Identifica y supera los principales riesgos de fraude

Cómo proteger negocio y clientes contra el fraude.

PayPal

Contenido

Anticípate a los estafadores mundiales

La ciberdelincuencia está en todas partes. Cada año representa un gasto de casi 1 billón de dólares[1] y, por desgracia, nadie es inmune. Los estafadores atacan a todos los sectores en todos los países, sin importar si la organización es un pequeño negocio local o una gran empresa multinacional.

Ahora bien, al conocer los tipos de ataques más frecuentes en cualquier situación, los negocios pueden prepararse mejor para anticiparse y combatir el fraude.

USD 1B

es el costo global anual de la ciberdelincuencia.[2]

82%

de las empresas informó un aumento en los intentos de fraude en 2021.[3]

18%

es el aumento interanual de las pérdidas en eCommerce causadas por el fraude.[4]

3.3x

Cada dólar perdido por fraude cuesta alrededor de 3.3 veces en tiempo y otros gastos.[5]

1 de 5

inicios de sesión representa un intento de robo de cuenta.[6]

1 de 4

transacciones con tarjeta no presente en México constituye un intento de fraude.[7]

1, 2. Center for Strategic & International Studies (2020), *The Hidden Costs of Cybercrime* **3.** Cybersource (2021), 2021 Global Fraud Report **4.** Payments Dive (2021), *E-commerce fraud to surpass $20B in 2021, an 18% jump over last year, report finds*
5. LexisNexis (2020), *2020 True Cost of Fraud Study – E-Commerce/Retail Report* **6.** Arkose Labs (2022), *2022 State of Fraud & Account Security Report* **7.** Vesta (2021), *Vesta Report: Analyzing the Latest Evolution of Card-Not-Present Fraud*

Por qué la ciberseguridad debe ser tu máxima prioridad

El fraude y la ciberdelincuencia no son buenos para los negocios. Está claro que hay una pérdida potencial de ingresos o de bienes adquiridos de forma maliciosa. Pero también existe el enorme costo de hacer frente a los intentos de fraude: más de 3 veces que los ingresos perdidos.[8]

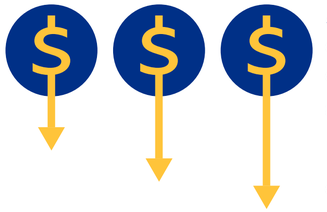
Al sufrir pagos fraudulentos, pueden ocurrir tres tipos de pérdidas en tu negocio.

- Te roban tus productos o servicios, lo que implica una pérdida directa y tienes que pagar para reponer tu inventario.
- El verdadero titular de la tarjeta quiere que le devuelvas su dinero que, junto con una comisión de contracargo que cobra el procesador de pagos, supone una pérdida de ingresos más los costos operativos adicionales.
- Tienes que dedicar tiempo y recursos a gestionar el fraude y las quejas de los clientes reales cuyas cuentas han sido hackeadas. El resultado es un aumento de los gastos de funcionamiento de tu negocio.

Las empresas también pueden sufrir daños en su reputación por ataques a gran escala o bien difundidos. Incluso si estos no llaman la atención del público, un alto índice de contracargos u otros intentos de fraude puede hacer que el negocio sea considerado de mayor riesgo por su proveedor de pagos, lo que se traduce en requisitos más exigentes y mayores gastos de procesamiento.[9]

Las violaciones de datos o el trámite involuntario de transacciones fraudulentas pueden dar lugar a sanciones o multas por parte de las autoridades reguladoras, incluyendo las que combaten el lavado de dinero (AML).

En esta guía se examinan algunos de los tipos de fraude más comunes en diferentes sectores y cómo manejarlos.



Asimismo, hay que tener en cuenta el enorme costo que conlleva hacer frente a los intentos de fraude:

más del triple

de los ingresos perdidos.[8]

8. LexisNexis (2020), *2020 True Cost of Fraud Study – E-Commerce/Retail Report* **9.** Forbes (2021), High-Risk Merchant Account: What It Is And How It Works

Tipos comunes de pagos fraudulentos

Fraude por robo de cuentas (ATO)

El robo de cuentas es una forma de suplantación de identidad en la que los delincuentes acceden a la cuenta de un cliente real para realizar compras no autorizadas o robar los datos personales y de pago de la cuenta. Las formas más comunes de hacerlo son:

- **Relleno de credenciales:** los robots lanzan miles de combinaciones de nombres de usuario y contraseñas a los inicios de sesión de las cuentas, que suelen comprarse en grandes cantidades en la web oscura.
- **Suplantación de identidad y otras técnicas de ingeniería social:** se engaña a los clientes para que revelen sus credenciales, con frecuencia a través de correos electrónicos o llamadas telefónicas fraudulentas.

