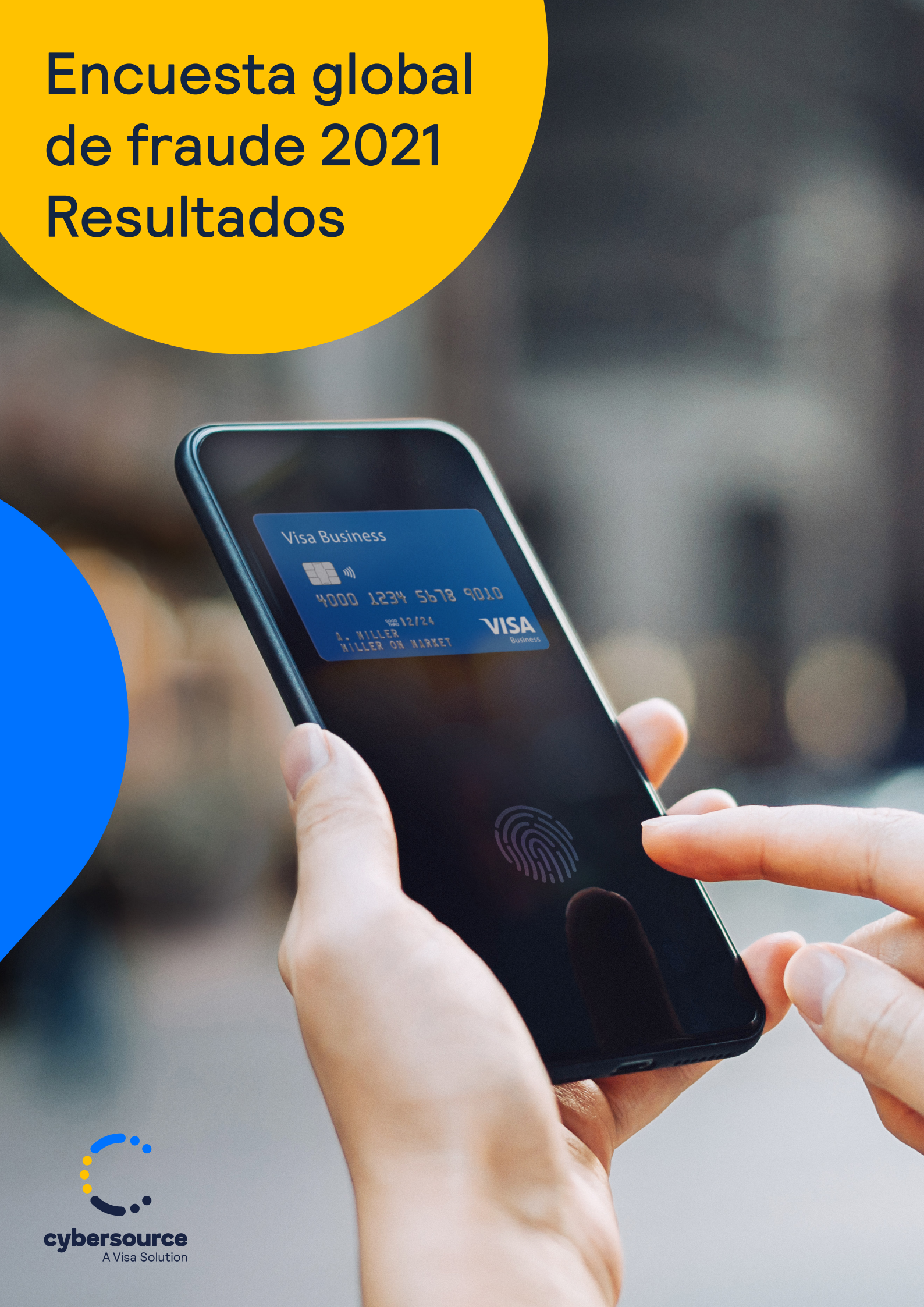
Encuesta global de fraude 2021 Resultados



cybersource
A Visa Solution

Contenido

Panorama

Cybersource y Merchant Risk Council (MRC) presentan los resultados de la encuesta global de fraude 2021, un informe educativo elaborado a partir de una encuesta transparente e imparcial. Este informe se basa en encuestas a empresarios de todo el mundo, a quienes se les preguntó acerca de su experiencia de fraude en eCommerce y las prácticas para mitigarlo.

Los resultados de la encuesta acercan a la comunidad de comercios los datos de fraude más recientes en la industria, los métodos de administración de fraude que utilizan sus pares y un conjunto de acciones de referencia que pueden utilizar para optimizar su negocio. Las encuestas se realizaron entre marzo y abril de 2021.

Cybersource les agradece a los participantes que se tomaron el tiempo de completar la encuesta online, a MRC por su alianza continua y a B2B International por dirigir el programa y realizar el análisis.

Resumen ejecutivo

Los resultados y hallazgos principales que surgen de la encuesta de este año están organizados dentro del informe en tres focos, cada uno de los cuales trata una cuestión central y esencial para comprender el estado del fraude en eCommerce y la administración de fraude en los comercios.

En primer lugar, el informe estudia el impacto del fraude en el negocio para entender sus efectos en los comercios y cómo varía según la región y los segmentos por tamaño. Luego, el informe ahonda en la variedad de ataques de fraude que sufren los comercios para entender los tipos de amenazas que existen y los puntos en los que los comercios son más vulnerables. Por último, el informe explora las estrategias de prevención de fraude para comprender las medidas estratégicas y tácticas que los comercios están utilizando para combatir el fraude de pagos.

Aquí presentamos los datos clave de cada una de estas áreas:

El impacto comercial del fraude: ¿qué efectos tiene el fraude?

- A causa de la pandemia por COVID, tres de cuatro comercios en el mundo sufrieron un aumento en los intentos de fraude y en los índices de fraude por ingresos; los más afectados fueron los comercios de Asia Pacífico y las grandes y medianas empresas
- Aumentaron los intentos de fraude, los costos y otros KPI de administración de fraudes, con mayor efecto durante este año turbulento sobre los comercios de Asia Pacífico y de América Latina y las medianas empresas
- Los comercios destinan más de un tercio del gasto en prevención de fraude en eCommerce para cubrir los costos relacionados con la revisión de órdenes. La mayoría de los comercios quieren depender menos de la revisión manual en un futuro (ya sea en parte o por completo)

Tipos de ataque de fraude: ¿dónde están las mayores vulnerabilidades de los comercios?

- Son menos los tipos de ataque de fraude que sufren los comercios (a pesar de que el volumen de ataques es mayor)
- El fraude amigable y por prueba de tarjeta son ahora los ataques más comunes a nivel mundial, por encima del phishing/pharming y el robo de identidad
- Afortunadamente, la mayoría de los comercios cuenta con una estrategia formal para combatir el fraude amigable, como las diversas notificaciones al cliente, la implementación de políticas visibles y los métodos de verificación y revisión de los historiales de compra

Estrategias de prevención de fraude: ¿cómo están tratando este tema los comercios?

- Para los comercios, la nueva estrategia imprescindible en relación con las prácticas de administración de fraude es proteger y mejorar las experiencias de compra y del cliente
- A nivel táctico, los comercios están racionalizando sus herramientas de administración de fraude y eligen basar su confianza en las herramientas más utilizadas (principalmente la verificación de e-mail y del código CVN)
- Muchas de las herramientas más efectivas no están entre las que los comercios más utilizan ni entre las prioritarias que adoptarían en un futuro

Demografía de las empresas para la encuesta

La encuesta se realizó entre marzo y abril de 2021. Participaron 650 comercios involucrados en las decisiones de prevención de fraude en eCommerce en sus compañías. La muestra incluye comercios en cuatro regiones geográficas, de todos los tamaños, canales de ventas y categorías. Los cuadros a continuación muestran el desglose de los comercios por dato demográfico clave a nivel general.

Región

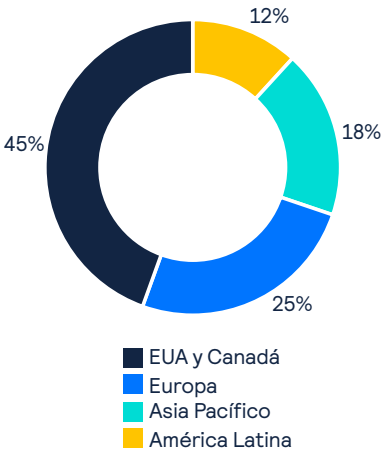


Imagen 1

Tamaño de la compañía

(ingreso anual por eCommerce)

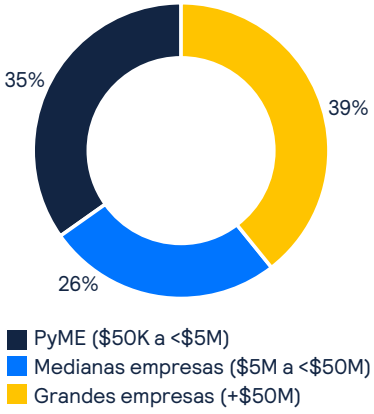


Imagen 2

Canales de compra utilizados y con seguimiento del fraude de pagos

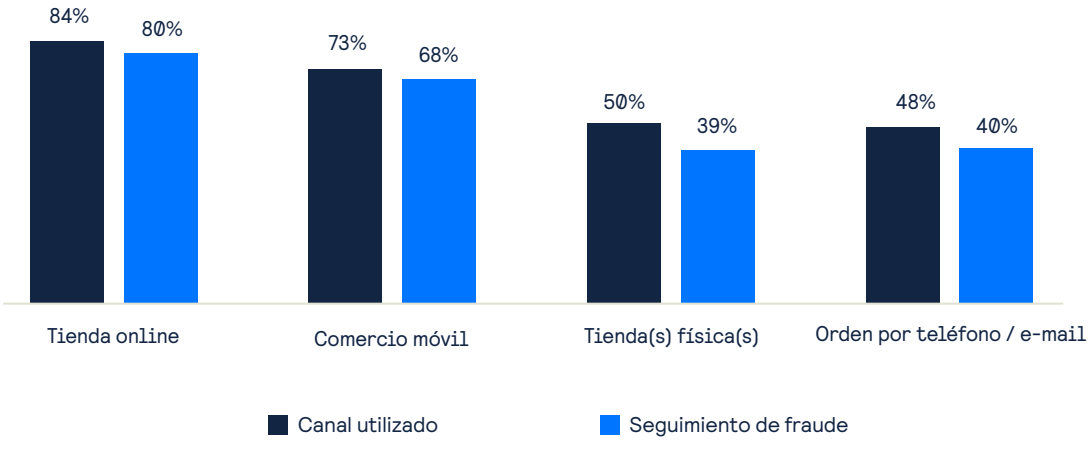


Imagen 3

El nivel de participación en la muestra de comercios que brindan soporte de compras a través del comercio móvil y de órdenes telefónicas o por e-mail tuvo un aumento considerable este año en comparación con el estudio anterior de 2019: de un 65 % a un 73 % y de un 34 % a un 48 %, respectivamente. Sin dudas, ambos canales ganaron atractivo e importancia para los comercios en los últimos dos años, debido a las restricciones por COVID a las compras en la tienda, a una mayor penetración de Internet y a la creciente popularidad de smartphones en todo el mundo.

