuestra sólida base en el crédito básico hacia áreas como la mercadotecnia, el fraude, el riesgo y el análisis avanzado. Como resultado, los consumidores y las empresas pueden realizar transacciones con confianza y lograr grandes cosas. A esto lo llamamos Information for Good® – y genera oportunidades económicas, excelentes experiencias y empoderamiento personal para millones de personas en todo el mundo.

transunion.co/empresas

© Derechos de autor 2026 TransUnion, sus subsidiarias y/o afiliadas. Todos los derechos reservados. GFS-26-459080

TransUnion