

2019

Estudio de
Medios de Pago
y Fraude Online



adigital



CONFIANZA ONLINE

Nos encontramos ante un momento de numerosos cambios para el ecommerce en nuestro país y en el conjunto de la UE. Evoluciona la tecnología, cambian los hábitos de los consumidores y, con el nuevo contexto, se adaptan también las normativas. Sin ir más lejos, a finales del año pasado comenzaba a ser de aplicación la nueva Directiva de Medios de Pago (PSD2) con todo lo que esta ha supuesto para los negocios que operan online: desde comprender sus implicaciones hasta adaptar sistemas o preparar a sus equipos.



Este año no ha sido diferente. Los últimos meses nos han tenido pendientes de una de las medidas clave de esa PSD2, la Autenticación Reforzada de Cliente (o SCA, por sus siglas en inglés). Sin embargo, pese al impacto que tendrá esta medida tanto sobre la gestión de los pagos como sobre la experiencia de compra, el 66,97% de las empresas encuestadas aseguran que no conocen las novedades que esta introduce. El porcentaje aumenta si nos fijamos en el número de **negocios que declaran no sentirse preparados para minimizar el impacto que la SCA** tendrá sobre sus ventas: casi 8 de cada 10.

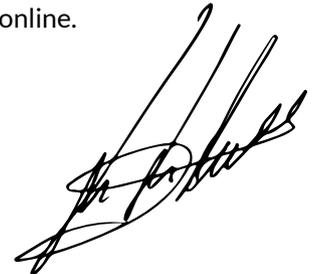
Los medios de pago son uno de los factores más estratégicos del comercio electrónico. Según los datos de Baymard Institute, en todo el mundo, las tasas de abandono del carrito de la compra rozan a día de hoy el 70%. Los problemas o dificultades a la hora de realizar el pago son una de las principales razones de esos frenos en el proceso de compra. **Teniendo en cuenta que una mala experiencia de pago puede llegar a reducir los ingresos de las empresas entre un 10 y un 15%**, es totalmente necesario mantener el foco en los medios de pago como elemento clave de un negocio digital.

Esta nueva edición del **Estudio de Medios de Pago y Fraude Online** arroja luz sobre algunos de estos puntos. Pensando en las opciones de pago que existen, aunque las **tarjetas, las transferencias y PayPal** continúan como protagonistas, resulta llamativo observar la evolución que se produce en otros sistemas que no existían hace unos años. Es el caso del **wallet, que crece un 7% con respecto al año pasado** entre los métodos de pago ofrecidos por las empresas encuestadas y triplica su peso sobre el total de las transacciones. Mientras, continúa el descenso de los pagos contrarrembolso -con una caída del 36%- y las tarjetas de prepago -6%-.

Esto nos obliga a poner la vista sobre qué ocurrirá con otras alternativas como **las criptomonedas y las oportunidades de la blockchain**, y, por supuesto, sobre cómo los nuevos sistemas de identificación digital (como el uso de la voz, de la huella dactilar o del latido de nuestro corazón) van a transformar la interacción con el cliente. ¿Cuánto tardarán en implantarse? ¿Cómo será la aceptación del usuario? Como siempre, el reto más grande al que nos enfrentaremos será el de acoplar y sacar el máximo partido a esa tecnología aumentando la seguridad de las transacciones con la menor fricción posible para el cliente.

Hablando de seguridad es inevitable pensar también en la otra parte, el proveedor del servicio. Este año crece casi en 10 puntos con respecto a 2018 (hasta el 83%) el número de empresas que declaran una **tasa de fraude anual inferior al 0,25%**, medido en porcentaje sobre su facturación. También aumenta en un 35% el porcentaje de empresas que utilizan un sistema de gestión de fraude. Estos datos no solo son relevantes a efectos de negocio: incluso para acceder a las exenciones del SCA por bajo riesgo, por ejemplo, se solicita un 0.1% de fraude, por lo que las empresas que quieran utilizarlas necesitan tener el fraude muy controlado.

Así pues, con el comercio electrónico creciendo día a día en nuestro país, mejorar y mantener actualizada la experiencia de pagos tanto para el usuario como para la empresa debe convertirse en una prioridad. Es una garantía de eficacia y sostenibilidad para cualquier negocio que opera online.



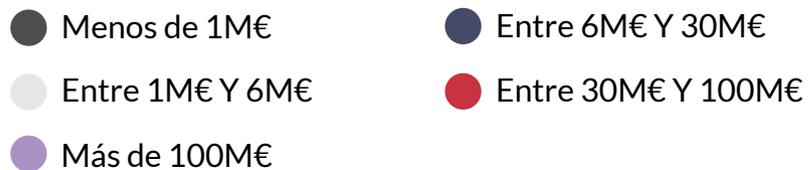
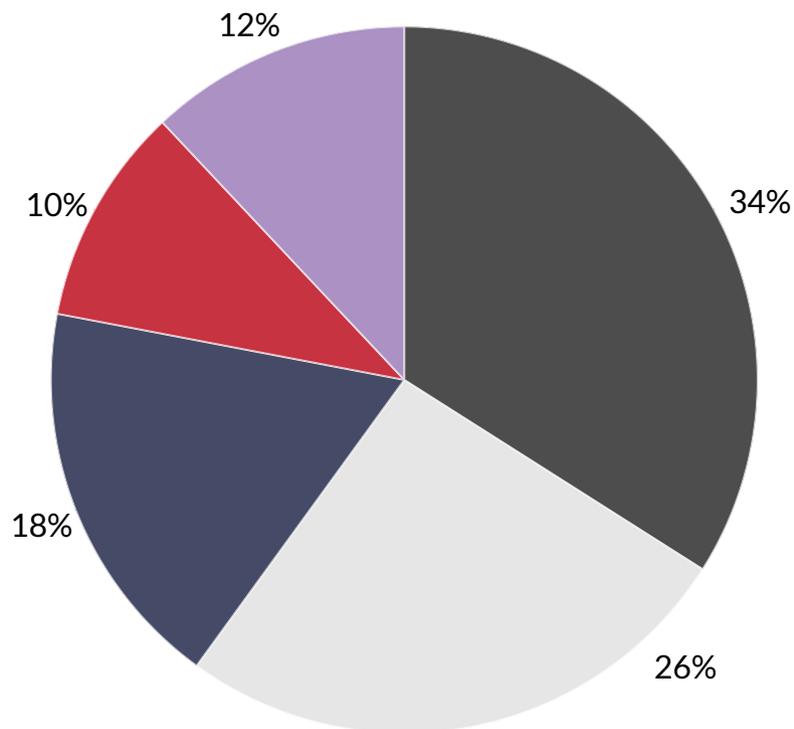
José Luis Zimmermann
Director general de Adigital

Caracterización de las empresas encuestadas



Informe realizado en base a una encuesta enviada a las más de 3.000 empresas de comercio electrónico asociadas a Adigital o adheridas a Confianza Online sobre el uso de los distintos medios de pago y la gestión del fraude online. Las respuestas válidas ascendieron a 250.

