

Medios de pago online

Emilio Raya López



Revista Digital de ACTA

2021

Publicación patrocinada por



ACTA representa en CEDRO los intereses de los autores científico-técnicos y académicos. Ser socio de ACTA es gratuito.

Solicite su adhesión en acta@acta.es

Medios de pago online

© 2021, Emilio Raya López

© 2021, 

Cualquier forma de reproducción, distribución, comunicación pública o transformación de esta obra solo puede ser realizada con la autorización de sus titulares, salvo excepción prevista por la ley.

Se autorizan los enlaces a este artículo.

ACTA no se hace responsable de las opiniones personales reflejadas en este artículo

La gente necesita servicios de banca, pero no necesariamente bancos.

Asociación Española de Fintech

INTRODUCCIÓN

Los medios o instrumentos de pago son aquellos mecanismos comúnmente aceptados en el mercado para satisfacer económicamente la compra o adquisición de determinados bienes o servicios. Como vemos, debe tratarse de mecanismos admitidos de forma general o extendida, ya sea por otros particulares, por una entidad comercial, por la administración pública o por cualquier otra institución.

En el inicio de la historia de la humanidad, el medio de pago más común fue el trueque, en el que las mercancías se intercambiaban entre sí. De esa forma, cada parte interviniente en una transacción ofrecía un cierto producto (cereales, pieles de animales, alimentos, etc.) o la realización de un servicio (cierta tarea como por ejemplo trabajar la tierra) como pago por otro determinado producto o servicio.

Más adelante y durante mucho tiempo, el medio de pago general y comúnmente utilizado fue el dinero en efectivo -monedas y billetes-, suplido, o más bien complementado, con el paso del tiempo por fórmulas de crédito -como tarjetas bancarias de crédito o débito fundamentalmente y por medios de pago entre empresas -con las letras de cambio o pagarés como ejemplo-.

En fechas mucho más recientes, la evolución de las tecnologías de la información y las comunicaciones han propiciado que un gran número de transacciones comerciales se realicen, a día de hoy, de forma digital, en internet. De esa forma, esas mismas tecnologías han permitido la aparición de medios de pago online, esto es, aquellos que por sus características pueden ser utilizados en cualquier transacción online de comercio electrónico por medio de internet.



Figura 1. Las compras en internet, en expansión (<https://elobservatoriocetelem.es/>).

En este sentido, no podemos perder de vista que el comercio electrónico a través de internet es todavía a día de hoy una tendencia en clara expansión. Adicionalmente, sumado a esto, la situación de pandemia por coronavirus sufrida a lo largo de los últimos meses, ha supuesto un empujón al uso de este tipo de transacciones online -ampliando tanto el número de usuarios como de entidades comerciales que se han añadido a esta práctica-.

De manera adicional, la enorme difusión del uso de terminales móviles, ha hecho que se hagan presentes en prácticamente la totalidad de las actividades de nuestra vida cotidiana -presencia en redes sociales, seguimiento de actividad física, agenda digital, accesos a herramientas profesionales, etc.-, incluyendo también, como no podía ser de otra forma, el pago por compras y servicios, tanto en internet como en muchos establecimientos.

Como respuesta a esta importante evolución tecnológica, la Unión Europea -UE- se ha esforzado en conseguir un efectivo desarrollo de un mercado único integrado de pagos electrónicos seguros, como mecanismo esencial para apoyar el crecimiento de la economía de la Unión y para garantizar que los consumidores, los comerciantes y las empresas en general disfruten de posibilidades de elección y condiciones de transparencia en los servicios de pago, de modo que puedan aprovechar plenamente las ventajas del mercado interior.



Figura 2. Medios de pago.

De acuerdo con todo lo anterior, este artículo se centra, fundamentalmente, en aportar una perspectiva actual de los medios de pago online. Para ello, inicialmente se realiza una revisión de la normativa europea aplicable en la materia para, posteriormente, presentar y describir los principales aspectos de los medios de pago online, el pago mediante dispositivos móviles -o *smartphones*- y las soluciones que, a día de hoy, permiten la transferencia de dinero entre particulares. Finalmente, a modo de conclusión, se añade una visión futura de un mundo en constante y rápida evolución.

REGULACIÓN NORMATIVA AL RESPECTO DE LOS SERVICIOS DE PAGO

En el mercado único de la Unión Europea -UE- las personas, las mercancías, los servicios y el dinero pueden circular libremente. Eso supone que los ciudadanos de la UE pueden estudiar, vivir,

hacer compras, trabajar y jubilarse en cualquier país de la unión, además de disfrutar de productos de toda Europa.