El impacto comercial del fraude: hallazgos principales

La primera área ilustra el impacto que el fraude en eCommerce tiene en el negocio de los comercios, cómo este impacto ha cambiado y evolucionado desde 2019 y en qué puntos los intentos de los comercios por desactivar y mitigar los daños a su organización tuvieron mayor éxito.

Además de analizar los cuatro hallazgos generales que se indican a continuación, se proporcionan datos en detalle sobre dos aspectos específicos para comprender cómo afecta el fraude a los comercios: por un lado, el estado actual de la revisión manual de las órdenes y, por el otro, la preparación y las expectativas de los comercios respecto de la enmienda reciente a la directiva de servicios de pago (PSD2) de la Unión Europea.

01 A causa de la pandemia por COVID, tres de cuatro comercios sufrieron un aumento en los intentos de fraude y en los índices de fraude por ingresos; desde 2019, hubo un aumento en todos los KPI de administración de fraude.

02 El gasto en la administración de fraude se disparó: desde 2019 se quintuplicó, como participación del ingreso por eCommerce. El segmento según el tamaño de los comercios que más está gastando es el de las medianas empresas.

03 Las organizaciones situadas fuera de EUA y Canadá son las que sufrieron un mayor impacto del fraude durante la pandemia por COVID. El golpe más duro lo sintieron las que se encuentran en Asia Pacífico, lo que incentivó un mayor enfoque en la administración de fraude y un mayor gasto en esta región.

Para muchos comercios en todo el mundo, el avenimiento de la pandemia por COVID-19 y las restricciones a las compras offline habituales durante los últimos dos años impulsaron las ventas online y resaltaron la importancia del eCommerce como un canal de ventas fundamental. Por ello, no resulta extraño que 9 de 10 comercios hoy consideren que administrar el fraude en eCommerce es “de alta o extrema importancia” para su estrategia comercial general (ver imagen 4). Además, para los comercios de la región de Asia Pacífico (APAC), la administración de fraude en eCommerce cobró relevancia; los datos indican el mayor incremento en la participación de los comercios que consideran que este asunto es de suma importancia para su estrategia comercial general, que pasó del 82 % en 2019 al 95 % este año.

La administración de fraude en eCommerce y su importancia en la estrategia comercial general

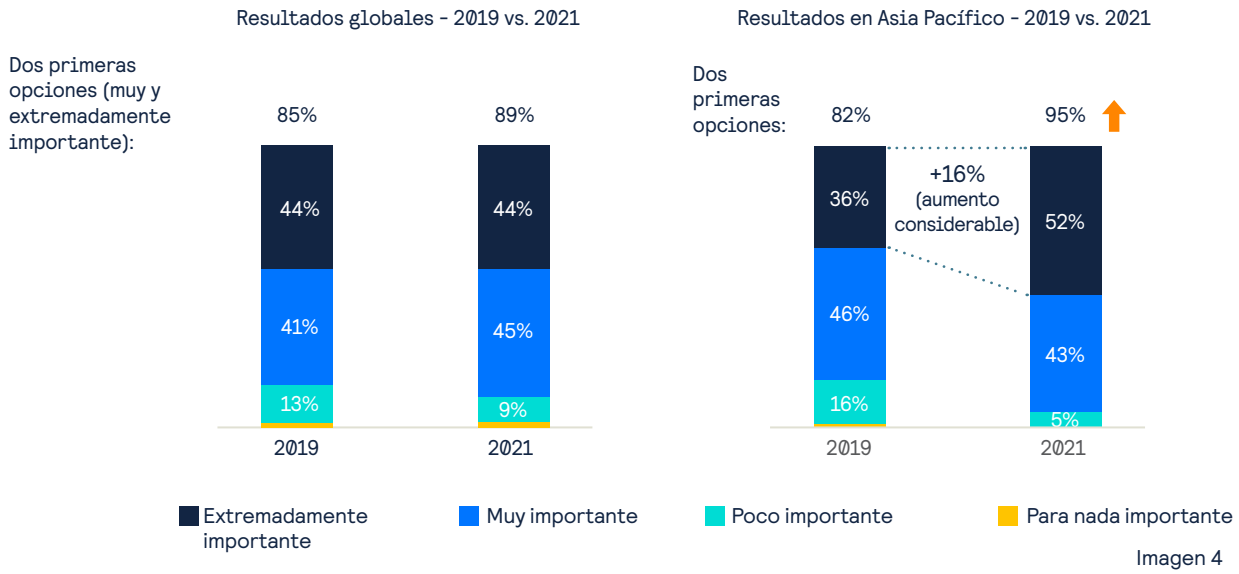


Imagen 4

La importancia de la administración de fraude en eCommerce no aumentó solamente por una mayor cantidad de ventas en eCommerce, sino también por un incremento en los intentos de fraude que sufrieron los comercios. En comparación con los días pre-COVID, alrededor de tres de cuatro comercios denunciaron incrementos en los intentos de fraude y en los índices de fraude por ingresos (imagen 5).

Proporción de las organizaciones que denunciaron incrementos en los intentos de fraude y en el índice de fraude por ingresos

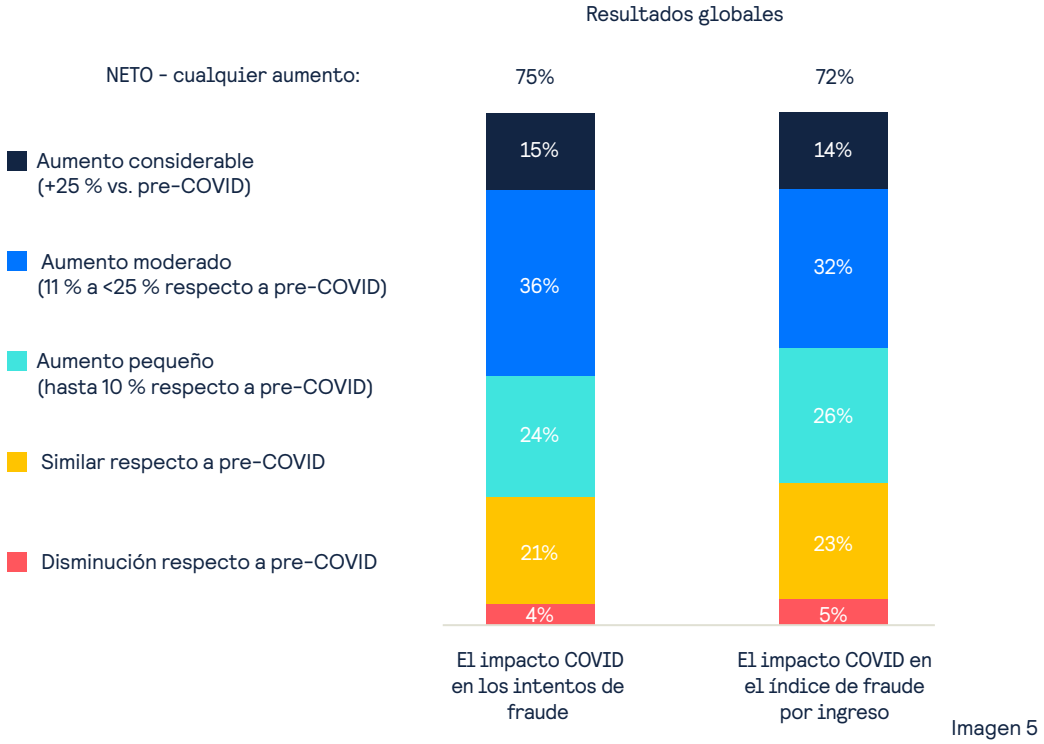


Imagen 5

Por COVID, hubo incrementos en los intentos de fraude y en el índice de fraude por ingresos. Esto tuvo un especial impacto en los comercios ubicados fuera de EUA y Canadá, y en las medianas y grandes empresas. Estos grupos ostentan los mayores ingresos online (imagen 6).

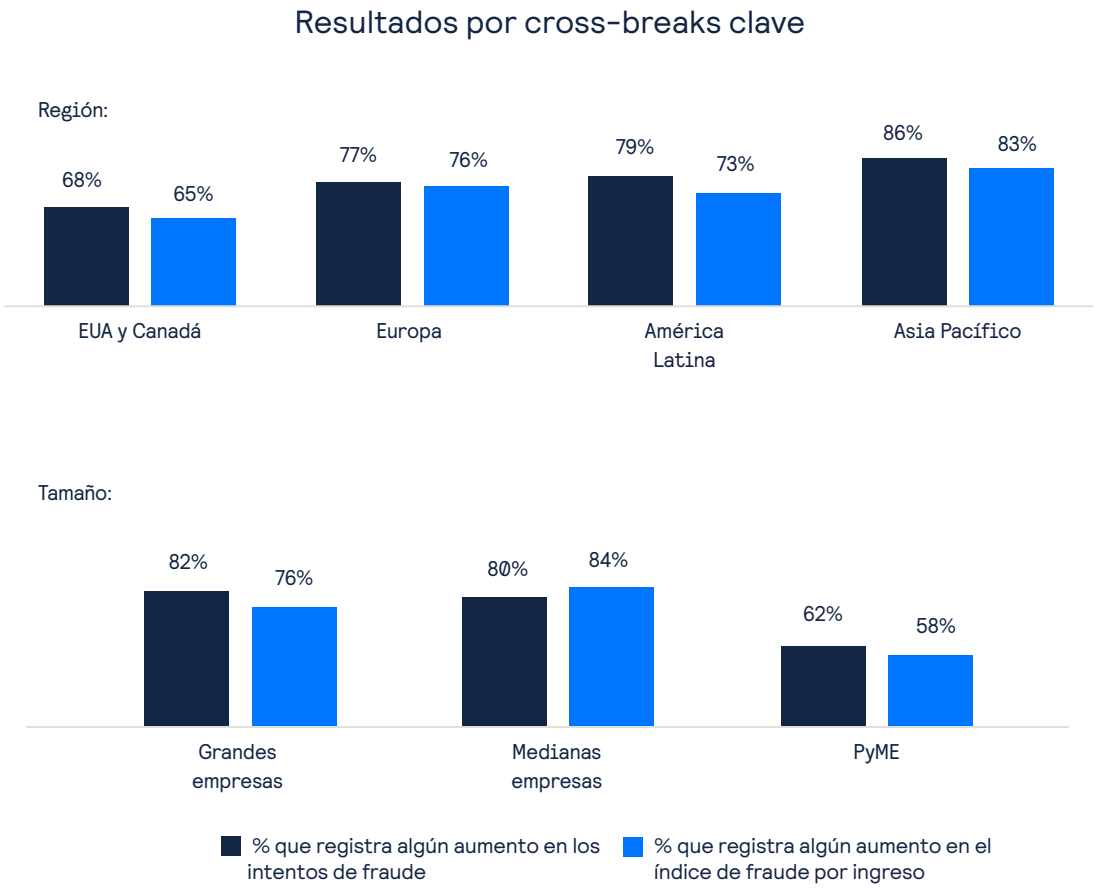


Imagen 6

Como consecuencia del aumento de los intentos de fraude y de los índices de fraude por ingreso, el promedio de los costos de la administración de fraude se quintuplicó, en comparación con los tiempos pre-COVID: de un 2 % de ingreso anual por eCommerce en 2019 a un 10 % este año (imagen 7).

