Expertos en equilibrio

Lo que se necesita para ser líder en prevención de fraude

Reporte global de fraude en *eCommerce* 2019

CyberSource®
A Visa Solution

Página de contenidos

Resumen ejecutivo 3

La prevención de fraude en un mundo dinámico 5

Liderar con equilibrio 7

Los expertos en equilibrio 10

La eficacia de las herramientas de evaluación de órdenes 23

Indicadores de desempeño (KPI) 31

Sobre este reporte 35

Significado de los colores

En este reporte, algunos resultados se presentan en amarillo y otros, en azul.

Se presentan en amarillo los que corresponden a organizaciones que dan la misma importancia a maximizar los ingresos, minimizar las pérdidas por fraude y minimizar los costos operacionales. Y en azul, a aquellas que no.

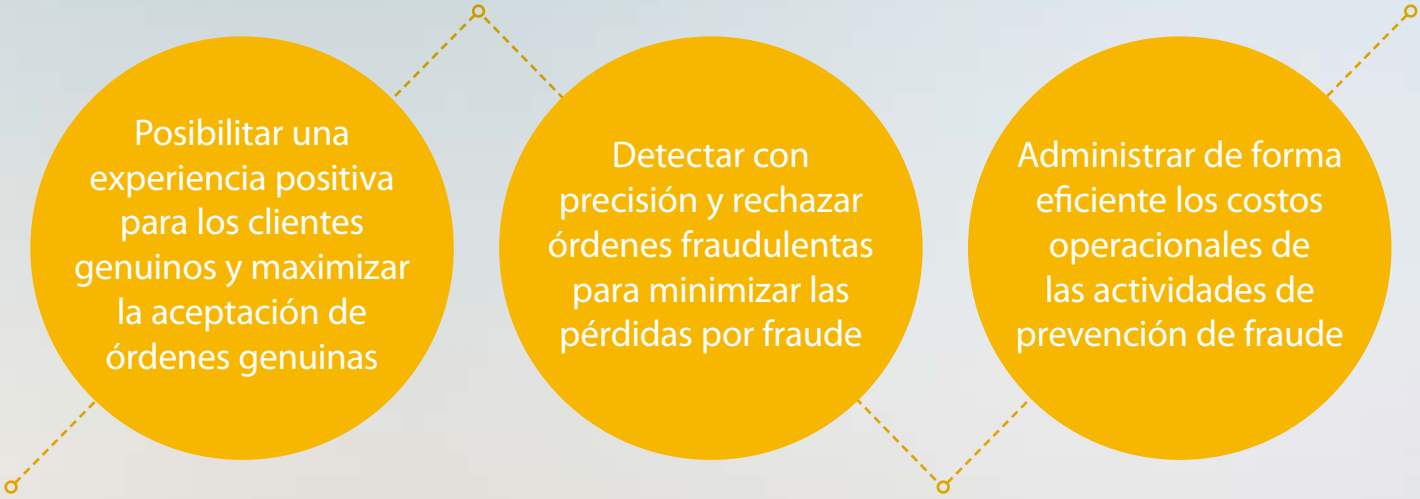
Preste especial atención a los resultados marcados con una estrella verde. La estrella indica resultados estadísticamente significativos y algunas de las perspectivas más valiosas que incluye este reporte.

En este reporte, el término *«eCommerce»* incluye reservas y órdenes de productos y servicios realizadas *online*, utilizando cualquier dispositivo (*mCommerce* se incluye en *eCommerce*).

Resumen ejecutivo

Este reporte global[1] analiza las opiniones de casi 2800 especialistas en prevención de fraude que representan a organizaciones de 34 países.

Ofrece perspectivas y consejos claves y analiza las características de esas organizaciones que prestan igual atención a las tres áreas de la ley de equilibrio en prevención de fraude:



Cuando comparamos a quienes prestan igual atención a los tres aspectos —los que parecen haber dominado el equilibrio— con los que no, vemos diferencias estadísticamente significativas que posicionan a los primeros como **líderes.**

[1] Todos los participantes son responsables por tomar o influenciar decisiones relacionadas a la prevención de fraude o están directamente involucrados en los procesos de prevención de fraude. Representan organizaciones de todos los tamaños, de cinco rubros y 34 países en EUA y Canadá, América Latina, Europa, Medio Oriente, África y Asia del Pacífico. Para más detalles sobre la encuesta, consulte el final del reporte.

La encuesta revela una cantidad importante de diferencias entre los que dan prioridad al equilibrio, un grupo al que denominamos **líderes**, y los que no, el resto de los participantes.

Solo el 18% de los participantes están categorizados como **líderes**. Los líderes:

1

Tienen índices de contracargos **cuatro veces más bajos** que los otros participantes[2]

LÍDERES	0.1%
OTROS	0.4%

2

Son **2.5 veces más proclives** a considerar los índices de fraude en *eCommerce* como extremadamente importante para la estrategia comercial de sus organizaciones

LÍDERES	83%
OTROS	35%

3

Enfrentan mejor el desafío de responder a los ataques de fraude emergentes

LÍDERES	38%
OTROS	46%

4

Tienen una gama significativamente mayor de capacidades que les brinda agilidad para responder al dinámico panorama en el que operan

5

Tienen mayor capacidad para utilizar la información de manera más eficaz

LÍDERES	67%
OTROS	39%

6

Realizan menos revisión manual…

LÍDERES	82%
OTROS	90%

…e invierten menos en esta área

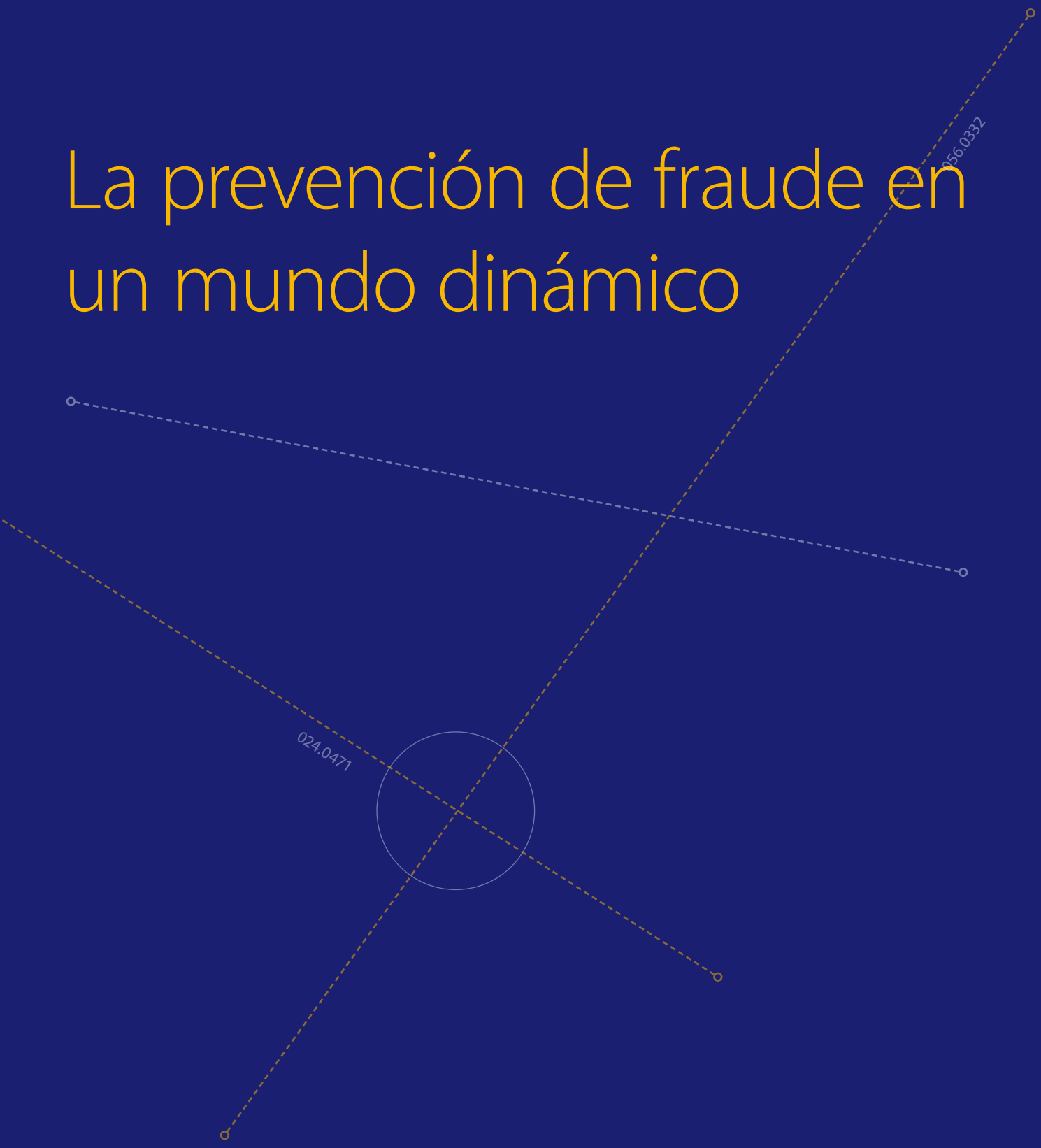
El porcentaje del presupuesto anual para prevención de fraude en *eCommerce* que los líderes destinan al pago del personal de revisión manual es menor

LÍDERES	37%
OTROS	42%

En este reporte exploraremos estas diferencias y ofreceremos perspectivas y consejos para ayudar a que su organización avance con sus propias estrategias y prácticas de prevención de fraude

[2] Resultados informados por los propios participantes.

La prevención de fraude en un mundo dinámico



Cada vez más, son los expertos en comercio digital quienes establecen las expectativas de los consumidores. Por ejemplo:

Minoristas que ofrecen la opción de retirar el producto de la tienda dentro de la primera hora de realizada la compra;

Restaurantes que les permiten a sus clientes realizar órdenes desde sus hogares a través de un dispositivo activado por voz;

Compañías de taxis cuyos servicios pueden ser solicitados y abonados directamente a través de la aplicación de chat que utilizan los usuarios.

No son solo las organizaciones nativas digitales las que están subiendo aún más la vara. Las empresas también están mejorando en brindarles a sus clientes experiencias convenientes, personalizadas e integradas que cruzan las fronteras digitales y físicas.

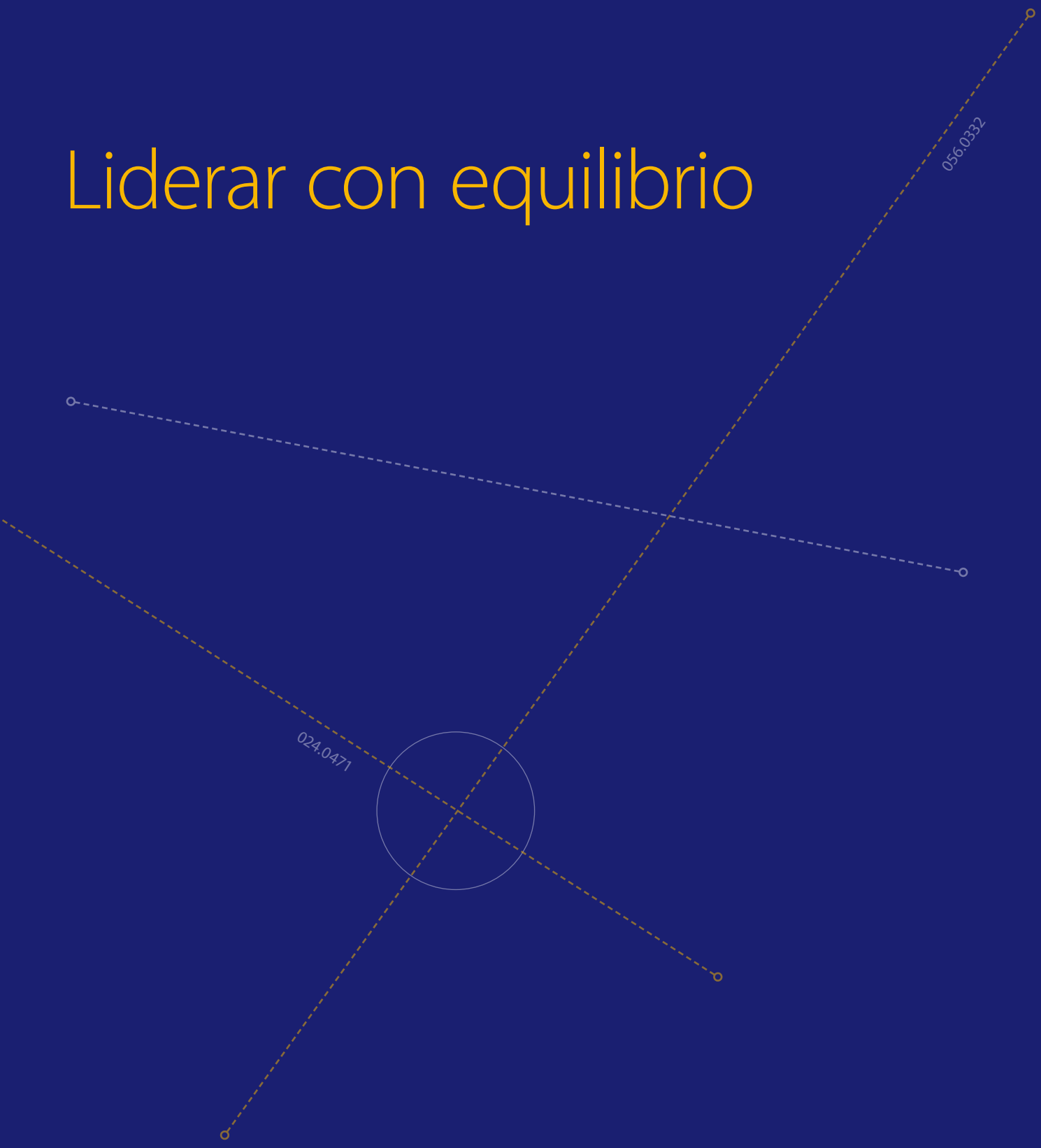
Prevención de fraude centrada en el consumidor

Tener reglas y controles estrictos de prevención de fraude podría significar que las órdenes de clientes genuinos sean marcadas como fraudulentas, generando así una experiencia negativa para ese cliente. Además de la pérdida de ingresos de esa venta en particular, existe una preocupación mayor: la de perder esos clientes para siempre, junto con los ingresos potenciales que podrían generar.