Acorde con esto, la Unión Europea consideró conveniente, en el año 2007, aprobar la Directiva 2007/64/CE sobre servicios de pago en el mercado interior, habitualmente conocida *Payment Services Directive* o *PSD* por sus siglas en inglés, con el objetivo de contribuir al desarrollo de un mercado único de pagos en la Unión Europea, y fomentar así la innovación, la competencia y la eficiencia en dicho sector en el territorio comunitario.

Tal y como reconoce dicha Directiva en su exposición de motivos, resulta fundamental, para el establecimiento del mercado interior, que desaparezcan todas las fronteras internas de la Unión, a fin de permitir la libre circulación de bienes, personas, servicios y capitales. Para ello es vital el correcto funcionamiento del mercado único de los servicios de pago. Sin embargo, en la actualidad -año 2007, momento en el que se aprueba la mencionada *PSD*-, la falta de armonización en este ámbito impide el funcionamiento de dicho mercado.

Pasados unos años y a la vista de los avances logrados con la aplicación de la *PSD*, en 2013, la Comisión Europea propuso una revisión de dicha normativa, buscando ahondar en los ya mencionados objetivos: mejora de la protección y seguridad del consumidor, impulso de la competencia e innovación en el sector, junto con el refuerzo de la seguridad en el mercado de pagos, lo que se espera que favorezca el surgimiento de nuevos métodos de pago y fomente, de esa forma, el comercio electrónico.

De acuerdo con esto, se aprobó la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015, sobre servicios de pago en el mercado interior, que representa, actualmente, la base de la regulación europea en el ámbito de los servicios de pago electrónicos.

Conocida como *PSD2* por sus siglas en inglés -*Payment Services Directive*-, viene a sustituir, como ya se ha mencionado, a la Directiva 2007/64/CE, modificando además las Directivas 2002/65/CE, 2009/110/CE y 2013/36/UE, junto con el Reglamento (UE) 1093/2010.



Figura 3. *Payment Services Directive, PSD2*

En España, el Real Decreto-Ley de servicios de pago y otras medidas urgentes en materia financiera transpone varias directivas europeas, entre ellas la *PSD2*, desarrollando el régimen jurídico

de las entidades de pago, el régimen específico de los nuevos proveedores, junto con las competencias del Banco de España en materia de autorización y registro. De forma específica, mejora la protección de los clientes de servicios de pago actuando en tres ámbitos.

- Se establece un procedimiento de autorización para los iniciadores de servicios de pago, y de registro para los agregadores de pagos -figuras que más adelante se describirán-, que pasarán a ser regulados y supervisados por el Banco de España.
- Se aumentan los requisitos de seguridad en la prestación de estos servicios. Las entidades de pago deberán disponer de una política de seguridad y un procedimiento para la supervisión, tramitación y seguimiento de los incidentes de seguridad y las reclamaciones de los usuarios.
- Las entidades de pago y dinero electrónico que concedan créditos deberán cumplir la normativa de transparencia bancaria, lo que redundará en una mayor protección para los clientes de servicios de pago que adicionalmente soliciten un crédito.

Para asegurar que las entidades de pago cumplen las normas de conducta, transparencia y protección establecidas, el Real Decreto establece que el Banco de España podrá solicitar la información que considere necesaria, para poder hacer efectivas tales tareas de supervisión que tiene encomendadas.

Asimismo, el nuevo marco jurídico de autorizaciones que se establece en el Real Decreto favorece la competencia, ya que permite la prestación de nuevos servicios y la incorporación de nuevos proveedores para realizar el ejercicio de su prestación. De forma específica, las entidades de dinero electrónico podrán realizar servicios de pago en las mismas condiciones que las propias entidades de pago.

Finalmente, se sigue avanzando en el fomento de la innovación en los servicios de pago, lo que constituye uno de los principales objetivos de la Directiva comunitaria. Para ello se establece el procedimiento de registro sin necesidad de autorización para las entidades de pago de pequeño tamaño -las denominadas *Small Payments Institutions*- lo que favorecerá la aparición de empresas innovadoras en el sector.

OBJETIVO DE LA PSD2: APERTURA Y COMPETENCIA EN SERVICIOS DE PAGO

Como se ha mencionado, el objetivo de la Directiva (UE) 2015/2366 de servicios de pago -PSD2- es aumentar la seguridad de los pagos en Europa, promover la innovación y favorecer la adaptación de los servicios bancarios a las nuevas tecnologías.