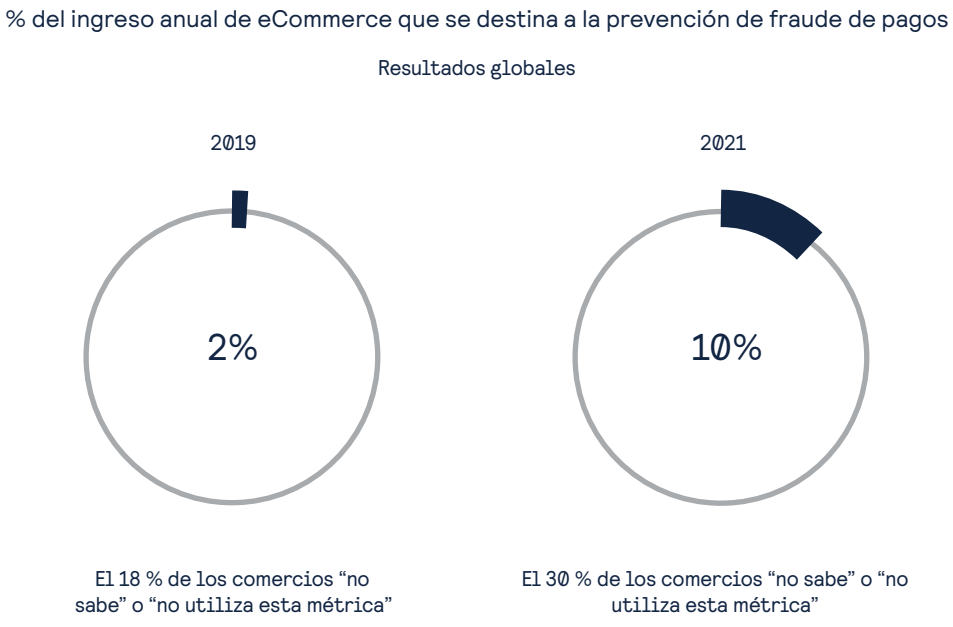
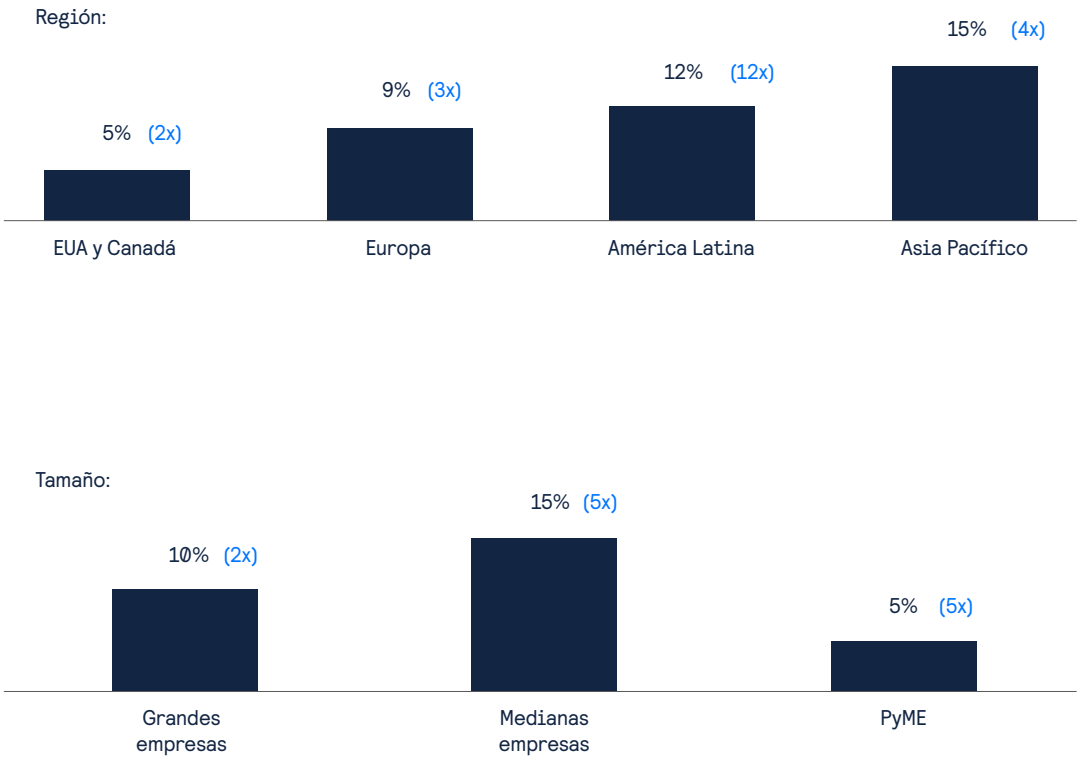


Imagen 7

En comparación con sus pares en otras regiones y segmentos de otros tamaños, las empresas de América Latina y Asia y las medianas empresas destinan una mayor parte de sus ingresos anuales a la administración de fraude (imagen 8).

% del ingreso anual de eCommerce que se destina a la prevención de fraude de pagos - Por breaks clave



(índice de aumento de la variación respecto a 2019)

Imagen 8

El patrón del aumento de los ataques de fraude, de los costos y del impacto en los comercios es claro y contundente cuando se examinan las métricas adicionales de administración de fraude y los KPI que este informe estudió durante los últimos dos años. Desde 2019, aumentaron todos los indicadores que evalúan el impacto del fraude de pagos: desde una mayor pérdida de ingresos por fraude de pagos hasta una mayor cantidad de órdenes en eCommerce que son rechazadas o generan contracargos.

Si bien esta acentuación del impacto del fraude la sienten los comercios de todo el mundo, los más golpeados son los que se encuentran en Europa, Asia y América Latina, y también las medianas empresas, cuyos ingresos anuales de eCommerce van de los US$5 millones a los US$50 millones. El creciente índice de variación en los KPI de administración de fraudes a nivel global tiene relación más directa con el incremento en estos indicadores en los comercios de Europa, Asia, América Latina, y en las medianas empresas que con cualquier otro segmento.

En la tabla se muestran los KPI de administración de fraudes

(Se muestran las medianas truncadas de todos los KPI)

			Por región - 2021				Por tamaño - 2021		
	2019	2021	EUA y Canadá	Europa	Am. Lat.	Asia Pacífico	Grandes empresas	Medianas empresas	PyME
% de pérdida de ingresos en eCommerce por fraude de pagos a nivel global	2.4	3.1	2.6	3.2	3.7	4.0	3.0	3.4	3.0
% de pérdida de ingresos en eCommerce por fraude de pagos en órdenes locales	2.1	3.0	2.5	2.9	3.9	3.9	3.1	3.4	2.7
Índice de rechazo de órdenes locales (%)	2.5	3.0	2.8	2.8	4.0	3.8	3.3	3.7	2.4
Índice de rechazo de órdenes internacionales (%)	5.1	5.6	5.0	5.6	6.9	5.7	5.5	6.2	5.1
% de órdenes de eCommerce que resultaron fraudulentas	2.3	2.6	2.2	2.5	3.5	3.6	2.7	3.0	2.3
% de órdenes de eCommerce que generaron contracargos	1.3	2.7	2.2	2.6	3.8	3.6	2.9	3.0	2.4

Imagen 9

Las conclusiones de los resultados finales a partir de los datos y las tendencias analizadas anteriormente: en primer lugar, el fraude de pagos en eCommerce va en aumento y, como resultado, los comercios sufren un mayor impacto en sus ventas e ingresos. En segundo lugar, hay más presión para gastar y hacer más que nunca con el fin de administrar efectivamente y mitigar esta creciente amenaza a sus negocios y clientes.

El impacto comercial del fraude

Datos en detalle sobre dos tendencias clave: la revisión manual y la normativa PSD2

El estudio de este año también reveló algunos hallazgos notables relacionados específicamente con la revisión manual de las órdenes y con el lanzamiento reciente de la enmienda a la directiva de servicios de pago de la Unión Europea, conocida como PSD2.

Analiza con detalle la revisión manual:

- Si bien en 2021 son menos las órdenes que se revisan manualmente, hay mayor cantidad de órdenes rechazadas, especialmente en Asia Pacífico
- Gran parte de las organizaciones considera incorporar la revisión manual a su estrategia de administración de fraude, pero la gran mayoría quiere depender menos de este proceso

La revisión manual de las órdenes de eCommerce sigue siendo un ingrediente básico pero esencial de la estrategia de prevención de fraude de prácticamente todos los comercios. Los datos muestran que, si bien disminuyó la proporción de órdenes que se revisan manualmente (del 25 % al 20 %), la cantidad de órdenes revisadas que actualmente rechazan los comercios es apenas superior. Este año, los comercios rechazaron el 17 % de las órdenes revisadas, en comparación con el 12 % en 2019 (ver imagen 10).

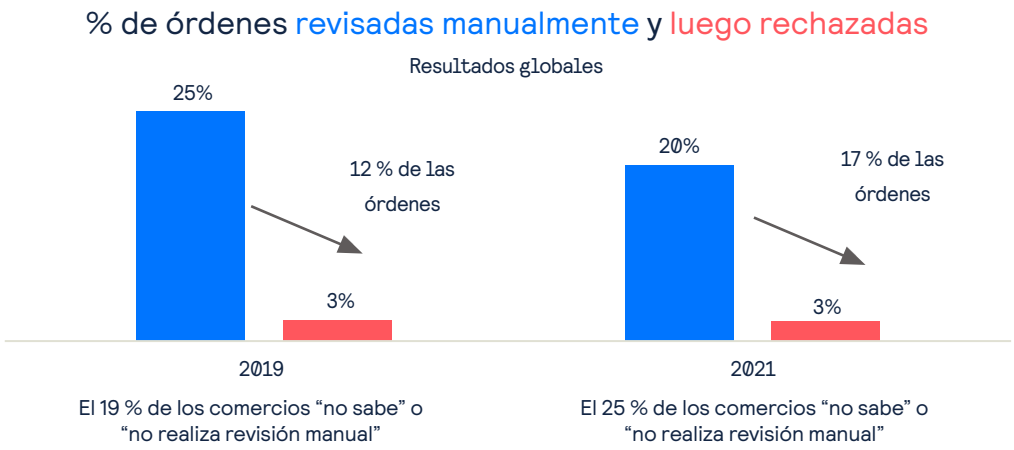
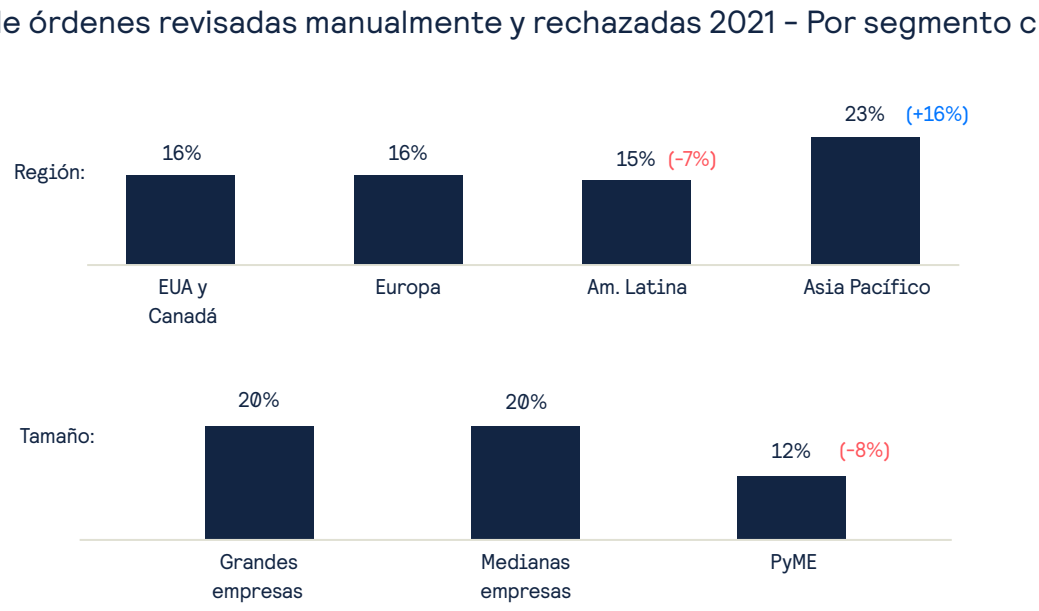