También existe la posibilidad de que esa experiencia negativa se transmita de boca en boca, o que el cliente la comente en ámbitos sociales en los que interactúan varios clientes reales o potenciales, afectando así la reputación de una marca.

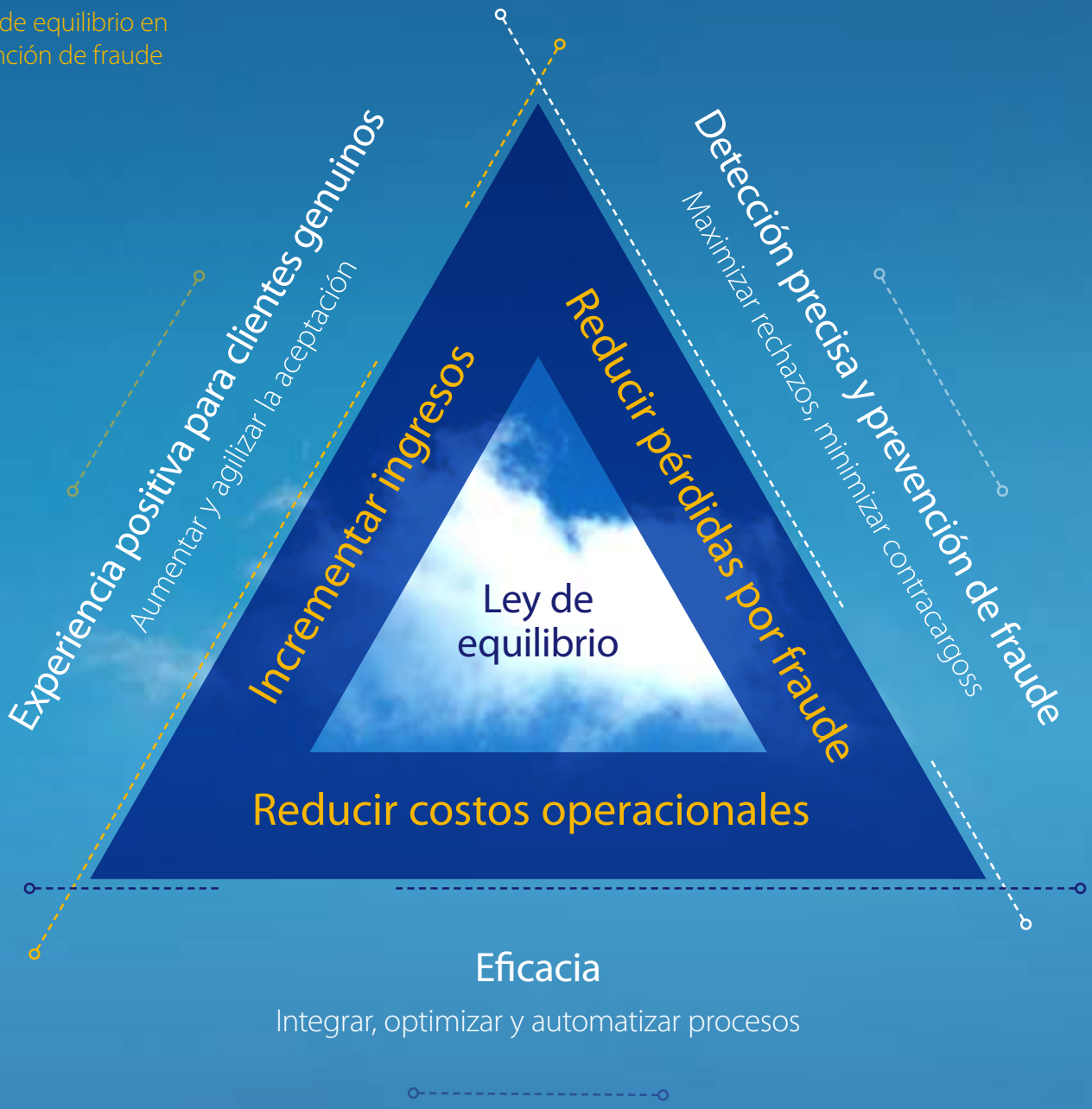
Una estrategia eficaz de prevención de fraude debería centrarse en el cliente, teniendo como objetivo principal garantizar la aceptación automática de los clientes genuinos.

Liderar con equilibrio



La prevención eficaz de fraude requiere un equilibrio cuidadoso de tres dimensiones independientes:

Figura 1.
La ley de equilibrio en prevención de fraude



Las conductas de clientes y defraudadores se adaptan continuamente a los desarrollos tecnológicos, culturales y económicos. Los objetivos y presupuestos de prevención de fraude cambian con la evolución de las realidades comerciales. Este panorama dinámico exige recalibrar y optimizar las reglas y procesos para mantener el equilibrio ideal.

Calibrar, revisar y volver a calibrar

El punto óptimo de equilibrio es único para cada actividad. Por eso, cuando se trata de prevención de fraude, un enfoque de tipo «configúrelo y olvídese» no dará los mejores resultados. Por ejemplo, no le permitirá tratar los SKU específicos en forma diferente, o adaptarse a eventos breves que provocan cambios temporales en el comportamiento del cliente (como sucede durante la temporada alta o de promoción).

Elija un enfoque que le permita flexibilidad en la optimización y sofisticación en su respuesta a las tendencias dinámicas de fraude. Para tener resultados óptimos, una solución de prevención de fraude debería tener capacidad para:

- Utilizar el *machine learning* para mantenerse actualizado sobre los principales cambios en tendencias de fraude mediante la detección de patrones en grandes conjuntos de datos;
- Complementar con reglas de configuración flexible, para control de precisión y adaptabilidad a factores influyentes específicos
- Aprovechar las técnicas avanzadas del *machine learning* para sugerir reglas, basadas en sus propios datos históricos, que lo ayuden a alcanzar sus objetivos de prevención de fraude.

> “ El índice de aceptación de transacciones y el índice de fraude son contradictorios.
>
> Si somos demasiado estrictos con nuestras reglas de prevención de fraude, se reduciría el índice de aceptación y eso puede afectar la experiencia del cliente, pero el índice de fraude sería más bajo. Si somos demasiado laxos con las reglas de prevención de fraude y aceptamos algunas transacciones riesgosas, entonces la experiencia del cliente podría mejorar de manera obvia. El fin último es lograr un equilibrio dinámico entre la experiencia del cliente, el índice de aceptación de transacciones y el índice de fraude.[3]
>
> **Función:** Toma de decisiones en *eCommerce* | **Segmento:** Viajes | **País:** China

[3] Esta cita se tradujo del chino al inglés, originalmente.

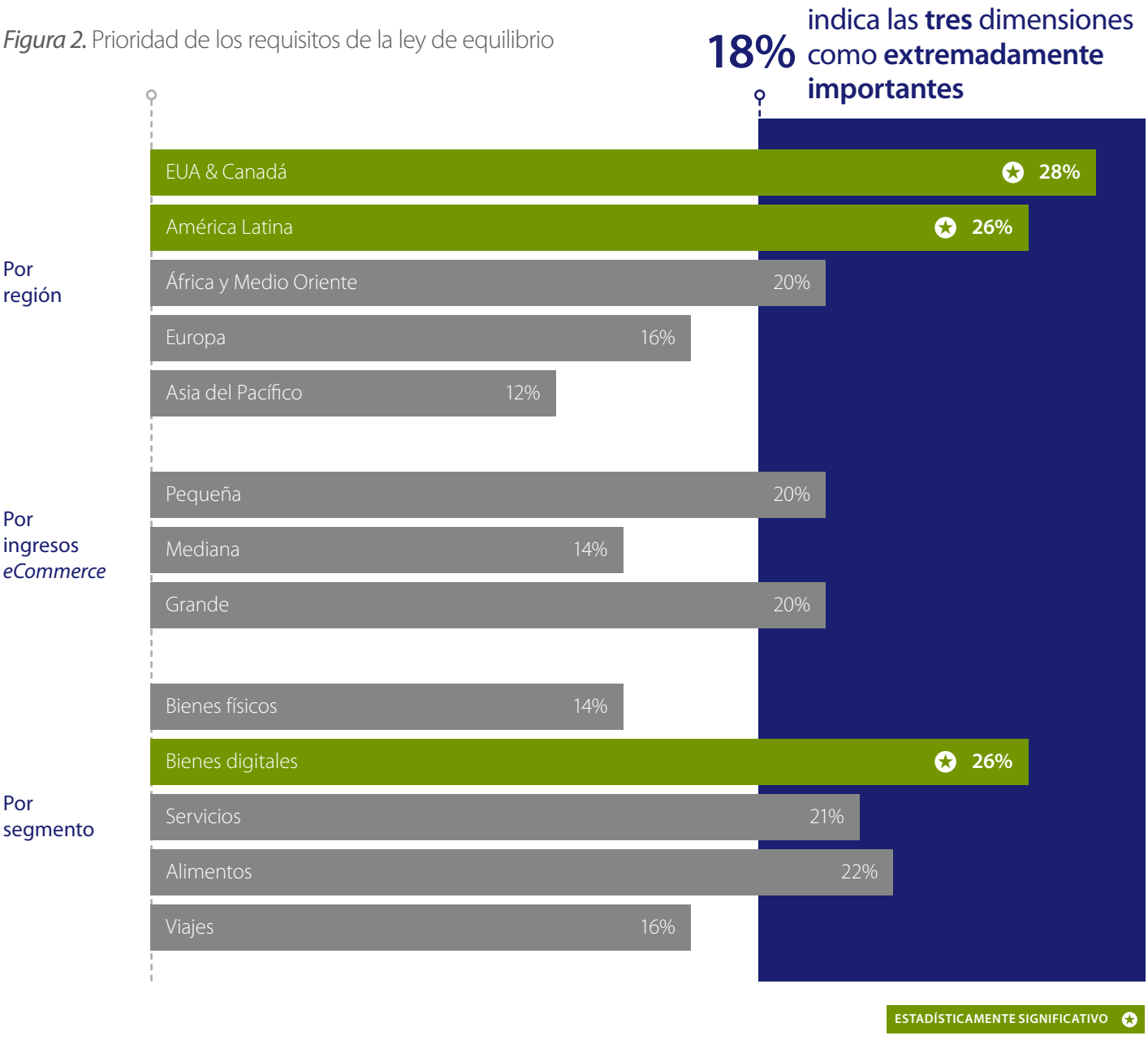
Los expertos en equilibrio

Cuando se les pidió a los participantes que evaluaran la importancia de cada dimensión de la ley de equilibrio, solamente el 18% de ellos —menos del 20% del total— indicó estas tres como las de mayor prioridad.

Las organizaciones de EUA y Canadá, las de América Latina y las que ofrecen bienes digitales son las más proclives a priorizar el equilibrio.

Cuando comparamos las organizaciones que prestan igual atención a los tres aspectos de la ley de equilibrio —las que parecen haberlo dominado— con las que no, vemos diferencias significativas en seis áreas principales que indican a las primeras como líderes.

Figura 2. Prioridad de los requisitos de la ley de equilibrio



Base 1970 (No incluye el sureste de Asia y Australia)
Pregunta: ¿Qué tan importante es cada una de las siguientes para su organización al momento de diseñar las estrategias de prevención de fraude? Mejorar la experiencia del cliente, reducir el fraude y los contracargos, minimizar los costos operacionales relacionados con fraude
Opciones de respuestas: Extremadamente importante, muy importante, poco importante, no muy importante, nada importante.