Facturación de las empresas encuestadas

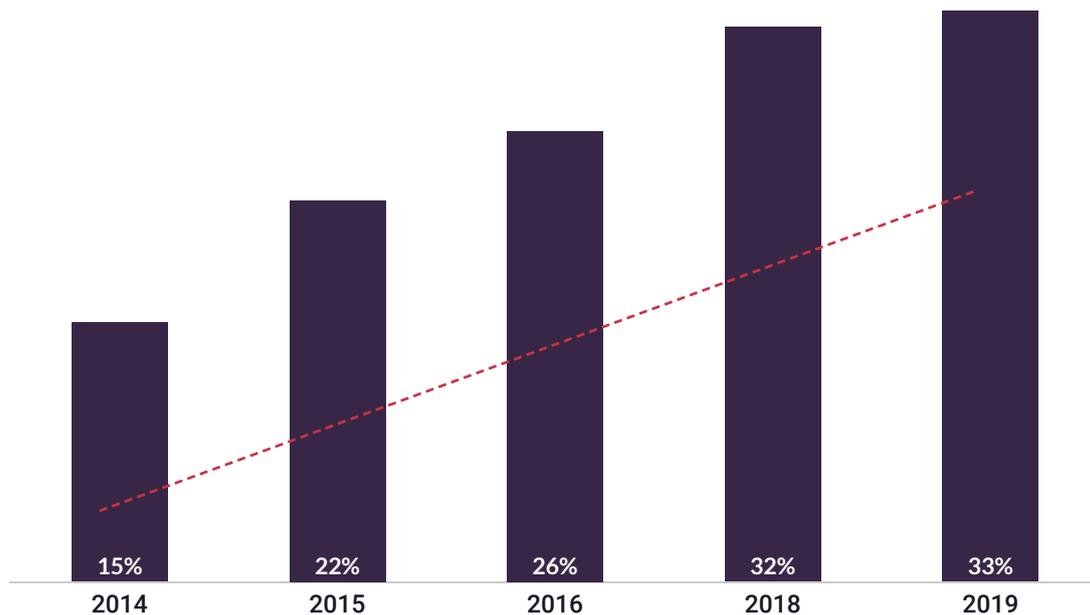




Porcentaje de facturación
proveniente de
dispositivos móviles

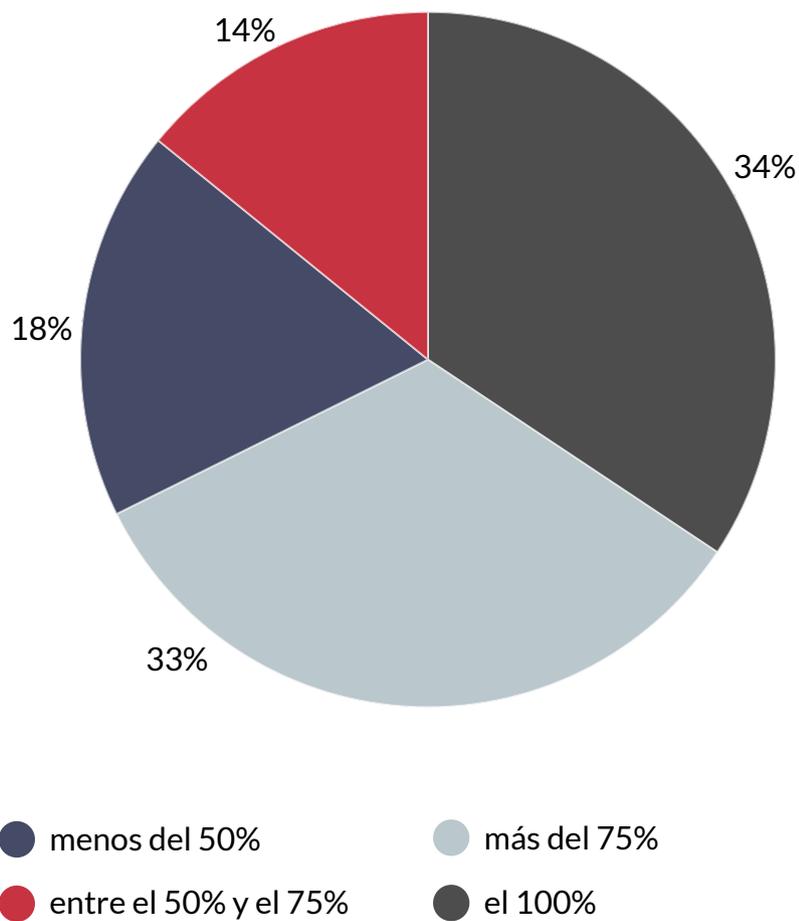
33%

Evolución de la facturación procedente de dispositivos móviles (%)



•• La facturación procedente de *mobile* continúa con su tendencia ascendente: aumenta un 1% frente a 2018.

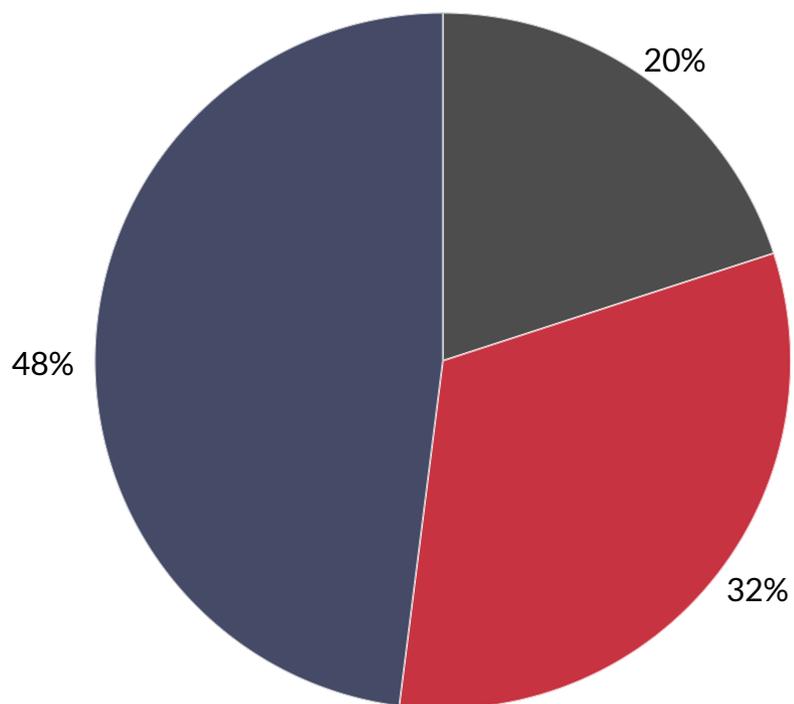
Porcentaje de facturación en España de las empresas encuestadas



Sistema de Procesamiento de Pagos

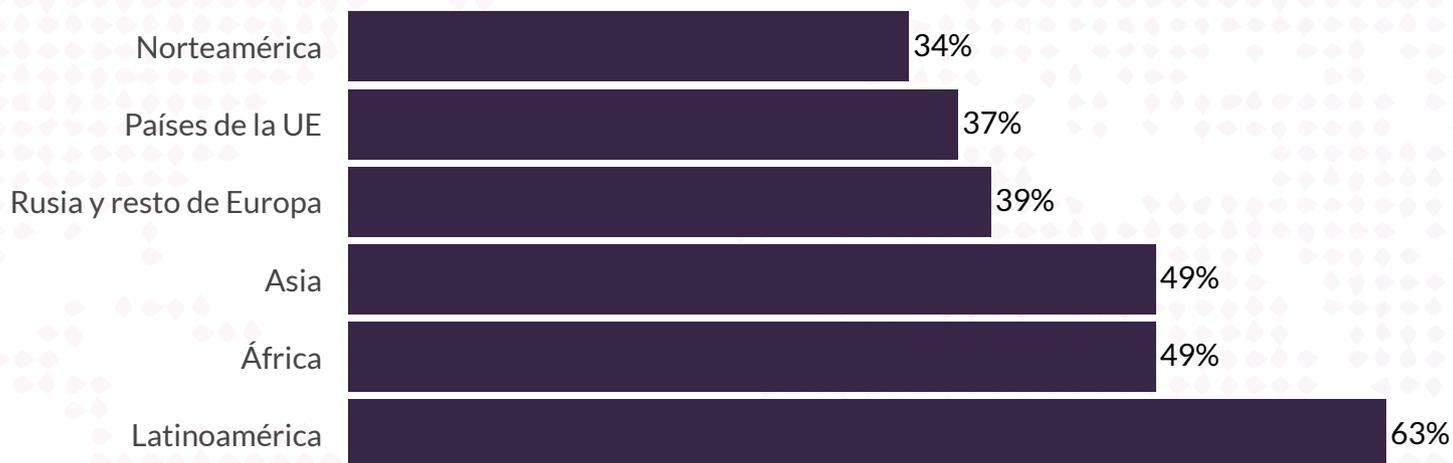
- › El 80% de las empresas acepta pagos de otros países
- › El banco sigue siendo el principal proveedor usado para el procesamiento de pagos

Empresas que aceptan pagos de otros países



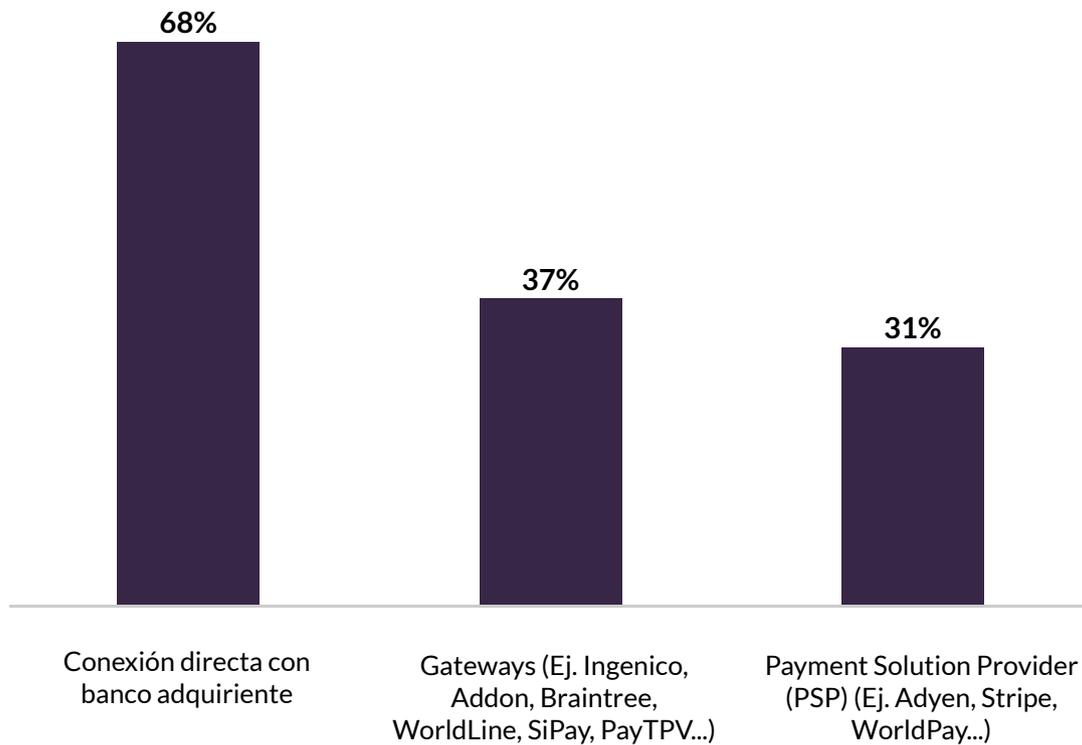
- No
- Sí, pero con excepciones
- Sí, siempre

