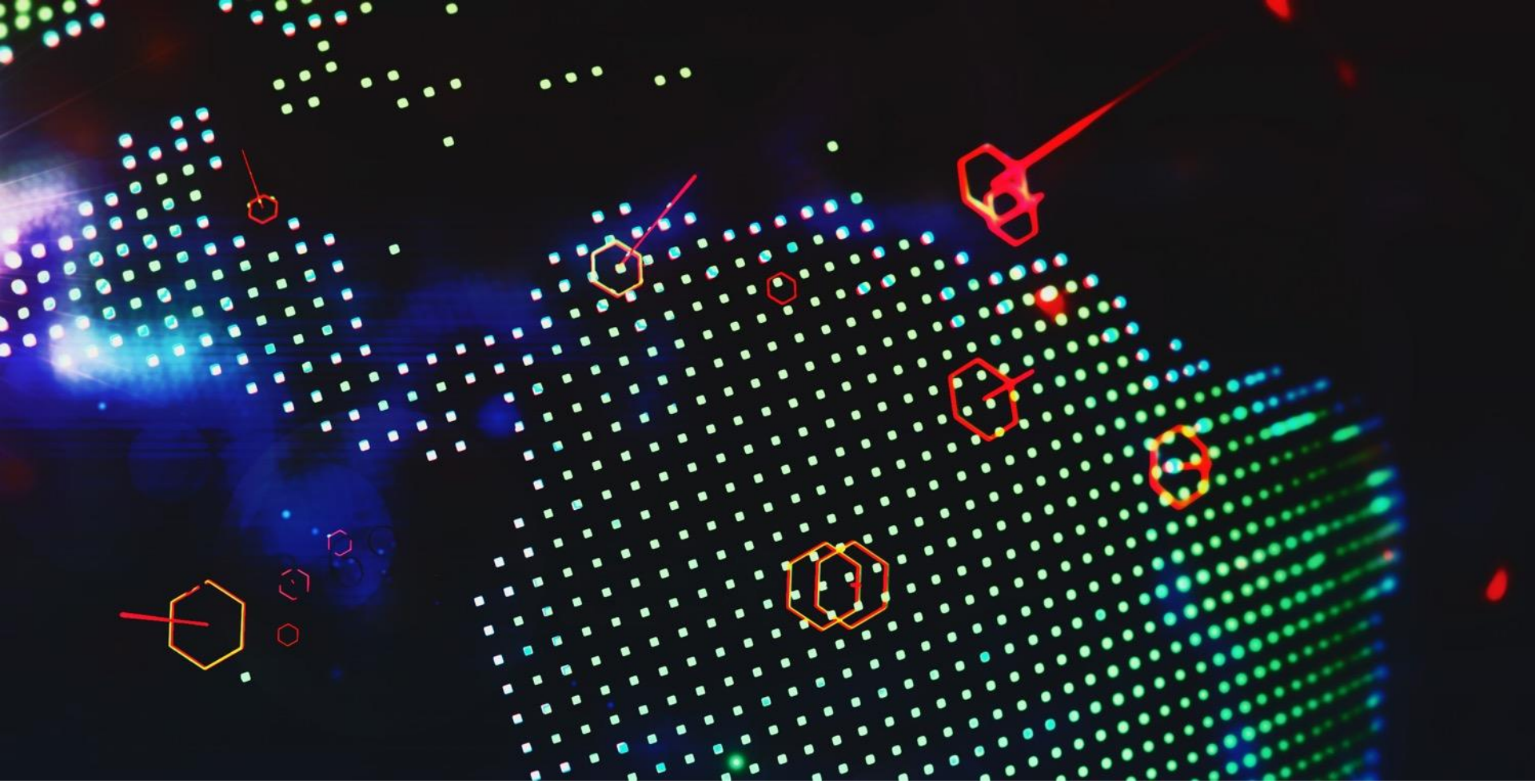


El Verdadero Costo del Fraude en América Latina – 2019

Informe de Colombia

LexisNexis®
RISK SOLUTIONS

El estudio de LexisNexis® Risk Solutions 2019 True Cost of Fraud℠ (El Verdadero Costo del Fraude) en América Latina ayuda a los comerciantes y a las empresas de servicios financieros a hacer crecer sus negocios de manera segura y a administrar el costo del fraude, mientras fortalece la confianza y la lealtad del cliente.

Colombia

La investigación proporciona un panorama de:

Tendencias actuales de fraude en los mercados minoristas, de comercio electrónico y servicios financieros de Colombia

Puntos críticos clave relacionados con agregar nuevos mecanismos de pago, realizar transacciones a través de canales en línea y móviles, y expandirse internacionalmente

Definiciones de fraude

El fraude se define como:

- Transacciones fraudulentas y/o no autorizadas;
- Solicitudes fraudulentas de reembolso / devolución, cheques sin fondos;
- Mercancías perdidas o robadas, así como los costos de redistribución asociados con la devolución de los artículos comprados;
- Aplicaciones fraudulentas (es decir, proporcionar intencionalmente información incorrecta sobre uno mismo, como ingresos, empleo, etc.);
- Toma de control de una cuenta por personas no autorizadas; y
- Uso de cuentas para el lavado de dinero.

Esta investigación cubre los métodos de fraude dirigidos al consumidor

- No incluye fraude interno o fraude de empleados.

El *LexisNexis Fraud Multiplier℠*

- Estima la cantidad total de una pérdida que un comerciante/ empresa produce en función del valor real de una transacción fraudulenta.

LexisNexis® RISK SOLUTIONS

Los datos del estudio se recopilaron en línea y por teléfono en junio y julio de 2019 con un total de 450 entrevistas con tomadores de decisiones de riesgo y fraude, distribuidos en 5 mercados de LATAM. El siguiente informe refleja los resultados de Colombia.

Colombia

	México	Brasil	Colombia	Argentina	Chile
Minorista	30	30	30	30	30
Comercio electrónico	30	30	30	30	30
Servicios financieros	30	30	30	30	30
TOTAL	90	90	90	90	90

Las categorías de comercio minorista y comercio electrónico incluyen:

- Ropa
- Piezas de automóviles
- Libros/música
- Computadoras/software
- Medicinas/salud y belleza
- Alimentos y bebidas
- Hardware/mejoras para el hogar
- Mercancía en general
- Hotel/viajes
- Artículos/muebles para el hogar
- Material de oficina
- Artículos deportivos

Las categorías de servicios financieros incluyen:

- Minoristas/bancos comerciales
- Cooperativas de crédito

- Inversiones
- Fideicomisos

- Gestión de patrimonios

Definiciones de segmentos:

m-commerce
Permite transacciones a través del navegador web móvil, aplicaciones móviles o facturación a teléfono móvil.

Digital
Negocios minoristas o de comercio electrónico que solo venden productos digitales y físicos; empresas de servicios financieros con 50% o más de ingresos anuales a través de los canales en línea y móviles.

LexisNexis® RISK SOLUTIONS

Resultados clave

Colombia

1

El costo de las tendencias de fraude al alza para los minoristas, comerciantes de e-commerce y las empresas de servicios financieros en Colombia.

Para cada transacción fraudulenta, el costo para los comerciantes colombianos y los servicios financieros asociados ha aumentado 3,21 veces la cantidad del valor perdido de la transacción (comparado con 3,27en 2018), y parece continuar siendo impulsado por los servicios financieros.

2

El canal móvil continúa contribuyendo al riesgo de fraude.

Esto incluye el navegador web móvil y, cada vez más, aplicaciones móviles, que están creciendo en su uso para llegar a la población no bancarizada.

3

La verificación de la identidad del cliente es la clave tanto para los canales móviles como en línea.

Los factores son variados para el canal en línea.

4

El costo del fraude continúa siendo más alto para quienes ofrecen m-commerce (comercio electrónico en móviles). Pero las empresas de servicios financieros digitales (regionalmente) sufren aún más.

Para cada transacción fraudulenta, el costo para los comerciantes colombianos de m-commerce ha aumentado a 3,52 veces la cantidad del valor perdido de la transacción (comparando con 3,40 en 2018), totalizando costos de fraude que ahora son 1,75% de los ingresos anuales. Y este costo es aún más alto, hasta 4,10 veces la cantidad del valor perdido de la transacción, para empresas de servicios financieros digitales en distintos países.

5

Las empresas aun no luchan eficazmente contra el fraude.

Una parte considerable aún no realiza un seguimiento de las transacciones exitosas de fraude tanto por canal como por método de pago. Además, ***una cuarta parte*** de las transacciones marcadas continúan enviándose para revisiones costosas y que consumen mucho tiempo.

6

Y, a medida que el fraude se vuelve más sofisticado, el uso de soluciones más sofisticadas sigue siendo limitado.

El uso de soluciones más avanzadas, y aquellas orientadas a la detección de fraudes móviles, tales como los dispositivos de ID/huella digital, geolocalización, factor OTP/2 y detección de transacciones en tiempo real, son un tanto limitadas.

LexisNexis® RISK SOLUTIONS

1

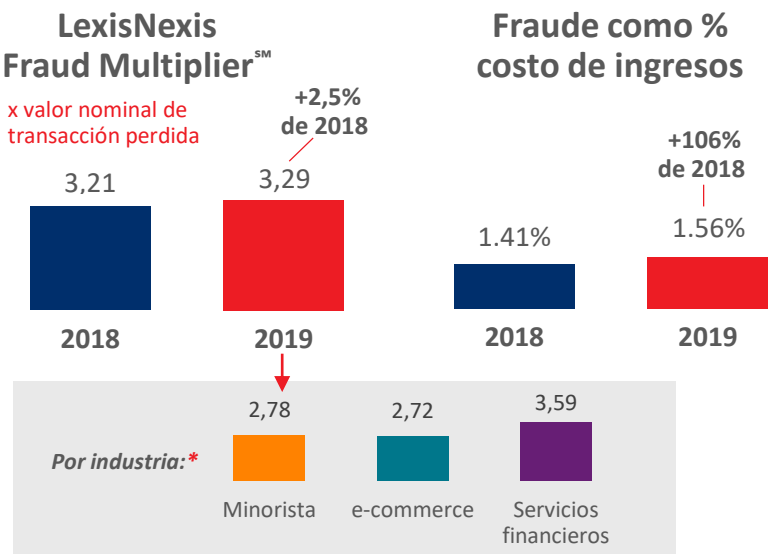
El costo del fraude en aumento para minoristas, comerciantes de e-commerce y las empresas de servicios financieros en Colombia.

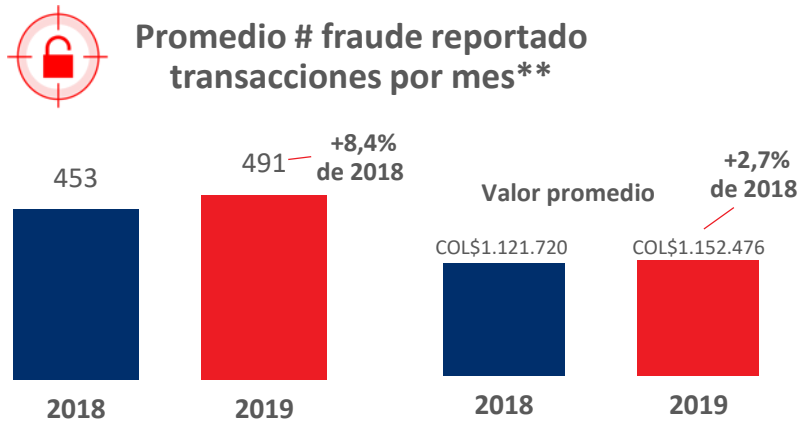
LexisNexis®
RISK SOLUTIONS

El Fraud Multiplier℠ de LexisNexis aumenta desde el año pasado a 3,29 entre minoristas, e-commerce y empresas de servicios financieros.

Colombia

- Esto significa que por cada transacción fraudulenta, el costo para las empresas colombianas es ahora 3,29 veces la cantidad del valor perdido de la transacción. Esto se traduce en costos de fraude que representan el 1,56% de los ingresos anuales en general.
- Los volúmenes y costos de fraudes a nivel país continúan siendo impulsados, en parte, por el sector de servicios financieros, donde los volúmenes y los costos son más altos.* Y aunque anecdótico (dados tamaños de base pequeños), el costo de fraude para los servicios financieros continúa direccionalmente más alto en Colombia (3,59 veces el valor nominal de la transacción perdida) que en los Estados Unidos (3,25 veces). *Las transacciones de servicios financieros de Sudamérica son las **más probables** en ser atacadas en la región. Esto adicionalmente ilustra la vulnerabilidad de la región para el fraude, a medida que las ofertas en línea y móvil continúan evolucionando .*[1]





*Las empresas de servicios financieros experimentan transacciones exitosas de fraude de 5 veces el volumen y 5 veces el monto monetario de negocios de minoristas y de e-commerce **

[1] ThreatMetrix H2 2018 Cybercrime Report

* PRECAUCIÓN: pequeño número de casos, los datos solo deben utilizarse de forma direccional

** Basado en números auto informados y probable recuerdo; no pretende ser exacto; puede aumentar o disminuir según la estacionalidad

P16a: Al pensar en las pérdidas totales por fraude sufridas por su empresa, indique la distribución de varios costos de fraude directo en los últimos 12 meses.

P10: ¿Cuál es el valor aproximado de las pérdidas totales por fraude de su empresa en los últimos 12 meses, como porcentaje de los ingresos totales?

P22 / 24: En un mes típico, ¿aproximadamente cuántas transacciones fraudulentas se evitan / completan con éxito su empresa?

P23 / 25: ¿Cuál es el valor promedio de tal transacción?

LexisNexis® RISK SOLUTIONS

Factores que contribuyen al fraude en Colombia.