De esa forma, pese a que, probablemente, muchas de las implicaciones que traerán los cambios introducidos por la PSD2 son, a día de hoy, desconocidas, hay una que está resultando fundamental: la apertura por parte de los bancos de sus servicios de pagos a terceras empresas, los denominados TPPs -*Third Party Payment Service Providers*- o nuevos proveedores de servicios de pago.

Hasta fechas relativamente recientes, los servicios de pago han sido cosa, prácticamente en exclusiva, de las entidades bancarias. Los TPPs -nuevos proveedores de servicios de pago- se en-

contraban múltiples obstáculos que les impedían ofrecer sus soluciones a gran escala en los distintos estados de la Unión Europea. De esa forma, la *PSD2* busca la eliminación de estas barreras, para conseguir una mayor competencia con la entrada de nuevos actores y la generalización de la provisión de estos servicios por parte de los actores ya existentes. En contraprestación, los *TPPs* tendrán que cumplir con las mismas reglas que los proveedores de servicios de pago tradicionales, es decir, la necesidad de registro y autorización, junto con el sometimiento a supervisión por las autoridades competentes.

De acuerdo con esto y más allá del reforzamiento de la seguridad para consumidores y clientes, la *PSD2* busca el fomento de la competencia y la innovación, mediante la apertura del sector a la aparición de nuevos actores -los denominados *TPPs* o nuevos proveedores de servicios de pago- en el mismo.

A nivel tecnológico, este cambio, que supone una importante necesidad de interconexión, pone de manifiesto, una vez más, la creciente importancia que está adquiriendo el mundo de las APIs o *Application Program Interface* en los distintos sectores financieros y bancarios. Más adelante, se aporta mayor detalle sobre la importancia del papel de estas piezas software de interconexión en la construcción de servicios de pago online.

PUNTOS CLAVE DE LA PSD2

Como mecanismo de apertura y búsqueda de ampliación de la competencia, la *PSD2* regula y armoniza dos clases de servicios que ya existían cuando se adoptó la primera *PSD* en 2007, pero que, no cabe duda, han proliferado y se han popularizando enormemente durante los últimos años:

- Los servicios de información de cuenta -*Account Information Services* o *AIS* en terminología inglesa-. Consistente en recoger y almacenar la información de las distintas cuentas bancarias de un cliente en un solo lugar, permitiendo, de esa forma, a los clientes tener una visión global de su situación financiera y analizar fácilmente sus gastos y sus necesidades financieras.
- Los servicios de iniciación de pagos -*Payment Initiation Services* o *PIS* en terminología inglesa-, en los que terceros proveedores facilitan el uso de la banca online para realizar pagos por internet. Estos servicios ayudan a iniciar un pago desde la cuenta del consumidor a la cuenta del comercio mediante la creación de una interfaz puente entre ambas cuentas, rellenando la información necesaria para la transferencia (cuantía de la transacción, número de cuenta, mensaje) e informando al comercio del inicio de la transacción. Asimismo, la *PSD2* también posibilita al cliente la realización de pagos a terceros desde la aplicación de un banco utilizando cualquiera de sus cuentas (pertenezcan o no a esa entidad).

De esa forma, como se detalla más adelante, la *PSD2* introduce la regulación de los actores o proveedores *TPPs* que realizan las actividades o prestan los dos servicios anteriormente descritos: *Account Information Services Provider* -*AISP*- y *Payment Initiation Services* -*PISP*- respectivamente. Tanto los *AISP* como los *PISP* son actores que realizan labores de intermediación entre los usuarios -clientes o consumidores- y las entidades bancarias -Proveedores de Servicios de Pago y Datos de Cuenta en terminología propia de la *PSD2*-.



Figura 4. AISP y TPSP, nuevos actores regulados por la PSD2

Adicionalmente, la otra gran novedad de la *PSD2* es la introducción de nuevos requisitos de seguridad, lo que se conoce como Autenticación Reforzada de Clientes -*Strong Customer Authentication* o *SCA* en inglés-. Esto implica el uso de dos factores de autenticación en operaciones bancarias que antes no lo requerían, incluyendo pagos con tarjeta, transferencias y acceso a cuentas online o a través de apps, así como una definición más estricta de lo que puede servir como factor de autenticación.