Excepciones: Empresas que no aceptan pagos desde las siguientes regiones/países (%)

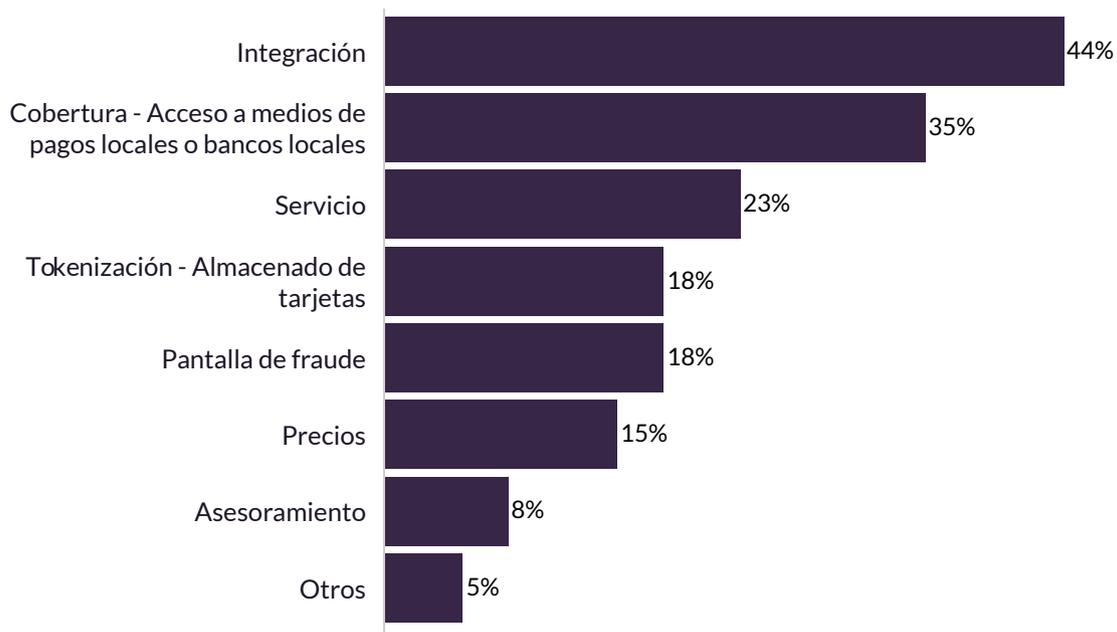




Tipo de proveedor usado para el procesamiento de pagos



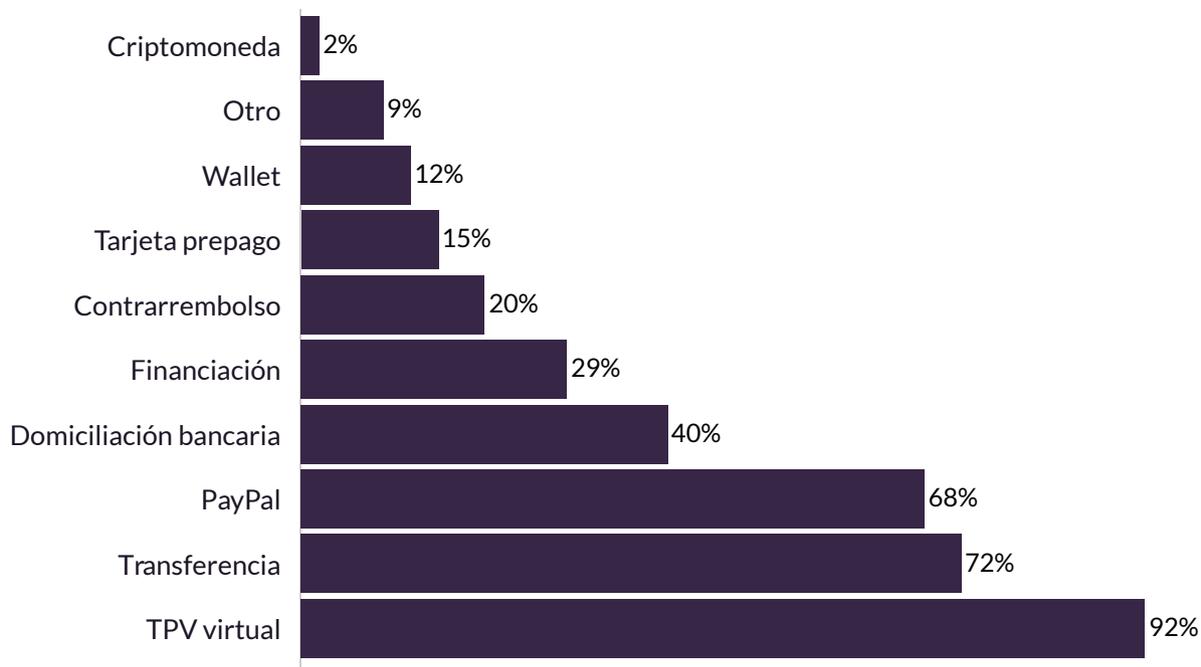
Motivos para utilizar PSPs y/o Gateways



Medios de Pago

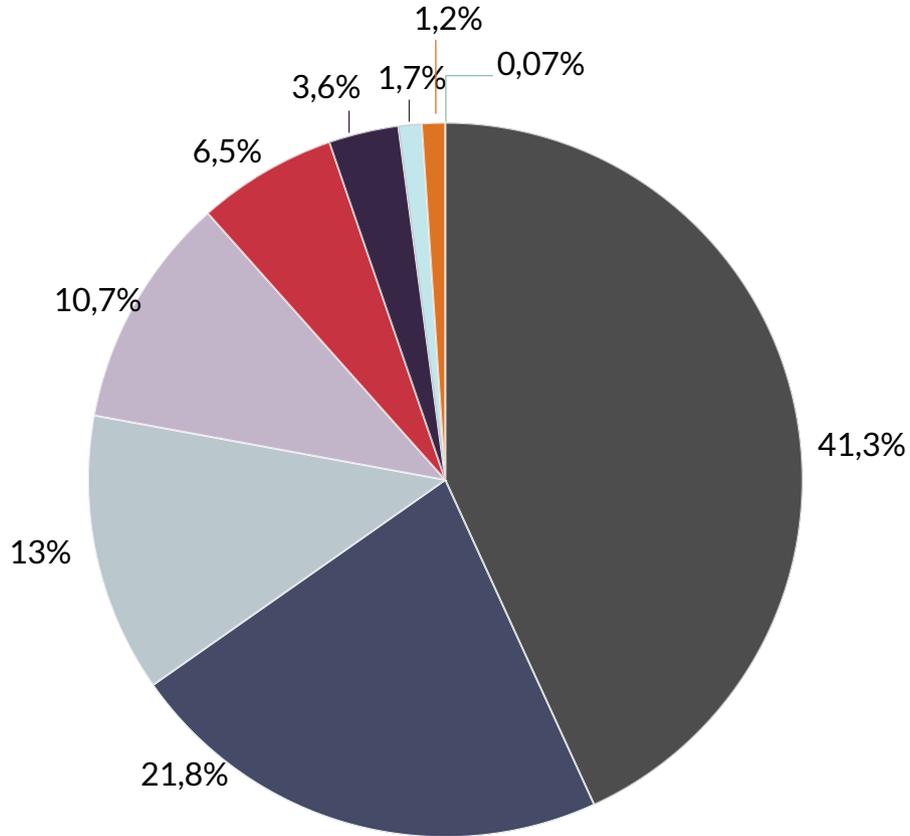
- › 41% de las transacciones se realizan con tarjeta, que continúa a la cabeza
- › El *wallet* ya representa un 1,20% frente al 0,36% de 2018

Métodos de pago ofrecidos por la empresa



- Los tres medios de pago más utilizados siguen siendo las Tarjetas (TPV Virtual), las Transferencias y PayPal.
- Destaca el descenso del Contrarrembolso, con una caída del 36%, y la tarjeta de prepago que desciende un 6%. Y, frente a ello, el crecimiento de otras opciones como el Wallet.