Imagen 10

Además, si bien el porcentaje de órdenes que se revisan manualmente es similar para todos los comercios a nivel global (20 %), el estudio muestra que los comercios en la región de Asia Pacífico superan ampliamente a los de las demás regiones en la cantidad de órdenes que luego rechazan. Esta diferencia se gestó durante los últimos dos años, en los que la proporción de órdenes revisadas y rechazadas por los comercios de esta región aumentó un 16 %. Esto establece un fuerte contraste con los índices de rechazo que se mantienen estables o en descenso en las demás regiones, y puede ser una señal de inseguridad por parte de los comercios de Asia en relación con las decisiones de rechazo automatizadas y sistematizadas, ya que han sido los más golpeados por los aumentos en los intentos de fraude y en los costos relacionados (como se analizó en la sección anterior).

Los datos también revelan una discrepancia en la cantidad de órdenes revisadas que rechazan los comercios de los distintos segmentos de tamaño: las grandes y medianas empresas, que son de mayor tamaño y resultan más atractivas para los estafadores, rechazan un quinto de las órdenes que revisan, sin variación respecto del índice de rechazo en 2019. Las PyME, que generan menos de US$5 millones por año, redujeron en un 8 % la proporción de órdenes rechazadas durante los últimos dos años y en la actualidad rechazan, en promedio, alrededor del 12 % (ver imagen 11). Es probable que la relativa falta de medidas sofisticadas para la prevención de fraudes (entre ellas, el uso de menos herramientas de detección de fraude) sea una de las causas por las que las PyME envían a revisión manual una mayor proporción de órdenes genuinas.



(Entre paréntesis se indican las tendencias más destacables respecto a 2019: el texto en azul indica un aumento y el texto en rojo indica una disminución)

Imagen 11

En el orden estratégico, la revisión manual de las órdenes sigue cumpliendo un rol crucial en los métodos de administración de fraude de los comercios, como se evidencia en el 36 % del total de gasto en prevención de fraude en eCommerce que los comercios destinan a los costos de revisión, a nivel global (imagen 12). Esta cifra es similar a la de 2019, cuando un 42 % del gasto se destinaba a los costos de revisión a nivel global.

Distribución del gasto en prevención de fraude en eCommerce

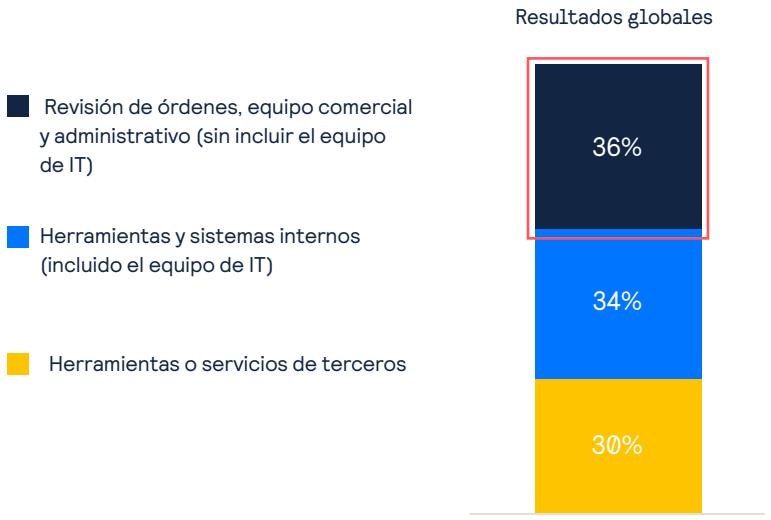
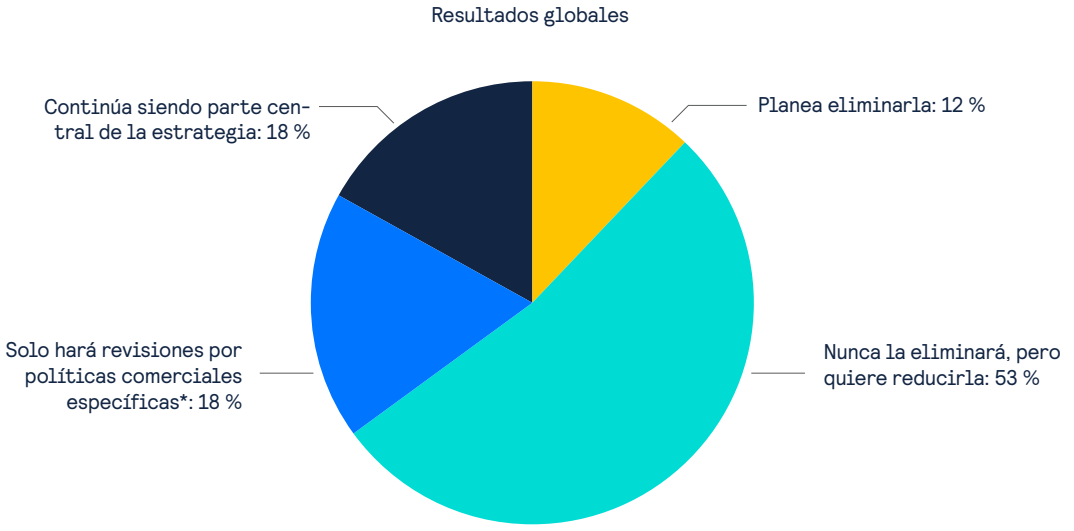


Imagen 12

De acuerdo con los datos obtenidos este año, la mayoría de los comercios considera que la revisión manual seguirá teniendo un rol importante en sus estrategias de administración de fraude. Sin embargo, la mayoría planea reducir la cantidad de tiempo, trabajo y dinero invertido en este proceso. Más de la mitad (53 %) considera que siempre realizará algún tipo de revisión manual, pero quiere reducir la cantidad; por su parte, el 18 % aclara que solo hará revisiones cuando haya políticas comerciales que así lo requieran. El 12 % expresa tener planes para eliminar por completo la revisión manual de órdenes. Menos de la quinta parte (18 %) de los comercios planea conservar la revisión manual como un elemento central de la prevención y mitigación de fraude en el futuro cercano.

El rol de la revisión manual en los futuros planes estratégicos contra el fraude



*(*las políticas incluyen 1 PS5 por cliente, solo envíos a ciertos países, etc.)*

Imagen 13

Análisis en detalle de la normativa PSD2:

- Los comercios se sienten cada vez más preparados para la enmienda a la directiva de servicios de pago de la Unión Europea. La mayoría considera que la PSD2, en particular la autenticación reforzada de clientes (SCA), aumentará la complejidad general de la administración de pagos y del fraude de pagos.

Respecto de la PSD2 y la SCA, los datos reflejan un sentido de preparación mayor entre los comercios a nivel global. La proporción de comercios que sienten estar "algo preparados" permanece igual (9 de 10 tanto en 2019 como en 2021), pero dos de tres dicen estar "muy preparados o extremadamente preparados" para la enmienda a la PSD2 y los requisitos para la SCA. Esto marca un aumento considerable respecto del 50 % que dio la misma respuesta en 2019 (ver imagen 14).

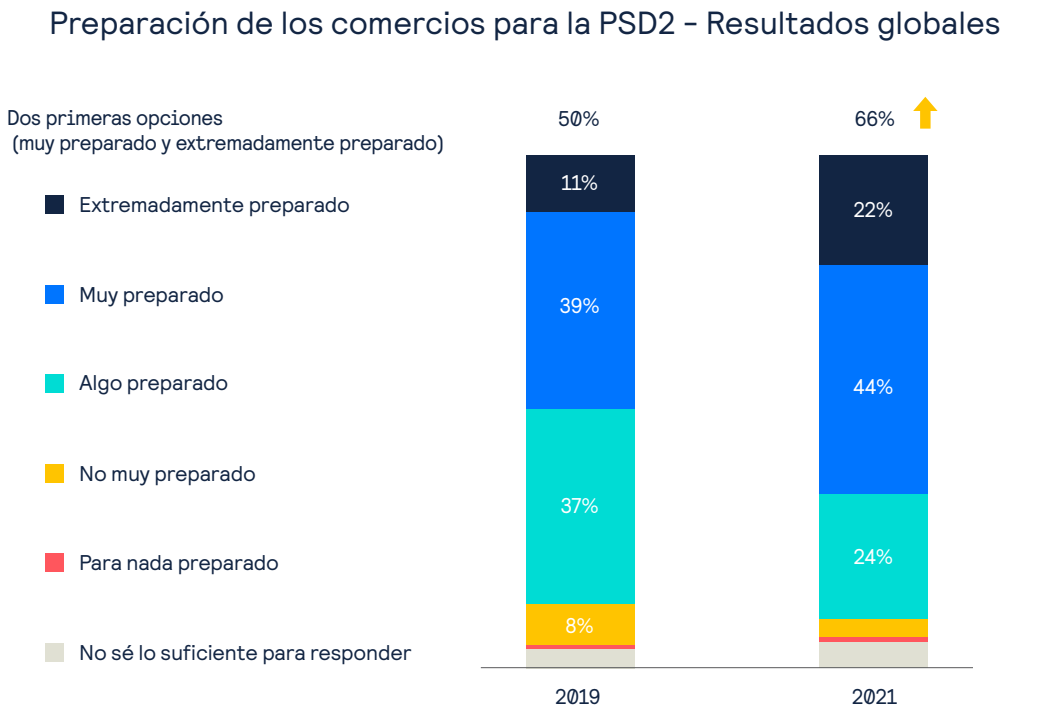


Imagen 14

Si bien ahora más comercios se sienten al menos muy preparados para la PSD2 y SCA, la proporción que considera que tendrá un mayor impacto en su organización es similar a la de 2019: 56 % este año, en comparación con el 53 % de dos años atrás. En particular, más de la mitad (56 %) de los comercios cree que la PSD2 traerá "más complejidad a la administración de pagos" y "más complejidad a la administración de fraude". Menos de la cuarta parte (23 %) piensa que "aumentará la complejidad en la gestión del cumplimiento de normas".