De esa forma, y tomando como ejemplo las compras *online* realizadas en internet, los clientes percibirán cambios en la forma en que autorizan dichas compras, fundamentalmente en los factores de autenticación que utilizan, ya que, al haberse convertido la autenticación reforzada en el nivel de seguridad exigido por defecto, han dejado de ser simplemente la información impresa en la tarjeta bancaria -nombre, número, caducidad y el código de verificación *CVV*- factores válidos para la autenticación.

PROVEEDORES DE SERVICIOS DE INFORMACIÓN DE CUENTA -AISP-

El artículo 4 de la Directiva *PSD2* define el servicio de información sobre cuentas, como aquel servicio en línea -*online*- cuya finalidad consiste en facilitar información agregada sobre una o varias cuentas de pago de las que es titular el usuario del servicio de pago, bien en otro proveedor de servicios de pago, bien en varios proveedores de servicios de pago. Lógicamente, actuarán como proveedor de servicios de información de cuentas aquellos agentes que realicen las actividades anteriores -como hemos visto, suelen ser conocidos como *AISP* o *Accounting Information Services Provider* por su acepción inglesa-.

Con la liberación de este servicio, el cliente, que realmente es el dueño (propietario) de los datos, puede dar permiso a terceros para operar u obtener información de cuentas que este tiene en otras entidades. De esta forma, las cuentas de tarjetas de crédito, las de inversión u otras pueden quedar anotadas en un solo lugar, como, por ejemplo, una aplicación externa al banco. Así, una de las utilidades más frecuentes de esta posibilidad abierta por la *PSD2* es conocer en todo momento y de forma rápida cuál es la situación de un determinado grupo de cuentas.

En cualquier caso, el artículo 67 de la *PSD2*, como mecanismo de protección y supervisión, establece un conjunto de normas que deben ser observadas por los proveedores de servicios de información sobre cuentas:

- a) prestarán sus servicios exclusivamente sobre la base del consentimiento explícito del usuario;
- b) garantizarán que las credenciales de seguridad personalizadas del usuario de servicios de pago no sean accesibles a terceros;
- c) en cada comunicación, se identificará ante el resto de actores intervinientes y se comunicará de manera segura con ellos;
- d) accederá únicamente a la información de las cuentas de pago designadas y las operaciones de pago correspondientes;
- e) no solicitará datos de pago sensibles vinculados a las cuentas de pago que gestione;
- f) no utilizará, almacenará o accederá a ningún dato, para fines distintos de la prestación del servicio de información sobre cuentas expresamente solicitado por el usuario, de conformidad con las normas sobre protección de datos.

PROVEEDOR DE SERVICIOS DE INICIACIÓN DE PAGOS -PISP-

El artículo 4 de la Directiva *PSD2* define el servicio de iniciación del pago como aquel servicio que permite iniciar una orden de pago, a petición del usuario del servicio de pago, respecto de una cuenta de pago abierta con otro proveedor de servicios de pago. Y, lógicamente, la directiva define al proveedor de servicios de iniciación de pagos como aquel que ejerce, a título profesional, estas actividades -suelen ser conocidos como *PISP* o *Payment Initiation Services Provider* por su acepción inglesa-.

De esta manera, cuando el usuario realiza una compra online, ya no tiene necesariamente que relacionarse directamente con un determinado banco -proveedor de servicios de pago gestor de cuenta en terminología de la *PSD2*-, sino que son los *PISPs* los que pueden realizar dicha acción a modo de intermediación.

Eso hace que el usuario puede efectuar su compra a través de Internet de una forma totalmente transparente y segura, resultando beneficioso este servicio para ambas partes de la transacción:

- Al vendedor, porque le ofrece la seguridad de que el pago se ha efectuado, lo que permite que este inicie la entrega del bien o preste el servicio sin demora, justo en el momento que se da la orden.
- Al consumidor, porque le ofrecen la garantía de no tener que facilitar sus datos bancarios al comercio cada vez que realiza una compra.

En cualquier caso, el artículo 66 de la *PSD2* establece, como mecanismo de supervisión y protección, un conjunto de normas que deben ser observadas por los proveedores de servicios de información sobre cuentas:

- a) en ningún momento entrará en poder de los fondos del ordenante en relación con la prestación del servicio de iniciación de pagos;

- b) garantizará que las credenciales de seguridad personalizadas del usuario de servicios de pago no sean accesibles a terceros, y que las transmite a través de canales seguros y eficientes;
- c) garantizará que cualquier otra información sobre el usuario de servicios de pago obtenida al prestar servicios de iniciación de pagos se facilita exclusivamente al beneficiario;
- d) cada vez que se inicie un pago, se identificará ante el proveedor de servicios de pago gestor de cuenta del titular de la cuenta y se comunicará de manera segura con él;
- e) no almacenará datos de pago sensibles del usuario de servicios de pago;
- f) no solicitará al usuario de servicios de pago ningún dato distinto de los necesarios para prestar el servicio de iniciación del pago;
- g) no utilizará, almacenará o accederá a ningún dato para fines distintos de la prestación del servicio de iniciación de pagos expresamente solicitado por el ordenante;
- h) no modificará el importe, el destinatario ni ningún otro elemento de la operación.