Reparto de las transacciones por medio de pago



● TPV virtual

● Tránsito

● PayPal

● Domiciliación bancaria

● Financiación

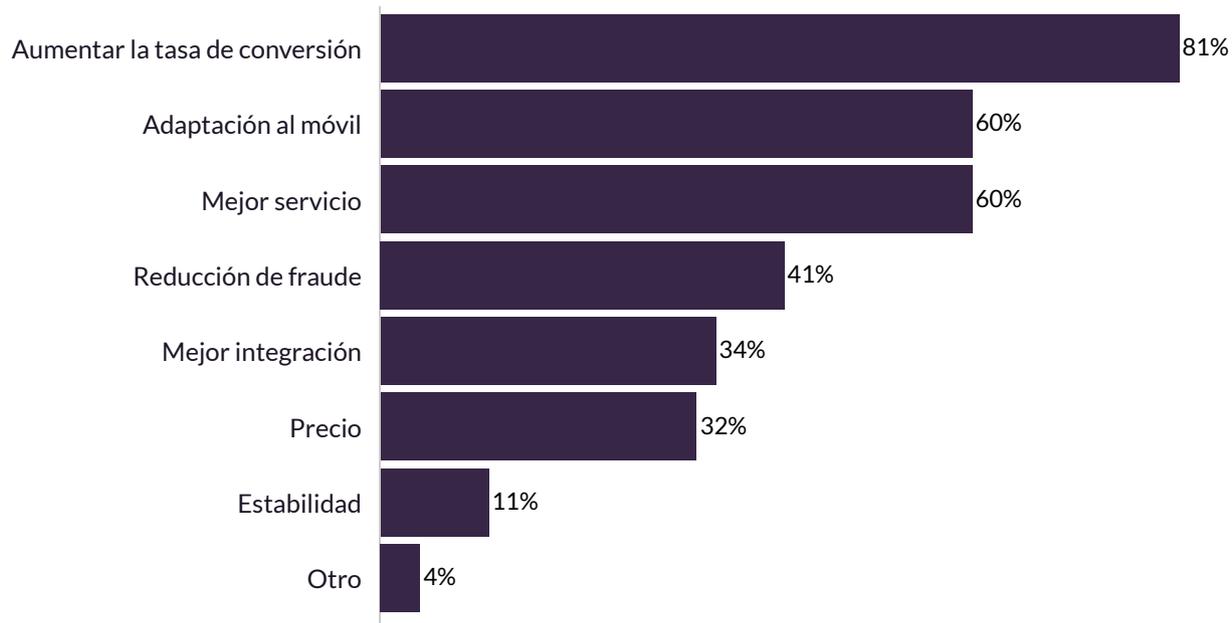
● Tarjeta Prepago

● Contrarrembolso

● Wallet

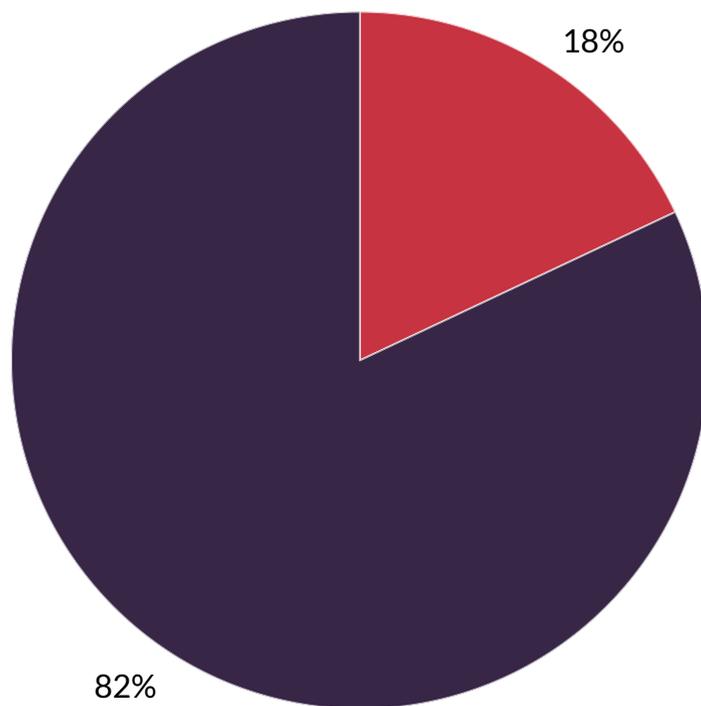
● Criptomonedas

Razones para cambiar de medios de pago



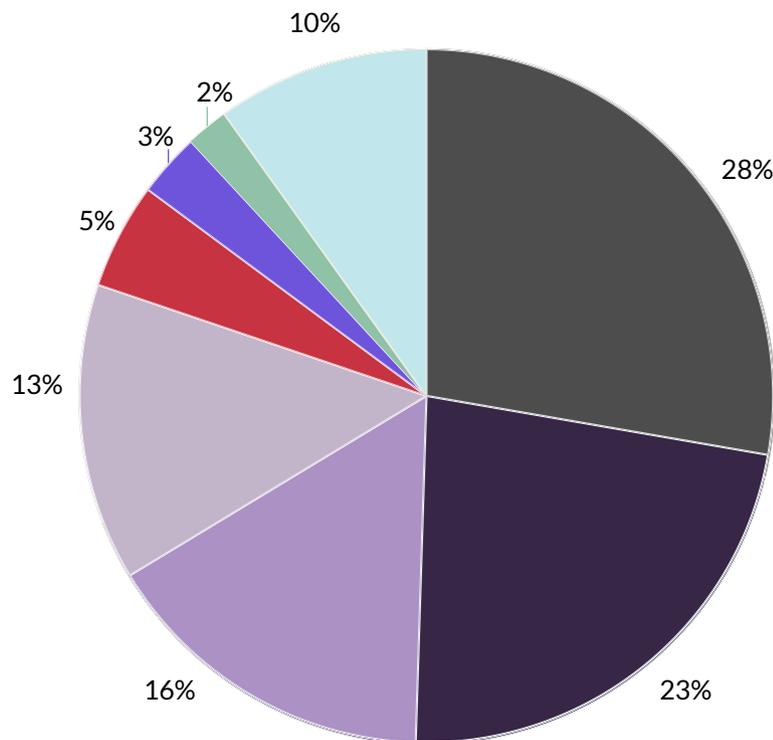
- Las tres razones para cambiar de medio de pago que más pesan son el aumento de la tasa de conversión, la adaptación a versión v y ofrecer un mejor servicio.
- Pierde importancia el precio y destaca positivamente la búsqueda de una reducción del fraude, que crece un 36% con respecto a 2018.

Empresas que cargan un
sobrepeso al cliente por el uso
de algún medio de pago específico