Seis características de los expertos en equilibrio

La encuesta revela varias diferencias estadísticamente significativas entre los que dan prioridad al equilibrio y los que no.

Los expertos en equilibrio:

1. Tienen un índice promedio de contracargos **cuatro veces más bajo** que el de otros participantes
2. Son **2.5 veces más propensos** a considerar la prevención de fraude en *eCommerce* como extremadamente importante para la estrategia comercial de su organización
3. Enfrentan mejor los ataques emergentes de fraude
4. Tienen una variedad significativamente mayor de capacidades que les brinda agilidad para responder al panorama dinámico en el que operan
5. Utilizan la información de manera más eficaz
6. Realizan menos revisiones manuales e invierten menos tiempo en esta área

1 Índices de contracargo más bajos

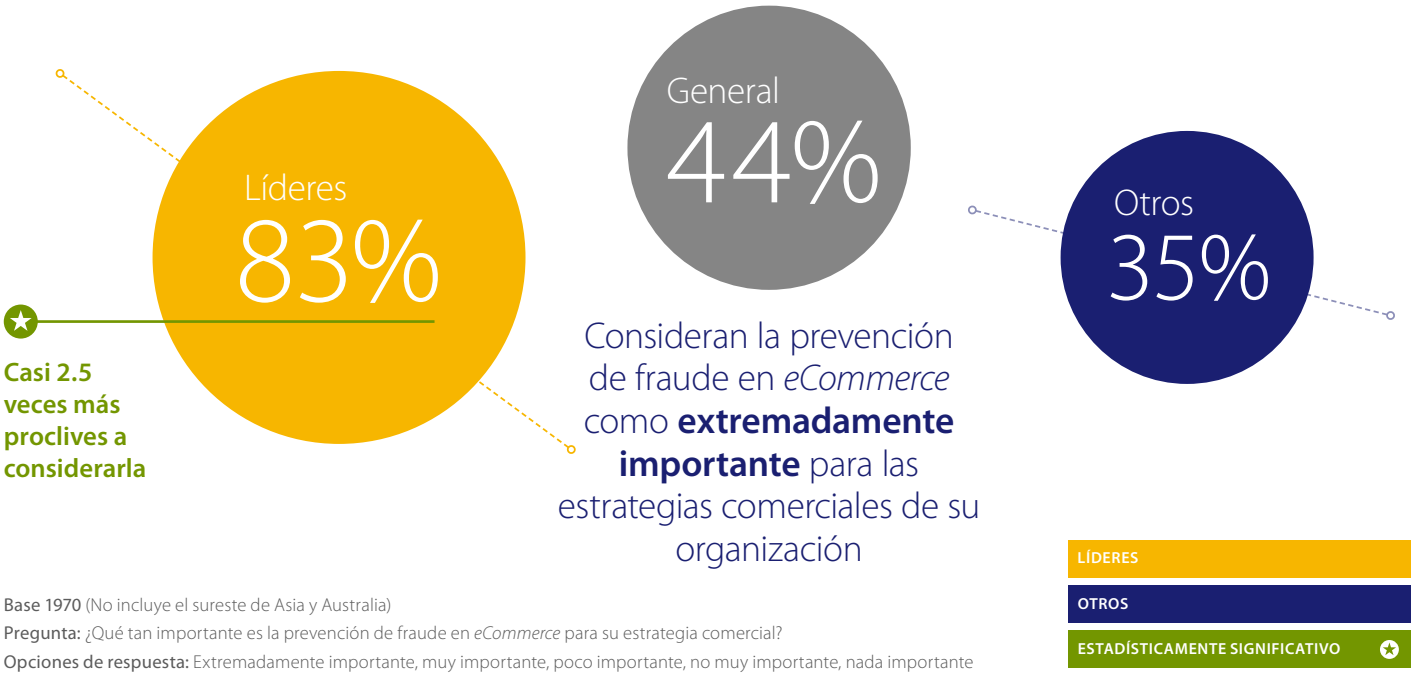
Los líderes tienen un índice promedio de contracargos por fraude cuatro veces más bajo que el de los demás participantes (0.1% vs. 0.4%). Esto demuestra que es posible ir tras mejorar la experiencia del cliente y, al mismo tiempo, reducir pérdidas por fraude.[4]

2 Más posibilidades de considerar la prevención de fraude como estratégica

Los líderes fueron casi 2.5 veces más proclives que el resto a considerar que la prevención de fraude en *eCommerce* es extremadamente importante para la estrategia comercial de su organización.

Cuando las organizaciones valoran la importancia que la prevención de fraude tiene para el éxito de su actividad, aparentemente, tienen mejores resultados.

Figura 3. Importancia estratégica de la prevención de fraude



Base 1970 (No incluye el sureste de Asia y Australia)
Pregunta: ¿Qué tan importante es la prevención de fraude en *eCommerce* para su estrategia comercial?
Opciones de respuesta: Extremadamente importante, muy importante, poco importante, no muy importante, nada importante

> [El fraude en *eCommerce*] es extremadamente importante para nuestras actividades…
>
> Diría que hace cuatro años, o incluso cinco, porque las cantidades no eran lo suficientemente importantes para que interviniéramos e hiciéramos algo, simplemente considerábamos ese riesgo como aceptable. Ok, está bien. Perdemos un poco de dinero, pero no es nada para preocuparse. Luego vimos que se cuadruplicó durante el año siguiente, y al siguiente nuevamente se duplicó. Así es que, al tercer año, perdíamos grandes cantidades y, entonces… ¡Bueno! Necesitamos considerar esto en serio y hacer algo al respecto.
>
> **Función:** Toma de decisiones | **Segmento:** Viajes | **País:** Canadá

[4] Los resultados son informados por los propios participantes.

3 Más facilidad para enfrentar los ataques emergentes de fraude

En la actualidad, el desafío más grande en administración de fraude es responder a los ataques emergentes de fraude. Esto tiene sentido dada la creciente sofisticación de los defraudadores y su rapidez para aprovechar nuevos puntos vulnerables.

Sin embargo, los líderes enfrentan este desafío —junto con casi cualquier otro desafío en prevención de fraude— con más facilidad que los demás participantes.

Figura 4. Desafíos en prevención de fraude
(% de los que experimentaron el desafío el año anterior)

Base 1410 (No incluye el sureste de Asia y Australia).
Pregunta: ¿Cuál de los siguientes desafíos relacionados con la prevención de fraude en *eCommerce*, si los hubo, experimentó durante los últimos 12 meses?

Manténgase al día con la evolución del fraude

Las técnicas avanzadas del *machine learning*, que aprovechan la magnitud y profundidad de los datos, pueden facilitar considerablemente el desafío de identificar y responder a los ataques emergentes.

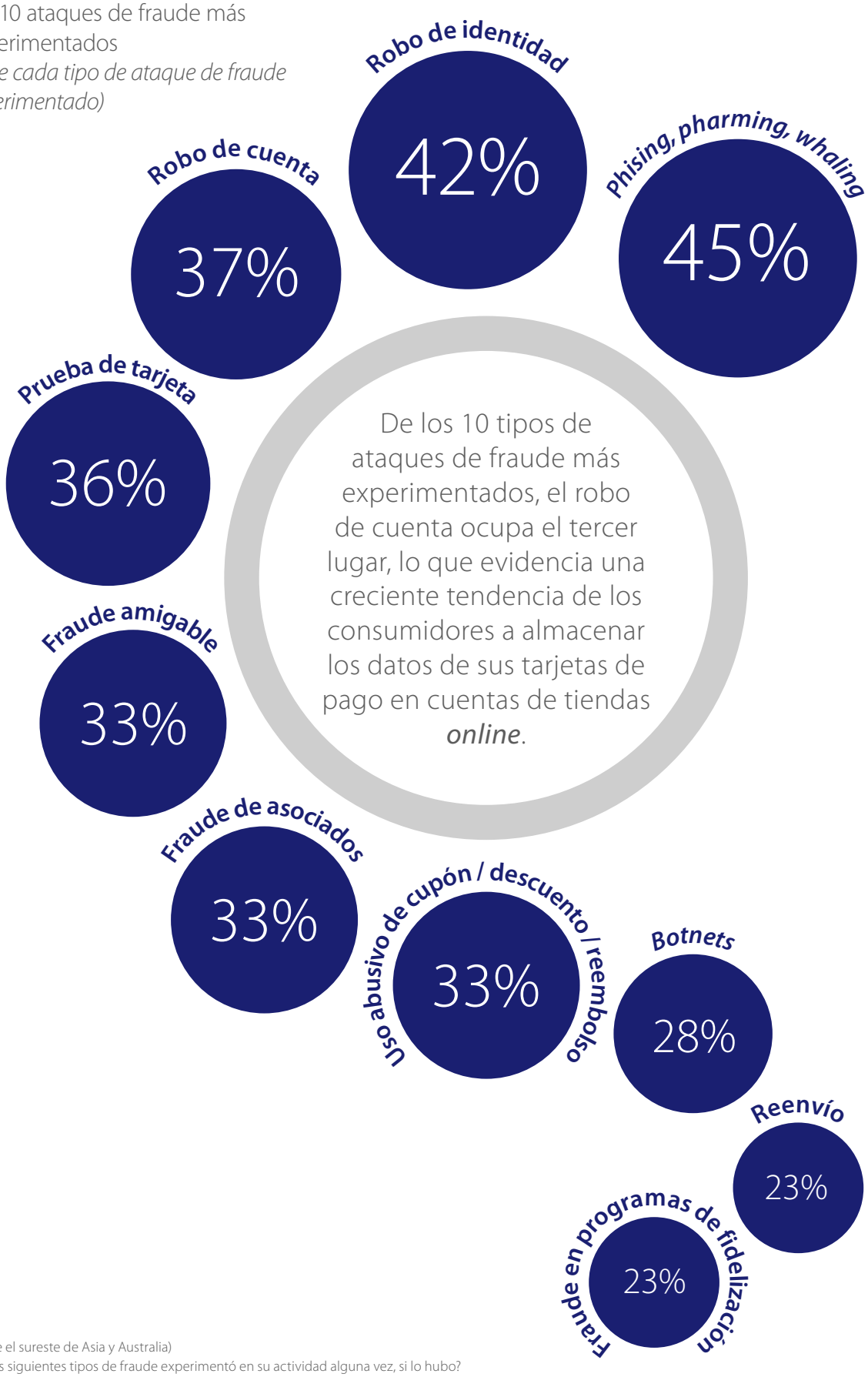
Una solución de prevención de fraude sofisticada que combina modelos estáticos y de autoaprendizaje analizará y procesará datos nuevos, actualizando de forma autónoma sus modelos para reflejar las últimas tendencias, permitiéndole concentrar sus esfuerzos en garantizar que las órdenes de sus clientes genuinos no sean rechazadas.

Los **modelos estáticos** aprenden a identificar el fraude en un momento determinado analizando millones de transacciones. Son muy eficaces para identificar patrones históricos de fraude.

Los **modelos de autoaprendizaje** incorporan datos de las nuevas transacciones para reconocer y adaptarse a los patrones de fraude en constante evolución. Los modelos de autoaprendizaje resultan muy eficaces para identificar las últimas tácticas de fraude.

Tenga en cuenta el robo de cuenta *(account takeover)*

Figura 5. Los 10 ataques de fraude más experimentados
(% de cada tipo de ataque de fraude experimentado)



De los 10 tipos de ataques de fraude más experimentados, el robo de cuenta ocupa el tercer lugar, lo que evidencia una creciente tendencia de los consumidores a almacenar los datos de sus tarjetas de pago en cuentas de tiendas *online*.

Base 1970 (No incluye el sureste de Asia y Australia)
Pregunta: ¿Cuál de los siguientes tipos de fraude experimentó en su actividad alguna vez, si lo hubo?

Figura 6. Se anticipa un incremento en el robo de cuentas

El **59%** de los participantes anticipa un aumento en los ataques de robo de cuenta en los próximos 12 meses.

ESTADÍSTICAMENTE SIGNIFICATIVO

Las grandes organizaciones y las del segmento de los bienes digitales son las más proclives a anticipar un aumento en el robo de cuentas en el próximo año

Cómo evitar el robo de cuenta

El fraude por robo de cuenta puede evitarse mediante la detección de actividad sospechosa en cuenta antes de que se la utilice para intentar realizar una compra.

Para ello, una solución para la prevención de fraude debe tener la capacidad para:

- Autenticar o bloquear las acciones de una cuenta basándose en el monitoreo de creación de cuenta, accesos a la misma y actualizaciones
- Considerar los datos relacionados con nombres de usuario, contraseñas, direcciones y dispositivos utilizados
- Considerar cruzamiento de datos entre comercios
- Utilizar los resultados de monitoreo de cuentas para informar reglas de prevención de fraude para intentos de compras

Base 1410 (No incluye el sureste de Asia y Australia)
Pregunta: Durante los próximos 12 meses, considera que el robo de cuenta...
Opciones de respuestas: se incrementará mucho; se incrementará un poco; permanecerá más o menos igual; disminuirá un poco; disminuirá mucho.