De manera adicional, cuando el ordenante de su consentimiento expreso para que se efectúe un pago, el proveedor de servicios de pago gestor de cuenta tomará las siguientes disposiciones, para garantizar que el ordenante pueda ejercer su derecho a utilizar el servicio de iniciación de pagos:

- a) establecerá una comunicación segura con los proveedores de servicios de iniciación de pagos;
- b) inmediatamente después de la recepción de la orden de pago procedente de un proveedor de servicios de iniciación de pagos, le facilitará o pondrá a su disposición toda la información sobre el inicio de la operación de pago y toda la información a la que tenga acceso con relación a la ejecución de la operación de pago al proveedor de servicios de iniciación de pagos;
- c) tratará las órdenes de pago transmitidas a través de los servicios de un proveedor de servicios de iniciación de pagos sin discriminación alguna con respecto a las órdenes de pago transmitidas directamente por el ordenante, salvo por causas objetivas, en particular en lo que se refiere a los plazos, la prioridad o los gastos aplicables.

Finalmente, es importante reseñar que la prestación de servicios de iniciación de pagos no se su-
peditará a la existencia de una relación contractual a tal fin entre los proveedores de servicios de
iniciación de pagos y los proveedores de servicios de pago gestores de cuentas -es decir, las en-
tidades bancarias fundamentalmente-.

MARCO INSTITUCIONAL EUROPEO: VELAR POR EL CUMPLIMIENTO DE LA PSD2

La Autoridad Bancaria Europea -*EBA* por sus siglas en inglés- es la institución europea que vela por el cumplimiento de los principios de la Segunda Directiva de Servicios de Pago -*PSD2*-.

La *EBA* fue creada a comienzos del año 2011, en plena crisis financiera internacional tras la explosión de las hipotecas *subprime* en Estados Unidos, para hacerse cargo de todas las competencias y responsabilidades que tenía encomendadas el antiguo Comité de Supervisores Bancarios

Europeos (*CSBE*). Tiene su sede en Londres y, entre sus funciones, se encuentra la ejecución de los test de estrés de los bancos europeos, para evaluar posibles debilidades de capital en dichas entidades y asegurar que se dan las condiciones para una mayor transparencia e innovación en el sector bancario.

En febrero de 2017 la *EBA* propuso a la Comisión Europea el proyecto de aprobación de las Normas Técnicas de Reglamentación *-RTS* por sus siglas en inglés- sobre la autenticación reforzada del cliente *-Strong Customer Authentication* o *SCA*- y la comunicación común y segura *-Common and Secure Communication* o *CSC*- entre los diferentes actores intervinientes.



Figura 5. La *EBA*, guardiana de los principios de la *PSD2*

Los requisitos técnicos planteados por la *EBA* en dichas Normas Técnicas de Reglamentación para garantizar privacidad y seguridad en la operativa de los proveedores de servicios, pasan por aspectos tales como la autenticación de usuarios con dos factores o la vinculación dinámica de las operaciones a un importe y un beneficiario específico.

Más allá de dichas *RTS*, la autoridad europea también ha redactado otros seis documentos más, legalmente vinculantes para los Estados Miembros relacionados con la aplicación de la *PSD2*: cinco Guías y un Estándar de Implementación Técnica *-IPS*, por sus siglas en inglés-, que garantiza que se dan las condiciones necesarias para una competencia equitativa entre los distintos grupos empresariales y actores del sector.

LAS APIs BANCARIAS COMO MECANISMO TECNOLÓGICO FUNDAMENTAL

En cualquier caso, con los nuevos requerimientos de interconexión entre los diferentes actores, hay una pieza que se vuelve fundamental, desde el punto de vista técnico, para materializar todo este proceso: las APIs bancarias. Gracias a ellas, se permite, de una manera automatizada, que cualquier actor *TPPs* pueda acceder a los datos bancarios de los clientes en tiempo real e integrar toda esta información en sus aplicaciones de una forma sencilla, ágil y, por supuesto, tanto automatizada como estandarizada.