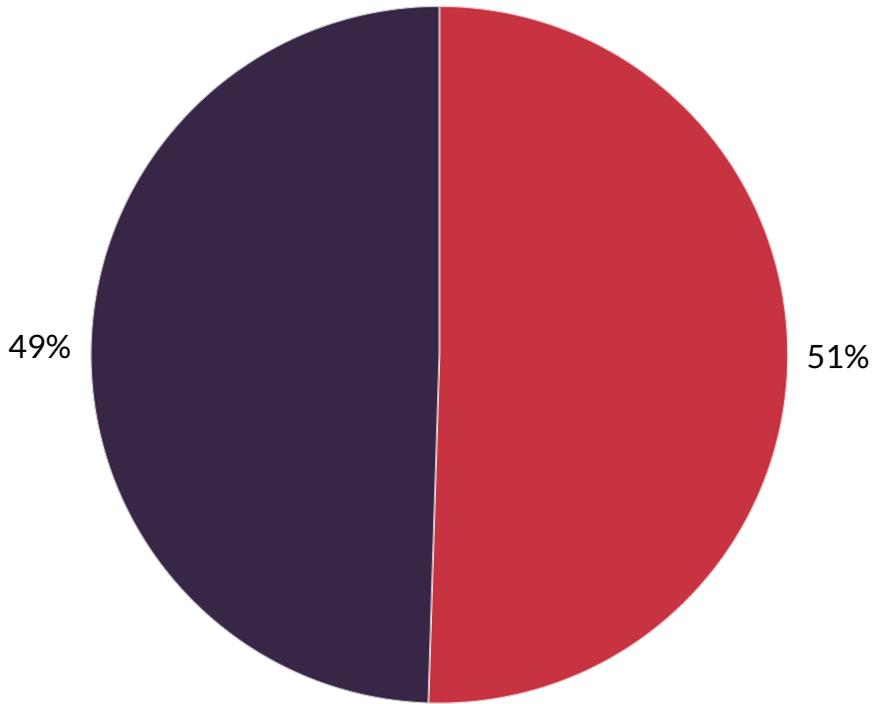
- Sí
- No

Principales bancos adquirientes con los que trabaja la empresa en España



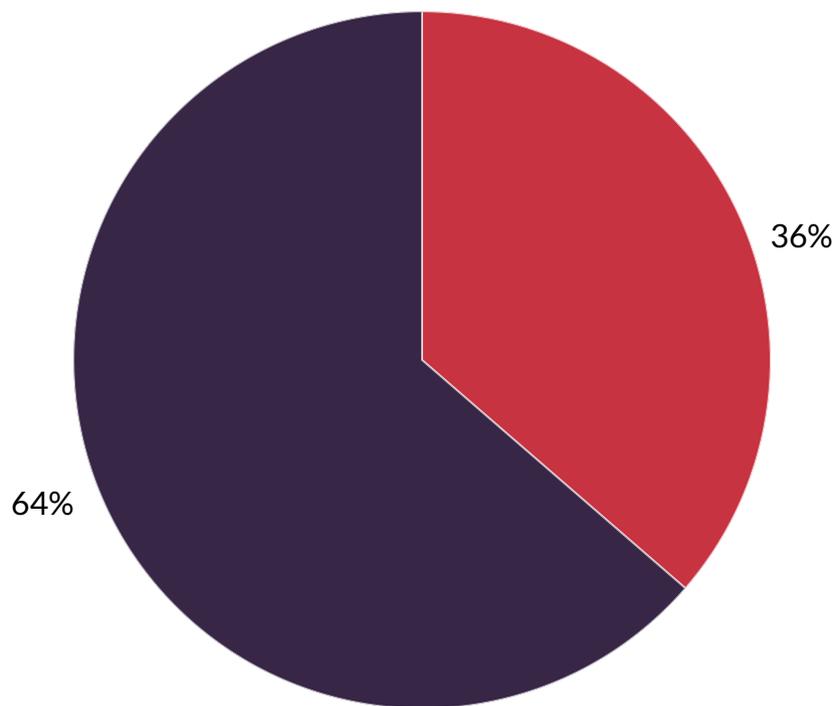
- Banc Sabadell
- CaixaBank
- Santander
- Bankia
- Universal Payments (Popular)
- Bankinter
- BBVA - Catalunya Caixa
- Otro

Empresas que realizan algún seguimiento de la tasa de conversión de los pagos de forma periódica



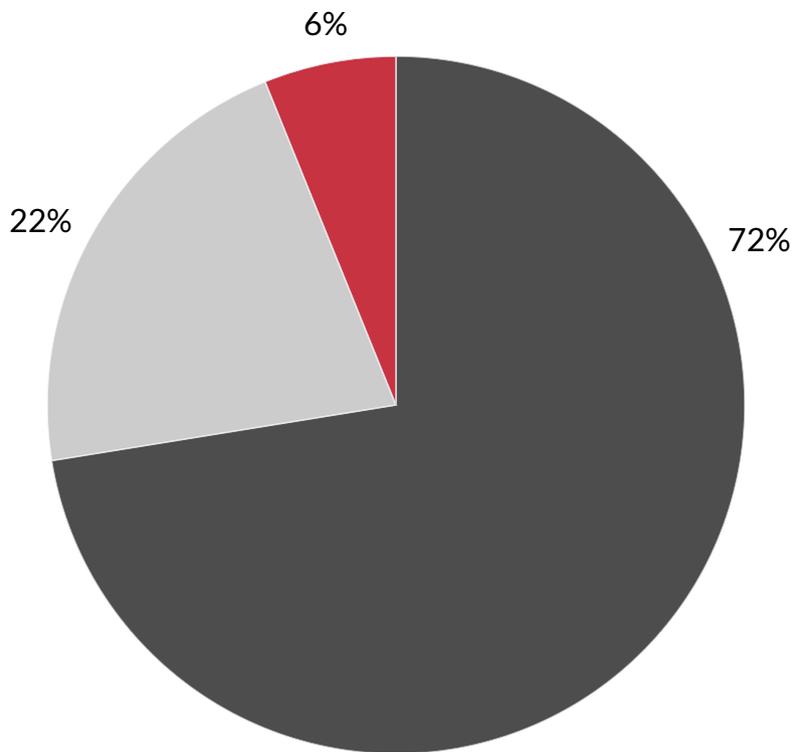
- Sí
- No

Empresas que afirman tener un proceso para disputar los chargebacks o contracargos con el banco



- Sí
- No

Chargebacks o contracargos que reciben las empresas de su banco (% frente a las transacciones totales)

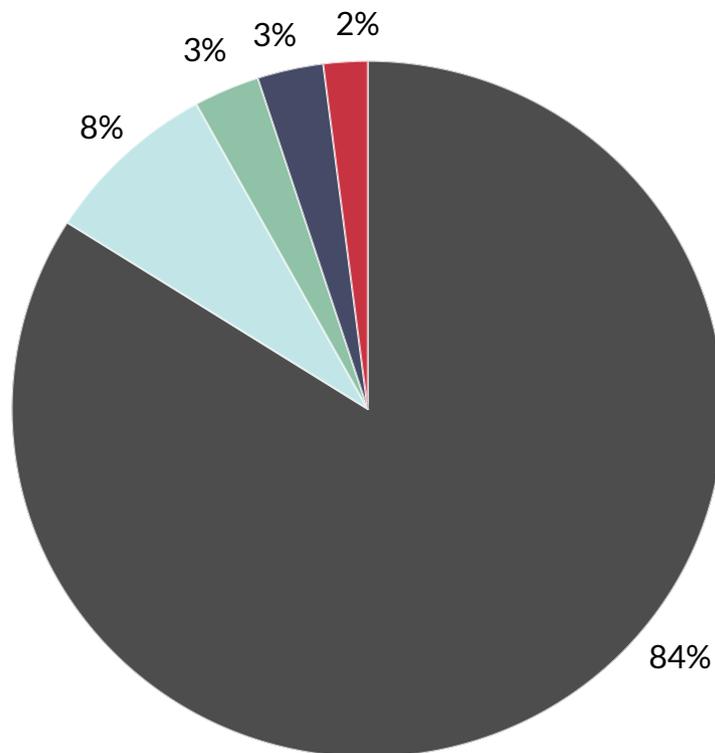


- Menos de 0,2%
- Entre 0,2% y 0,5%
- Más de 0,5%

Gestión del Fraude Online

- › La gran mayoría de las empresas (91,8%) declara un nivel de fraude inferior al 0,5%
- › También aumenta en un 35% el número de empresas que utilizan sistemas de gestión del fraude online

Tasa de fraude anual (*)



● Menos del 0,25%

● Entre el 0,25% y el 0,5%

● Entre el 0,5% y el 1%

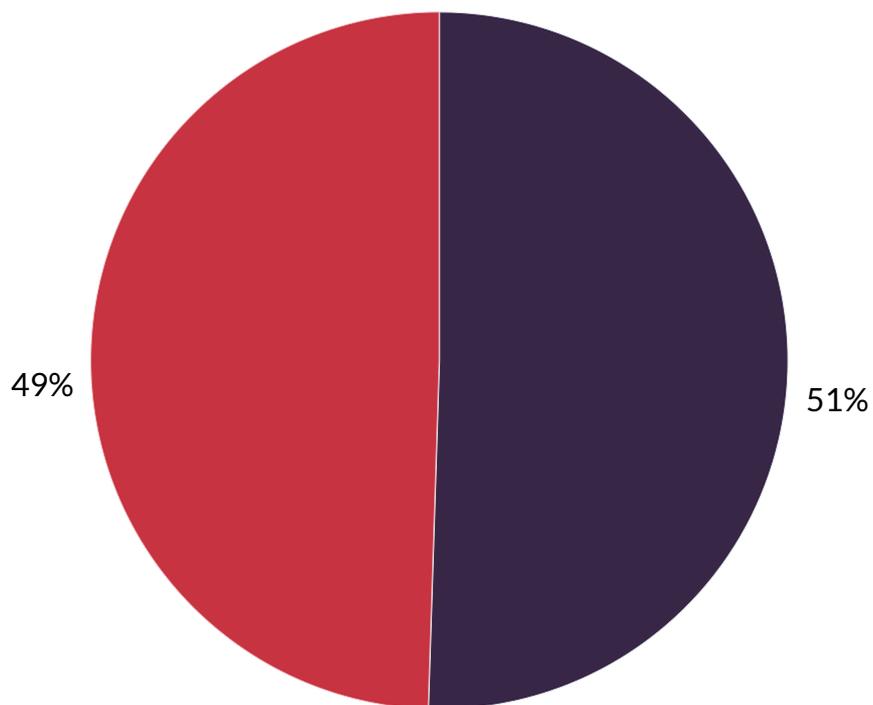
● Entre el 1% y el 2%

● Más del 2%

■ Aumenta en un 13,4% el número de empresas que tienen una tasa de fraude anual menor al 0,25% .