Sin embargo, tanto la preparación para la PSD2 y SCA como las expectativas de un gran impacto varían según la región y el tamaño de los comercios. Es probable que los comercios ubicados en Europa, América Latina y Asia Pacífico, más que los de EUA y Canadá, se sientan preparados y esperen que la PSD2 tenga un gran impacto en su organización. No obstante, debe observarse que uno de diez comercios de EUA y Canadá en nuestra muestra no conoce la PSD2, en contraste con solo el 1 % de los comercios de otras regiones. Posiblemente, esto sea así porque los comercios de EUA y Canadá no operan dentro de la Unión Europea o del Espacio Económico Europeo. De modo similar, las medianas y grandes empresas superan a otras en ambas métricas de actitud, en comparación con las PyME (ver imagen 15).

Resultados por cross-breaks clave - 2021

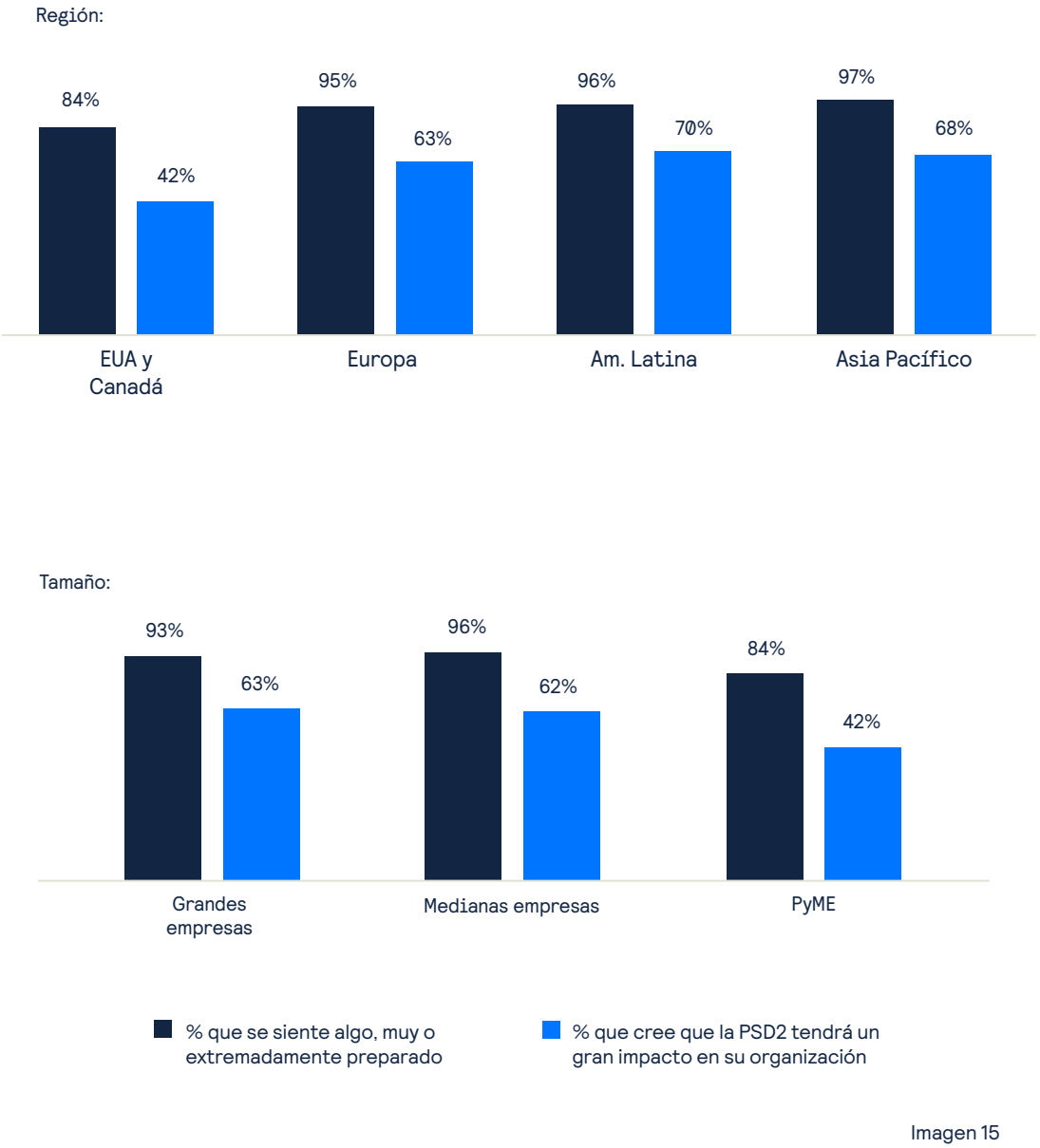


Imagen 15

Tipos de ataque de fraude: hallazgos principales

La próxima área se concentra en el volumen y la variedad de ataques de fraude que sufren los comercios y en cómo cambiaron en los últimos años. También se concentra en qué están haciendo los comercios para ser menos vulnerables en la lucha contra las formas de fraude que más prevalecen y más daño les hacen a sus organizaciones, mientras lidian con desafíos adicionales relacionados con el fraude.

01 Si bien aumentó el volumen de ataques de fraude, disminuyó la variedad (es decir que sufren más cantidad de ataques, pero menos variados).

02 El phishing, el fraude amigable, por prueba de tarjeta y por robo de identidad son los tipos de ataque que más prevalecen actualmente y que impactan a la mayor porción de comercios a nivel global.

- La mayoría de los comercios cuenta con una estrategia formal para combatir el fraude amigable, como las diversas notificaciones al cliente, la implementación de políticas visibles y la verificación y revisión de los historiales de compra.
- Desde 2019, disminuyó la prevalencia de los ataques de robo de cuenta por comercio, en parte debido a la mayor implementación de herramientas diseñadas para monitorear y mitigar esta forma de fraude.

03 Los comercios deben lidiar con un abanico de desafíos relacionados, más allá de detectar y prevenir el fraude propiamente y de afrontar los altos costos de la administración de fraude, los cuales presentan grandes dificultades que los comercios deben superar.

Como se analizó en la primera parte de este informe, tres de cuatro comercios vieron un incremento en el volumen de ataques de fraude desde el inicio de la pandemia por COVID. Sin embargo, los comercios también notaron una disminución en la variedad de los ataques de fraude que sufrieron sus organizaciones durante el mismo período. En 2019, en promedio, los comercios sufrieron cuatro tipos diferentes de ataques de fraude; este año, el promedio bajó a tres. En resumen, los comercios están siendo atacados con mayor frecuencia, pero los tipos de ataque varían menos.

Los tipos de fraude de pagos más comunes también cambiaron de manera significativa a partir de 2019: el fraude amigable (en el que el cliente le solicita un contracargo a su banco luego de haber recibido el producto o servicio comprado) y el fraude por prueba de tarjeta son ahora los dos ataques más comunes a los comercios, por encima del phishing/pharming y el fraude por robo de identidad. El fraude amigable es especialmente problemático para los comercios de Asia Pacífico y de EUA y Canadá, donde la incidencia aumentó en un 9 % y un 16 %, respectivamente, en comparación con 2019. En la imagen 16 se incluyen datos de los tipos de ataques de fraude más comunes.

	Posición en 2019	Posición en 2021	% global afectado (2021)
Fraude amigable	5	1	39%
Prueba de tarjeta	4	2	37%
Phishing/pharming/whaling	1	3	34%
Robo de identidad	2	4	28%
Abuso de cupón/descuento/reembolso	7	5	27%
Fraude en programas de fidelización	10	6	27%
Robo de cuenta	3	7	23%
Fraude de afiliados	6	8	21%
Esquema de triangulación	11	9	20%
Botnets	8	10	19%
Lavado de dinero	12	11	16%
Reenvío	9	12	15%

= bajó de posición = subió de posición

Imagen 16

Como se indican en las posiciones diagramadas en la imagen 17, existen variaciones en los tipos de ataques de fraude más comunes que sufren los comercios según el tamaño y la región donde se encuentran. Así como es importante notar estos matices y las diferencias entre los segmentos, estos datos subrayan la prevalencia y la relevancia a nivel universal del fraude amigable, el fraude por prueba de tarjeta y phishing/pharming como los tres tipos de fraude de pagos que prácticamente todos los comercios sufrirán sin importar su ubicación geográfica o sus ingresos online.

Ataques de fraude más comunes por región

	EUA y Canadá	Europa	América Latina	Asia Pacífico
1	Prueba de tarjeta	Phishing / pharming / whaling	Fraude Amigable	Phishing / pharming / whaling
2	Fraude Amigable	Fraude Amigable	Prueba de tarjeta	Fraude Amigable
3	Phishing / pharming / whaling	Robo de cuenta	Abuso de cupón / descuento / reembolso	Fraude en programas de fidelización
4	Robo de identidad	Fraude en programas de fidelización	Phishing / pharming / whaling	Robo de identidad
5	Abuso de cupón / descuento / reembolso	Prueba de tarjeta	Fraude de afiliados	Prueba de tarjeta
				Abuso de cupón / descuento / reembolso

Ataques de fraude más comunes por tamaño de la compañía

	PyME	Medianas Empresas	Grandes Empresas
1	Fraude Amigable	Fraude Amigable	Fraude Amigable
2	Prueba de tarjeta	Prueba de tarjeta	Prueba de tarjeta
3	Phishing / pharming / whaling	Robo de identidad	Phishing / pharming / whaling
4	Robo de identidad	Phishing / pharming / whaling	Fraude en programas de fidelización
5	Abuso de cupón / descuento / reembolso	Abuso de cupón / descuento / reembolso	Abuso de cupón / descuento / reembolso

Imagen 17

A nivel global, el fraude amigable es el tipo de ataque más común que sufren los comercios, quienes calculan que alrededor del 1.2 % de las órdenes de eCommerce aprobadas eventualmente terminan siendo casos de fraude amigable. El fraude amigable constituye una preocupación mayor para los comercios de América Latina y Asia, dado el porcentaje de órdenes aprobadas que terminan siendo casos de fraude amigable (imagen 18).

	Región - 2021				Tamaño - 2021		
	EUA y Canadá	Europa	América Latina	Asia Pacífico	Grandes empresas	Medianas empresas	PyME
% de órdenes aprobadas que resultan en fraude amigable	1.0	1.3	1.6	1.5	1.3	1.4	1.0

Imagen 18

¿Cómo están respondiendo los comercios al aumento de los últimos dos años en los ataques de fraude amigable a sus organizaciones?

El 80 % de los comercios a nivel global cuenta con una estrategia formal para combatir el fraude amigable (pero esto aplica al 71 % de los comercios de EUA y Canadá, y al 68 % de las PyME). De los cuatro comercios cada cinco que cuentan con una estrategia formal, la mayoría optó por un método múltiple que comprende un abanico de tácticas específicas, como notificaciones al cliente, políticas claras de pago y de devolución, y diversas medidas de verificación para corroborar y confirmar la identidad del cliente (imagen 19).