Colombia

Condiciones del mercado

Colombia está entre los países con más rápido crecimiento en e-commerce.[2]

- El crecimiento del comercio electrónico e-commerce en Colombia está aumentado en un 31% anualmente, y experimenta un incremento anual del 64% en las ventas de comercio móvil.[3]
- Al igual que Chile, el gobierno colombiano fomenta el crecimiento al celebrar un día anual de compras cibernéticas, "Cyberlunes".[4]
- El valor proyectado para el mercado de e-commerce colombiano es de USD $ 8 mil millones para el 2022.[5]

En Colombia el actual crecimiento entorno a actividades en línea está atrayendo más estafadores de lo normal.

- En 2018, cerca del 25% de los registros de cuentas nuevas fueron rechazados como fraudulentos.[6]

Barreras para asegurar métodos de pago; considerable población no bancarizada que requiere que los comerciantes atraigan a estos consumidores a través de dispositivos de pago alternativos y dispositivos móviles que no siempre son seguros.

Riesgos de transacciones

- A medida que las transacciones de e-commerce y de m-commerce aumentan, **los canales donde estas compras en línea / móviles están ocurriendo se encuentran** cada vez más atacados por estafadores y más riesgosos / menos seguros.
- El **uso intensivo de navegadores móviles y aplicaciones móviles también aumenta el riesgo** para aquellos que venden bienes y servicios digitales.
- Dentro de las compras en navegadores móviles y aplicaciones, **existe la necesidad de un tiempo real para la detección de fraude y la verificación de identidad** dada la velocidad y la naturaleza de la transacción (i.e., descargado rápidamente, sin dirección de entrega para apoyar la verificación) entre e-commerce, minoristas y negocios de servicios financieros.
- **En el uso de soluciones de mitigación de riesgo** que abordan específicamente bienes/servicios móviles y digitales **los riesgos están aumentando, pero aún se encuentran limitados.**

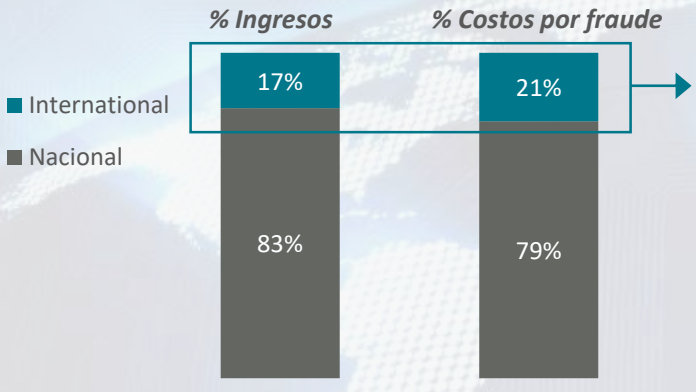
LexisNexis® RISK SOLUTIONS

[2] https://www.optimum7.com/blog/e-commerce/ecommerce-in-latin-america.html
[3] Ibid.
[4] https://www.ccce.org.co/noticias/cyberlunes-evento-ventas-online-colombia
[5] https://www.statista.com/statistics/804022/latin-america-e-commerce-sales/
[6] https://business.ebanx.com/en/colombia

Los principales ingresos y perdidas por fraude provienen de transacciones basadas en Colombia.

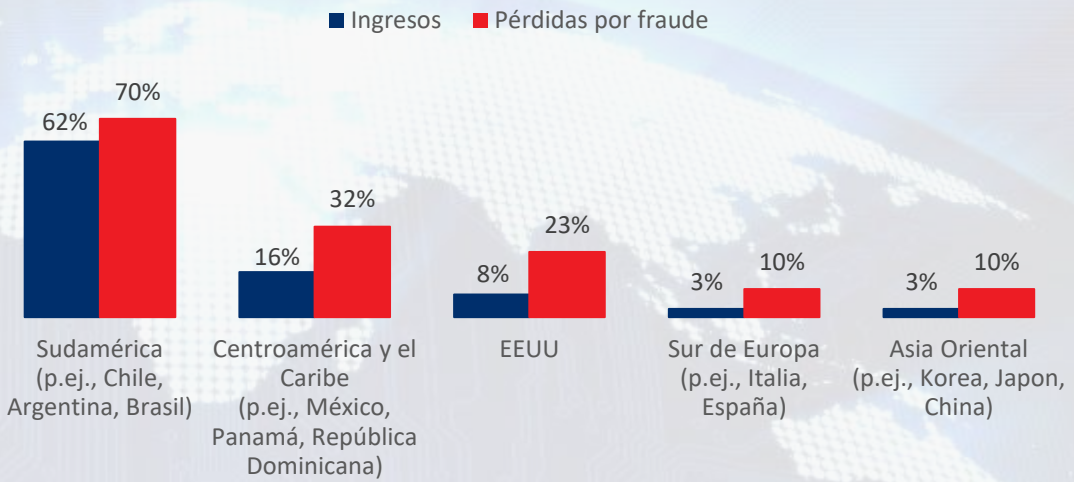
- Donde ocurre el fraude no colombiano, casi tres cuartos proviene de otros mercados sudamericanos. De hecho, Colombia es uno de los 5 principales destinos para los ataques que se originan en Brasil.[7]
- Existe un grado desproporcionado de fraude, particularmente de los EUA, en comparación con la contribución de ingresos. Esto sigue una tendencia creciente con dispersión de ataque, en el cual los atacantes comienzan a dirigirse a mercados fuera de su región.[8]

Nacional vs. internacional…



2018	Internacional	18%	17%
	Nacional	82%	83%

% Distribución internacional por geografía



LexisNexis® RISK SOLUTIONS

[7] ThreatMetrix H2 2018 Cybercrime Report
[8] Ibid.

P9 / 13: Indique el porcentaje de los ingresos anuales / costos de fraude generados a través de transacciones nacionales en comparación con las transacciones internacionales en los últimos 12 meses.
P9b / 14c: Asigne 100 puntos a lo siguiente para indicar la distribución que representa cada región de sus ingresos totales por transacción internacional / costos de fraude internacional.

2

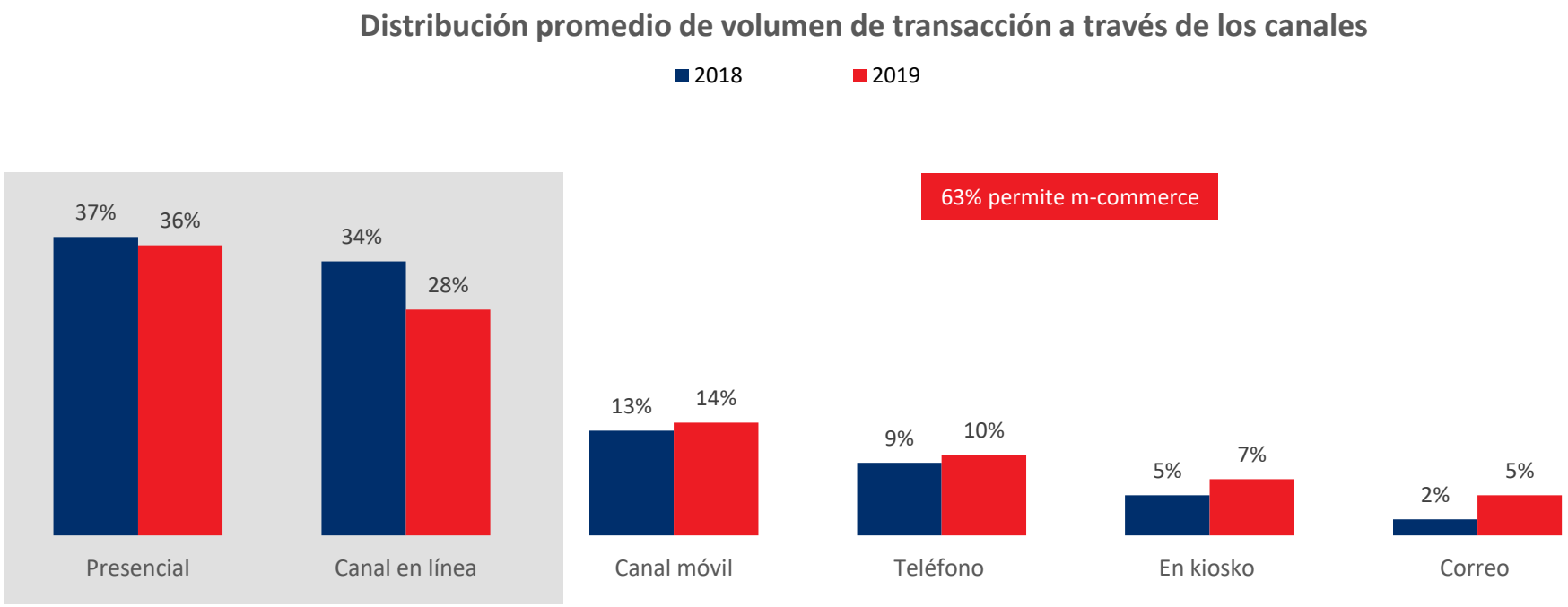
El canal móvil continúa contribuyendo al riesgo de fraude.

LexisNexis®
RISK SOLUTIONS

Una gran mayoría de las transacciones de los minoristas, e-commerce y los servicios financieros continúan a través de los canales en persona y en línea, seguidos por el canal móvil.

Colombia

Aunque los volúmenes de transacciones del canal móvil son direccionalmente menores comparados con los presenciales y en línea, se informa que el comercio electrónico móvil está creciendo en Colombia, lo que representa un aumento anual del 64%.[9] El crecimiento está impulsado en gran medida por la alta penetración de usuarios de internet en teléfonos inteligentes, que es casi dos veces mayor que la penetración de usuarios de internet en computadoras portátiles.[10]



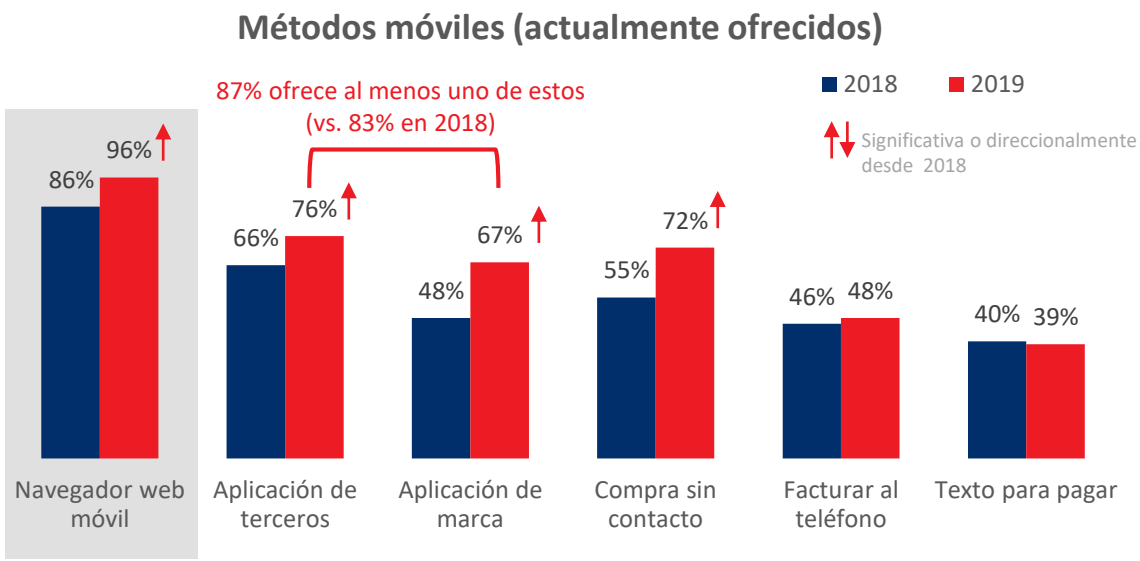
LexisNexis® RISK SOLUTIONS

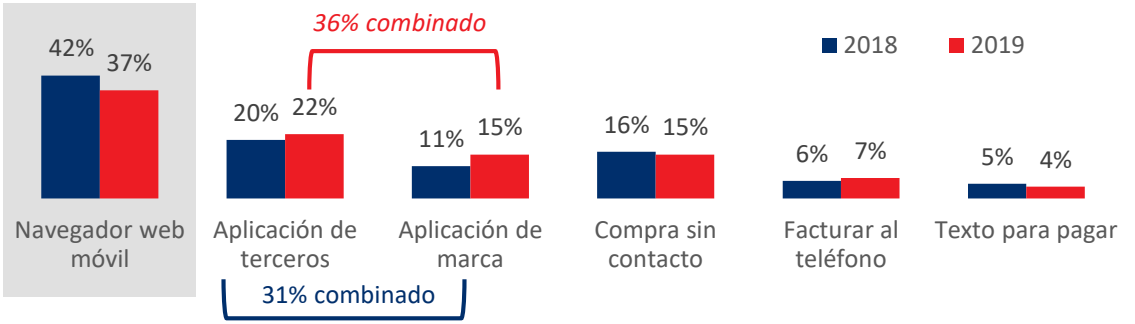
[9] https://www.optimum7.com/blog/e-commerce/ecommerce-in-latin-america.html
[10] https://markets.businessinsider.com/news/stocks/latin-america-b2c-e-commerce-market-2018-high-adoption-of-m-commerce-cross-border-online-shopping-and-omnichannel-shopping-1027716688Payments-Market-Led-by-Cards.html
P2: Indique el porcentaje de transacciones completadas (en los últimos 12 meses) para cada uno de los siguientes canales utilizados por su empresa.

Aunque las transacciones del canal móvil continúan produciéndose en gran medida a través de navegadores web, el volumen a través de aplicaciones tiende a aumentar.