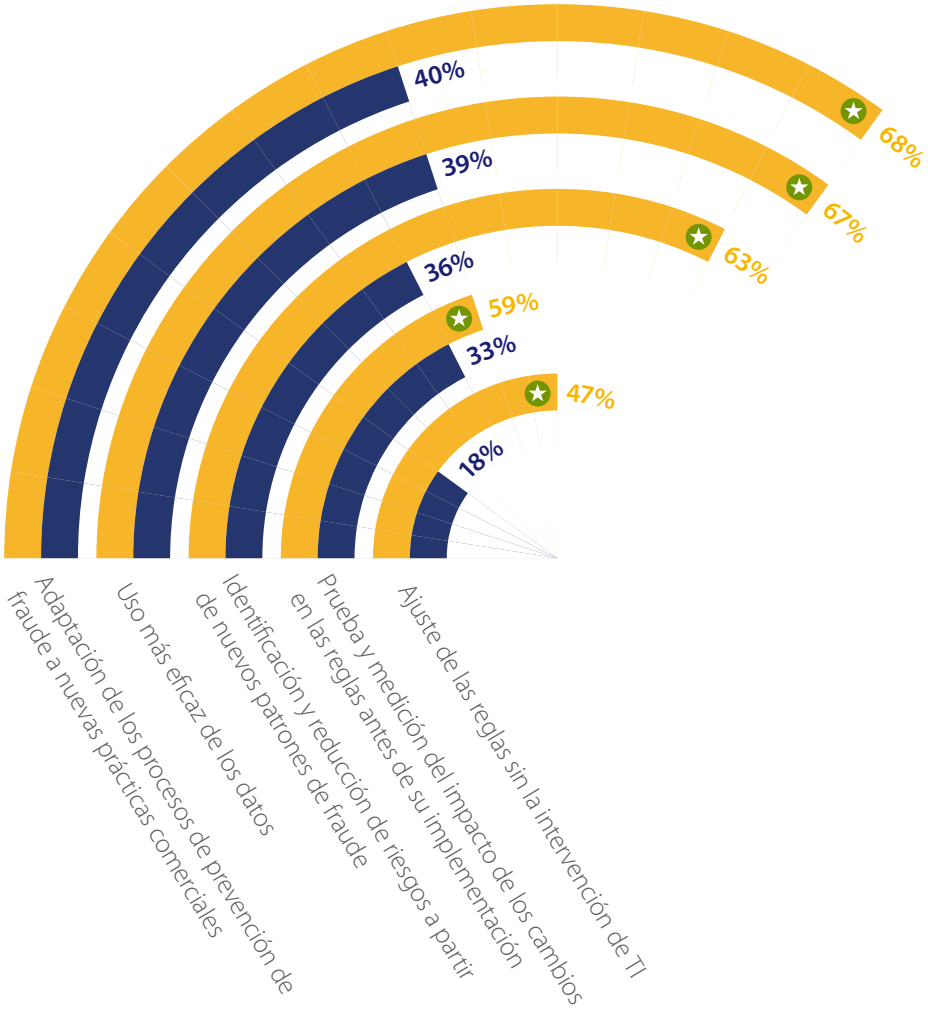
4 Liderazgo en capacidades de prevención de fraude

Es más probable que los líderes tengan una gama de capacidades en prevención de fraude que les brinde agilidad para responder al panorama dinámico en el que operan.

Entre estas capacidades, está la de adaptarse a los procesos y reglas de prevención de fraude, identificar y mitigar los riesgos de nuevos patrones de este delito, y utilizar los datos de manera eficaz para prevenirlo.

Muchos líderes están muy de acuerdo en que sus organizaciones logran las siguientes cinco cosas:

Figura 7. Capacidades importantes para la prevención de fraude



Base 1970 (No incluye el sureste de Asia y Australia)

Pregunta: Indique en qué medida está de acuerdo o en desacuerdo con cada una de las siguientes afirmaciones sobre la forma en que su empresa combate el fraude en *eCommerce*.

Opciones de respuesta: Muy de acuerdo; algo de acuerdo; algo en desacuerdo; muy en desacuerdo

La agilidad brinda estabilidad

Reunir suficientes datos sobre contracargos para evaluar el impacto de los cambios de reglas puede tomar semanas. Para cuando los tenga, las tendencias de fraude pueden haber cambiado totalmente o haber evolucionado aún más. La flexibilidad para optimizar las reglas ayuda a brindar un mayor control sobre las estrategias de prevención de fraude.

Una solución de prevención de fraude es ágil cuando:

- Puede realizar análisis «what if» para probar cualquier regla en los datos de transacciones históricas del comercio
- Puede evaluar el posible impacto de las reglas propuestas antes de implementarlas en un entorno real

5 Uso de datos más eficaz

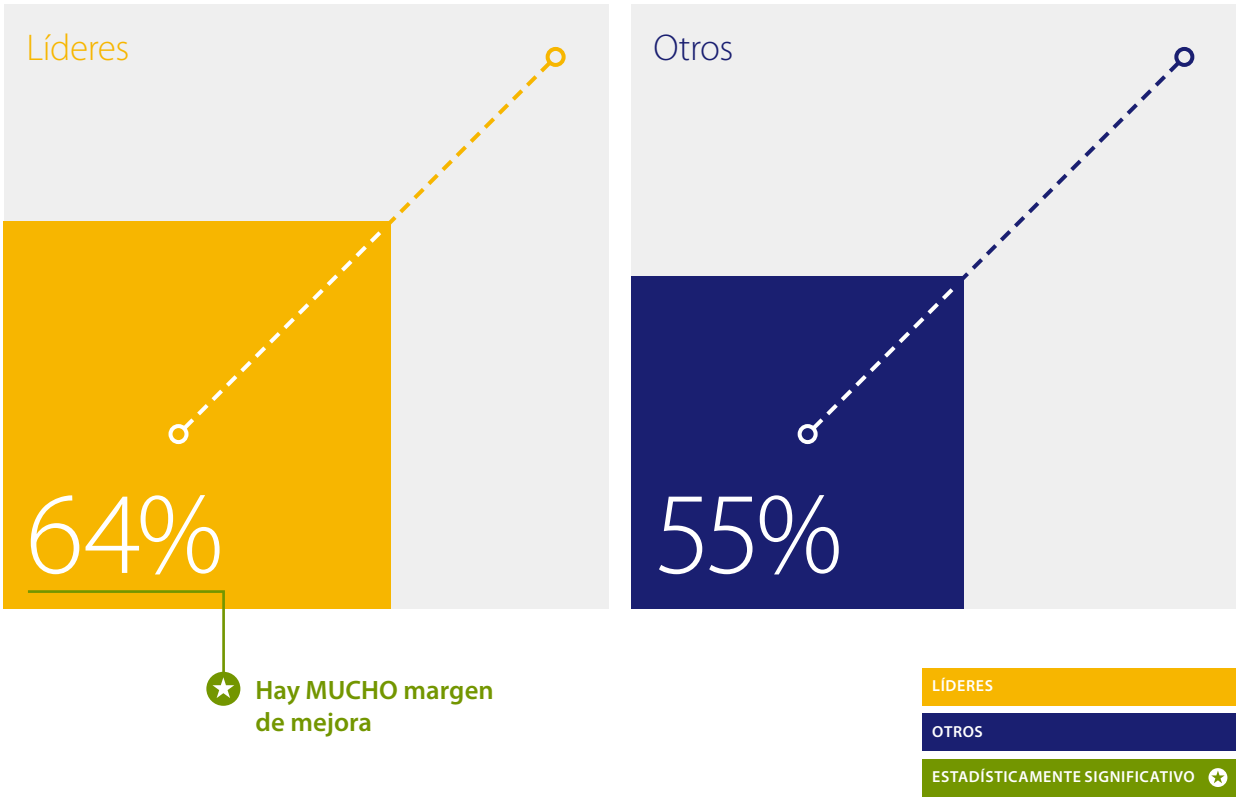
Los líderes tienen mayor capacidad para hacer uso de los datos de forma más eficaz para prevenir el fraude (**67% vs. 39%**, como se muestra en la *figura 7)*.

Cuando se les preguntó cuánto margen de mejora ven en el uso de los datos de su organización para prevenir el fraude, casi dos tercios de los líderes (64%) respondieron que hay mucho margen de mejora, en comparación con poco más de la mitad (55%) de los otros participantes.

Esto sugiere que cuanto más eficaces son las organizaciones en el uso de los datos, más ventajas ven y desean aprovechar esas ventajas aún más.

Cada vez más líderes creen que hay margen para mejoras cuando se trata del uso de datos para prevenir fraude.

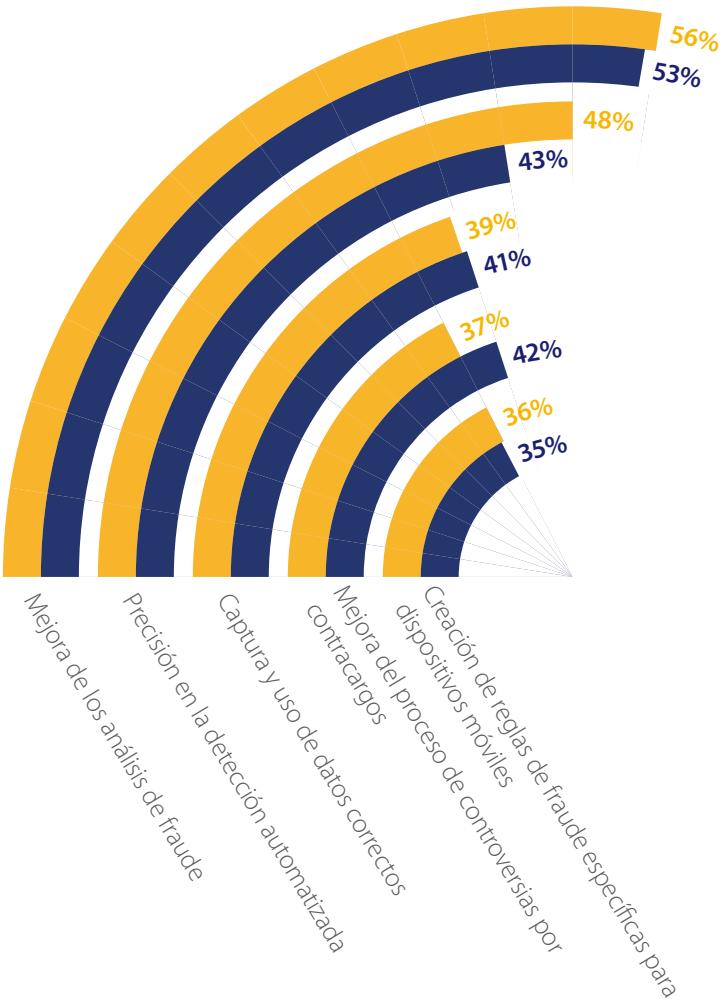
Figura 8. Margen de mejora en el uso de datos para prevención de fraude



Base 1410 (No incluye el sureste de Asia y Australia)
Pregunta: ¿Qué margen de mejora ve en la forma en que su organización debería utilizar los datos para prevenir el fraude?
Opciones de respuesta: Mucho; Poco; Ninguno

Cuando se les solicitó que indicaran cuáles de las ocho opciones eran áreas de mejoras para su organización durante el siguiente año, tanto los líderes como los demás seleccionaron, entre sus cinco principales, tres opciones centradas en datos.

Figura 9. Principales cinco áreas de mejoras para el año próximo
(% de los que seleccionaron la opción)



Base 1410 (No incluye el sureste de Asia y Australia)
Pregunta: Pensando en los próximos 12 meses, ¿cuáles de las siguientes, si las hay, son áreas de mejoras para su organización?
Opciones de respuesta: Precisión en la detección automatizada, optimización de las tareas de revisión manual y del flujo de trabajo, mejora de los análisis de fraude, creación de reglas de fraude específicas para dispositivos móviles, mejor prevención de fraude omnicanal, mejora del proceso de controversias por contracargos, tercerización de partes de la operación de revisión/evaluación, captura y uso de los datos correctos, otros.

En las entrevistas, muchos administradores de fraude reconocieron que las herramientas y estrategias de prevención son útiles solamente si los datos que se les proporcionan son precisos y de calidad.

Las organizaciones grandes están buscando que las herramientas ayuden con el análisis y los informes sobre fuentes de datos ya existentes, mientras que las organizaciones medianas están más enfocadas en el acceso a más datos para complementar lo que ya tienen.