Estrategias agrupadas: % que selecciona al menos una

Notificaciones y visibilidad	68%
Comprobación e identificación	61%
Identificación de transacciones y verificación	60%
Requisitos mejorados	52%
Presentaciones y reclamos	47%

Imagen 19

Así como aumenta el fraude amigable en los comercios, disminuye el fraude por robo de cuenta (es decir, cuando los estafadores acceden a los datos de cuenta del cliente o los manipulan). En 2019, el fraude por robo de cuenta fue el tercer tipo de ataque de fraude más común, que afectó al 37 % de los comercios. Este año, sin embargo, el robo de cuenta cayó a la posición #7 e impactó a menos de la cuarta parte (23 %) de los comercios a nivel global (imagen 20).

La disminución en el fraude por robo de cuenta se debe en parte a la adopción de herramientas especializadas para monitorear y prevenir este tipo de ataque, ya que aumentó la proporción de organizaciones con esta herramienta. En términos de la implementación de dichas herramientas especializadas, los comercios de EUA y Canadá y las PyME están algo atrasados respecto de los comercios de las demás regiones y tamaños (ver imagen 20).

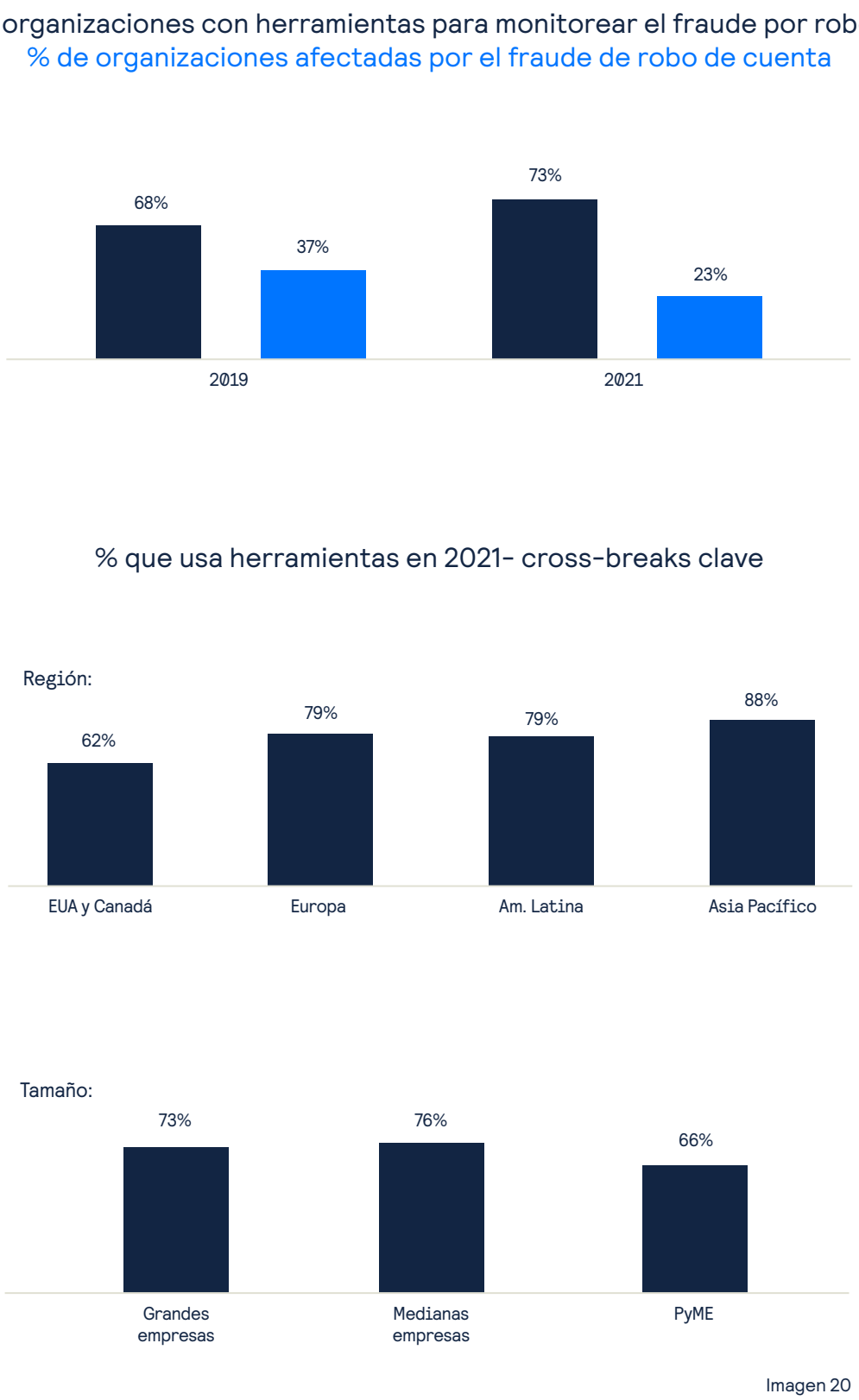


Imagen 20

Un factor que hace que la administración de fraude en eCommerce resulte tan difícil y compleja para los comercios es que tienen que lidiar con un abanico de desafíos comerciales que implica más que monitorear y prevenir el fraude de pagos propiamente. En la imagen 21, se indican los diferentes desafíos de administración de fraude, su incidencia y la gravedad. Estos desafíos afectan al 92 % de los comercios a nivel mundial:

Incidencia y gravedad de los desafíos de administración de fraude que vivieron los comercios en los últimos 12 meses

Imagen 21

Los comercios en 2021 se han enfrentado al menos a tres de los desafíos anteriormente indicados durante los últimos 12 meses, y muchos continúan luchando para superar varios desafíos en simultáneo. Por ejemplo, es más probable que las grandes empresas enfrenten la mayoría de los desafíos listados en la imagen 21, en comparación con las medianas empresas y las PyME: durante el último año, más de la cuarta parte (26 %) de las grandes empresas atravesó cinco o más de los desafíos mencionados, mientras que esto fue así para el 12 % de las medianas empresas y el 9 % de las PyME.

Cada desafío presenta diversos grados de dificultad o gravedad para los comercios. Tres de los cinco desafíos más prevalentes son considerados, además, los más graves; pero existe también un segundo grupo de problemas, indicados en amarillo en la imagen 21, que generan mucho daño y que impactan a una porción menor de comercios a nivel mundial. Es importante asumir que estos últimos pueden ser un problema tan grande para los comercios que los sufren como lo son los primeros.

De acuerdo con los resultados, combatir de manera efectiva el fraude en eCommerce significa reducir el volumen de ataques que apuntan a los comercios, comprender y atacar los diversos tipos de ataques de fraude (que continúan surgiendo y evolucionando) y superar una serie de desafíos adicionales relacionados con el fraude, que obstaculizan y limitan en varias medidas las capacidades de prevención de fraude de los comercios.

Estrategias de prevención de fraudes: hallazgos principales

En la última área de este informe se abordan las estrategias de prevención de fraude de los comercios. ¿Qué están haciendo los comercios para abordar y combatir el fraude de pagos en eCommerce en la actualidad y a futuro?

01 A pesar del aumento en los ataques y en la pérdida de ingresos, los comercios priorizan las mejoras que se realizan en la experiencia del cliente y de compra, y las ven como parte de las prácticas para prevenir el fraude (en contraste con minimizar los costos operativos relacionados con el fraude, por ejemplo).

02 A nivel táctico, los comercios están racionalizando sus herramientas de administración de fraude y eligen basar su confianza en las herramientas más utilizadas, en contraste con 2019.

03 Con excepción de la verificación del número de tarjeta (CVN), la autenticación de dos factores por teléfono y la autenticación 3DS, muchas de las herramientas más efectivas para la detección de fraude (de acuerdo con la opinión de los participantes encuestados) no son las más utilizadas ni están entre las primeras que se adoptarían en un futuro.

Para comprender las estrategias de prevención de fraude de los comercios, es fundamental conocer las metas y los objetivos que priorizan, a diferencia de otros, como parte de sus estrategias de administración de fraude. Los datos muestran que la meta estratégica principal que los comercios veían en 2019 como parte de la administración de fraude era la reducción de la cantidad de fraudes y contracargos.

Este año, la mitad de los comercios elige darle prioridad a mejorar la experiencia del cliente (CX), el 40 % continúa enfocándose en reducir el fraude y solo el 11 % prioriza reducir los costos (ver imagen 22).

La imagen 22 también muestra algunas diferencias notables en las metas estratégicas que los comercios deciden sacar de sus prioridades, con distinción de región, tamaño y sector industrial. Como las decisiones de administración de fraude de los comercios se enfocaron más en mejorar la experiencia del cliente, los comercios de América Latina y las grandes empresas pusieron menos énfasis en la reducción de la cantidad de fraudes y contracargos. Los comercios de Europa, las medianas empresas, las PyME y los comercios que se dedican a la venta de bienes digitales y de productos y servicios relacionados con viajes y turismo fueron los que mejor lograron pensar menos en los costos operativos generados por el fraude. Es probable que los comercios de EUA y Canadá, al igual que los comercios que venden bienes físicos en el sector minorista, también logren pensar menos en reducir el fraude y los costos, ya que su prioridad es mejorar la experiencia del cliente.