Colombia

- El porcentaje de empresas que ofrecen transacciones móviles a través de navegadores web móviles y aplicaciones móviles de marca ha aumentado significativamente desde el año pasado.
- Esto continúa aumentando el riesgo de fraude. Los navegadores web móviles aún no siempre son seguros si faltan ciertos tipos de características de seguridad que se encuentran comúnmente en los navegadores web de escritorio.
- Y, los estafadores se están enfocando cada vez más a las aplicaciones móviles a nivel global[11], impulsadas en parte por la inundación de clics y ataques botnet, por medio de compras y juegos, siendo las aplicaciones financieras las más afectadas. Las botnets atacan los dispositivos a través de malware y luego pueden imitar transacciones legítimas provenientes de una aplicación móvil. Es posible que los propietarios de los dispositivos ni siquiera se den cuenta de esto.
- Además de lo anterior, la tasa de ataque móvil en América del Sur es una de las más altas de toda la región.[12]





LexisNexis® RISK SOLUTIONS

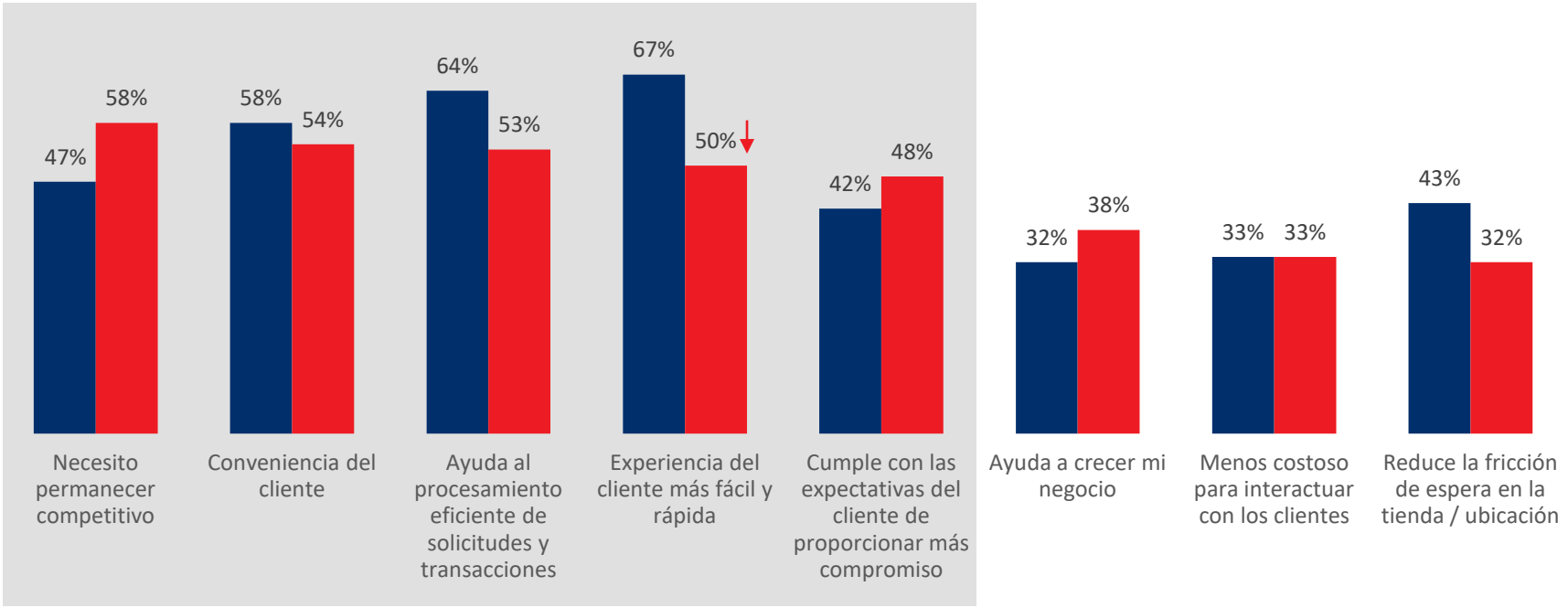
[11] https://www.appsflyer.com/resources/the-state-of-mobile-fraud-q1-2018/
[12] ThreatMetrix H2 2018 Cybercrime Report
P4: ¿Cuál es la distribución de transacciones a través de cada uno de los canales móviles que utiliza / acepta su empresa?

El riesgo de canal móvil continúa siendo aceptado como una compensación para los negocios crecientes, incluso a través de la oferta de conveniencia del cliente.

Colombia

Razones para aceptar transacciones móviles

(entre aquellos que hacen transacciones a través del canal móvil)



LexisNexis® RISK SOLUTIONS

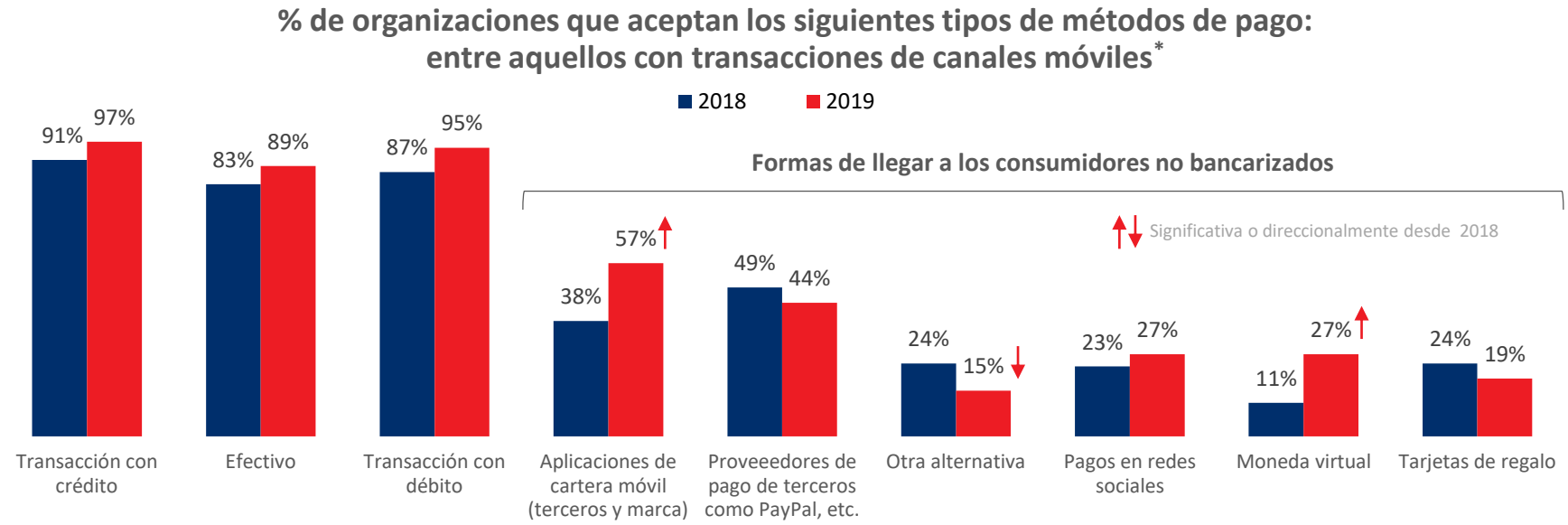
Significativa o direccionalmente desde 2018

P5: Cuáles fueron las razones por las que su empresa decidió comenzar a aceptar transacciones o la originación de cuentas móviles?

Los métodos de pago tradicionales siguen siendo los más aceptados (crédito, efectivo, tarjetas de débito), pero el uso de aplicaciones móviles está creciendo. Esto agrega riesgos adicionales a medida que las empresas continúan llegando a los no bancarizados.

Colombia

- Los colombianos tienen una tasa de inclusión financiera más alta que otros países de la región, con casi el 80% de la población con al menos un producto financiero. Sin embargo, reducir la dependencia del efectivo de las empresas y los consumidores, es un paso crucial para una inclusión financiera más generalizada en el país.[13] Con ese fin, Colombia se ha convertido en el tercer ecosistema Fintech más grande de la región. En el ultimo año y medio han surgido 78 nuevas empresas, lo que representa una tasa de crecimiento anual del 20%.[14]
- Las criptomonedas y las tecnologías blockchain están ganando terreno en Colombia. El Senado colombiano está discutiendo cómo gobernar tales compañías para evitar la evasión de impuestos y el lavado de dinero.[15]



* No necesariamente se usa con transacciones de canales móviles, ya que los comerciantes y las empresas son multicanal.

[13] https://latam.tech/three-pillars-supporting-colombias-fintech-growth/4393/
[14] https://www.finnovista.com/fintech_radar_colombia_2019/?lang=en
[15] https://latam.tech/three-pillars-supporting-colombias-fintech-growth/4393/

P3: Indique el porcentaje de cada método aceptado por su empresa / utilizado para financiar transacciones o desembolsar fondos (en los últimos 12 meses).

LexisNexis® RISK SOLUTIONS

3

Verificación de la identidad del cliente es la clave para canales en línea y móvil.

LexisNexis®
RISK SOLUTIONS

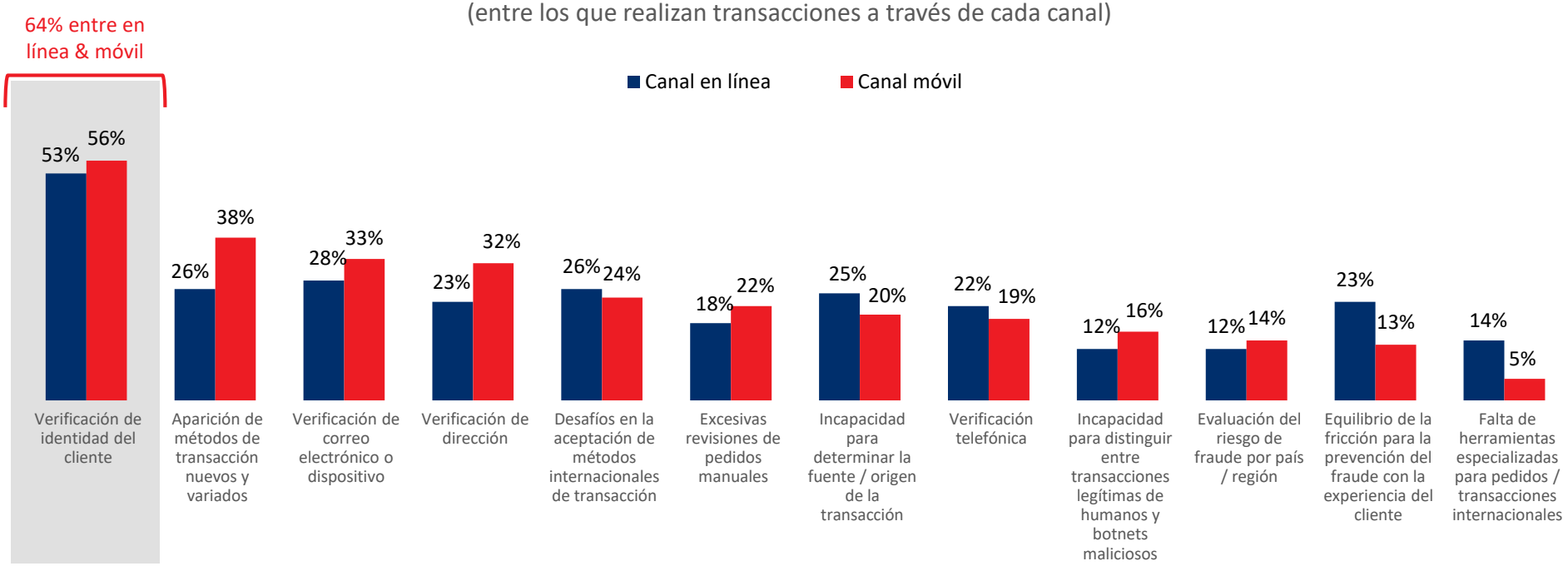
La verificación de la identidad del cliente es el desafío clave cuando se atiende a los clientes a través de los canales en línea y móviles.

Colombia

La suplantación de identidad continúa siendo el vector de ataque más frecuente en la región LATAM, particularmente para la industria de servicios financieros.[16]

Los 3 principales desafíos relacionados con el fraude al atender a los clientes a través de…

(entre los que realizan transacciones a través de cada canal)



LexisNexis® RISK SOLUTIONS

[16] Threat Metrix Q2 2018 Cybercrime Report

P20: Clasifique los 3 principales desafíos relacionados con el fraude cuando atiende a clientes en el canal en línea / móvil.

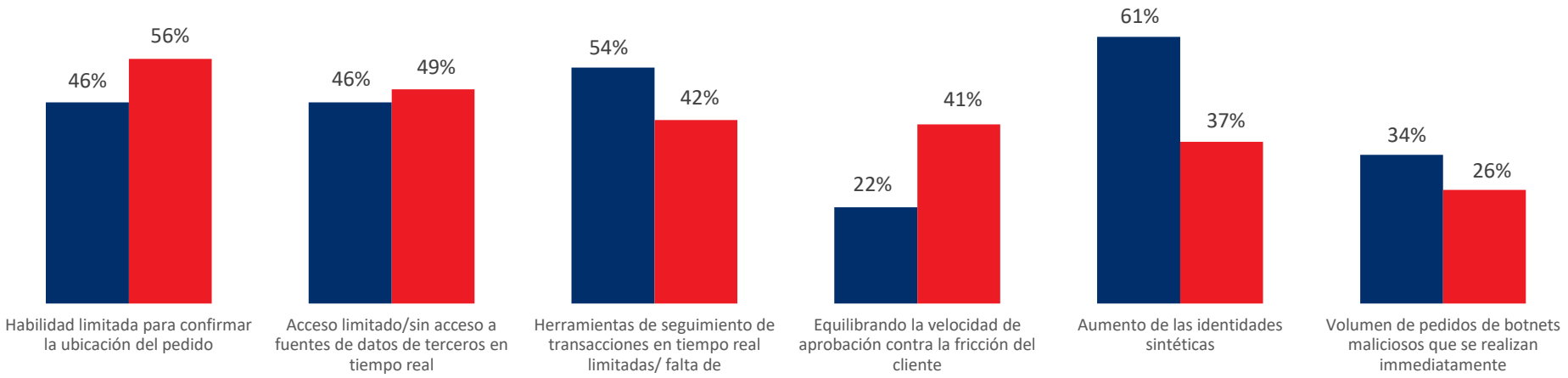
Los desafíos varían según el canal.