(*)Medido en porcentaje sobre la facturación, incluyendo contracargos y transacciones bloqueadas por riesgo de fraude.

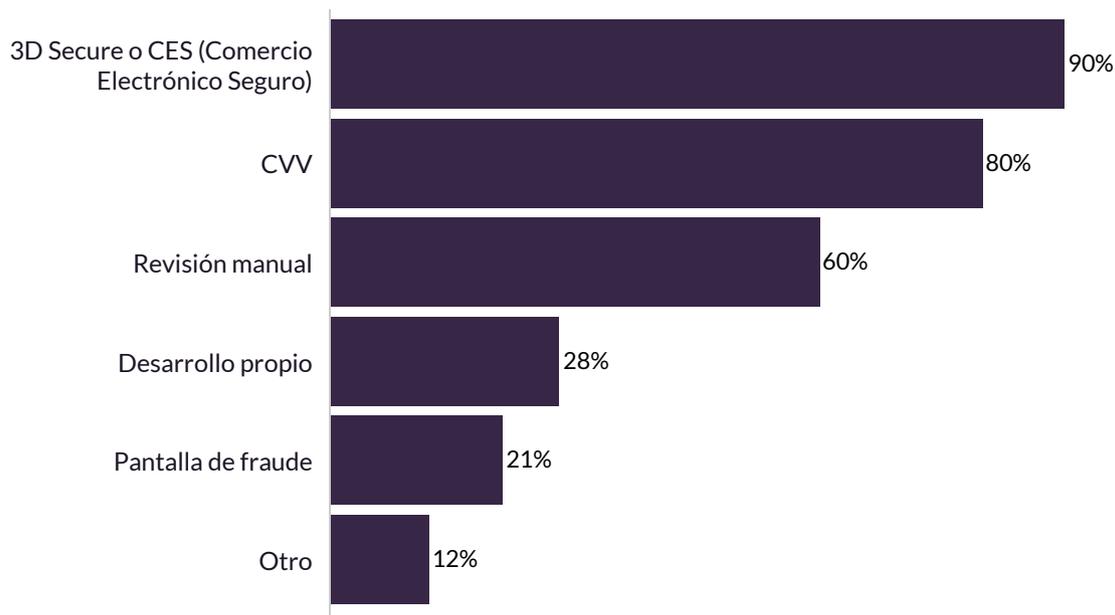
Empresas que utilizan un sistema de gestión del fraude online



- Sí
- No

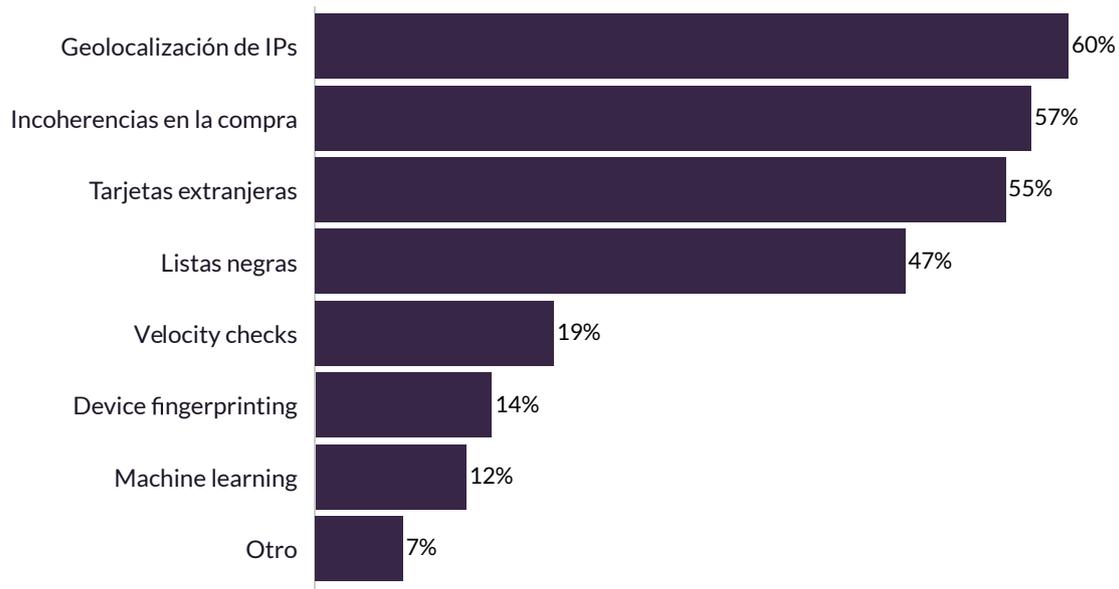
•• El porcentaje de empresas que sí utilizan un sistema de gestión de fraude crece un 35% con respecto a 2018.

Sistemas utilizados para la gestión del fraude



- Acompañando al incremento del número de empresas que emplean algún sistema para la gestión del fraude, crece también el uso de todos los sistemas de gestión.
- Destacan el aumento en el uso de pantallas de fraude y desarrollos propios, aunque el ranking de los sistemas más usados lo lideran 3D Secure o CES y CVV.

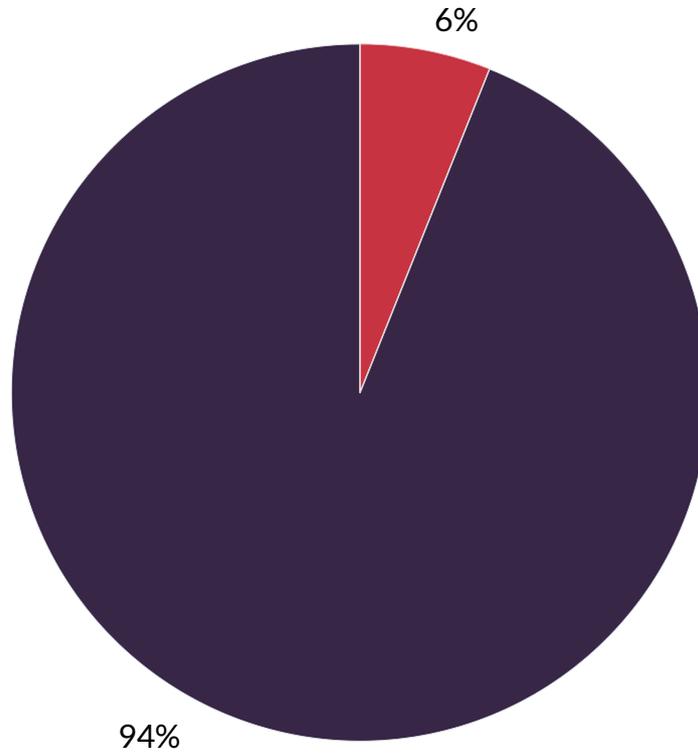
Acciones usadas para la detección de patrones de fraude



- Dentro de las acciones de detección del fraude, el uso de las incoherencias en la compra aumenta casi un 21% con respecto a 2018.

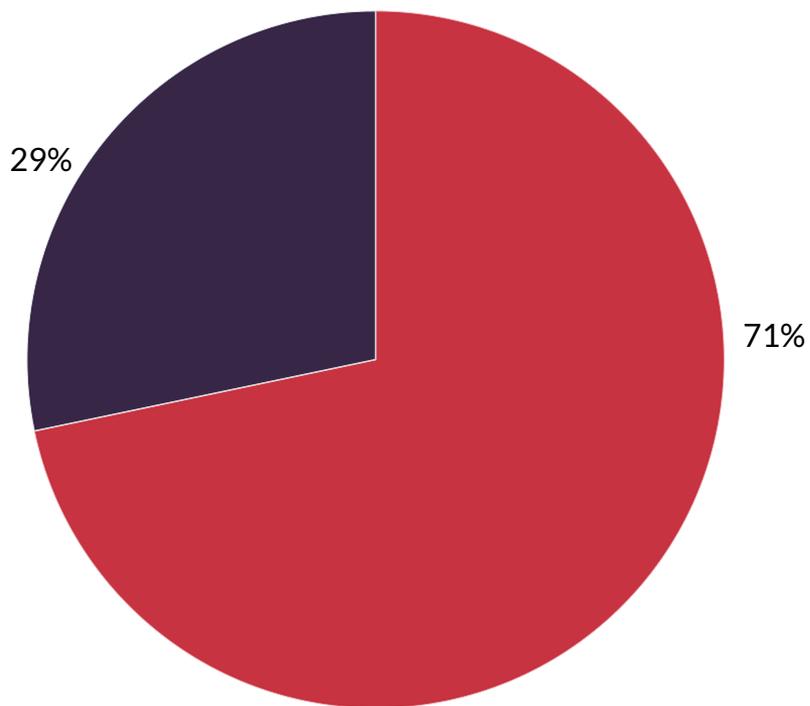


Empresas que han procesado transacciones con 3DS 2.0.