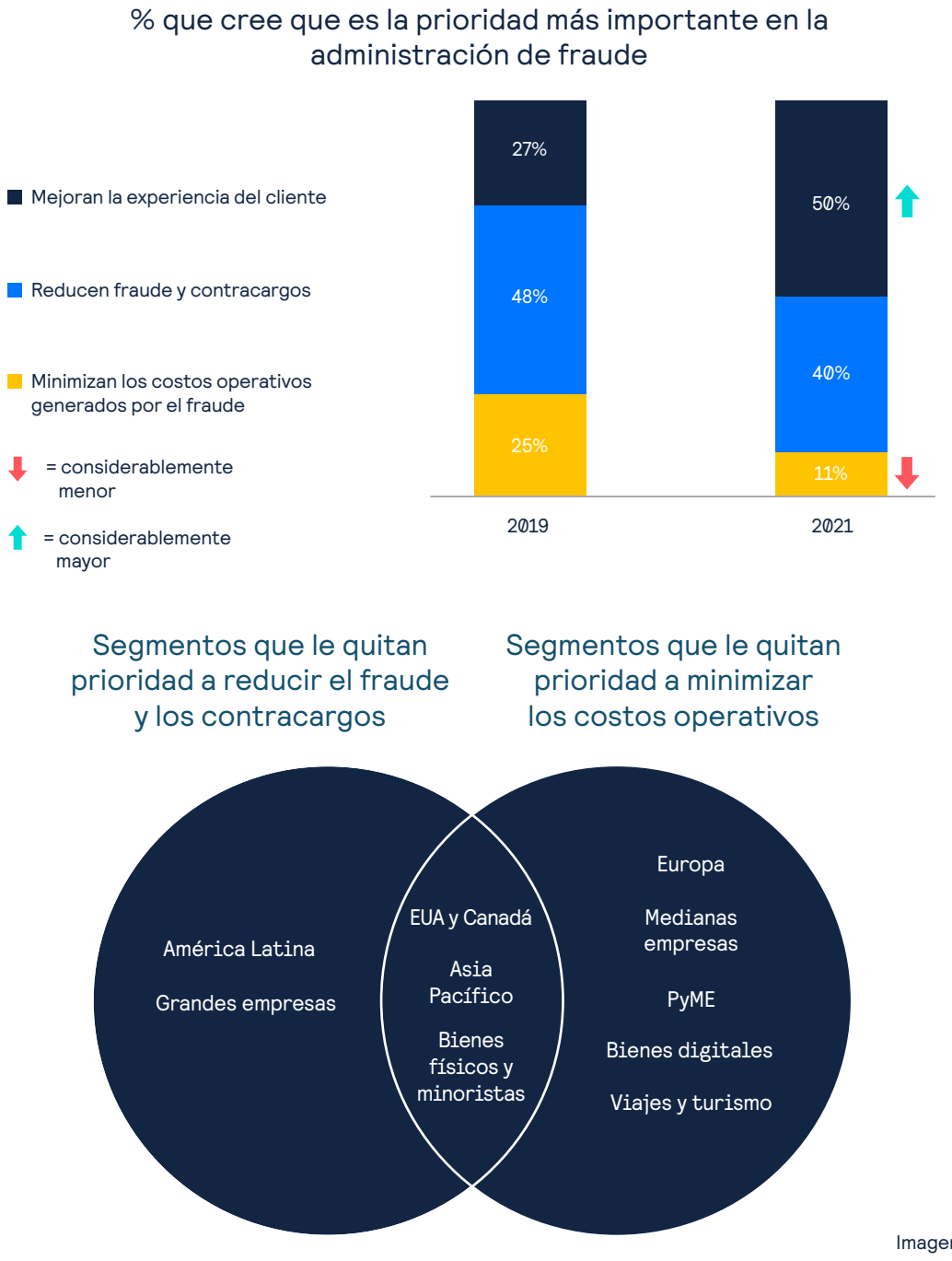


Imagen 22

Este cambio estratégico de los comercios en la administración de fraude busca conseguir un mejor equilibrio que les permita proteger los activos y las operaciones de la empresa, por un lado, y ofrecerle al cliente una experiencia de compra y de pago excelente, por el otro.

Durante los últimos dos años, a nivel de la organización, las estrategias de prevención de fraude de los comercios evolucionaron; de modo similar, a nivel táctico, también evolucionó la calidad de las herramientas de administración de fraude que utilizan. En lugar de implementar toda una gama nueva de herramientas y tecnologías contra el fraude, los comercios decidieron racionalizar las soluciones de prevención de fraudes. La cantidad promedio de herramientas con la que cuenta cada comercio se redujo a la mitad: de 10 en 2019 pasó a 5 este año.

Las 15 herramientas de detección de fraude más utilizadas	Posición en 2019*	Posición en 2021*	% global que usa la herramienta (2021)
Verificación del número de tarjeta (CVN)	2	1	54%
Verificación por e-mail	3	2	43%
Historial de órdenes del cliente	1	3	38%
Verificación de domicilio (AVS)	4	4	37%
Autenticación 3-D Secure	5	5	36%
Verificación de número telefónico y por búsqueda inversa	13	6	31%
Validación de la dirección postal	8	7	27%
Listas de negativos / listas negras (listas propias)	6	8	24%
Comportamiento del cliente en la web / análisis de patrones	10	9	23%
Listas de positivos / listas blancas	9	10	21%
Monitoreo de velocidad de orden	19	11	21%
Indicadores geográficos / mapas	17	12	18%
Geolocalización de país/ciudad, etc.	7	13	18%
Autenticación de dos factores por teléfono (In-App, SMS, etc.)	11	14	18%
Sitios de redes sociales	18	15	18%

**Solo Europa, EUA y Canadá (para un seguimiento consistente)*

= bajó de posición = subió de posición

Imagen 23

Como se muestra en la imagen 24, las herramientas de detección de fraude que más prevalecen son más o menos las mismas en todas las regiones y tamaños. Sin embargo, existen algunas diferencias notables en los tipos y la cantidad de herramientas en las que los comercios de cada grupo confían: por ejemplo, es más probable que los comercios de Europa y de Asia Pacífico implementen la autenticación 3DS (esto en Europa puede ser a causa de la necesidad de cumplir con los requisitos SCA y PSD2; y en Asia Pacífico, a la mayor cantidad de ataques de fraude, como ya se explicó en este informe). Asimismo, en promedio, lógicamente las grandes empresas se basan en una gama más amplia de herramientas de detección de fraude que las medianas empresas y las PyME.

Herramientas de detección de fraude más usadas por región

	EUA y Canadá	Europa	América Latina	Asia Pacífico
1	CVN	CVN	Verificación por e-mail	Autent. 3DS/ SafeKey
2	Verificación por e-mail	Autent. 3DS/ SafeKey	CVN	CVN
3	Historial de órdenes del cliente	Verificación por e-mail	Historial de órdenes del cliente	Verificación por e-mail
4	AVS	AVS	AVS	Verificación del número telefónico
5	Verificación del número telefónico	Customer order history	Verificación de historial crediticio	AVS
N.º promedio de herramientas de detección usadas	5	4	6	6

Herramientas de detección de fraude más usadas por tamaño

	PyME	Medianas empresas	Grandes empresas
1	CVN	CVN	CVN
2	Verificación por e-mail	Autent. 3DS/ SafeKey	Verificación por e-mail
3	Historial de órdenes del cliente	Verificación por e-mail	AVS
4	AVS	Historial de órdenes del cliente	Autent. 3DS/ SafeKey
5	Validación de la dirección postal	AVS	Historial de órdenes del cliente
		Verificación del número telefónico	
N.º promedio de herramientas de detección usadas	4	4	6

Imagen 24

Conforme los comercios continúan evaluando nuevas herramientas contra el fraude para implementar en un futuro, para otros será necesario tener presentes las últimas dos imágenes de esta sección a continuación, en las que se segmentan 25 herramientas de prevención de fraudes con base en su nivel de uso y, aun más importante, en la opinión de los comercios respecto de su efectividad para detectar y prevenir el fraude. En la imagen 25 se muestra el nivel de uso actual y el plan de implementación de las herramientas que los comercios consideran que son las más efectivas para desactivar el fraude. La imagen 26 muestra las mismas estadísticas para las herramientas que, en promedio, los comercios consideran que son las menos efectivas.

% que usa o planea implementar las herramientas de detección de fraude “más efectivas”

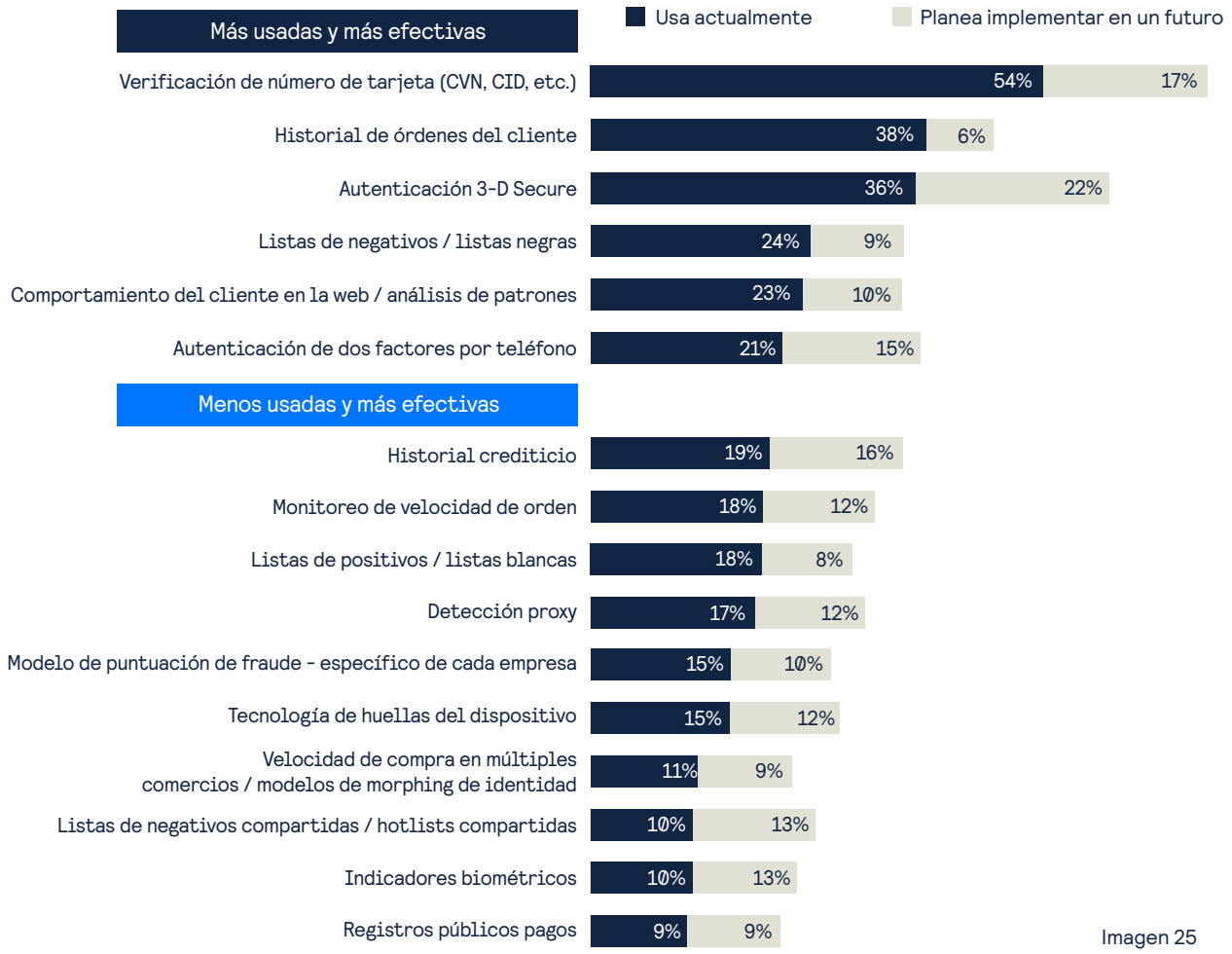


Imagen 25

% que usa o planea implementar las herramientas de detección de fraude “menos efectivas”