Colombia

La capacidad limitada para confirmar la ubicación del pedido y el acceso limitado/nulo a fuentes de datos de terceros en tiempo real son problemas para el canal móvil, mientras que no existen herramientas de seguimiento en tiempo real y el aumento de identidades sintéticas para el canal en línea.

Loa 3 factores más importantes que hacen que la verificación de identidad de un cliente sea un desafío a través de…

(entre los que realizan transacciones a través de cada canal)



LexisNexis® RISK SOLUTIONS

P20c/d: clasifique los 3 factores principales que hacen que la verificación de identidad del cliente sea un desafío cuando se atiende a clientes a través del canal en línea / móvil.

Las identidades sintéticas son una seria amenaza. Su propia naturaleza hace que sea extremadamente difícil de detectar antes de que se produzca el daño.

Colombia

Las identidades sintéticas están compuestas de información personal real y/o falsa. Se crean utilizando información de:

Múltiples personas reales en una sola identidad falsa, con una dirección de envío válida, número de identificación fiscal/seguro, fecha de nacimiento, nombre, etc. – ninguno de los cuales coincide con ninguna persona. Este tipo se puede usar para ganancias de fraude a corto plazo, como artículos más grandes.

Una persona real mediante el uso de parte de su información combinada con datos falsos. En este caso, es probable que el estafador esté nutriendo esta identidad, usándola para establecer un buen historial crediticio antes de finalmente arruinar el mismo.

Personas no identificadas en las que la información de identificación personal no pertenezca a ningún consumidor. Está completamente fabricado y puede nutrirse para obtener ganancias a más largo plazo y es útil cuando se hace pasar por un consumidor poco bancarizado con una huella de compra menos establecida (es decir, personas más jóvenes).

Riesgos y desafíos

Extremadamente difícil de distinguir de los clientes legítimos.

Se enfoca en nutrir la identidad para imitar a un buen cliente; establece buen crédito, paga a tiempo, etc. antes de "corromperse".

Difícil de detectar con las soluciones tradicionales de verificación/ autenticación de identidad.

Estos son estafadores profesionales. A menudo conocen los tipos de información necesarios para obtener la aprobación y pasar ciertos puntos de control. El uso de datos de identidad reales les ayuda a hacer esto.

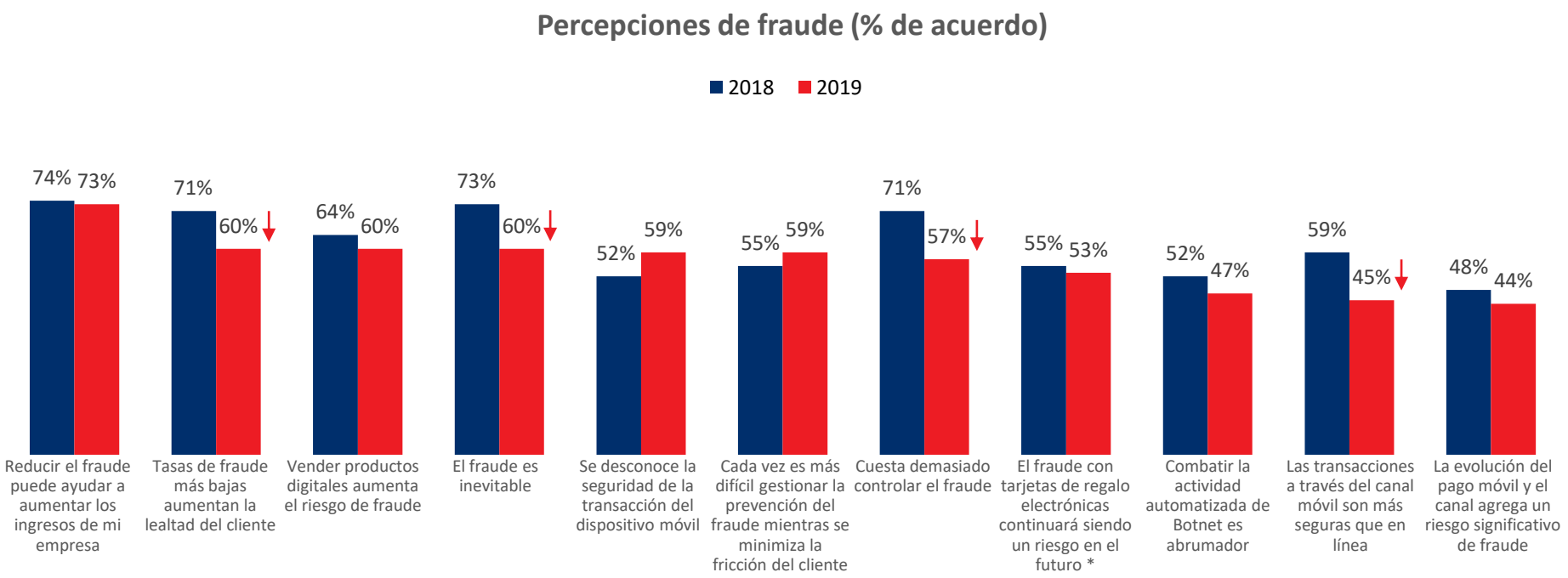
Los clientes reales no ayudan; los comportamientos hacen que sea difícil detectar anomalías con las soluciones de identificación actuales.

Los consumidores tienen más formas de comprar, desde diferentes ubicaciones en cualquier lugar y en cualquier momento. Pueden compartir contraseñas y usar diferentes dispositivos en distintos momentos. Es más difícil hacer conexiones físicas y digitales que distingan patrones fraudulentos de patrones legítimos.

LexisNexis® RISK SOLUTIONS

La mayoría sigue confiando en que la reducción de las tasas de fraude puede aumentar la lealtad y los ingresos de los clientes, pero les preocupa que el creciente canal móvil aumente el riesgo de fraude.

Colombia



Significativa o direccionalmente desde 2018

*Solo se le preguntó al minorista / comercio electrónico que vende productos digitales

P33: Usando una escala de 5 puntos, donde "5" es "estar completamente de acuerdo" y "1" es "no estar de acuerdo en absoluto", califique el grado en que está de acuerdo o en desacuerdo con las siguientes declaraciones.

LexisNexis® RISK SOLUTIONS

4

El costo del fraude continúa siendo mayor para quienes ofrecen m-commerce.

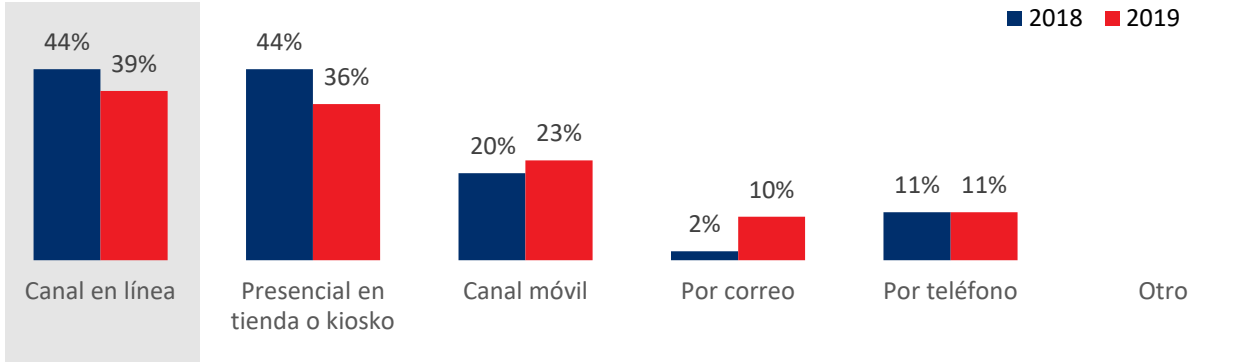
LexisNexis®
RISK SOLUTIONS

El fraude sigue siendo más probable que ocurra a través del canal en línea, seguido de en persona.

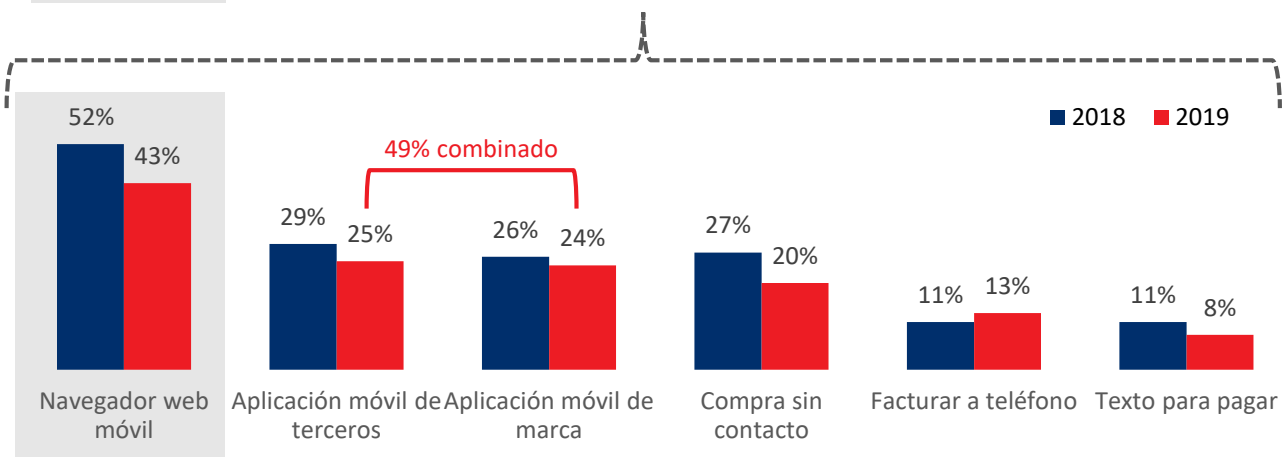
Colombia

- Las aplicaciones móviles (de marca y de terceros) continúan contribuyendo tanto a las pérdidas por fraude móvil como los navegadores web móviles.
- Los ataques a aplicaciones a menudo pueden ser desde botnets móviles e inundaciones de clics, atacando a través de malware y luego obteniendo acceso/control sobre las transacciones de aplicaciones móviles.

% de fraude por canal de transacción ***(como% del total de pérdidas anuales por fraude)****



Fraude móvil por canal ***(como % de pérdidas por fraude móvil)****



*% puede agregar mes de 100% ya que las respuestas se basan en el uso de un canal

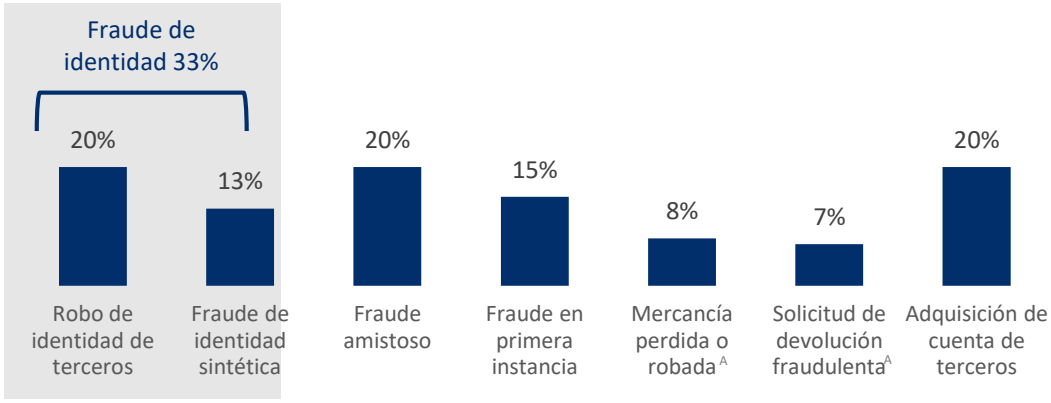
P15: : Indique el porcentaje de costos de fraude generados a través de cada uno de los siguientes canales de transacción utilizados actualmente por su empresa (como porcentaje de las pérdidas anuales totales por fraude).
P17: Indique la distribución del fraude en los distintos canales móviles que utiliza / acepta.

El fraude de identidad (robo de identidad de terceros/fraude de identidad sintética) es responsable de más de un tercio de las pérdidas por fraude.