Las siglas *API*, de *Application Programming Interface*, pueden traducirse al español como interfaz de programación de aplicaciones. Pueden entenderse como puntos de interconexión a un sistema, de tal forma que permite a terceros sistemas acceder o consumir las funcionalidades que, mediante dichas interfaces, publica el primero.



Figura 6. Las APIs bancarias como pieza clave (CambioDigital Online).

Es decir, podrían entenderse como las ventanillas de un sistema en las que hay que preguntar para obtener cierta parte de su funcionalidad asociada. Por ejemplo, en el ámbito de los servicios de pagos, una entidad bancaria podría publicar una API a la que, preguntándole por un DNI de un cliente, devolviera los datos bancarios asociados a dicho identificador. De esa forma, las aplicaciones de terceros -fundamentalmente de los TPPs en este caso- podrán comunicarse y consumir servicios de banca online de diferentes entidades bancarias a través de las correspondientes APIs que dichas entidades publiquen.

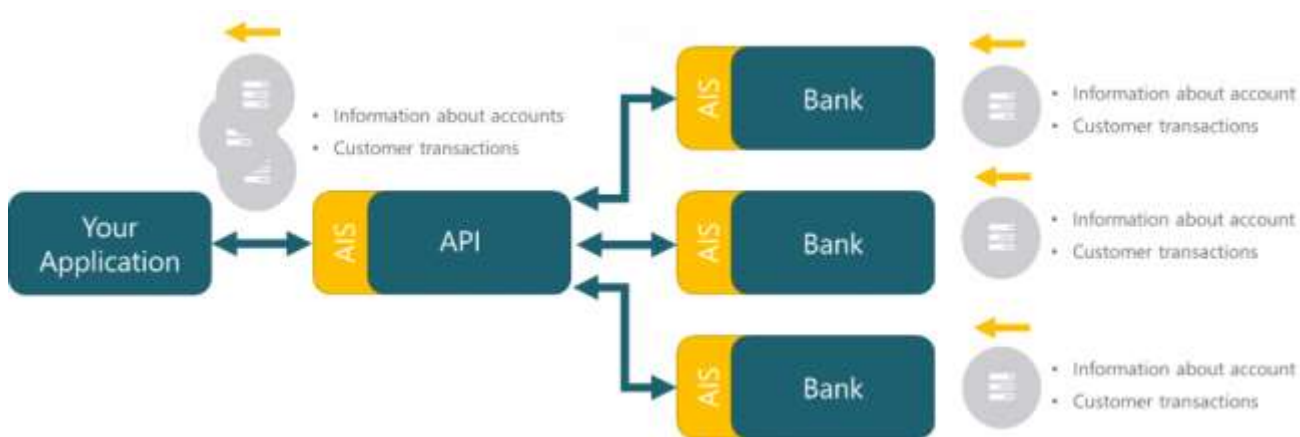


Figura 7. Las APIs bancarias facilitan una interconexión estandarizada.

Adicionalmente, como hemos visto, la PSD2 encomienda a la Autoridad Europea de Supervisión - como Autoridad Bancaria Europea o ABE en la terminología utilizada por la PSD2-, en cooperación con el Banco Central Europeo -BCE- y tras consultar a todas las partes interesadas pertinentes, a fin de reflejar todos los intereses involucrados, elaborará proyectos de normas técnicas de regulación dirigidas entre otras, a establecer los requisitos para unos estándares de comunicación abiertos comunes y seguros a efectos de identificación, autenticación, notificación e información, así como para la aplicación de medidas de seguridad entre los proveedores de servicios de pago gestores de cuenta, los proveedores de servicios de iniciación de pagos, los proveedores de servicios de información sobre cuentas, los ordenantes, los beneficiarios y otros proveedores de servicios de pago.

AUTENTICACIÓN REFORZADA DE CLIENTES

Como se ha mencionado anteriormente otro de los objetivos de la *PSD2* es reforzar la protección y la seguridad de los clientes y usuarios en el consumo de los diferentes servicios de pago.



Figura 8. Autenticación reforzada de clientes en la *PSD2*.

El artículo 4 de la Directiva *PSD2*, define autenticación como el procedimiento que permita al proveedor de servicios de pago comprobar la identidad del usuario de un servicio de pago o la validez de la utilización de determinado instrumento de pago, incluida la utilización de credenciales de seguridad personalizadas del usuario.