6 Menos probabilidad de realizar revisión manual

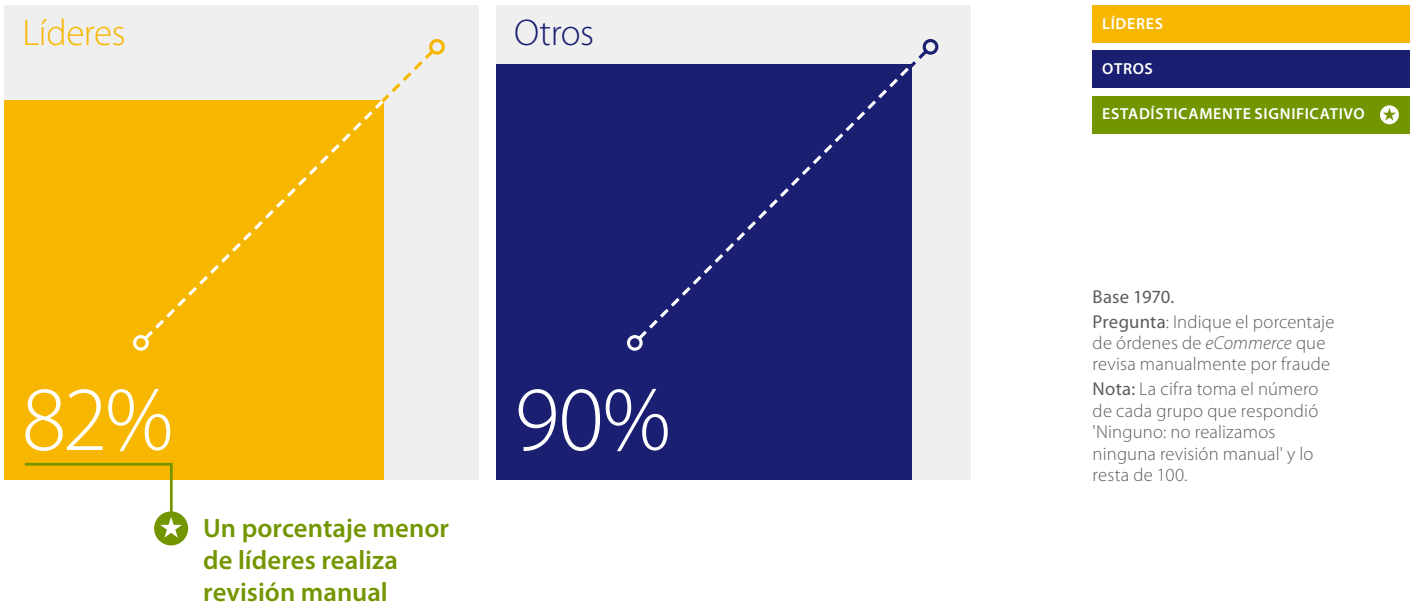
Casi todos los participantes revisan órdenes de forma manual, pero entre los líderes el número de los que realizan este tipo de revisión es menor (**82% vs. 90%**).

Los líderes también:

- Invierten en revisión una proporción más pequeña de su presupuesto de prevención de fraude en *eCommerce* —invirtiendo relativamente más en el uso eficaz de las herramientas de administración de fraude (figura 11)
- Invierten menos tiempo en promedio para revisar una orden (10 minutos vs. 15 que demora el resto)

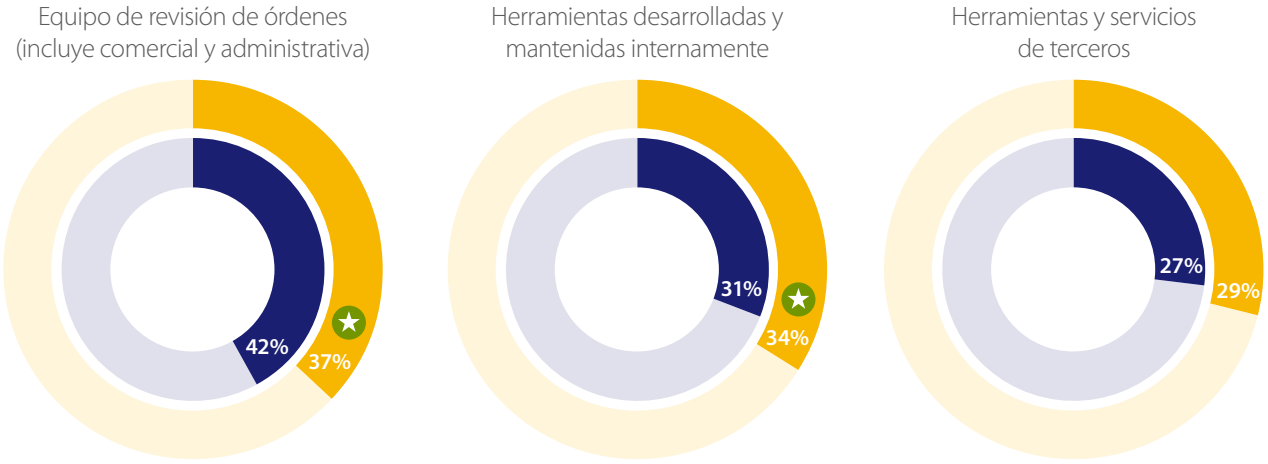
Todo esto sugiere que los líderes tienen un mayor enfoque en el análisis y la toma de decisiones automatizada.

Figura 10. La mayoría de los participantes realiza revisión manual
(% de órdenes que se revisan manualmente por sospecha de fraude)



Base 1970.
Pregunta: Indique el porcentaje de órdenes de *eCommerce* que revisa manualmente por fraude
Nota: La cifra toma el número de cada grupo que respondió 'Ninguno: no realizamos ninguna revisión manual' y lo resta de 100.

Figura 11. Detalle de presupuesto de prevención de fraude en *eCommerce*



Base 1970.
Pregunta: Indique el porcentaje de gasto anual actual en administración de fraude en *eCommerce* que le asigna a cada una de las siguientes áreas.

Cinco consejos para la automatización eficaz de la prevención de fraude

Depender en exceso de la revisión manual se torna menos viable a medida que crece la cantidad de órdenes en *eCommerce*.

Cuando considere automatizar más la toma de decisiones, siga estos consejos:

1

Utilice una variedad de herramientas de administración de fraude eficaz, que incluya servicios de validación, datos protegidos, datos de los diferentes comercios y rastreo del dispositivo de compra

2

Mantenga listas de positivos y negativos que le permitan aceptar sin inconvenientes las órdenes de clientes genuinos y rechazar automáticamente las de defraudadores ya conocidos

3

Cree reglas centradas en el cliente para evitar que los clientes genuinos se vean afectados —garantizando la continua revisión y calibración de estas reglas

4

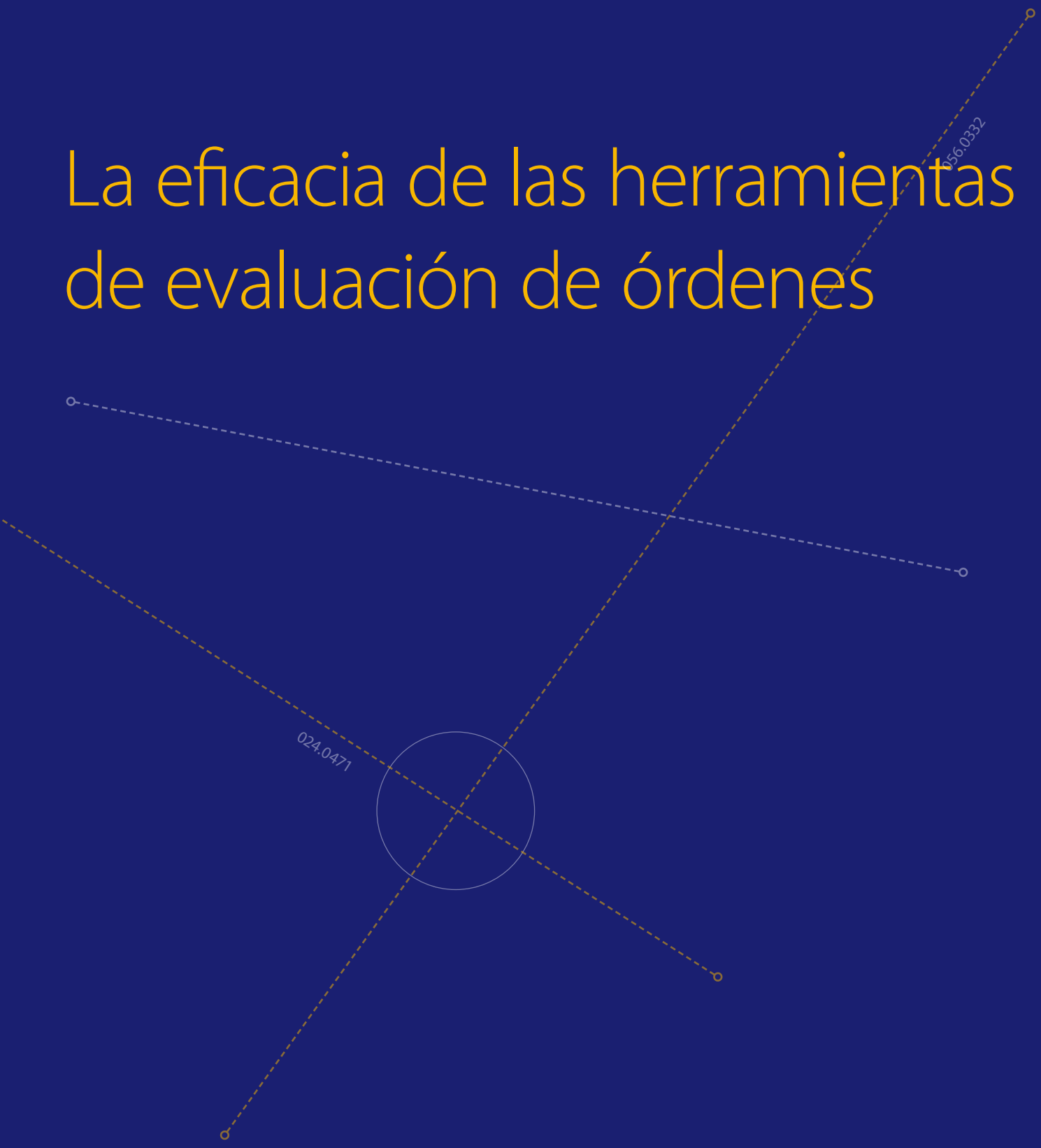
Optimice los procesos de revisión utilizando un sistema de gestión de casos eficaz, que reúna todas las herramientas que los revisores necesitan para perseguir buenos resultados

5

Asegúrese de que haya un ciclo de retroalimentación de manera que las perspectivas que surjan del equipo de revisión puedan ser incorporadas a sus reglas automatizadas y las listas de positivos/negativos

Cuando se les preguntó, los administradores de fraude contestaron que creen que el *machine learning* y la inteligencia artificial irán absorbiendo cada vez más el proceso de revisión manual, y que ésta evolucionará para enfocarse en los casos más complejos y difíciles.