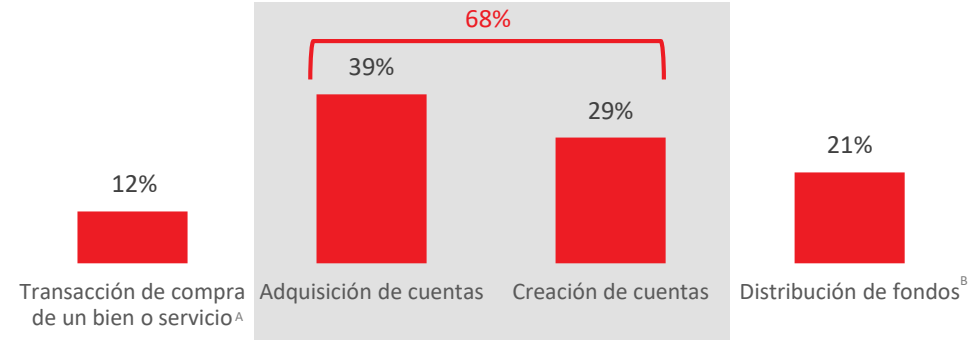
- El fraude de apropiación y creación fraudulenta de cuentas representa mucho más fraude de identidad que el que proviene de compras o transacciones.
- En 2018, casi el 25% de los nuevos registros de cuentas en línea en Colombia fueron rechazados como fraudulentos.[17]

Colombia

Distribución porcentual de pérdidas por fraude por método



Tipos de fraude relacionados con la identidad



[17] https://business.ebanx.com/en/colombia

[A] Preguntado solo a minorista / e-commerce

[B] Preguntado solo a servicios financieros

P12: Indique, a su leal saber y entender, la distribución porcentual de los siguientes métodos de fraude a continuación, ya que se atribuyen a su pérdida anual total por fraude en los últimos 12 meses.

- Fraude amistoso (una persona asociada con / que tiene acceso a una cuenta realiza una transacción sin el conocimiento o permiso del propietario de la cuenta principal)
- Fraude de terceros (el propietario del usuario autorizado de la cuenta comete el fraude)
- Fraude de identidad de terceros (transacción no autorizada utilizando la información real / existente de otras personas)
- Fraude de identidad sintética (creación de una nueva identidad utilizando una combinación de información real y fabricada, a veces completamente ficticia

P12b: Para el fraude relacionado con la identidad, ¿cuál es la distribución de estos por los siguientes tipos de actividades?

LexisNexis® RISK SOLUTIONS

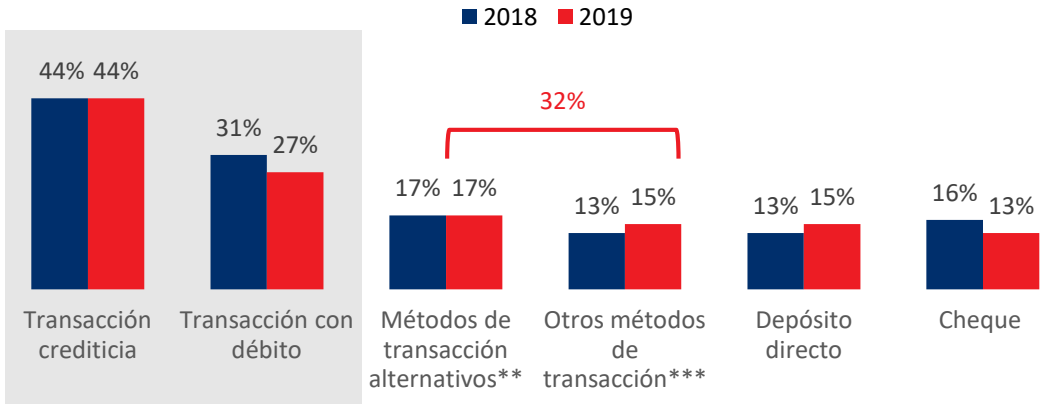
Si bien el crédito sigue siendo el método de transacción fraudulenta más importante, las pérdidas atribuidas a métodos alternativos/ otros (que incluyen opciones de pago en línea/móviles) están a la par con el fraude de débito.

Las transacciones con tarjeta representan un 71% combinado de las pérdidas anuales totales por fraude. Esto presenta un problema en un país que se considera que tiene potencial de crecimiento en el uso de tarjetas para transacciones. La penetración de la tarjeta de crédito es del 26% en un país donde casi la mitad del país compra en línea.[18]

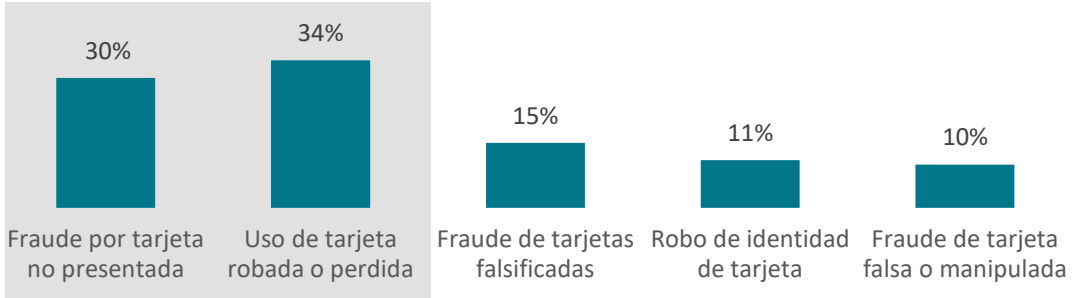
[18]https://www.naspers.com/technology/access-to-credit-in-growth-markets

Colombia

Fraude por método de transacción
*(como % del total de pérdidas anuales por fraude)**



Fraude relacionado con pérdidas de tarjetas



*% puede agregarse a más del 100% ya que las respuestas se basan en si se usa un canal
** *Los métodos de transacción alternativos incluyen PayPal, BillMeLater, eCheck*
*** *Otros métodos de transacción incluyen efectivo, carteras basadas en dispositivos móviles, tarjetas de regalo*

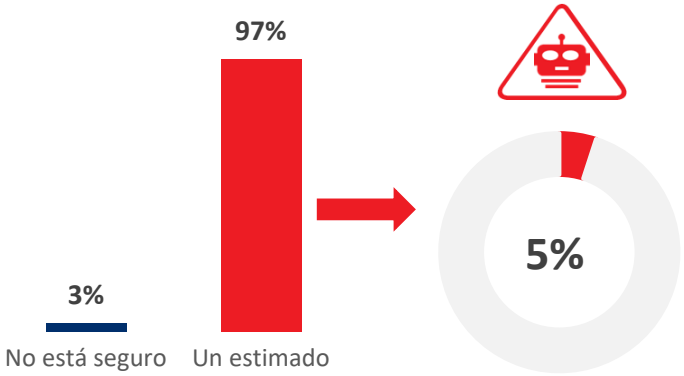
P18: Indique la distribución porcentual de los métodos de pago utilizados para cometer fraude contra su empresa.
P18e: De sus pérdidas por fraude relacionadas con tarjetas de crédito o débito, indique la distribución entre los siguientes tipos de fraude con tarjeta.

LexisNexis® RISK SOLUTIONS

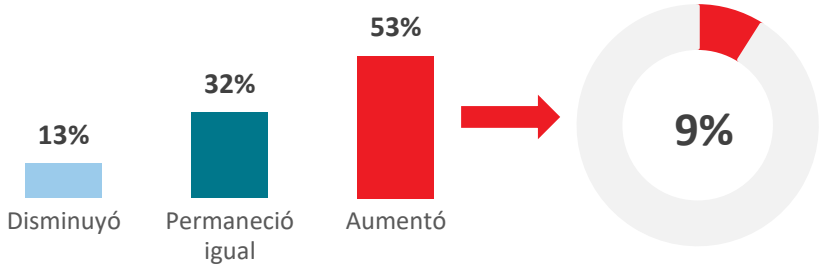
Casi la mitad de las empresas informaron un aumento en la actividad automatizada de botnets durante el año pasado. Esto se estima a una tasa de crecimiento del 9%.

Colombia

Actividad de botnet como % de transacciones por mes



Cambio en el volumen de actividad de botnet durante el año pasado



B1a: En un mes típico, ¿qué porcentaje de sus transacciones se determina que son ataques automatizados maliciosos de bot?
B1b / c: ¿Cómo se compara esto con la misma época del año pasado? ¿Diría que el porcentaje de ataques automatizados mensuales de bot malicioso tiene:

La combinación de estos factores contribuye a aumentar el riesgo.

Colombia

Móvil

- **Aumento de los ataques botnets móviles;** el malware infecta dispositivos sin conocimiento del consumidor; roba identidad, piratea cuentas, realiza compras fraudulentas.[19]
- **Comportamientos de riesgo del consumidor** – el uso de redes WiFi abiertas aumenta el riesgo de smishing (phishing basado en SMS) y la intercepción de códigos de acceso utilizados por el Man in the Middle para la autenticación de múltiples factores[20]; los hábitos de "mantenerme conectado" se convierten en un punto de entrada desbloqueado a las cuentas.
- **Grupo creciente para oportunidades de estafadores** a medida que más personas realizan transacciones móviles.

Transfronterizo

- **Incertidumbre, puntos ciegos y nuevos métodos de pago;** se hace difícil determinar el origen de la transacción; falta de datos verificables sobre los consumidores (particularmente con GDPR).

Digital

- **Transacciones rápidas**; los bienes / servicios digitales, como descargas y suscripciones, tienden a ocurrir rápidamente; la falta de una dirección de entrega física elimina el período de amortiguación para la verificación de fraude antes del envío; con miedo al abandono, los comerciantes luchan por equilibrar la prevención del fraude y minimizar la fricción del cliente.
- **Objetivos fáciles**; las identidades sintéticas y los datos robados dificultan la distinción entre ataques maliciosos y clientes legítimos en el canal anónimo.
- **Objetivo favorito para pruebas de tarjetas de estafadores;** el uso de bots para probar la información de tarjetas de crédito robadas con bienes/servicios de menor valor (típico de los bienes/servicios digitales) tiende a despertar menos sospechas.

LexisNexis® RISK SOLUTIONS

[19] Informe de Cybercrime ThreatMetrix Q2 2018
[20] 4 tendencias de fraude móvil para buscar en 2019; https://threatmetrix.com/digital-identity-blog/fraud-prevention/4-mobile-fraud-trends-look-out-for-2019

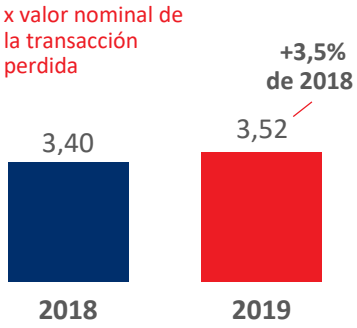
Esto continúa resultando en mayores volúmenes y costos de fraude para las empresas que ofrecen m-commerce.

Colombia

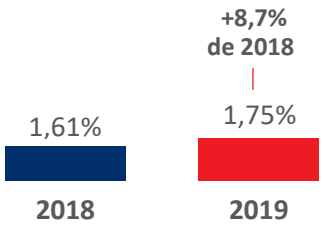
- Cada **transacción fraudulenta** realmente cuesta a estas empresas de comercio móvil **3,52 veces el valor de la transacción perdida,** en comparación con el promedio (3,29) en todas las organizaciones en general. Los costos de fraude como porcentaje de los ingresos también son más altos entre aquellos que permiten m-commerce que todas las organizaciones en general (1,56%).
- Además, el número de transacciones fraudulentas exitosas y sus montos monetarios asociados han crecido desde 2018 y continúan siendo más altos que para todas las empresas en conjunto.

Entre las empresas que ofrecen m-commerce

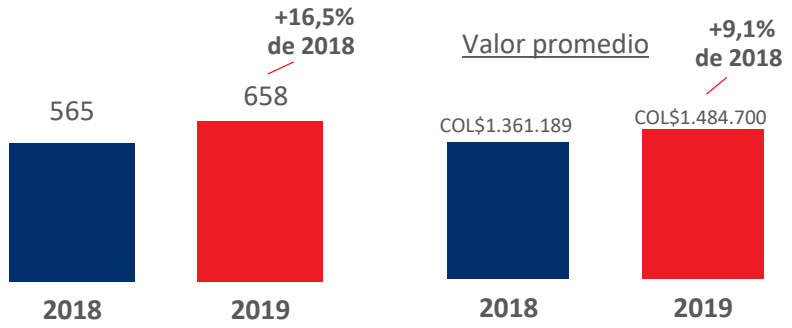
LexisNexis Fraud Multiplier℠



Fraude como % costo de ingresos



Promedio de transacciones reportadas por mes*



* Basado en números auto informados y probable recordación; no pretende ser exacto; puede aumentar o disminuir según la estacionalidad

P16a: Al pensar en las pérdidas totales por fraude sufridas por su empresa, indique la distribución de varios costos de fraude directo en los últimos 12 meses.
P10: ¿Cuál es el valor aproximado de las pérdidas totales por fraude de su empresa en los últimos 12 meses, como porcentaje de los ingresos totales?
P22 / 24: En un mes típico, ¿aproximadamente cuántas transacciones fraudulentas se evitan / completan con éxito su empresa?
P23 / 25: ¿Cuál es el valor promedio de tal transacción?

LexisNexis® RISK SOLUTIONS

A nivel regional, las empresas que son "digitales" continúan teniendo riesgos y costos aún mayores asociados con el fraude, que tiende a superponerse con m-commerce.