Igualmente, ese mismo artículo cuarto de la Directiva *PSD2* define autenticación reforzada de cliente, habitualmente conocida como *SCA* -*Strong Customer Authentication*- por sus siglas en inglés, como la autenticación basada en la utilización de dos o más elementos categorizados como conocimiento -algo que solo conoce el usuario-, posesión -algo que solo posee el usuario- e inherencia -algo que es el usuario-, que sean independientes, es decir, que la vulneración de uno no compromete la fiabilidad de los demás, concebida de manera que se proteja la confidencialidad de los datos de autenticación.



Figura 9. *SCA* como mecanismo de autenticación multifactor en la *PSD2*.

De esa forma, la *PSD2* establece que los Estados miembros -*EEMM*- velarán por que los proveedores de servicios de pago apliquen la autenticación reforzada de clientes cuando el ordenante realice alguna de las siguientes operaciones:

- a) acceda a su cuenta de pago en línea;
- b) inicie una operación de pago electrónico;
- c) realice por un canal remoto cualquier acción que pueda entrañar un riesgo de fraude en el pago u otros abusos.

En concreto, en lo que se refiere a la iniciación de las operaciones de pago electrónico, los Estados miembros velarán por que, respecto de las operaciones remotas de pago electrónico, los proveedores de servicios de pago apliquen una autenticación reforzada de clientes que incluya elementos que asocien dinámicamente la operación a un importe y un beneficiario determinados.

Hasta ahora, cuando realizabas una compra y necesitabas autorizar el pago asociado, era habitual recibir un código a través de *SMS* para confirmar ciertas operaciones. A partir de ahora, con la entrada en vigor de esta nueva normativa, dichas autorizaciones requerirán que te identifiques para confirmarlas, reforzando de esa forma la seguridad de las mismas. Por ello, ahora resulta habitual que tengas que autenticarte ante la entidad bancaria para activar el proceso de envío de *SMS* que actuará como confirmación del pago. Eso hace que, para poder seguir comprando online, sea indispensable tener actualizados datos como el teléfono registrado y la clave de acceso asociados a los servicios bancarios online.

No obstante, la normativa prevé algunas excepciones de la que es potestad del Banco su aplicación, que te permitirán finalizar la compra sin pasar este proceso, fundamentalmente asociadas a la cuantía del pago. Entre estas exenciones o excepciones pueden citarse aquellas transacciones consideradas de bajo riesgo, pagos por debajo de 30 o 50€, suscripciones regulares de importe fijo, transacciones iniciadas por el comerciante, ventas telefónicas o pagos corporativos.



Figura 10. Excepciones SCA en la PSD2.

Finalmente, la *PSD2*, en su artículo 74, en el ámbito de las responsabilidades establece que, si el proveedor de servicios de pago del ordenante no exige autenticación reforzada de cliente, el ordenante solo soportará las posibles consecuencias económicas en caso de haber actuado de forma fraudulenta. En el supuesto de que el beneficiario o el proveedor de servicios de pago del beneficiario no acepten la autenticación reforzada del cliente, deberán reembolsar el importe del perjuicio financiero causado al proveedor de servicios de pago del ordenante.

LAS EMPRESAS TECNOLÓGICAS Y LAS ENTIDADES BANCARIAS

Con la evolución de la aplicación de la *PSD2* y la aparición de nuevos actores *TPPs*, la irrupción de las grandes tecnológicas en el sector financiero puede ser una alternativa interesante para los usuarios finales y, en cierta forma, entenderse como una potencial amenaza para los actores tradicionales del sector y sus reguladores. En este sentido, las estadísticas señalan que el volumen de crédito concedido por este tipo de empresas en Europa en el año 2018 ha triplicado el de 2016, según el Banco de Pagos Internacionales.

De esta forma, muchas empresas no pertenecientes al sector financiero tradicional, están utilizando la tecnología para proponer soluciones innovadoras, que no se limitan exclusivamente a ofrecer los servicios tradicionalmente asociados a las instituciones financieras -mayoritariamente bancos-, sino que los mejoran, mediante la incorporación de una visión tecnológica novedosa y totalmente centrada en la experiencia y necesidades del usuario del servicio. Así, como más adelante veremos, tecnologías emergentes como los algoritmos de inteligencia artificial -*IA*- o el *Big Data*, permitirán a los actores ser más proactivos, prestando unos servicios muy ajustados a las necesidades de los usuarios y clientes.



Figura 11. Puntos de irrupción de las empresas tecnológicas en el sector financiero (BBVA).