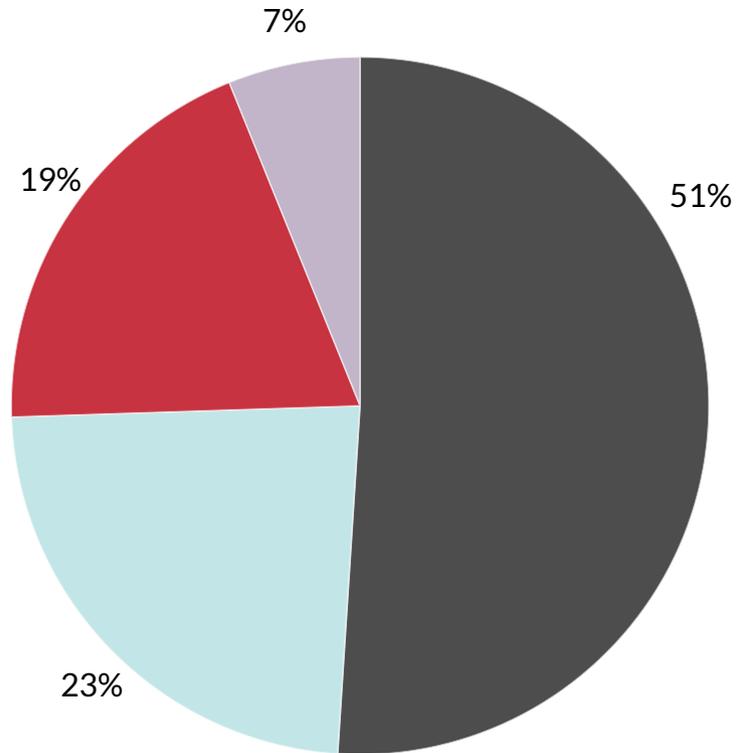
- Sí
- No

Empresas que han podido ver una mejora en la tasa de conversión de 3DS 2.0 (o 2.1.) vs 3DS 1.0

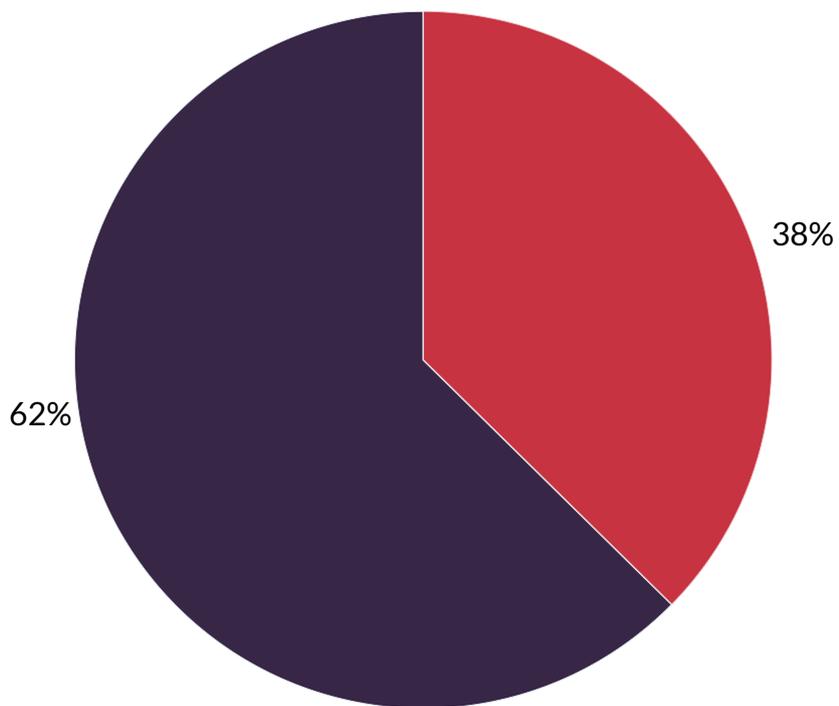


- Sí
- No

Áreas donde está ubicada la
responsabilidad de Pagos y
Fraude dentro de la empresa



Empresas que disponen
de un equipo dedicado a
gestionar pagos y fraude

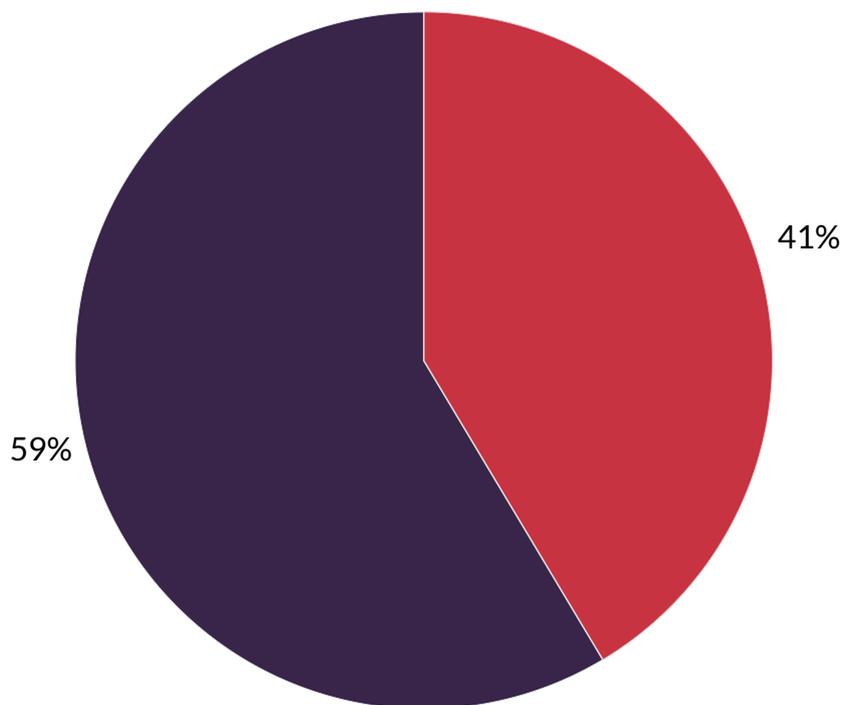


- Sí
- No

Regulación y Compliance

- › El 59% de las empresas encuestadas asegura desconocer las implicaciones de la PSD2.
- › El porcentaje es mayor (67%) entre las que no conocen los cambios que supone la SCA.

Empresas que conocen las implicaciones de la nueva normativa de medios de pago (PSD2) en el comercio electrónico

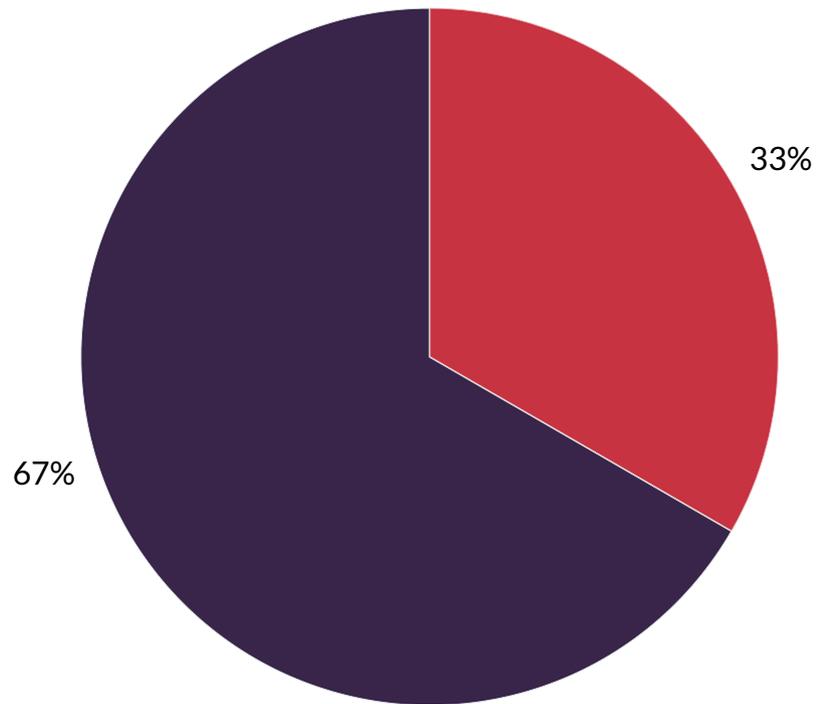


● Sí

● No

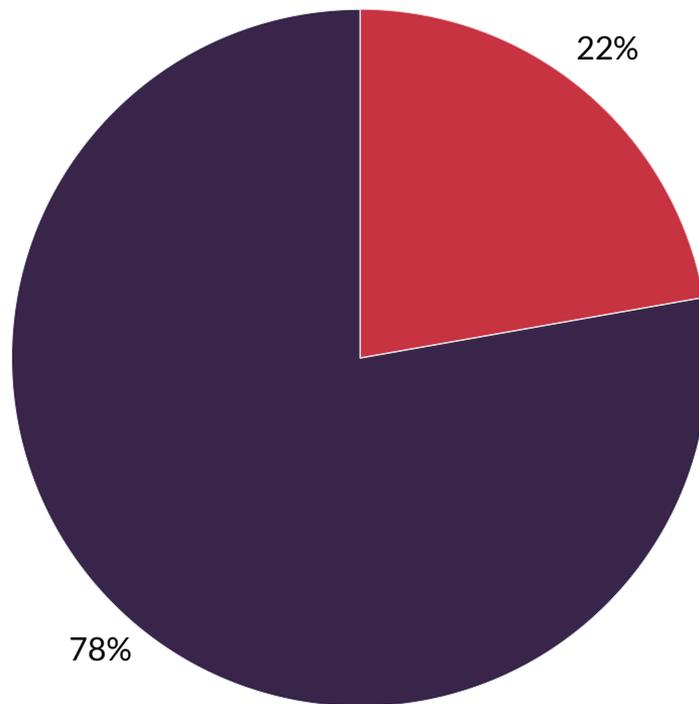
•• Pese a ser de aplicación desde 2018, este año aumenta el número de empresas que asegura desconocer las implicaciones de la normativa de medios de pago PSD2 en 9 puntos.