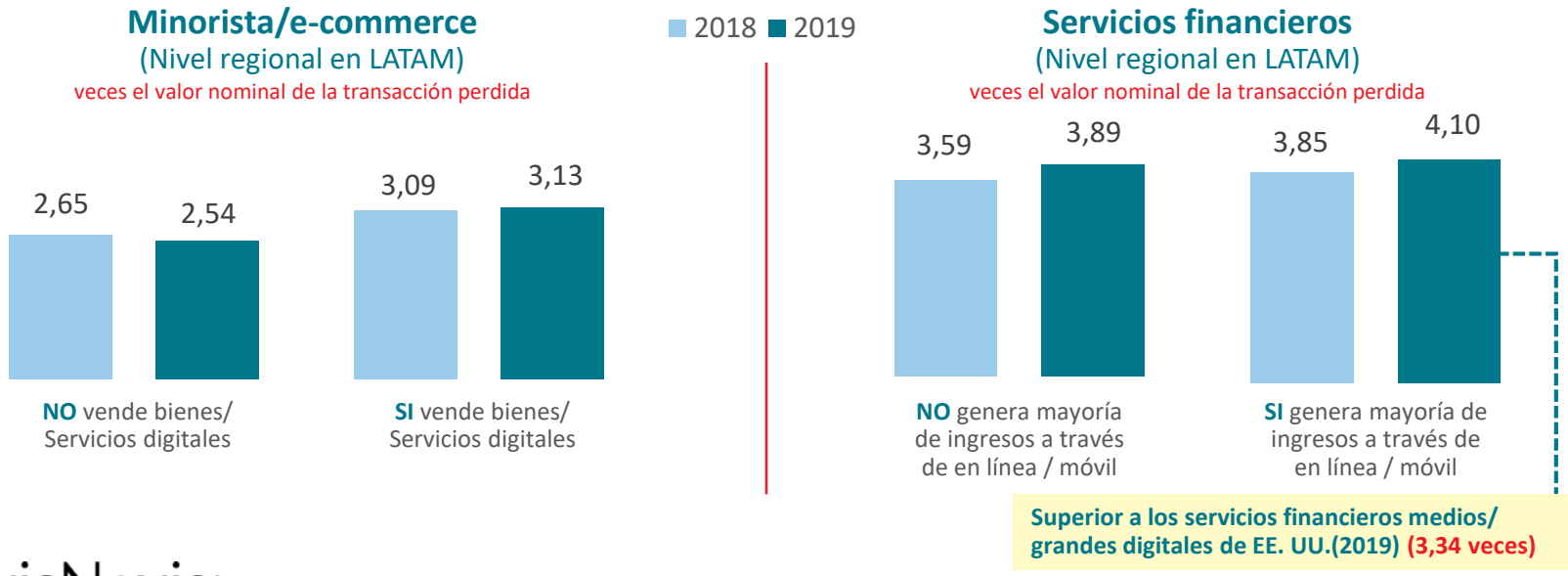
Resultados Regionales

Para los minoristas digitales, los comerciantes de comercio electrónico y las empresas de servicios financieros, la verificación de identidad es un desafío y un riesgo.

- Para los minoristas / comerciantes de comercio electrónico, la velocidad y el tipo de transacción son el problema. Los bienes / servicios digitales implican una mayor inmediatez de distribución / descarga; mientras que los comerciantes que venden productos físicos tienen una dirección de entrega para el envío y un tiempo de amortiguación entre la transacción y el envío para confirmar la identidad y la legitimidad de la venta, este no es el caso para aquellos que venden productos digitales. Hay más necesidad en tiempo real de esfuerzos de detección de fraude.
- Para las empresas de servicios financieros, el anonimato del canal hace que la verificación de identidad sea mucho más difícil.
- Y, con todos los segmentos, los dispositivos (computadoras, tabletas, teléfonos móviles) pueden confundir cosas con suplantación de identidad y malware.

En todas las industrias, las que son digitales continúan siendo golpeadas con un mayor costo de fraude.

LexisNexis Fraud Multiplier℠



LexisNexis® RISK SOLUTIONS

P16a: Al pensar en las pérdidas totales por fraude sufridas por su empresa, indique la distribución de varios costos de fraude directo en los últimos 12 meses.

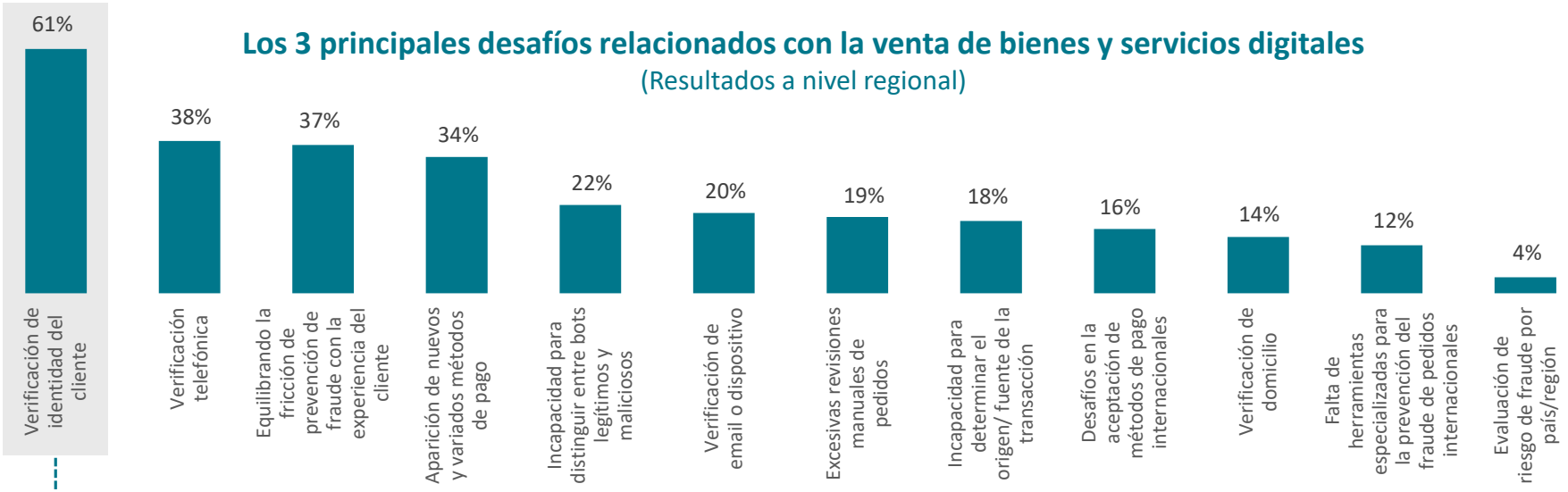
A nivel regional, la gestión de la verificación de riesgos y la fricción del cliente es un desafío para los minoristas/ comerciantes de e-commerce que venden productos digitales, particularmente entre aquellos que carecen de herramientas de seguimiento de transacciones en tiempo real y la capacidad de confirmar el origen de las transacciones.

Resultados Regionales

Esto también se ve agravado por la necesidad de realizar verificaciones telefónicas, equilibrar los esfuerzos de detección de fraude con la mínima fricción del cliente y tratar con métodos de pago nuevos y diferentes. Para más de la mitad, el aumento de las identidades sintéticas complica ese esfuerzo.

Los 3 principales desafíos relacionados con la venta de bienes y servicios digitales

(Resultados a nivel regional)



El 59% de los que clasifican la verificación de identidad como un desafío atribuyen esto al aumento de las identidades sintéticas. Otro 46% atribuye esto a las herramientas de seguimiento de transacciones en tiempo real limitadas/no existentes y a la capacidad limitada para confirmar la ubicación del pedido (geográfico o por dispositivo).

LexisNexis® RISK SOLUTIONS

P19: Clasifique los 3 principales desafíos relacionados con el fraude que enfrenta su empresa cuando vende productos digitales a clientes.
P19_2: Clasifique los 3 factores principales que hacen que la verificación de identidad del cliente sea un desafío al vender productos digitales.

5

Las empresas aún no luchan eficazmente contra el fraude.

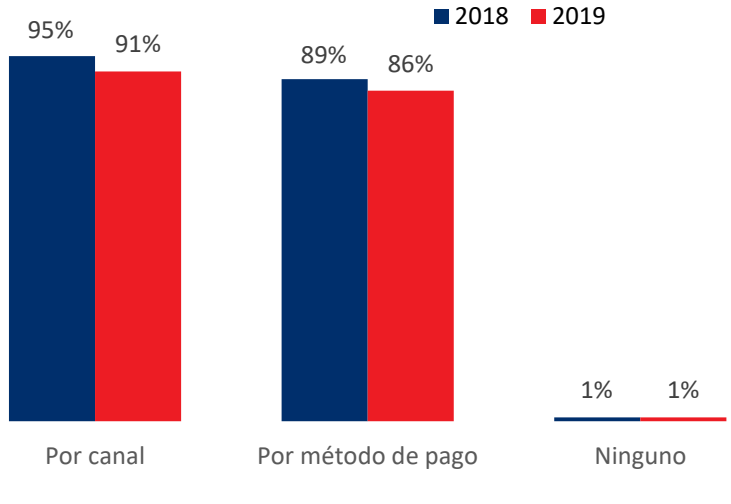
LexisNexis®
RISK SOLUTIONS

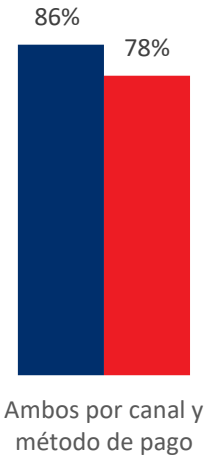
Según los informes, muchos siguen rastreando los costos de fraude por canal y método de pago.

- Sin embargo, menos parecen estar rastreando transacciones fraudulentas exitosas tanto por canal como por método de pago.
- Es importante hacer un seguimiento del fraude exitoso e prevenido por canal y método de pago para comprender los puntos débiles; los estafadores seguirán probando estos.

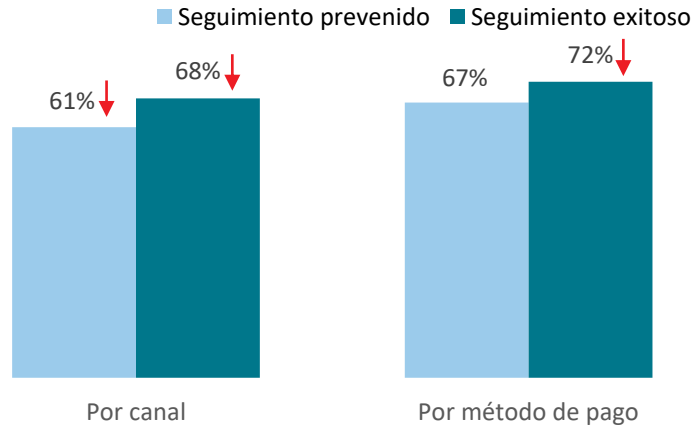
Colombia

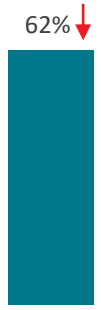
% de empresas que rastrean los costos de fraude por por canal o método de pago





% de seguimiento de transacciones fraudulentas EXITOSAS y/o PREVENIDAS





2018	76%	80%	70%	87%

78%

Significativa o direccionalmente desde 2018

P14: ¿Su empresa rastrea el costo de transacciones fraudulentas por canales o métodos de pago?
P26: ¿Su empresa rastrea el fraude exitoso por canales o métodos de pago?

LexisNexis® RISK SOLUTIONS

Y, aún, menos de un tercio de las transacciones son marcadas por un sistema automatizado.

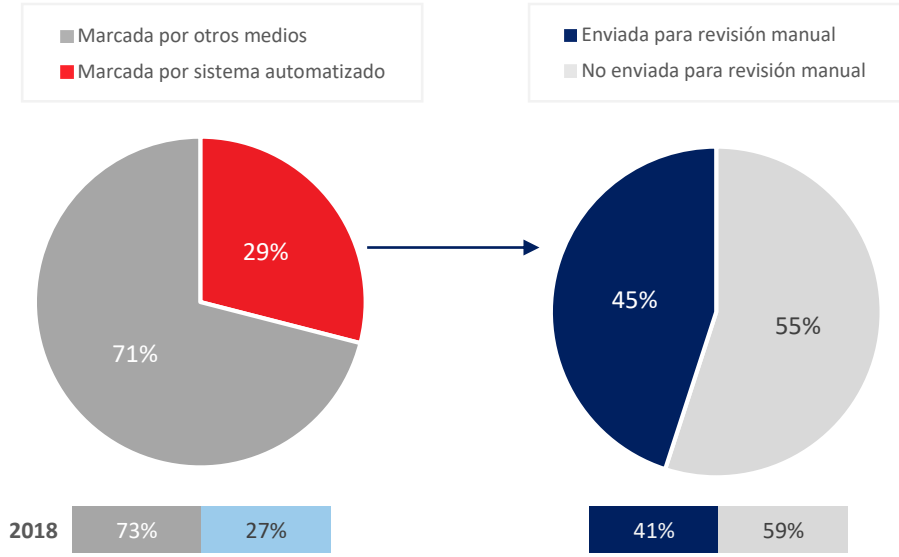
- Y entre las que están, más de ***4 de cada 10*** son enviadas a revisión manual.
- Y el número de falsos positivos no ha disminuido con más ***de una cuarta parte*** de las transacciones rechazadas que todavía resultan en falsos positivos.

P36: De todas las transacciones que su empresa marcó como potencialmente fraudulentas en los últimos 12 meses, ¿qué porcentaje fue marcado por su sistema automatizado?
P37: De esto (...), ¿qué proporción se envía para revisión manual?
P38: ¿Qué porcentaje de transacciones que su empresa inicialmente marca como potencialmente fraudulentas finalmente se rechazan?
P39: ¿Qué porcentaje de transacciones rechazadas resultaron ser falsos positivos?