Prueba de tarjetas

En este caso, los delincuentes prueban grandes volúmenes de datos de tarjetas robadas para ver si siguen siendo válidos. Suelen utilizar bots o scripts informáticos para realizar grandes cantidades de transacciones de poco valor. Las tarjetas que logran utilizar se emplean para realizar compras de mayor volumen o se venden a otros estafadores.

Fraude con tarjeta no presente (CNP)

El fraude CNP se produce cuando se utiliza una tarjeta para realizar una compra sin presentarla. En un principio, se trataba de compras por teléfono y por correo, pero hoy en día incluye todas las compras de eCommerce. El fraude CNP se presenta en dos formas: el tradicional, que utiliza los datos de la tarjeta robada, y el amigable (véase más abajo). Los dos tipos dan lugar a que el verdadero titular de la tarjeta presente un contracargo.

Fraude amigable

El llamado fraude amigable se produce cuando el titular de la tarjeta presenta una controversia sobre una transacción legítima. A veces se produce cuando no recuerda haber efectuado una compra o no sabe que un familiar ha utilizado su tarjeta para realizar una compra. En otras ocasiones, el comprador puede arrepentirse de una compra impulsiva o haber olvidado cancelar una suscripción y decide presentar una solicitud de contracargo en lugar de admitir su error. El fraude amigable también se da cuando un cliente hace una reclamación falsa de “artículos no entregados”.

Fraude por contracargo

Cuando un titular de una tarjeta presenta una controversia sobre un cargo, el banco o la empresa emisora de la tarjeta anula el cargo y cobra una tasa de contracargo al comercio. Los contracargos pueden surgir por problemas con la transacción (quizás no se entregaron los artículos o se cometió un error al hacer el cargo en la tarjeta). También los puede solicitar el titular legítimo de la tarjeta cuando detecta un fraude. Si bien muchos contracargos pueden ser auténticos, también se observa una tendencia creciente de solicitudes de contracargo fraudulentas.

Fraude de identidad sintética

Se trata de uno de los tipos de fraude financiero de más rápido crecimiento. Los delincuentes crean una identidad falsa con datos personales robados o totalmente ficticios y, poco a poco, se toman el tiempo necesario para crear un historial crediticio con la identidad inventada. Con un documento de identidad que parece válido, pueden solicitar tarjetas de crédito o préstamos y gastar hasta el límite antes de desaparecer. Este tipo de fraude es difícil de detectar cuando ya es demasiado tarde.

El perfil del fraude en tiendas digitales / eCommerce

El rápido crecimiento mundial del eCommerce en los últimos dos años ha sido acompañado por un gran aumento de todos los tipos de ataques de pagos fraudulentos.

El fraude amigable y la prueba de tarjetas son los ataques más comunes en todo el mundo.[10] Los negocios en línea informan de un aumento en todos los tipos de ataques, incluidos los contracargos y el fraude amigable.[11]

Más de la mitad de los comercios encuestados informaron de un aumento de los fraudes relacionados con la identidad y las cuentas, como el fraude de identidad sintética, el robo de cuentas, la suplantación de identidad y el fraude de cuentas nuevas.[12] El 59% de los comercios encuestados también informó un aumento de los fraudes con tarjetas no presentes.[13]

Según los expertos en fraude de Arkose Labs, 1 de cada 4 transacciones en tiendas fue un ataque.[14]

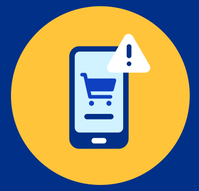
No es de extrañar que los vendedores de eCommerce de todo el mundo, de cualquier escala, consideren el fraude como un serio desafío:

3 de 5

comercios consideran que la pérdida de ingresos por pagos fraudulentos tiene un efecto sustancial o significativo en su negocio.[15]

3 de 5

comercios consideran también que la pérdida de productividad a causa de los pagos fraudulentos tiene un efecto sustancial o significativo en su negocio.[16]



9 de 10

comercios consideran ahora que la gestión del fraude en el eCommerce es “muy o extremadamente importante” para su estrategia empresarial global.[17]

1 de 5

comercios dice que la seguridad de los datos de los clientes es un reto crítico.[18]

10, 17. Cybersource (2021), 2021 Global Fraud Report **11, 12, 13, 15, 16, 18.** FIS Worldpay (2021), Global Payment Risk Mitigation **14.** Arkose Labs (2022), 2022 State of Fraud & Account Security Report

El perfil del fraude en los negocios de SaaS y servicios

Según Arkose Labs, las empresas tecnológicas tenían 5 veces más probabilidades de sufrir un ataque de fraude en 2021 en comparación con el año anterior.[19]

El SaaS, y cualquier tipo de negocio de suscripción, es el más vulnerable a los ataques de fraude ya que cada cuenta tiene asociados los datos de pago.