Empresas que conocen específicamente los cambios normativos en el proceso de autenticación de clientes (SCA)



- Sí
- No

Empresas que tienen una estrategia para minimizar el impacto de la SCA en sus ventas



- Sí
- No

Los retos regulatorios en medios de pago para 2019: después del 14 de septiembre

El día 14 de septiembre de 2019 se implementó en todos los países del Espacio Económico Europeo la Autenticación Fuerte de Usuario (SCA, por sus siglas en inglés), prevista dentro de la Segunda Directiva de Pagos.

Si bien es cierto que, especialmente durante las semanas previas, se habló mucho de esta medida y del impacto que iba a tener sobre quienes venden productos y servicios *online*, la realidad es que la forma de procesar transacciones *online* desde ese 14 de septiembre no ha cambiado en nada con respecto a la forma en que se hacía unos días antes. Por el contrario, la gran mayoría de comercios *online* han seguido procesando sus transacciones sin autenticar o con 3DS 1.0 –pese a ser formulaciones que no se ajustan a los Estándares Técnicos Regulatorios definidos previamente por la Autoridad Bancaria Europea –.

Y, sin embargo, esta falta de adaptación no ha tenido consecuencias, porque el mismo 14 de septiembre comenzaba a ser de aplicación una moratoria (de tiempo incierto en la fecha en que se escriben estas líneas) necesaria para evitar un problema de grandes dimensiones para compradores, bancos y comercios en el entorno *online*, dado que las posibles soluciones propias de la AFU no se habían implementado en cada uno de los pasos de la cadena de valor del pago *online*.

Implicaciones de la Autenticación Fuerte de Usuario

Uno de los principales objetivos de la Autenticación Fuerte de Usuario es mejorar la seguridad y protección de los usuarios en sus pagos *online*.

Según las asociaciones de banca, el porcentaje de transacciones fraudulentas con tarjetas

españolas en comercios españoles con procesamiento autenticado es del 0,022% frente al 0,069% en el caso de las transacciones no autenticadas. Por otro lado, este mismo estudio corrobora que el 72% de los comercios españoles aseguran tener un fraude por debajo del 0,2%. Los tres datos representan, sin duda alguna, ratios muy bajos, tanto si los comparamos con la presión fraudulenta de otros países, como si los evaluamos desde un punto de vista de la rentabilidad en el comercio. Por tanto, un objetivo cuantitativamente tan pequeño como reducir estos niveles de fraude no tendría que generar efectos secundarios negativos, dado que correríamos el riesgo que el balance final no fuera positivo.

Si elevamos un poco la mirada y vemos cual es la tendencia en los pagos globales, estos evolucionan hacia formatos más convenientes para el usuario, más instantáneos en los procesos y más invisibles para todos. Desde las transacciones iniciadas por comercios hasta los sistemas de identificación basados en el comportamiento previo del pagador, nos referimos a modalidades de pago que mejoran la experiencia de usuario y, por tanto, también las tasas de conversión y los ingresos de los comercios. El riesgo que la industria corre si se produce una implementación deficiente de la AFU es el de revertir esta tendencia, añadiendo más fricción al proceso de pago al forzar al consumidor a autenticarse de formas que puedan llegar a tener impacto en la conversión.

De este modo, cuando la EBA determina que los “datos de la tarjeta + cvv + *one time password*” no se ajustan a los requisitos que ella misma había determinado para el AFU, está aumentando el riesgo de acabar generando procesos de pago demasiado engorrosos, largos y complicados, con el consiguiente abandono del usuario. Basta con recordar que, hace unos años, en la encuesta a los comercios que realizó Adigital, estos declaraban que el uso de un solo factor de autenticación llegaba a tener un impacto negativo en la tasa de conversión de 18 puntos.

Como es lógico el objetivo de la normativa no era perjudicar el *ecommerce* europeo frente al no europeo, por lo que el propio desarrollo de los estándares regulatorios abría dos grandes posibilidades para evitar una ficción innecesaria en la autenticación de los usuarios.

a) De una parte, las exenciones relacionadas con el bajo riesgo fraudulento (bajo importe, pagos recurrentes, *Transaction Risk Analysis*, comercios de confianza...) que debe solicitar el comercio para que el banco emisor no fuerce al titular del medio de pago a realizar una autenticación;

b) De otra, la posibilidad de que el banco emisor pueda no realizar *de motu proprio* el “challenge” de la doble autenticación en base a los datos del historial del usuario (*risk based analysis*).

Desgraciadamente estas dos posibilidades aún requieren de muchísimo desarrollo por parte de los emisores de los métodos de pago. Es más, es muy probable que, de haberse lanzado la SCA el 14 de septiembre, la aplicación real de las mismas hubiera sido insignificante.

Ahora bien, ¿estaremos preparados una vez finalice la moratoria?

Lo iremos viendo durante estos meses pero es de esperar que los bancos emisores prioricen asegurar que todos sus clientes puedan comprar cuando el cumplimiento de la AFU sea exhaustivo. Es lógico suponer que concentrarán sus esfuerzos en garantizar que sus clientes puedan llegar a comprar *online*, implementando los dos factores de autenticación para todas las tipologías de usuarios y medios de pago.

Se corre el riesgo de que las dos salvaguardas que tienen que limitar el impacto de una fricción excesiva y/o innecesaria en el comercio queden relegadas en los *pipelines* de desarrollo de las entidades emisoras. Por eso, la importancia de alargar los plazos de la moratoria.

Durante el proceso de negociación de la moratoria a nivel nacional, Adigital ha representado al comercio electrónico en la Comisión de Pagos del Banco de España. Con el objetivo de evitar un impacto negativo en los *ecommerce*, la Asociación ha abogado por una moratoria lo

suficientemente amplia y armonizada con el resto de países europeos (18 meses) y que se mantuviera el *statu quo* previo al 14 de septiembre de 2019.

Sean los meses que sean los que, finalmente, la EBA determine como moratoria, volverán a ser intensos para el *ecommerce* europeo, preocupado por encontrar el equilibrio perfecto entre la gestión del fraude y las conversiones de su página web.

Marc Nieto
Advisor of Payments & Fraud, Adigital.
Miembro del European Payments Council for Cards Fraud Prevention Forum



Adigital es la Asociación Española de la Economía Digital. Formada por más de 500 asociados, tiene como objetivo promover y apoyar la economía digital en España en sus diferentes aspectos, como son el desarrollo de los servicios de la sociedad de la información, el comercio electrónico, marketing y comunicación digital, las aplicaciones móviles, los contenidos digitales, la publicidad digital y otras actividades conexas como son los servicios de contact center, agencias y redes de publicidad, logística o medios de pago.

Adigital es socio, junto con Autocontrol, de Confianza Online, sello de calidad al que están adheridas más de 2.000 empresas y presente en más de 2.600 sites.



Es una asociación creada en 2003 por la Asociación para la Autorregulación de la Comunicación Comercial (AUTOCONTROL) y la Asociación de la Economía Digital (Adigital) con el fin de aumentar la confianza de los usuarios en Internet a través de su Sello, que se otorga a las empresas tras un profundo análisis legal. Cuenta con más de 2.700 webs adheridas que se comprometen a atender las reclamaciones a través de un sistema rápido y eficaz de mediación entre consumidor y empresa, sin ningún coste para el usuario. Este sistema cuenta con el respaldo institucional ya que utiliza los dos sistemas extrajudiciales de resolución de controversias reconocidos en España por la Comisión Europea y que forman parte de la EEJ Net: el Sistema Arbitral Nacional de Consumo y Jurado de la Publicidad de AUTOCONTROL.