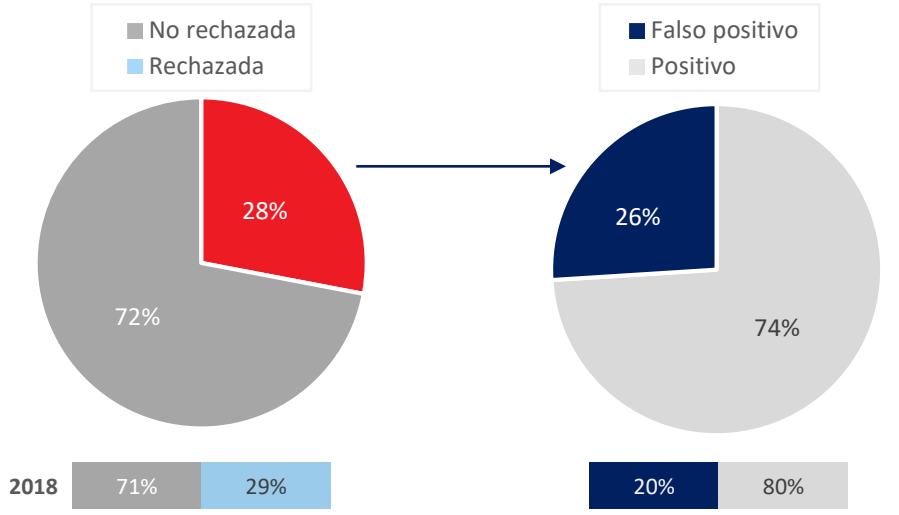
LexisNexis® RISK SOLUTIONS

Colombia

Porcentaje de transacciones marcadas por el sistema automático, enviadas para revisión manual



% de transacciones marcadas que se rechazan, falsos positivos



6

Y, a medida que el fraude se vuelve más sofisticado, el uso de soluciones más sofisticadas sigue siendo limitado.

LexisNexis®
RISK SOLUTIONS

El fraude se ha vuelto más complejo; varios riesgos pueden ocurrir al mismo tiempo sin una solución única. Las herramientas de fraude deben autenticar los criterios físicos y digitales, así como el riesgo de identidad y transacción.

PROBLEMAS DE FRAUDE

- **Bienes y servicios digitales:** transacciones rápidas, identidad sintética fácil y objetivos de botnet; ***necesita verificación de velocidad*** para determinar ***el riesgo de transacción*** junto con ***datos y análisis para autenticar al individuo***
- **Fraude relacionado con cuentas:** los datos vulnerados requieren más niveles de seguridad, además de ***autenticar a la persona de un bot o ID sintético***
- **Identidades sintéticas:** ***necesita autenticar a todo el individuo*** *detrás de la transacción para distinguir de la identidad falsa basada en datos reales parciales*
- **Ataques de botnet:** ataques masivos humanos o automatizados a menudo para probar tarjetas, contraseñas/credenciales o infectar dispositivos
- **Canal móvil:** el origen de la fuente y los dispositivos infectados agregan riesgo; los bots móviles y el malware malicioso dificultan la autenticación; **necesita evaluar el dispositivo y el individuo**

OPCIONES DE SOLUCIÓN

EVALUANDO EL RIESGO DE TRANSACCIÓN

Comprobaciones de velocidad/ puntuación de transacciones: monitorea los patrones de compra históricos de un individuo contra sus compras actuales para detectar si el número de pedidos del titular de la tarjeta coincide o si parece haber una irregularidad ***(Ejemplos de soluciones: puntuación de transacciones en tiempo real; puntuación de transacciones automatizada)***

AUTENTICANDO A LA PERSONA FÍSICA

Verificación básica: verificar nombre, dirección, fecha de nacimiento o proporcionar un código CVV asociado con una tarjeta ***(Ejemplos de soluciones: servicios de verificación de cheques; autenticación de instrumentos de pago; verificación de nombre/ dirección/lugar de nacimiento)***

Autenticación de ID activo: uso de datos personales conocidos por el cliente para la autenticación; o donde el usuario proporciona dos factores de autenticación diferentes para verificar ***(Ejemplos de soluciones: autenticación por desafío o prueba; autenticación usando el factor OTP/2)***

AUTENTICANDO A LA PERSONA DIGITAL

Identidad digital/biometría conductual: analiza las interacciones humano-dispositivo y los patrones de comportamiento, como los clics del mouse y las pulsaciones de teclas, para discernir entre un usuario real y un impostor al reconocer el comportamiento normal del usuario y el estafador ***(Ejemplos de soluciones: autenticación por biometría; evaluación de riesgos por correo electrónico/teléfono; navegador/ seguimiento de malware; ID del dispositivo/ huella digital)***

Evaluación de dispositivo: Identificar de forma exclusiva un dispositivo informático o usuario remoto ***(Ejemplos de soluciones: ID del dispositivo/huella digital; geolocalización)***

LexisNexis® RISK SOLUTIONS

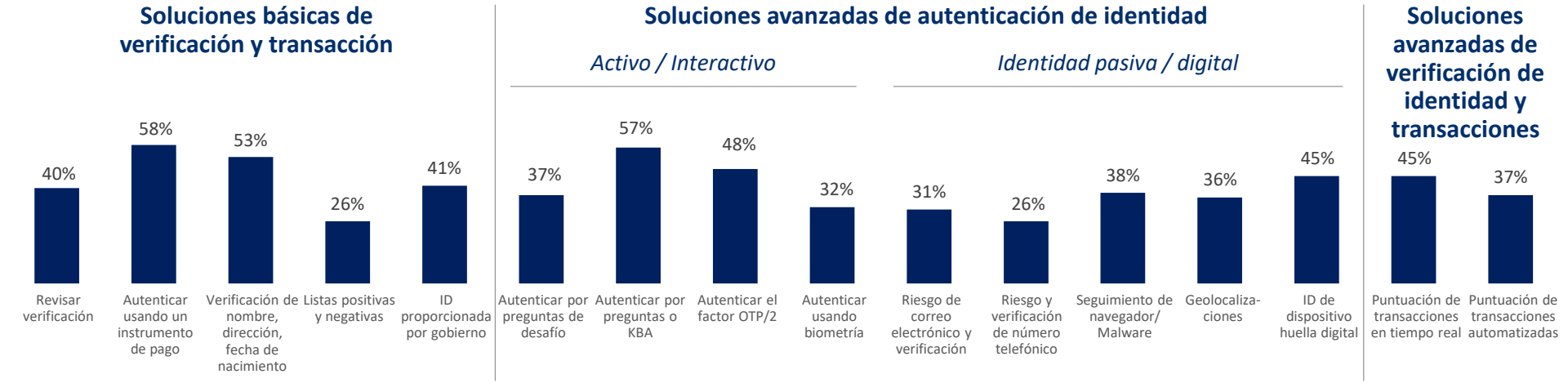
Se está utilizando un promedio de 5,7 soluciones de mitigación de fraude en negocios minoristas, comercio electrónico y servicios financieros.

Colombia

- Sin embargo, el uso de soluciones más sofisticadas para abordar la naturaleza complicada del fraude es limitado, particularmente con respecto a la biometría del comportamiento y otras soluciones de identidad digital que pueden combatir el fraude de identidad sintética y los ataques de botnet. Dadas las tasas de incidencia similares entre algunas de las soluciones físicas (verificación de cheques, identificación emitida por el gobierno) y digitales (puntuación de transacciones automatizadas), esto sugiere algunas capas de soluciones para una detección de fraude más efectiva. Sin embargo, todavía hay una parte importante de las empresas que no lo están haciendo.
- Además, el uso de soluciones para abordar las amenazas móviles (identificación del dispositivo, geolocalización) y el desafío acelerado de las transacciones digitales / anónimas (puntuación de transacciones en tiempo real) es más limitado. Y aunque las soluciones son una parte considerable de los presupuestos de mitigación de fraude, las revisiones manuales son más de la mitad de eso, lo que sugiere que los intentos actuales de prevención de fraude son carentes.

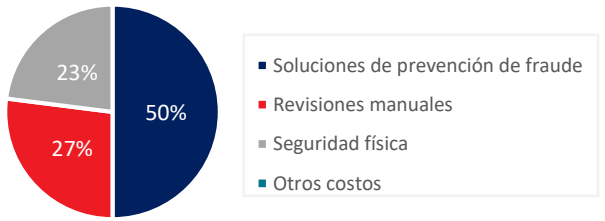
Uso de soluciones de mitigación de fraude

Media 5,7 soluciones utilizadas



P27: Cuál de las siguientes opciones describe mejor su conocimiento y uso de las soluciones de fraude enumeradas?
P41b: Cuál es la distribución porcentual de los costos de mitigación en las siguientes áreas en los últimos 12 meses ?

Distribución de costos de mitigación de fraude por porcentaje de gasto



LexisNexis® RISK SOLUTIONS

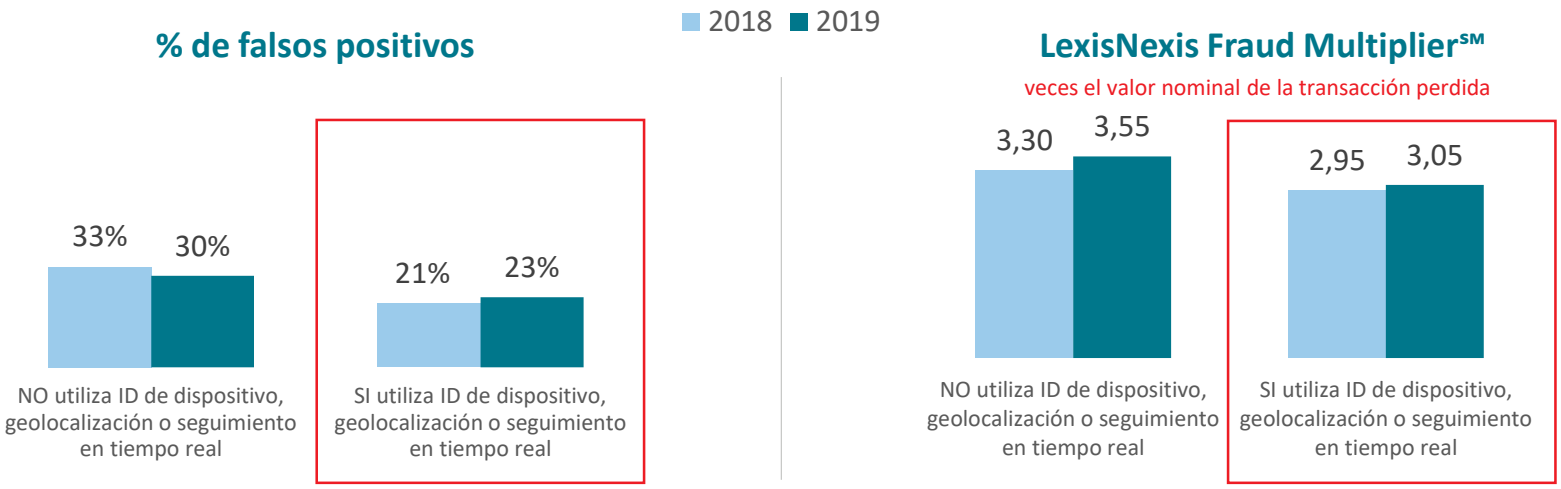
Pero aún no se trata de la cantidad de soluciones, más bien es importante hacer la combinación correcta de ellas para enfrentar las amenazas de tipos específicos de canales y transacciones.

Resultados Regionales

Los resultados continúan mostrando que en América Latina los minoristas digitales / comerciantes de e-commerce/ negocios de servicios financieros que agrupan soluciones para abordar las amenazas móviles (identificación del dispositivo / huellas digitales, geolocalización) y el desafío acelerado de las transacciones digitales / anónimas (puntuación de transacciones en tiempo real) pueden experimentar menos falsos positivos y menores costos de fraude en general.

Comerciantes LATAM / empresas de servicios financieros que son digitales * y permiten transacciones de canales móviles

(Resultados a nivel regional en LATAM)



LexisNexis® RISK SOLUTIONS

* Para minoristas / comerciantes de e-commerce, digital se refiere a la venta de bienes o servicios digitales; para las empresas de servicios financieros, digital se refiere a generar 50% o más ingresos a través de canales remotos (en línea o móviles)

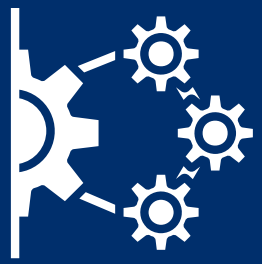
P27: ¿Cuál de las siguientes opciones describe mejor su conocimiento y uso de las soluciones de fraude enumeradas?
P39: ¿Qué porcentaje de transacciones rechazadas resultaron ser falsos positivos?

Recomendaciones.

LexisNexis®
RISK SOLUTIONS

Recomendación #1

Colombia



Las empresas deben implementar diferentes soluciones de mitigación de riesgos para abordar riesgos únicos de diferentes canales y modelos de ventas.

Las soluciones utilizadas para mitigar el riesgo con las transacciones de bienes físicos no mitigarán completamente aquellas con transacciones de bienes digitales porque la naturaleza de los bienes cambia el riesgo (es decir, más transacciones en tiempo real y más rápidas con bienes digitales).

Los canales móviles presentan diferentes desafíos y riesgos que en línea, dada la naturaleza de la movilidad. Junto con los productos digitales y el aumento del fraude de aplicaciones móviles, esto aumenta la complejidad.

Las soluciones de comprobación de velocidad y tiempo real específicas del dispositivo son ejemplos de tecnologías únicas para admitir estos entornos de transacción específicos.

LexisNexis® RISK SOLUTIONS

Recomendación #2

Colombia

Un enfoque de **múltiples capas de** soluciones es esencial para combatir el fraude y al mismo tiempo mitigar la fricción del cliente, particularmente para aquellos que venden productos digitales y usan el canal móvil.

Es fundamental abordar el fraude relacionado tanto con la identidad como con las transacciones. Estas son dos perspectivas diferentes.

La verificación/autenticación de identidad es importante para "dejar entrar a sus clientes" con la menor cantidad de fricción y riesgo.

El fraude relacionado con las transacciones se trata de mantener alejados a los "malos".