Las empresas tecnológicas tenían **5 veces** más probabilidades de sufrir un ataque fraudulento en 2021 en comparación con 2020.[19]

- **El fraude por robo de cuentas (ATO)** es una amenaza común para los negocios de SaaS. Una vez que las cuentas se han visto afectadas, se utilizan para comprar servicios y bienes o se venden a otros delincuentes.
- El uso de datos de tarjetas robadas para abrir cuentas falsas y realizar compras **(fraude CNP)** y el uso de cuentas falsas para abusar de las ofertas de pruebas gratuitas también son habituales en el espacio SaaS.
- Los **contracargos** son otro gran reto en este sector. De hecho, el sector del software tiene la mayor proporción de contracargos por transacción, con un 0.66%.[20] Algunos de ellos son inofensivos, ya que la gente se olvida de lo que ha contratado, pero muchos otros son fraudulentos.

19. Arkose Labs (2022), *2022 State of Fraud & Account Security Report* **20.** Expert Market (2021), *Chargeback Fraud Statistics 2022*

El perfil del fraude en la educación

El mundo de los pagos es cada vez más digital. Tanto quienes pagan como los acreedores se benefician de la comodidad de pagar en línea. Por desgracia, los pagos fraudulentos (que roban dinero tanto a instituciones como a padres y estudiantes) también están aumentando.

En 2021, la región de Latinoamérica experimentó el mayor número diario de ataques de fraude a nivel mundial,[21] y México estuvo entre los cinco principales lugares de origen y destino de este tipo de estafa.[22]

En promedio, 1 de cada 4 transacciones de tarjeta no presente (CNP) constituye un intento de fraude[23] y 4 de cada 10 ataques a transacciones digitales en México son exitosos.[24]

Por desgracia, el sector educativo no es inmune. Ya sea que se trate de transacciones de alto valor, de colegiaturas o de pequeños cobros regulares de libros, viajes y otros cargos, los estafadores encontrarán la manera de robar tu dinero.

Los tipos de fraude más comunes a los que debes prestar atención son los siguientes:

- **Fraude CNP –** Cuando el cliente y la tarjeta no están presentes, como en las transacciones en línea y por teléfono. Algunos ejemplos son el pago de colegiaturas o el pedido de otros bienes o servicios en línea. México tiene el mayor nivel de fraude CNP del mundo.[25]
- **Fraude por robo de cuentas (ATO),** en especial si existe la preocupación de que las cuentas de los estudiantes no tengan una protección adecuada con contraseñas seguras. Además de utilizar los datos personales y de pago almacenados para otros delitos, los estafadores podrían, por ejemplo, cambiar los datos de pago de la cuenta, cancelar una solicitud de curso y solicitar un reembolso (que se haría a la cuenta del delincuente).

Al tratarse de colegiaturas que suelen tener un valor relativamente alto, tus clientes (los padres o estudiantes que pagan las cuotas) son vulnerables a los ataques de fraude que los embaucan a pagar el dinero a cuentas falsas. Para evitar que esto ocurra, es necesario comunicar claramente las políticas de seguridad de los pagos de tu institución.

México es uno de los destinos más populares de América para los estudiantes de otros países.[26] En consecuencia, las universidades mexicanas pueden recibir pagos de tarjetas de crédito internacionales. Algunas soluciones de prevención antifraude generan un alto nivel de falsos positivos para las tarjetas de pago no nacionales, lo que resulta en el rechazo de pagos válidos y en el descontento de los estudiantes o padres. Por ello, conviene asegurarse de que la protección contra el fraude que se utiliza sea lo suficientemente sofisticada como para procesar con exactitud las tarjetas internacionales sin retrasos ni errores.