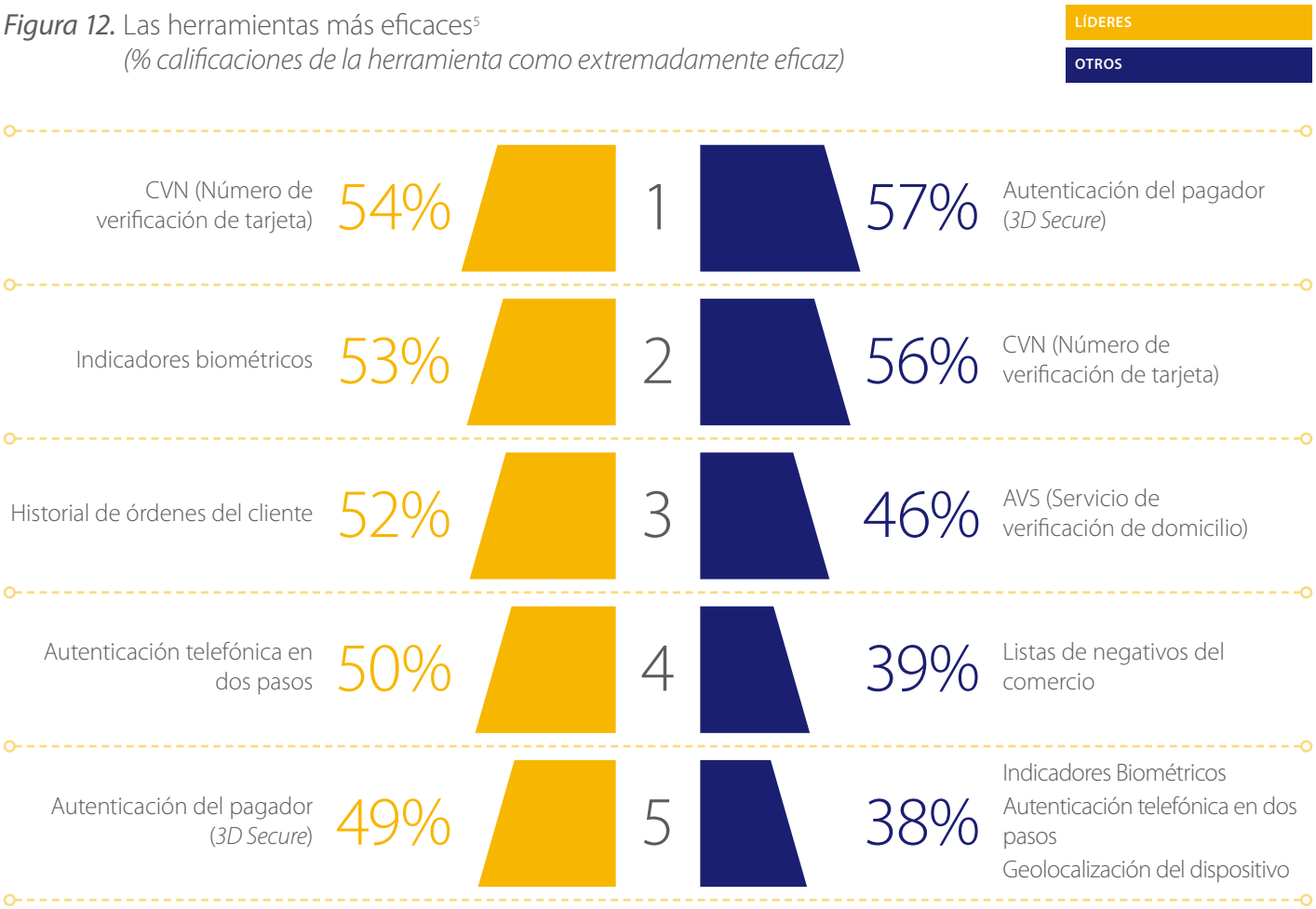
La eficacia de las herramientas de evaluación de órdenes



Todos los participantes usan la misma gama de herramientas para detectar el fraude, pero los líderes tienen una visión algo diferente sobre cuáles son las más eficaces. Hay media docena de herramientas cuya eficacia los líderes califican de manera muy diferente a los demás.

Esto indica que los líderes hacen un uso estratégico y práctico diferente de las herramientas clave, lo que puede explicar que logren posicionarse como líderes usando el mismo conjunto de herramientas.

Figura 12. Las herramientas más eficaces[5]
(% calificaciones de la herramienta como extremadamente eficaz)



Las herramientas más eficaces

Entre las herramientas calificadas como «extremadamente eficaces» por los participantes, las cinco más eficaces elegidas por los líderes son similares pero no idénticas a las elegidas por los demás.

Sistema de verificación de domicilio (AVS), listas de negativos del comercio y geolocalización del dispositivo móvil son relativamente menos importante para los líderes que para los otros participantes:

- AVS: en el puesto 18 en la lista para todos los líderes (38%); 3ro para otros (46%)
- Listas de negativos: en el puesto 10 para los líderes (44%), 4to para otros (39%)
- Geolocalización de dispositivo móvil: en el puesto 20 para los líderes (37%); 5to para todos los demás (38%)

Base 1147 (EUA, Canadá y Europa solamente)
Pregunta: A continuación, encontrará una serie de herramientas para detección de fraude. Para cada tipo, indique si su organización…
Opciones de respuesta: Actualmente utiliza esta herramienta, planea agregar esta herramienta el próximo año, o ninguna de las anteriores.

[5] Los porcentajes son aquellos en cada grupo que utiliza la herramienta y la califica como extremadamente eficaz.

Diferencias en la percepción de la eficacia

El valor atípico significativo en las cinco herramientas principales es el historial de órdenes del cliente. Esta es una de las herramientas para la detección de fraude de pagos de *eCommerce* que los líderes consideran mucho más eficaz que los otros participantes. Estas herramientas incluyen:

- Resultados de motores de búsqueda (líderes 43% vs. otros 18%)
- Monitoreo de *velocity* de la orden (45% vs. 23%)
- Modelos de *morphing* de identidad (43% vs. 21%)
- Historial de órdenes del cliente (52% vs. 33%)
- Modelos de puntuación de fraude: específicos por compañía (45% vs. 26%)
- Historial crediticio (46% vs. 28%)

Estas herramientas surgen de tres de las cuatro categorías de herramientas —servicios de validación, datos protegidos y fuentes de datos de diferentes comercios— indicando que los líderes comprenden el valor de utilizar diversas fuentes de datos para administrar el fraude de forma más eficaz.

Figura 13. Eficacia de las herramientas entre quienes las utilizan
(% calificaciones de la herramienta como extremadamente eficaz)

		Usuarios que priorizan el equilibrio	Usuarios que no priorizan el equilibrio
Servicios de validación	CVN (Número de verificación de tarjeta)	54%	56%
	Indicadores biométricos	53%	38%
	Autenticación telefónica en dos pasos	50%	38%
	Autenticación del pagador (*3D Secure*)	49%	57%
	Verificación de historial crediticio	46%	28%
	Resultados de motores de búsqueda	43%	18%
	Servicios de validación de domicilio postal	43%	29%
	Servicios pagos de registros públicos	42%	27%
	Verificación de email	41%	24%
	SafeKey	39%	22%
	Servicios de verificación de domicilio	38%	46%
	Indicadores geográficos / mapas	36%	24%
	Verificación de número telefónico / búsqueda inversa	36%	24%
Datos protegidos	Historial de órdenes del cliente	52%	33%
	Comportamiento de la orden *(velocity)*	45%	23%
	Listas de positivos / listas blancas	45%	34%
	Modelo de puntuación de fraude - específico por compañía	45%	26%
	Listas de negativos / listas negras	44%	39%
	Detección de proxy	43%	26%
	Comportamiento del cliente en el sitio /análisis de patrón	35%	27%
Datos de comercios múltiples	Comportamiento *(velocity)* de compra en comercios múltiples / modelos de *morphing* de identidad	43%	21%
	Listas de negativos compartidas – *hotlists* compartidas	38%	35%
Rastreo de dispositivo de compra	*Device fingerprint*	41%	30%
	Geolocalización – dispositivo móvil, tableta	37%	38%
	Geolocalización - laptop/desktop tradicional	36%	37%

Base 1147 (EUA, Canadá y Europa solamente)
Priorizan el equilibrio (n=219). No priorizan el equilibrio (n=928)
Pregunta: ¿Qué tan eficaces son cada una de las siguientes herramientas para la detección de fraude en *eCommerce*?

La insatisfacción con las herramientas impulsa la inversión

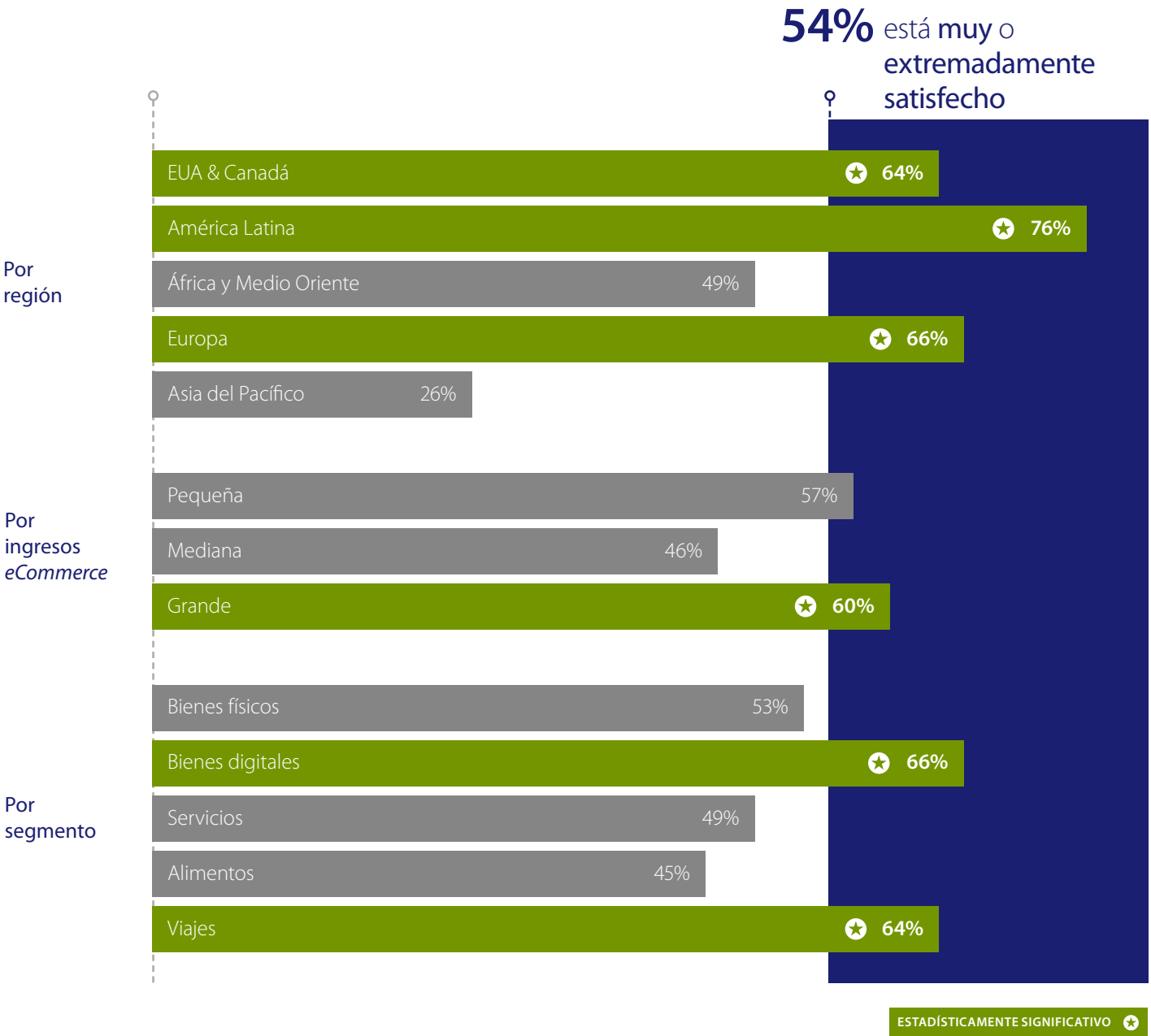
Un área en la que no hay diferencias significativas entre los líderes y los otros es la de satisfacción con su arsenal de herramientas de prevención de fraude.

En total, poco más de la mitad (54%) de los participantes están muy o extremadamente satisfechos con las herramientas disponibles (solo el 12% en el grupo está «extremadamente satisfecho»). Esto deja bastante margen para mejorar los niveles de satisfacción.

La relativa insatisfacción con las herramientas disponibles está impulsando un intento generalizado de los participantes de invertir en herramientas que no utilizan actualmente. Si ejecutan todos estos planes de inversión, entonces:

- Las cinco herramientas más utilizadas en la actualidad —CVN, historial de compras del cliente, verificación de email, *3D Secure* y listas internas de negativos— continuarán siendo las más utilizadas.

Figura 14. Satisfacción con las herramientas de prevención de fraude



Base 1710 (No incluye Asia del Pacífico)
Pregunta: ¿Qué tan satisfecho está con las herramientas de prevención de fraude de las que dispone?
Opciones de respuesta: Extremadamente satisfecho; Muy satisfecho; Poco satisfecho; Para nada satisfecho

Los participantes pertenecientes a organizaciones grandes señalaron como principal factor de insatisfacción la falta de una única solución que satisfaga sus necesidades, por lo que se ven obligados a integrar las mejores herramientas de cada clase para poder obtener una solución adecuada. Algunas organizaciones más pequeñas están muy satisfechas con derivar mayor parte de su administración de fraude a un tercero confiable. Otras consideran que la mayoría de las herramientas son caras: la inversión, con frecuencia, es mayor que las pérdidas por fraude que intentan reducir.