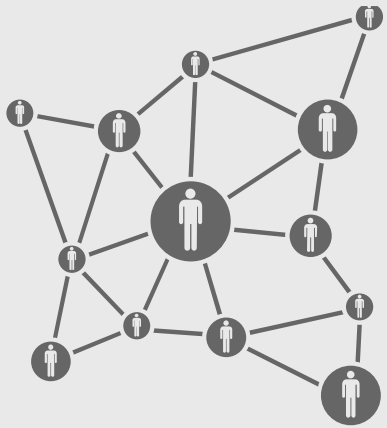
Un enfoque en capas puede reducir los costos asociados con revisiones manuales, intentos exitosos de fraude y menos falsos positivos.

LexisNexis® RISK SOLUTIONS

Recomendación #3

Colombia

Las empresas deben buscar proveedores externos con recursos profundos de datos y de análisis para abordar de manera más efectiva los desafíos de fraude basados en la identidad, particularmente para los tipos de ataques más nuevos y sofisticados.



El fraude de identidad puede ser complicado, con varias capas de máscaras y conexiones en segundo plano.

Invertir en un enfoque de solución en capas será mucho más efectivo si proviene de un socio de soluciones que brinde capacidades de vinculación únicas que identifiquen y vinculen relaciones ocultas, arrojen luz sobre actividades o transacciones sospechosas e identifiquen la colusión.

Estos patrones no son fácilmente descubiertos por una serie de soluciones de riesgo en el mercado actual.

LexisNexis® RISK SOLUTIONS

Recomendación #4

Colombia

Los comercios y las empresas de servicios financieros que realizan m-commerce deben enfocarse especialmente en las soluciones de evaluación de dispositivos para combatir el creciente fraude de aplicaciones móviles.

Debido a que las botnets y el malware pueden comprometer los dispositivos móviles, las aplicaciones móviles utilizadas para las transacciones también son vulnerables. Por lo tanto, la verificación y la autenticación no son solo sobre el usuario, sino también sobre el dispositivo y si la aplicación móvil ha sido manipulada.

Para minimizar la fricción del cliente y evitar el abandono de la transacción, la evaluación del dispositivo se vuelve importante para verificar instantáneamente la identidad del dispositivo y los atributos de ubicación, VPN y proxies, malware y bots.

LexisNexis® RISK SOLUTIONS

Recomendación #5

Colombia

Las empresas necesitan rastrear tanto el pago como el fraude de canales, en términos de costos e intentos exitosos. Pero esto debe ser parte de un enfoque más amplio que implique soluciones de detección de fraude diseñadas para abordar riesgos únicos.

Ya que el fraude ocurre de diferentes maneras dependiendo de la venta de bienes físicos o digitales y si se usa el canal móvil, esto crea múltiples puntos finales y formas en que los estafadores pueden atacar. Continúan probando los enlaces más débiles y dónde pueden operar sin ser detectados. Saber dónde han tenido éxito es importante para "cerrar las brechas"; pero también es importante saber dónde han intentado y fallado para mantener la vigilancia.

Dicho esto, el aumento de las identidades sintéticas facilita que el fraude pase desapercibido. Sin la ayuda de soluciones de mitigación de riesgos diseñadas para identificar características de identidad fraudulentas, los enfoques de seguimiento perderán ciertas pistas; esto debilitará los esfuerzos de seguimiento.

LexisNexis® RISK SOLUTIONS

LexisNexis® Risk Solutions puede ayudar.

LexisNexis®
RISK SOLUTIONS

LexisNexis® Risk Solutions proporciona potentes herramientas de verificación y autenticación de identidad y puntuación de transacciones para combatir el fraude.

LexisNexis® Risk Solutions:

- Amplios recursos de datos
- \+
- Tecnología de datos masivos
- \+
- Vinculación y análisis
- \+
- Experiencia y conocimientos de cada sector

= Soluciones enfocadas en el cliente

Verificación de identidad

- Valide nombre, dirección e información del teléfono
- Concilie variaciones de nombre, duplicados, múltiples direcciones y muchas otras inconsistencias y enlaces
- Realice comprobaciones de identidad globales con capacidades integradas y de informes

Puntuación de riesgo de transacción

- Identifique los riesgos asociados con las identidades de facturación y envío con una única puntuación de riesgo numérico
- Detecte rápidamente patrones de fraude y aísle las transacciones de alto riesgo
- Resuelva fallas de sistemas de verificación de direcciones y falsos positivos

Soporte de investigación manual

- Acceda a miles de millones de registros de datos de consumidores y empresas
- Descubra vínculos entre personas, empresas y activos
- Aproveche las herramientas especializadas para la debida diligencia, gestión de cuentas y cumplimiento

Autenticación de la identidad

- Autentique identidades en el acto utilizando cuestionarios basados en conocimiento
- Ajuste dinámicamente el nivel de seguridad para adaptarse al escenario de riesgo
- Reciba resultados de aprobación / reprobación en tiempo real

LexisNexis® RISK SOLUTIONS

Para más información:
visite https://risk.lexisnexis.com/fraude o llame al 01 800 5 1 84181

Resumen Regional 2019

LexisNexis®
RISK SOLUTIONS

El fraude sigue siendo considerable en todas las empresas de LATAM, pero sigue siendo más pronunciado para la industria de servicios financieros, así como para las empresas de todo tipo que realizan transacciones a través del canal móvil.

Resultados Regionales

- Estas empresas continúan experimentando altos volúmenes de fraude y cantidades de transacciones exitosas, a pesar de que de alguna manera tienden a usar más soluciones de mitigación de fraude.
- También continúan contribuyendo con más pérdidas por fraude al fraude de identidad que otras empresas.

↑↓ Significativa o direccionalmente desde 2018

2019	Región en general	Industria			Ofrece m-commerce	
		Minorista	e-commerce	Servicios financieros	Si	No
LexisNexis Fraud Multiplier℠	3,46 ↑	2,61	2,96 ↑	3,96 ↑	3,65 ↑	2,52
Costos de fraude como % de ingresos	2,16%	2,38%	2,23%	2,03%	2,35% ↑	1,72% ↑
Media # soluciones de mitigación de fraude	5,6	4,6	5,3	6,1	5,0	4,7
Media # transacciones mensuales de fraude EXITOSAS	598 ↑	288 ↑	303 ↑	815 ↑	742 ↑	232
Media $ cantidad de transacciones mensuales de fraude EXISTOSAS	COL$1.926.387	COL$789.672	COL$698.390 ↑	COL$2.764.283	COL$2.311.091	COL$1.341.535 ↑
% de m-commerce que ofrece aplicaciones móviles	77% ↑	79%	58% ↑	79% ↑	77% ↑	
% de distribución de pérdidas relacionadas con fraude de identidad	34% (12% sintética)	23% (7% sintética)	31% (10% sintética)	40% (15% sintética)	37% (3% sintética)	28% (11% sintética)
% clasificación de verificación de identidad como un desafío principal en línea/móvil	56%	56%	57%	56%	62%	40%

LexisNexis® RISK SOLUTIONS

Y al mirar dentro *de las industrias*, **los comerciantes de bienes digitales y las empresas de servicios financieros** digitales siguen siendo los más afectados por el fraude.

Resultados Regionales

- Los productos digitales representan más de la mitad de las pérdidas por fraude minorista/e-commerce, mientras que los canales en línea/móviles representan las tres cuartas partes de las pérdidas por fraude de servicios financieros.
- Estas empresas continúan teniendo mayores volúmenes y valores de fraude exitosos que otros, lo que contribuye a mayores costos de fraude.
- Las empresas que son de naturaleza digital (ya sea por tipo de bien vendido o por canal de transacción) siguen siendo muy propensas a permitir transacciones a través de aplicaciones móviles de alto riesgo, lo que agrava aún más los desafíos que enfrenta la verificación de identidad, incluidas las identidades sintéticas.

↑↓ Significativa o direccionalmente desde 2018

* Los productos digitales más vendidos incluyen software descargable, juegos / juegos en línea, aplicaciones móviles y suscripciones digitales
** Gana más del 50% de los ingresos a través de los canales en línea / móviles

2019	Minorista/ e-commerce		Servicios financieros	
	Vende productos digitales*	Solo vende bienes físicos	Digital**	No digital
LexisNexis Fraud Multiplier℠	3,13	2,54	4,10 ↑	3,89 ↑
Costos de fraude como % de ingresos	2,76%	2,01%	2,42% ↑	1,83%
% de pérdidas por fraude de…	Bienes digitales= 53%		En línea/canales móviles= 74%	En línea/canales móviles= 55%
Media # soluciones de mitigación de fraude	5,0	4,7	6,5	5,9
Media # transacciones mensuales de fraude EXITOSAS	395	191 ↑	1,200 ↑	621 ↑
Media $ cantidad de transacciones mensuales de fraude EXISTOSAS	COL$1.058.131	COL$538.966	COL$4.891.166 ↑	Col$2.398.663
% de m-commerce que ofrece aplicaciones móviles	79%	67% ↑	77%	81% ↑
% de distribución de pérdidas relacionadas con fraude de identidad	28% (9% sintética)	23% (8% sintética)	42% (13% sintética)	39% (16% sintética)
% clasificación de verificación de identidad como un desafío principal en línea/móvil	44%	43%	83%	43%
% clasificación de identidades sintéticas como principal desafío para la verificación de identidad	60%			

LexisNexis® RISK SOLUTIONS

El fraude sigue siendo considerable en todos los países de LATAM, pero continúa siendo direccionalmente más alto para Brasil, donde los volúmenes y montos de fraude son más altos.

Resultados Regionales

2019	Región en general	País				
		México	Brasil	Colombia	Argentina	Chile
LexisNexis Fraud Multiplier℠	3,46	3,55	3,61	3,29	3,35	3,52
Costos de fraude como % de ingresos	2,16%	1,96%	2,68%	1,56%	1,73%	2,02%
Media # soluciones de mitigación de fraude	5,6	5,5	5,8	5,7	4,9	5,7
Media # transacciones mensuales de fraude EXITOSAS	598	562	691	491	536	564
Media $ cantidad de transacciones mensuales de fraude EXISTOSAS	COL$1.925.300	COL$1.960.587	COL$2.683.101	COL$1.152.476	COL$1.155.188	COL$1.605.384
% de m-commerce que ofrece aplicaciones móviles	77%	83%	73%	87%	74%	70%
% de distribución de pérdidas relacionadas con fraude de identidad	34% (12% sintética)	37% (12% sintética)	31% (12% sintética)	33% (13% sintética)	31% (12% sintética)	35% (12% sintética)
% clasificación de verificación de identidad como un desafío principal en línea / móvil	56%	54%	59%	64%	51%	52%

LexisNexis® RISK SOLUTIONS

Apéndice.

LexisNexis®
RISK SOLUTIONS

Resultados Regionales

	Región en general	Industria			Ofrece m-commerce	
		Minorista	e-commerce	Servicios financieros	Si	No
LexisNexis Fraud Multiplier℠	3,27	2,59	2,71	3,78	3,42	2,54
Costos de fraude como % de ingresos	2,0%	2,06%	2,29%	1,92%	2,18%	1,17%
Media # soluciones de mitigación de fraude	4,6	3,8	4,1	5,2	4,8	3,7
Media # transacciones mensuales de fraude EXITOSAS	491	249	244	673	551	235
Media $ cantidad de transacciones mensuales de fraude EXISTOSAS	COL$1.783.409	COL$677.444	COL$324.543	COL$2.615.247	COL$2.007.123	COL$387.561
% de m-commerce que ofrece aplicaciones móviles	66%	78%	32%	65%	66%	

LexisNexis® RISK SOLUTIONS

Resultados Regionales

	Minorista/ e-commerce		Servicios financieros	
	Vende productos digitales*	Solo vende bienes físicos	Digital**	No digital
LexisNexis Fraud Multiplier℠	3,09	2,65	3,84	3,59
Costos de fraude como % de ingresos	2,44%	1,88%	2,24%	1,79%
% de pérdidas por fraude de…	Bienes digitales = 45%		En línea/canales móviles = 71%	En línea/canales móviles = 52%
Media # soluciones de mitigación de fraude	3,6	4,1	5,4	5,1
Media # transacciones mensuales de fraude EXITOSAS	382	81	917	331
Media $ cantidad de transacciones mensuales de fraude EXISTOSAS	COL$992.534	COL$406.466	COL$2.857.866	COL$2.041.783
% de m-commerce que ofrece aplicaciones móviles	84%	52%	71%	59%
% de distribución de pérdidas relacionadas con fraude de identidad	40% (15% sintética)	32% (12% sintética)	54% (25% sintética)	56% (26% sintética)

LexisNexis® RISK SOLUTIONS

* Los productos digitales más vendidos incluyen software descargable, juegos / juegos en línea, aplicaciones móviles y suscripciones digitales
** Gana más del 50% de los ingresos a través de los canales en línea / móviles

Resultados Regionales

	Región en general	País				
		México	Brasil	Colombia	Argentina	Chile
LexisNexis Fraud Multiplier℠	3,27	3,39	3,44	3,21	3,27	3,34
Costos de fraude como % de ingresos	2,0%	1,75%	2,47%	1,41%	1,59%	1,97%
Media # soluciones de mitigación de fraude	4,6	4,6	4,7	5,0	4,0	5,0
Media # transacciones mensuales de fraude EXITOSAS	491	468	579	453	448	495
Media $ cantidad de transacciones mensuales de fraude EXISTOSAS	COL$1.783.409	COL$1.657.373	COL$2.233.988	COL$1.121.720	COL$1.326.529	COL$1.565.997
% de m-commerce que ofrece aplicaciones móviles	66%	76%	65%	83%	48%	53%

LexisNexis® RISK SOLUTIONS

Para mayor información visite: risk.lexisnexis.com/fraude