21, 22. LexisNexis (2021), *Redefining Trust and Risk, The LexisNexis Cybercrime Report* **23.** Vesta (2021), *Vesta Report: Analyzing the Latest Evolution of Card-Not-Present Fraud*
24. LexisNexis quoted on MexicoBusiness.com (2021), *Payment Security and Fraud Prevention* **25.** A16z (2021), *Latin America's Fintech Boom* **26.** Global Scholarships (2022), *5 Best Universities in Mexico for International Students*

El perfil del fraude en las telecomunicaciones

El sector de las telecomunicaciones es un blanco atractivo para los delincuentes, ya que ofrece oportunidades para robar credenciales valiosas, hardware de alto valor y tarjetas SIM.[27]

Hay tres tipos de pagos fraudulentos que afectan especialmente al sector de las telecomunicaciones.[28]

Fraude de suscripción para adquirir dispositivos

Los delincuentes intentan conseguir equipos caros, como teléfonos móviles, sin pagar, o bien realizando un pequeño pago por adelantado. Normalmente, se crean nuevas cuentas con datos de pago robados e identidades robadas o sintéticas. Suelen hacer pedidos con entrega en el mismo día o al día siguiente, con la esperanza de ganarle la partida al control de fraudes. También es habitual solicitar la entrega en un punto de recogida en lugar de una dirección personal.

A veces, los estafadores utilizan los datos de su propia tarjeta de crédito y luego tramitan un contracargo alegando que la mercancía no ha llegado. A continuación, cancelan el pago de la suscripción mensual.

Fraude con tarjetas SIM de prepago

Las tarjetas SIM de prepago, de recarga o de pago por uso (PAYG) presentan dos tipos de fraude.

En primer lugar, la naturaleza del bajo valor y alto volumen de ventas de tarjetas SIM las convierte en un objetivo atractivo para la prueba de tarjetas.

En segundo lugar, las SIM de prepago suelen usarse para pagar a los delincuentes como una forma de moneda. Con frecuencia, esto puede detectarse mediante la supervisión de patrones de compra inusuales, como adquirirlas en grandes cantidades.

Fraude por robo de cuentas (ATO)

Al igual que en otros sectores, los ataques ATO son una amenaza cada vez más frecuente. Además de los típicos objetivos de robar los datos personales y de pago de los clientes, los delincuentes que atacan las cuentas de telecomunicaciones suelen cambiar la dirección de envío de la cuenta robada, pedir un nuevo dispositivo y hacer el cargo en la factura mensual o la tarjeta de pago del titular de la cuenta.

27. LexisNexis (2021), *Redefining Trust and Risk, The LexisNexis Cybercrime Report* **28.** Cybersource (2021), *Five key fraud trends in telco*

Cómo prevenir el fraude a la hora de pagar

Frena los ataques de robo de cuentas

Algunas plataformas de pago, como PayPal, ofrecen autenticación multifactor (MFA) o autenticación de dos factores (2FA). Este sistema puede ser una forma eficaz de evitar tanto el relleno como el uso de credenciales robadas en ataques de phishing. De hecho, la autenticación de dos factores fue considerada "muy importante" por casi la mitad de los comercios.[29]

Al activar la MFA/2FA, se pide al cliente que proporcione una forma adicional de autenticación (como un código numérico de un solo uso) que se envía a su teléfono móvil o cuenta de correo electrónico previamente registrados. Con ello se evita que los estafadores utilicen credenciales robadas, ya que también necesitan acceder al dispositivo móvil o al correo electrónico del verdadero propietario.

Dado que el primer paso en el robo de una cuenta (el uso de bots para realizar ataques de relleno de credenciales) suele estar automatizado, un paso sencillo como la introducción de la tecnología CAPTCHA, que requiere la intervención humana, también puede ser eficaz.

Cómo detectar y hacer frente a las pruebas con tarjetas

Estos ataques implican grandes volúmenes de pequeñas transacciones en un corto lapso de tiempo. En escenarios de gran volumen como el eCommerce, las transacciones de prueba de tarjetas pueden pasar fácilmente desapercibidas y, sin protección, los vendedores pueden sufrir en poco tiempo una oleada de contracargos a causa de un ataque. Los ataques de prueba de tarjetas también pueden afectar a la disponibilidad de la infraestructura de un vendedor con excesivos intentos de autorización fallidos.

PayPal utiliza algoritmos de Machine Learning y toma de decisiones en tiempo real para ayudar a diferenciar entre transacciones buenas y malas, e identificar con rapidez patrones fraudulentos como la prueba de tarjetas. PayPal compara las tendencias históricas y la información de las transacciones, como la dirección IP, el tipo y el ID del dispositivo, la dirección de correo electrónico y otros datos.