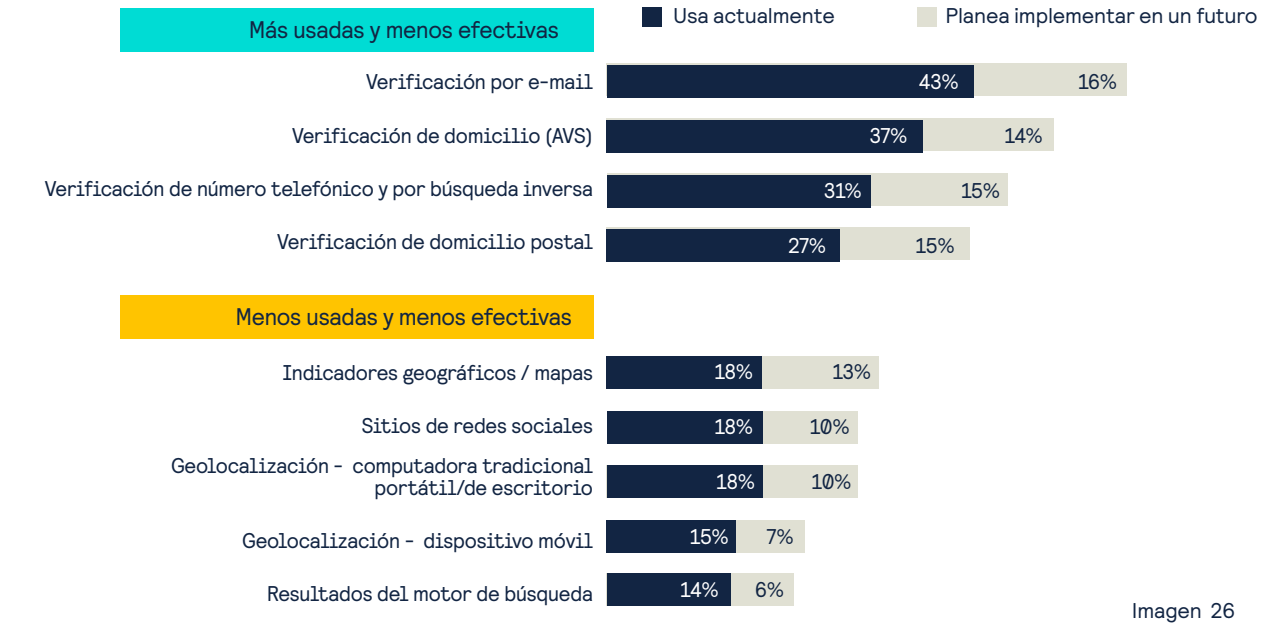


Imagen 26

Las imágenes 25 y 26 deberían alertar a los comercios y servir como orientación táctica a la hora de elegir las soluciones de prevención de fraude en las que invertirán en el futuro: los datos aquí expuestos muestran que las herramientas de detección de fraude más efectivas no son las más utilizadas ni son las primeras en los planes de implementación de los comercios en un futuro. Para potenciar la capacidad de lucha contra el fraude y lograr los mejores resultados a nivel táctico, los comercios deberían considerar invertir en herramientas que quizás no son tan utilizadas como otras, pero que son más efectivas, como la verificación del historial crediticio, el monitoreo de la velocidad de orden, las listas de positivos y listas blancas, la detección proxy, la tecnología de huellas del dispositivo y los modelos de puntuación de fraude específicos de cada empresa.

Conclusión

Los resultados y los hallazgos principales analizados en este informe resaltan cuán crítico, complejo y desafiante se tornó el fraude de pagos en eCommerce para los comercios. El presente informe muestra diversas tendencias e indicadores positivos, que, en conjunto, incentivan la capacidad que tienen los comercios para mejorar y potenciar efectivamente las tácticas y estrategias de administración de fraude, y así, en el futuro, proteger mejor a sus organizaciones y a sus clientes de las amenazas y de los daños que genera el fraude. Cybersource tiene el compromiso de acompañar a los comercios en sus esfuerzos de prevención y de administración de fraude. Por ello, continuará patrocinando y promocionando investigaciones y estudios sobre estos temas tan importantes en los años venideros.

Sobre los autores

Cybersource es una plataforma global y modular de administración de pagos construida sobre la estructura segura de Visa con los beneficios y los conocimientos de una gran red de procesamiento global de US$427 000 millones. Esta solución ayuda a que las empresas operen ágilmente y alcancen sus objetivos de comercio digital gracias a una experiencia del cliente mejorada, al aumento de los ingresos y a la mitigación de los riesgos. Para los socios adquirientes, Cybersource ofrece una plataforma tecnológica, experiencia en pagos y servicios de asistencia que los ayuda a aumentar y administrar su portafolio comercial para cumplir con su promesa de marca.

Para más información, visita: cybersource.com

Como asociación comercial independiente sin fines de lucro, la misión de Merchant Risk Council es facilitar la colaboración entre los pagos en eCommerce y los profesionales de las áreas de gestión de riesgos. A lo largo de todo el año, MRC ofrece valiosos recursos para sus miembros, entre los que se incluyen contenidos educativos exclusivos, webinars, mejores prácticas, tendencias en la industria, informes de benchmarking y documentos técnicos. Además, MRC organiza cuatro conferencias anuales en EUA y Europa, y diversos eventos regionales de networking que les permiten a los profesionales de la industria forjar lazos con las partes interesadas.

Para más información, visita: merchantriskcouncil.org

B2B International es una empresa global de investigación de mercado con servicio integral, especializada en los mercados B2B. Ayudamos a que nuestros clientes utilicen la información para tomar decisiones inteligentes y logren sus objetivos.
B2B International es parte de un consorcio conformado por las mejores agencias B2B del mundo, que juntas forman Merkle B2B. Como agencia de Merkle B2B, ofrecemos la primera solución B2B end-to-end completamente integrada del mundo. ¿Nuestra única promesa? Generar la mejor experiencia B2B del cliente.

Para más información, visita: b2binternational.com

Apéndice – Preguntas

En esta sección se muestran las preguntas que se realizaron a los encuestados para obtener la información expuesta en este informe.

Imagen 1: ¿En qué país tienes base?

Imagen 2: Indica el ingreso anual por eCommerce de tu organización. Por 'eCommerce' nos referimos a cualquier canal a través del que un cliente puede realizar una orden fuera de la tienda. Puede ser desde tu sitio web o desde un dispositivo móvil.

Imagen 3 – "canales utilizados": ¿Cuál de los siguientes canales de órdenes opera tu organización?

Imagen 3 – "seguimiento de fraude": ¿En cuál de los siguientes canales tu organización realiza un seguimiento del fraude de pagos?

Imagen 4: ¿Qué importancia tiene la administración de fraude en eCommerce para la estrategia comercial general de tu organización?

Imágenes 5 y 6:

- El impacto COVID en los intentos de fraude: ¿Hasta qué punto crees que la pandemia por COVID impactó en el volumen de los intentos de fraude en tu organización?
- El impacto COVID en el índice de fraude por ingreso: ¿Qué impacto tuvo la pandemia por COVID en la pérdida de ingresos de eCommerce anual debido al fraude de pagos a nivel global, es decir, el índice de fraude por ingresos?

Imágenes 7 y 8: Indica el porcentaje de tus ingresos anuales de eCommerce que tu organización destina a la prevención de fraude, sin incluir las pérdidas por fraude reales.

Imagen 9:

- % de pérdida de ingresos en eCommerce por fraude de pagos a nivel global: Indica el porcentaje anual de pérdida de ingresos por fraude en eCommerce a nivel global, es decir, el índice de fraude por ingresos.
- % de pérdida de ingresos en eCommerce por fraude de pagos en órdenes locales: Indica el porcentaje anual de pérdida de ingresos por fraude de pagos en eCommerce en órdenes locales.
- Índice de rechazo de órdenes locales: Indica el índice de rechazo de órdenes locales, es decir, el porcentaje de órdenes rechazadas por sospecha de fraude.
- Índice de rechazo de órdenes internacionales: Indica el índice de rechazo de órdenes internacionales, es decir, el porcentaje de órdenes rechazadas por sospecha de fraude.
- % de órdenes de eCommerce que resultaron fraudulentas: Indica el porcentaje de la cantidad anual de órdenes de eCommerce aceptadas que resultaron fraudulentas.
- % de órdenes de eCommerce que generaron contracargos: Indica el porcentaje de órdenes de eCommerce por las que recibiste contracargos por fraude en los últimos 12 meses.

Imagen 10:

- % de órdenes revisadas manualmente: Indica el porcentaje de órdenes de eCommerce que analizas manualmente en búsqueda de fraude.
- % de órdenes que luego fueron rechazadas: De las órdenes revisadas manualmente por tu organización, indica el porcentaje que rechazas (cancelas) por sospecha de fraude.

Imagen 11: % de órdenes revisadas manualmente que son rechazadas: De las órdenes revisadas manualmente por tu organización, indica el porcentaje que rechazas (cancelas) por sospecha de fraude.

Imagen 12: Distribución del gasto en prevención de fraude en eCommerce: Indica el porcentaje del gasto anual actual en prevención de fraude en eCommerce que tienes en cada una de las siguientes áreas.

Imagen 13: El rol de la revisión manual en los futuros planes estratégicos contra el fraude: ¿De qué manera se incluye la revisión manual en los futuros planes estratégicos de prevención de fraude de tu organización?

Imagen 14: ¿Qué tan preparada dirías que está tu organización para la PSD2?

Imagen 15:

- Preparación para la PSD2: ¿Qué tan preparada dirías que está tu organización para la PSD2?
- % que consideraba que la PSD2 tendría un gran impacto en su organización: ¿Qué tipo de impacto crees que tendrá la PSD2 en tu organización? [Opción de respuesta: Un gran impacto].

Imágenes 16 y 17: ¿Cuál de los siguientes tipos de fraude has sufrido en tu organización?

Imagen 18: Indica el porcentaje de órdenes de eCommerce aprobadas en los últimos 12 meses que resultaron ser casos de fraude amigable o fraude por contracargos, es decir, cuando el cliente solicitó un contracargo a su banco luego de haber recibido el producto o servicio comprado.

Imagen 19: ¿Qué estrategia formal para combatir el fraude amigable / fraude por contracargos describe a tu organización; es decir cuando un cliente le solicita un contracargo a su banco luego de haber comprado el producto o servicio?

Imagen 20:

- % de organizaciones con herramientas para monitorear el fraude por robo de cuenta: ¿Cuentas con herramientas instaladas para monitorear el fraude de robo de cuenta durante el proceso de creación de cuenta y de inicio de sesión del cliente? [Opción de respuesta: Sí].
- % de organizaciones afectadas por el fraude de robo de cuenta: ¿Cuál de los siguientes tipos de fraude has sufrido en tu organización?

Imagen 21:

- La incidencia de los desafíos de la administración de fraude: ¿Cuál de los siguientes desafíos relacionados con la administración de fraudes en eCommerce tuvo tu organización en los últimos 12 meses?
- La gravedad de los desafíos de prevención de fraude: ¿Qué tan desafiante dirías que es cada una de las siguientes opciones para la administración de tu organización? [La escala va de extremadamente desafiante a para nada desafiante].

Imagen 22: ¿Cuál de las siguientes prácticas de administración de fraude dirías que es la más importante a la hora de evaluar las prioridades de la administración de fraude?

Imágenes 23 y 24: Indica las herramientas de prevención de fraude que tu organización usa actualmente.

Imágenes 25 y 26:

- Herramientas actualmente en uso: Indica las herramientas de prevención de fraude que tu organización usa actualmente.
- Herramientas que las organizaciones planean implementar en un futuro: Indicaste que tu organización actualmente no usa ninguna de las herramientas de detección de fraude a continuación. ¿Qué herramientas planea implementar tu organización en un futuro?
- Efectividad de las herramientas: Y bien, ¿qué tan efectiva es cada una de las siguientes herramientas para detectar el fraude de pagos en eCommerce? [La escala va de extremadamente efectiva a para nada efectiva].

Para más información,
visita: cybersource.com

cybersource
A Visa Solution