> “ En mi opinión, el desafío es que no hay una única herramienta que solucione todos los problemas.
>
> Entonces, lo que uno está haciendo constantemente es tener administradores de fraude en las organizaciones, esencialmente desarrollando su propia herramienta *Frankenstein* para prevención de fraude, en la que reúnen dos, tres o cuatro tipos diferentes de soluciones, apilándolas una sobre otra, para poder obtener el resultado esperado.
>
> **Función:** Toma de decisiones | **Segmento:** *Retail* | **País:** EUA

Figura 15. Uso de herramientas de prevención de fraude: actual y en un año

		En uso	Planea agregar el próximo año
Servicios de validación	CVN (Número de verificación de tarjeta)	67%	20%
	Verificación de *email*	62%	26%
	Autenticación del pagador *(3D Secure)*	62%	25%
	AVS (Servicio de verificación de domicilio)	59%	25%
	Servicios de validación de domicilio postal	53%	24%
	Autenticación telefónica en dos pasos	45%	31%
	Verificación de historial crediticio	45%	30%
	Verificación de número telefónico / Búsqueda inversa	45%	31%
	Resultados de motor de búsqueda	43%	30%
	Mapas/Indicadores geográficos	43%	33%
	Sitios de redes sociales	40%	32%
	Indicadores biométricos	32%	36%
	Servicios pagos de registros públicos	29%	34%
Datos protegidos	Historial de órdenes del cliente	67%	21%
	Listas de negativos/Listas negras (listas internas)	60%	26%
	Listas de positivos/listas blancas	49%	28%
	Análisis de comportamiento del cliente en el sitio/de patrones	46%	34%
	Modelos de puntuación de fraude: específico para cada compañía	43%	34%
	Monitoreo de *velocity* de la orden	39%	36%
	Detección de *Proxy*	38%	34%
Información de múltiples comercios	Listas de negativos compartidas / *hotlists* compartidas	44%	31%
	Velocity de compras en múltiples comercios / modelos de *morphing* de identidad	31%	38%
Rastreo de dispositivo	Geolocalización: *laptop / desktop*	51%	27%
	Geolocalización: dispositivo móvil / tableta	47%	30%
	Device fingerprinting (huella del dispositivo)	30%	39%

MÁS UTILIZADO

MENOS UTILIZADO

Base 1147 (EUA, Canadá y Europa solamente)
Pregunta: A continuación, encontrará una serie de herramientas para detección de fraude. Para cada tipo, indique si su organización…
Opciones de respuesta: Actualmente utiliza esta herramienta, planea agregar esta herramienta el próximo año, o ninguna de las anteriores.

La nueva cara del *3D Secure*

A pesar de la inquietud sobre la pobre experiencia del cliente que abandona el carro de compra, *3D Secure* (3DS) es una de las herramientas de prevención de fraude más utilizadas.

Esta popularidad probablemente refleja el hecho de que 3DS se ha convertido, cada vez más, en una herramienta basada en riesgo. En lugar de autenticar cada transacción por desafío, los emisores solo autentican a aquellos que los analistas indican como riesgo de fraude. De hecho el beneficio más seleccionado de 3DS ahora es «una mejor experiencia del usuario» (sin diferencias entre líderes y el resto).

Figura 16. Beneficios de *3D Secure*
(% de usuarios que indican los principales beneficios de 3D Secure)

La introducción del 3DS 2.0 en 2018 ha generado más beneficios a través de:

- Una experiencia del usuario más fluida y consistente a través de canales de compra y de pago, especialmente para navegadores, aplicaciones y billeteras móviles
- Un mayor intercambio de datos entre comercios y emisores, mejorando el análisis y la autenticación de transacciones basados en riesgo

Base: 712. (EUA, Canadá y Europa solamente)
Pregunta: En su opinión, ¿cuáles de los siguientes son los principales beneficios de utilizar la Autenticación del pagador (*3D Secure*)?

Directiva PSD2: mayor seguridad, mejores experiencias de pago

En Europa, la Directiva de servicios de pago revisada (PSD2) entró en vigencia en enero de 2018, con excepción de los requisitos relacionados con una mayor autenticación (SCA). Cuando tengan efecto, a partir del 14 de septiembre de 2019, se aplicará SCA a aquellas transacciones que superen los €30.[6]

PSD2 SCA es para todos los comercios que actualmente venden en Europa o planean hacerlo.

Esto requerirá que el comprador presente dos o más de los siguientes:

- Algo que conoce (por ejemplo, una contraseña de uso único, PIN)
- Algo que posee (por ejemplo, un generador de *token*, un dispositivo móvil, una tarjeta plástica)
- Algo intransmisible (por ejemplo, huella de un pulgar, registro de voz)

Solo el 50% de los participantes se siente preparado para PSD2 SCA.

Figura 17. Estado de preparación para PSD2 entre los participantes europeos:

Para mejorar su preparación:

- Revise su estrategia de autenticación, asegúrese de que puede soportar los requisitos de mayor autenticación antes del 14 de septiembre de 2019
- Comprenda cómo se pueden aplicar las excepciones, como listas blancas y análisis de riesgo de las transacciones, para ayudar a optimizar la experiencia del cliente una vez que SCA entre en vigencia
- Mantenga una estrategia de evaluación de fraude sólida, ya que los índices de fraude tendrán influencia sobre la capacidad de aplicar excepciones

Esta conexión entre las excepciones SCA y los índices de fraude crea una relación nueva y más directa entre la experiencia del cliente y la prevención de fraude, haciendo que la ley de equilibrio sea más importante a futuro.

Para más información sobre PSD2 y SCA, visite www.cybersource.com/psd2[7]

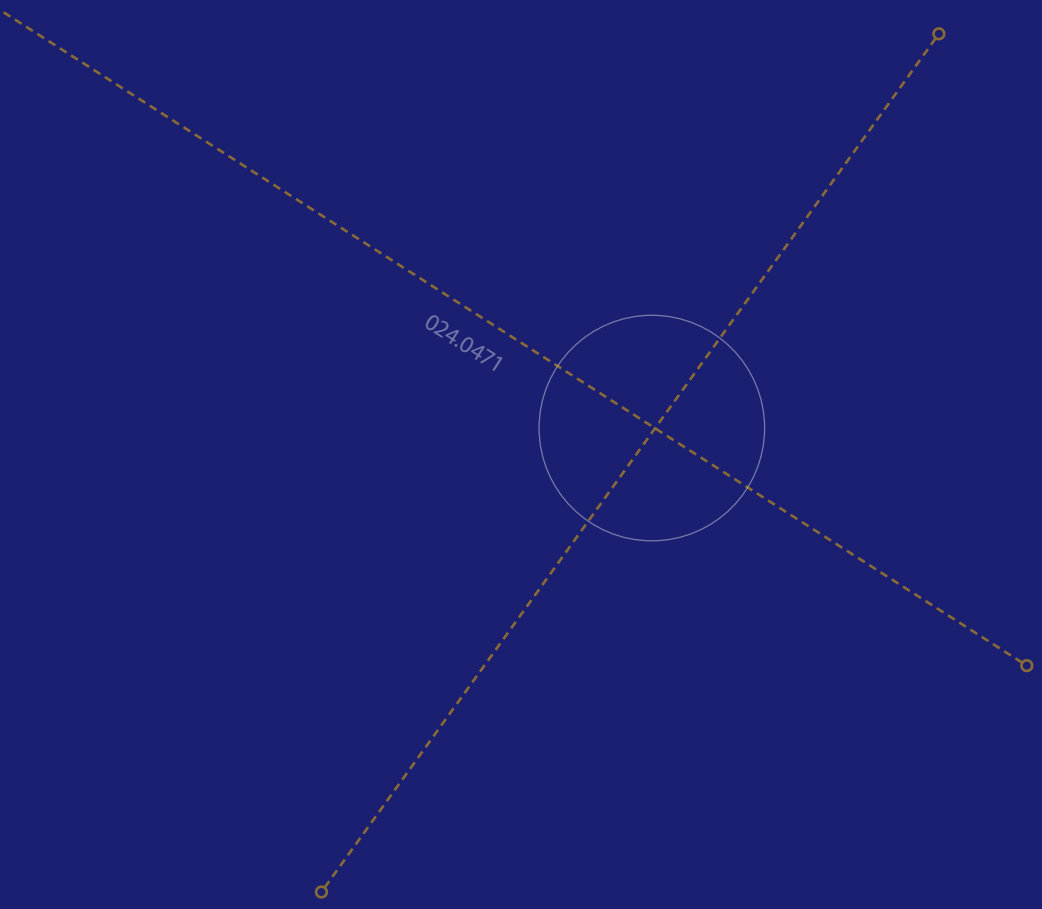
Base 817 (Solamente resultados de Europa)
Pregunta: ¿Qué tan preparada diría que está su organización para PSD2?

[6] Con excepción de las transacciones no contempladas en la Directiva o que tengan una exención válida.
[7] Esta información no constituye consejo legal, ni lo sustituye.

Indicadores de desempeño (KPIs)

La siguiente sección contiene:

- KPI globales vs. KPI regionales
- KPI por ingresos y segmentos *eCommerce*
- KPI regionales para: EUA y Canadá, América Latina, Oriente Medio y África, Asia del Pacífico, Europa



KPI globales

	Región							
	Global	EUA & Canadá	América Latina	Oriente Medio & África	APAC	Total Europa	Norte de Europa	Sur de Europa
% de ingresos anuales por *eCommerce* perdidos por fraude en pago de órdenes domésticas	1.6	1.5	1.3	1.8	1.5	1.9	1.6	2
% de órdenes domésticas rechazadas por sospecha de fraude	2.5	3	2.8	3	2	3	2.7	4
Fraude clasificado como índice de contracargos, como un % de los ingresos anuales por *eCommerce*	0.3	0.7	0.6	0.7	0.1	0.7	0.6	0.7
% de órdenes *eCommerce* enviadas a revisión por fraude	25	16	20	30	30	20	20	25
% de órdenes *eCommerce* rechazadas luego de revisión manual	3	10	20	15	1	10	11	8

	Ingresos *eCommerce*			Segmento				
	Pequeña	Mediana	Grande	Bienes físicos & *retail*	Bienes digitales	Servicios	Alimentos& QSR	Turismo
% de ingresos anuales por *eCommerce* perdidos por fraude en pago de órdenes domésticas	1.5	1.6	1.7	1.8	1	1.6	2.8	1.2
% de órdenes domésticas rechazadas por sospecha de fraude	2.7	2.4	2.5	2.6	2.5	2.1	3	2
Fraude clasificado como índice de contracargos, como un % de los ingresos anuales por *eCommerce*	0.5	0.2	0.4	0.4	0.4	0.2	0.1	0.3
% de órdenes *eCommerce* enviadas a revisión por fraude	30	25	20	25	30	30	15	27
% de órdenes *eCommerce* rechazadas luego de revisión manual	5	2.5	3	4	2	2	4	2

Nota: Se muestran los promedios para todos los KPI

KPI regionales

	Región	Ingresos *eCommerce*			Segmento				
	EUA & Canadá	Pequeña	Mediana	Grande	Bienes físicos & *retail*	Bienes digitales	Servicios	Alimentos & QSR	Turismo
% de ingresos anuales por *eCommerce* perdidos por fraude en pago de órdenes domésticas	1.5	1.5	2	1.2	1.3	2.5	3	1.9	1
% de órdenes domésticas rechazadas por sospecha de fraude	3	2.9	4	2.7	3	4.5	4.6	4.5	2.5
Fraude clasificado como índice de contracargos, como un % de los ingresos anuales por *eCommerce*	0.7	0.8	0.7	0.6	0.6	0.6	1	0.9	0.6
% de órdenes *eCommerce* enviadas a revisión por fraude	16	25	20	10	17.5	21	15	18	12.5
% de órdenes *eCommerce* rechazadas luego de revisión manual	10	5	8	15	9.5	15	5	4.5	22.5

	Región	ingresos *eCommerce*			Segmento				
	América Latina	Pequeña	Mediana	Grande	Bienes físicos & *retail*	Bienes digitales	Servicios	Alimentos & QSR	Turismo
% de ingresos anuales por *eCommerce* perdidos por fraude en pago de órdenes domésticas	1.3	1.3	1.5	1.2	1.4	1.2	5	3.1	1.3
% de órdenes domésticas rechazadas por sospecha de fraude	2.8	2.6	2.9	3	2.8	3	5	10	2.5
Fraude clasificado como índice de contracargos, como un % de los ingresos anuales por *eCommerce*	0.6	0.6	0.6	0.6	0.5	0.6	4	5	0.6
% de órdenes *eCommerce* enviadas a revisión por fraude	20	25	26	12	15	12	33	12.5	25
% de órdenes *eCommerce* rechazadas luego de revisión manual	20	20	28.5	15	20	10	11	20	32

	Región	Ingresos *eCommerce*			Segmento				
	APAC	Pequeña	Mediana	Grande	Bienes físicos & *retail*	Bienes digitales	Servicios	Alimentos & QSR	Turismo
% de ingresos anuales por *eCommerce* perdidos por fraude en pago de órdenes domésticas	1.5	1	1.5	2	2	1	1.1	3.1	1.0
% de órdenes domésticas rechazadas por sospecha de fraude	2	2.2	2	2	2.4	2	2	3	2
Fraude clasificado como índice de contracargos, como un % de los ingresos anuales por *eCommerce*	0.1	0.1	0.1	0.2	0.1	0.2	0.2	0.05	0.2
% de órdenes *eCommerce* enviadas a revisión por fraude	30	30	30	25	25	40	30	14	32.5
% de órdenes *eCommerce* rechazadas luego de revisión manual	1	1	1	1	1.5	1	1	3	1