El Machine Learning depende del conjunto de datos del que aprende, un área en la que PayPal tiene una gran ventaja gracias a nuestra red bilateral. Con más de 400 millones de consumidores y 30 millones de cuentas de vendedores en una amplia gama de sectores, PayPal posee una gran cantidad de datos sobre consumidores y perfiles de riesgo. Esta información, tanto del lado del comercio como del cliente, nos permite determinar si una transacción es real o falsa, incluso en el caso de los comportamientos fraudulentos más sofisticados.[30]

Más de **400M de clientes** y **30M de comercios** usan PayPal.[30]

29. FIS Worldpay (2021), *Global Payment Risk Mitigation* **30.** PayPal (2020), *How Data Science, Machine Learning and Artificial Intelligence Lead to Higher Authorization Rates*

Cómo reducir el fraude de tarjetas no presentes (CNP)

Con el fraude CNP, lo mejor es solicitar toda la información posible a quien paga. Esto incluye pedir el código CVV y aplicar medidas de prevención antifraude como 3D Secure (3DS) y la autenticación multifactor (MFA).

Una vez más, las plataformas de pago como PayPal, que utilizan Machine Learning con datos en tiempo real, pueden ayudar a reducir los casos de fraude CNP. El uso vanguardista de PayPal de la tokenización de la red[31] dificulta a los delincuentes el uso fraudulento de los datos de las tarjetas robadas.

Cómo combatir el fraude amigable

El fraude amigable (también llamado fraude del titular) es común en los sectores del eCommerce y de videojuegos. Puede ser difícil de detectar y probar. Sin embargo, si se llevan buenos registros y políticas que demuestren que los artículos o servicios se pidieron, enviaron y recibieron legítimamente, se pueden refutar las reclamaciones falsas. Un ejemplo de ello sería exigir una firma al recibir los productos.

Muchas reclamaciones de fraude amigable comienzan como transacciones válidas, por lo que tener una política de devoluciones clara y generosa, un buen servicio de atención al cliente y una buena comunicación también pueden ayudar a evitar que algunos clientes presenten contracargos falsos.

Pedir siempre el código CVV de la tarjeta e implementar 3D Secure también dificulta el fraude amigable.

Los negocios pueden beneficiarse de la Protección al Vendedor de PayPal.[32]

Cómo reducir el fraude por contracargos

Dado que casi todos los pagos fraudulentos dan lugar a contracargos, mejorar los mecanismos generales de defensa contra este delito te ayudará a reducir el fraude por contracargos.

Una de las mejores formas de reducir el fraude por contracargos es trabajar con un procesador de pagos como PayPal que utilice tecnología avanzada de prevención antifraude. Las técnicas de fraude están en constante evolución, y por ello necesitas una solución que lo evite y se adapte constantemente a la amenaza, a partir de datos en tiempo real.

Prevención del fraude de identidad sintética

Las identidades sintéticas funcionan porque muchas instituciones financieras utilizan sistemas de puntuación poco sofisticados o automáticos para ofrecer créditos. El aprovechamiento de mayores volúmenes de datos, incluidos los de terceros, puede revelar a menudo las incoherencias que son habituales en las identidades falsas.

Los datos de la gran red bilateral de PayPal de vendedores y consumidores son una gran fuente para nuestros modelos de Machine Learning de detección antifraude.

31. PayPal (2020), *How Network Tokenization Leads to Higher Authorization Rates and a Better Customer Experience* **32.** Aplican términos y condiciones

Cómo puede ayudar PayPal a controlar el riesgo de fraude

La tecnología de pagos de PayPal, desarrollada a lo largo de 20 años, tiene como finalidad disminuir el riesgo de fraude y aumentar la confianza de los clientes al realizar sus compras.

En todo el mundo, la marca PayPal es reconocida y de confianza. Los clientes valoran el hecho de que sus datos personales nunca se compartan. Pueden beneficiarse de una experiencia de pago diseñada para la comodidad fácil y segura que esperan los compradores de hoy en día.

Con PayPal, los vendedores pueden ofrecer una amplia variedad de métodos de pago (incluidos los locales alternativos) con una sola integración, lo que les facilita la gestión y la organización centralizada de los pagos.

Los negocios también pueden beneficiarse de la Protección al Vendedor de PayPal en las transacciones que cumplen los requisitos[33]

y de los estándares de prevención antifraude, como 3D Secure.

PayPal ofrece funciones avanzadas de prevención antifraude. Nuestra red de más de 400 millones de usuarios activos en todo el mundo proporciona una gran fuente de datos que se incorporan a nuestros modelos de Machine Learning para una detección de fraude más precisa, adaptable y en tiempo real. Como resultado, se disminuyen los rechazos de transacciones innecesarios, así como la posibilidad de tratar como estafadores por error a tus buenos clientes.

El gran conjunto de datos de los vendedores de PayPal, las técnicas avanzadas de Machine Learning y los conocimientos en ciencia de datos también agilizan la identificación de las nuevas tendencias de actividades fraudulentas y actúan en consecuencia en todos los demás comercios de la red.

Nuestras relaciones globales con bancos, adquirentes y reguladores también nos colocan en una buena posición para detectar el fraude antes de que ocurra.

La protección contra el fraude de PayPal está diseñada para las necesidades de las empresas. Se trata de un conjunto de herramientas listo para usar integrado en PayPal Commerce Platform, diseñado para proporcionar a los comercios más visibilidad y control sobre el proceso de toma de decisiones de las transacciones.

Conoce más sobre cómo PayPal ayuda a las empresas a administrar los riesgos y mantener el cumplimiento normativo

Más información

Los resultados de la administración avanzada de riesgos de PayPal pueden incluir:

- Menos contracargos
- Menos falsos positivos
- Menor fricción con el cliente
- Menos pérdidas por fraude
- Aumento de la eficiencia operativa
- Agilización de la experiencia del cliente

33. Aplican términos y condiciones

Referencias

1. Center for Strategic & International Studies (2020), *The Hidden Costs of Cybercrime*
2. Center for Strategic & International Studies (2020), *The Hidden Costs of Cybercrime*
3. Cybersource (2021), *2021 Global Fraud Report*
4. Payments Dive (2021), *E-commerce fraud to surpass $20B in 2021, an 18% jump over last year, report finds*
5. LexisNexis (2020), *2020 True Cost of Fraud Study – E-Commerce/ Retail Report*
6. Arkose Labs (2022), *2022 State of Fraud & Account Security Report*
7. Vesta (2021), *Vesta Report: Analyzing the Latest Evolution of Card-Not-Present Fraud*
8. LexisNexis (2020), *2020 True Cost of Fraud Study – E-Commerce/ Retail Report*
9. Forbes (2021), *High-Risk Merchant Account: What It Is And How It Works*
10. Cybersource (2021), *2021 Global Fraud Report*
11. FIS Worldpay (2021), *Global Payment Risk Mitigation*
12. FIS Worldpay (2021), *Global Payment Risk Mitigation*
13. FIS Worldpay (2021), *Global Payment Risk Mitigation*
14. Arkose Labs (2022), *2022 State of Fraud & Account Security Report*
15. FIS Worldpay (2021), *Global Payment Risk Mitigation*
16. FIS Worldpay (2021), *Global Payment Risk Mitigation*
17. Cybersource (2021), *2021 Global Fraud Report*
18. FIS Worldpay (2021), *Global Payment Risk Mitigation*
19. Arkose Labs (2022), *2022 State of Fraud & Account Security Report*
20. Expert Market (2021), *Chargeback Fraud Statistics 2022*
21. LexisNexis (2021), *Redefining Trust and Risk, The LexisNexis Cybercrime Report*
22. LexisNexis (2021), *Redefining Trust and Risk, The LexisNexis Cybercrime Report*
23. Vesta (2021), *Vesta Report: Analyzing the Latest Evolution of Card-Not-Present Fraud*
24. LexisNexis quoted on MexicoBusiness.com (2021), *Payment Security and Fraud Prevention*
25. A16z (2021), *Latin America's Fintech Boom*
26. Global Scholarships (2022), *5 Best Universities in Mexico for International Students*
27. LexisNexis (2021), *Redefining Trust and Risk, The LexisNexis Cybercrime Report*
28. Cybersource (2021), *Five key fraud trends in telco*
29. FIS Worldpay (2021), *Global Payment Risk Mitigation*
30. PayPal (2020), *How Data Science, Machine Learning and Artificial Intelligence Lead to Higher Authorization Rates*
31. PayPal (2020), *How Network Tokenization Leads to Higher Authorization Rates and a Better Customer Experience*
32. Aplican términos y condiciones
33. Aplican términos y condiciones