Nota: Se muestran los promedios para todos los KPI

KPI regionales

	Región	ingresos *eCommerce*			Segmento				
	Total Europa	Pequeña	Mediana	Grande	Bienes físicos & *retail*	Bienes digitales	Servicios	Alimentos & QSR	Turismo
% de ingresos anuales por *eCommerce* perdidos por fraude en pago de órdenes domésticas	1.9	1.6	2	2	1.9	2.2	2	1.4	1.5
% de órdenes domésticas rechazadas por sospecha de fraude	3	3	3.2	3	3	4	3	2.9	2.8
Fraude clasificado como índice de contracargos, como un % de los ingresos anuales por *eCommerce*	0.7	0.6	0.6	0.8	0.7	0.9	0.7	0.6	0.7
% de órdenes *eCommerce* enviadas a revisión por fraude	20	25	24	15	25	17	25	20	15
% de órdenes *eCommerce* rechazadas luego de revisión manual	10	7	10	10	10	8	8	9	22.5

	Región	ingresos *eCommerce*			Segmento				
	Oriente Medio y Norte de África	Pequeña	Mediana	Grande	Bienes físicos & *retail*	Bienes digitales	Servicios	Alimentos & QSR	Turismo
% de ingresos anuales por *eCommerce* perdidos por fraude en pago de órdenes domésticas	1.8	2	1.5	3	1.7	5	3.5	8.5	4
% de órdenes domésticas rechazadas por sospecha de fraude	3	2.9	2.8	4	2.8	10	3.7	5.5	2.3
Fraude clasificado como índice de contracargos, como un % de los ingresos anuales por *eCommerce*	0.7	0.6	0.8	0	0.7	3	0.3	6	0.8
% de órdenes *eCommerce* enviadas a revisión por fraude	30	36	23	23.5	30	37.5	42.5	10	32.5
% de órdenes *eCommerce* rechazadas luego de revisión manual	15	17.5	20	10	20	20	15	8	12.5

Si desea conocer más detalles sobre KPI específicos por país o sobre comparación de actividad, contáctese con su representante de cuentas o con CyberSource a través de www.cybersource.com/locations

Nota: se muestran los promedios para todos los KPI

Sobre este reporte

Durante algunos años, CyberSource ha realizado encuestas sobre prevención de fraude en *eCommerce* enfocadas por regiones. Este año, hemos llevado la encuesta a una nueva escala, capturando una muestra global representativa y sólida.

Mediante el uso de los conocimientos sobre investigación de mercado de GfK, hemos capturado las opiniones de casi 2800 especialistas en administración de fraude de organizaciones pequeñas, medianas y grandes en cinco segmentos. Representan 34 países en EUA y Canadá, América Latina, Europa, Medio Oriente, África y Asia del Pacífico[8]. Además de asegurar la representación de **cinco segmentos**.

Funciones de los participantes

Cuantitativa; 2769 participantes incluyendo aquellos que:

- Toman decisiones o tienen influencia sobre el proceso de toma de decisiones en la prevención de fraude en *eCommerce*: **49%**
- Están involucrados en la prevención de fraude en *eCommerce*: **51%**

Cualitativa; 49 participantes de 15 mercados realizaron una encuesta cuantitativa posterior

[8]La encuesta se realizó principalmente durante el período abril-junio de 2018. En el sureste de Asia y Australia, se realizó durante octubre y noviembre de 2017

Figura18. Distribución geográfica de la representación de ingresos

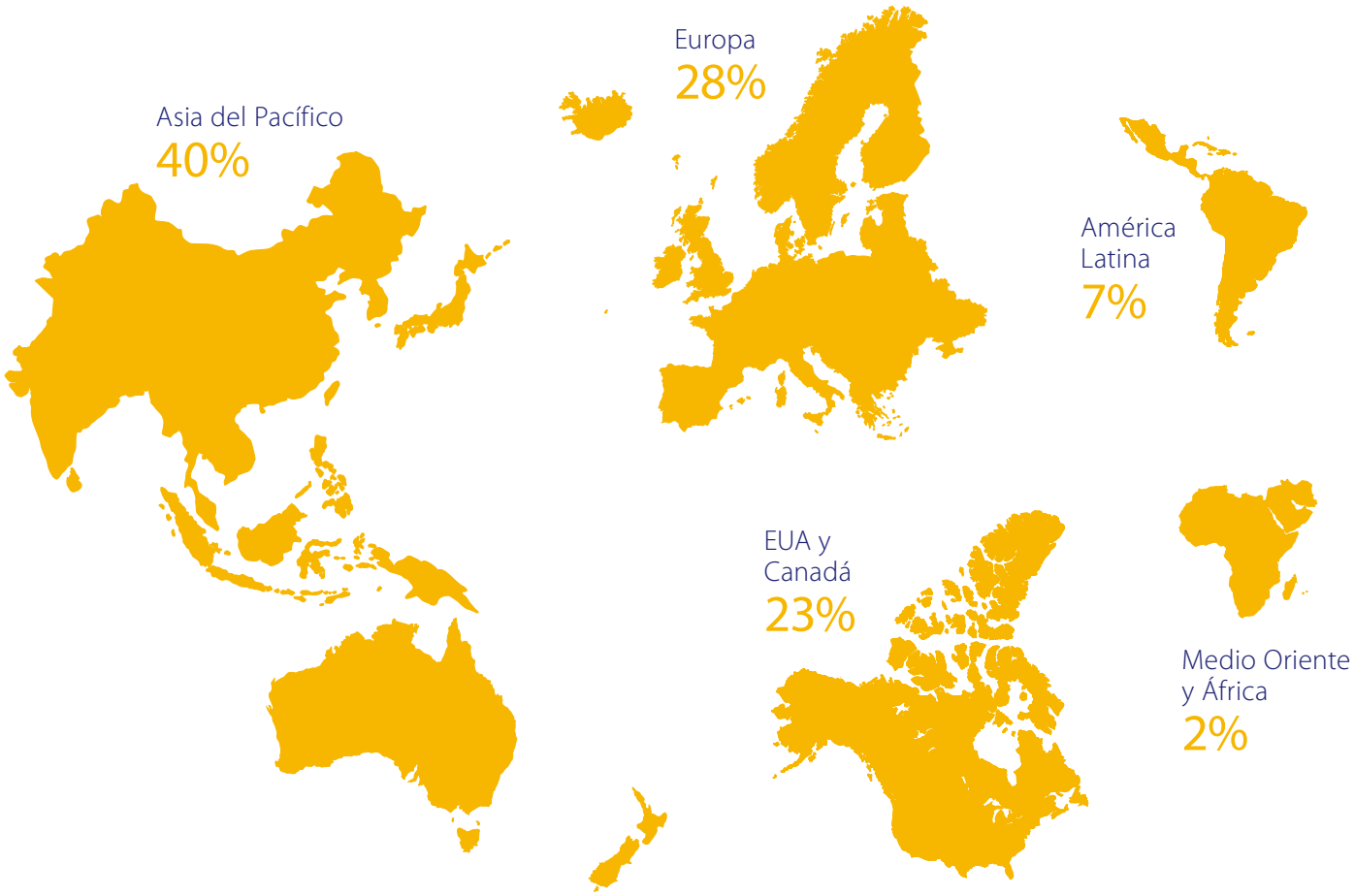


Figura 19.
Tamaño de la actividad según ingresos anuales por *eCommerce*

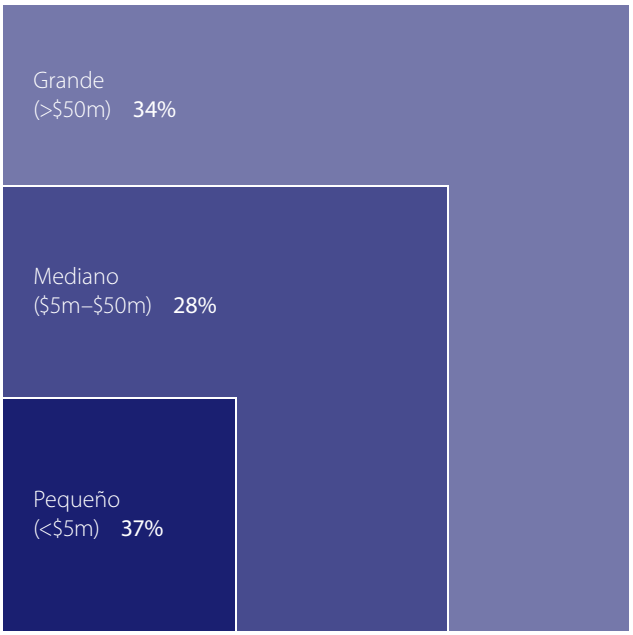
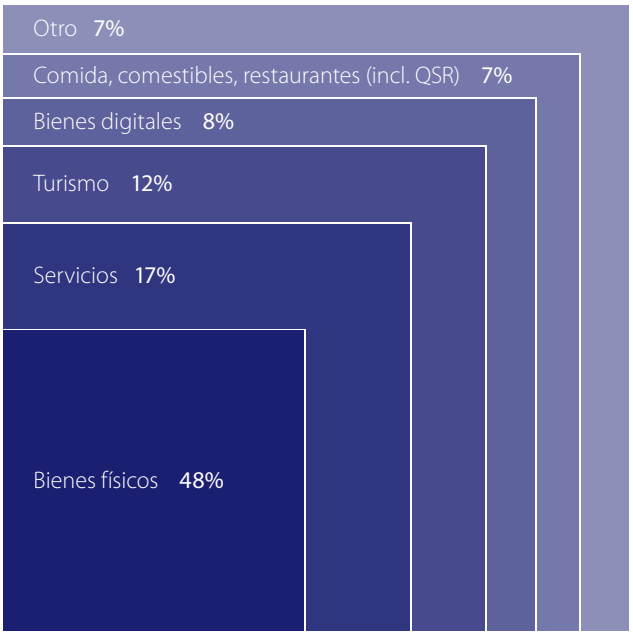


Figura 20.
Segmentos de mercado



Deslinde de responsabilidad

El único fin con el que se presenta la información, recomendaciones o «mejores prácticas» es el de informar. De ningún modo debe considerarse la información como consejos sobre operatoria, comercialización, aspectos legales, técnicos, impositivos o financieros o de cualquier otra índole. Cuando implemente nuevas prácticas o estrategias, debe asesorarse respecto de disposiciones legales que pueden resultar aplicables a sus circunstancias específicas. Los costos, ahorros y beneficios reales de cualquier recomendación, programa o «mejores prácticas» pueden variar según sus necesidades comerciales y los requisitos del programa. Por su naturaleza, las recomendaciones no constituyen garantía de futuros desempeños o resultados y están sujetas a riesgos, incertidumbres y suposiciones que son difíciles de predecir o cuantificar. Las suposiciones fueron realizadas por nosotros a la luz de nuestra experiencia y nuestras percepciones de tendencias históricas, condiciones actuales, desarrollos futuros esperados y otros factores que creemos apropiados a las circunstancias. Las recomendaciones están sujetas a riesgos e incertidumbres que pueden causar que los resultados y tendencias reales y futuros sean muy diferentes a los esperados. CyberSource deslinda responsabilidad por el uso que se haga de la información contenida en la presente, (incluidos errores, omisiones, inexactitudes o destiempos de cualquier naturaleza) o cualquier presunción o conclusión a la que se pueda llegar en virtud de la misma. CyberSource se abstiene de ofrecer garantías, expresas o implícitas, y expresamente deslinda responsabilidad por las siguientes garantías: de comercialización o de aptitud para un fin determinado, de que no se infrinjan derechos intelectuales de terceros, de que la información satisfará los requisitos de un cliente, de que la información esté actualizada y libre de errores. Siempre que las disposiciones legales aplicables así o permitan, CyberSource estará exenta de responsabilidad respecto de cualquier cliente o tercero en relación con daños que surjan o puedan surgir de cualquier teoría de derecho, incluidos, sin limitación, daños especiales, indirectos, emergentes o punitivos, como también estará exenta de daños por lucro cesante o cualquier otra pérdida económica, aunque se hubiere alertado sobre tales daños.

Contáctenos

Información de contacto en www.cybersource.com/locations

CyberSource es una plataforma modular global de administración de pagos dentro de la infraestructura segura de Visa con los beneficios y la visión de una red global de procesamiento de pagos por más de US$ 427 mil millones. Con esta solución, los comercios pueden operar con agilidad y alcanzar sus objetivos dentro del comercio digital mejorando la experiencia del cliente, aumentando sus ingresos y mitigando el riesgo. Para el caso de socios adquirentes, CyberSource ofrece una plataforma tecnológica, experiencia en pagos y servicios de soporte que los ayudarán a crecer y a administrar su portfolio de comercios, y así cumplir con su promesa de marca. Para más información, visite cybersource.com

© 2019 CyberSource Corporation. Todos los derechos reservados.

CyberSource®
A Visa Solution