El otro gran movimiento lo representa la respuesta del sector financiero a este rápido avance del sector tecnológico, que está haciendo que se produzca un replanteo de sus modelos de negocio de una manera urgente. El aumento de los costos, la reducción de márgenes, y el peso de los nuevos requerimientos regulatorios están presionando al sector financiero para buscar formas más rentables de gestión de sus negocios.

Estos cambios han hecho que el sector recurra cada vez más a la innovación tecnológica para ofrecer soluciones innovadoras, de forma que la aparición de las *FinTech* -contracción de los términos *finance* y *technology*, que engloba a las empresas del sector financiero que utilizan las nuevas tecnologías para crear productos financieros innovadores- está forzando el cambio entre los actores financieros tradicionalmente establecidos. Aprovechando su tamaño e influencia, las

organizaciones financieras están utilizando la tecnología mucho más intensamente para mejorar su oferta de productos y la prestación de servicios.

En cualquier caso, más allá de todo esto, a continuación, se citan brevemente las tecnologías emergentes que se están incorporando al sector financiero, junto con las posibilidades y funcionalidades novedosas que ofrecen -tanto hacia el exterior para la prestación de los diferentes servicios a los usuarios como, de forma interna, para los procesos de las propias entidades bancarias-:

- Autenticación y biometría. En un futuro cercano, es posible que no tengamos que recordar contraseñas complejas o preocuparnos por el robo de las mismas. Datos biométricos como huellas dactilares, el iris, el reconocimiento facial y de voz, la palma de la mano o hasta sistemas de reconocimiento de los latidos del corazón se están explorando para fines de autenticación. Los cajeros automáticos biométricos han sido integrados en varias partes del mundo -incluyendo algunos en países de nuestro entorno como Reino Unido-.

Adicionalmente, para aquellos usuarios que tengan una especial preocupación por su privacidad o con alguna discapacidad física que le impida el uso de los patrones biométricos anteriormente mencionados, la autenticación basada en *tokens* se ofrece como medio alternativo de seguridad.

- *Blockchain* como libros de contabilidad electrónicos distribuidos. La tecnología *blockchain* ofrece, esencialmente, un registro de propiedad descentralizada. Permite que un documento o activo sea codificado en un registro digital, que es irrevocable una vez que se ha introducido en el sistema. El registro digital se puede verificar por otras partes en el sistema, sin tener que pasar a través de una autoridad central.

Los beneficios potenciales esperados de un sistema de contabilidad distribuida incluyen procesamiento más rápido y eficiente, menor costo de operación o una mayor capacidad de resistencia frente a un fallo del sistema.



Figura 12. Las tecnologías emergentes aplicadas a servicios del sector financiero.

- *BigData*. Los datos generados por las redes sociales y en general por los usuarios y clientes, junto con los datos recopilados por los gobiernos y las empresas, equivalen a un universo de información digital que está creciendo a un 60% cada año. Al mismo tiempo, el coste de almacenamiento y procesamiento de datos ha estado cayendo dramáticamente.

Estas tendencias han creado la oportunidad de utilizar el análisis de esos datos para entender el mundo que nos rodea con una claridad y profundidad que antes no resultaba posible. De esa forma, algunos intermediarios financieros y otros actores del sector están invirtiendo y utilizando estas grandes cantidades de datos para obtener información que les sea útil y procesable.

- Inteligencia Artificial *-IA-*. De forma complementaria a lo anterior, estamos entrando en la era de la llamada tecnología cognitiva, cuyo mayor exponente es la inteligencia artificial, que está diseñada para aprender de los datos que se poseen y, además, en cierto sentido, podrán programarse -o aprender- a sí mismas para llevar a cabo nuevas tareas -realimentándose de la evaluación de los resultados y de los nuevos datos que se obtengan, incluyendo las interacciones con seres humanos-.
- *Cloud Computing* o computación en nube. Se trata de un modelo de servicio y entrega innovadora que permite el acceso bajo demanda a un conjunto compartido de recursos informáticos. De esa forma, proporciona economías de escala, posibles ahorros de costes, así como flexibilidad de adaptación de asignación de los recursos informáticos a medida que cambian los requisitos.

Adicionalmente, de manera paralela, la tecnología en la nube ha evolucionado considerablemente, con soluciones disponibles para hacer frente a los principales retos sobre seguridad y privacidad. Por ejemplo, las instituciones financieras o bancarias pueden ahora aplicar una fuerte autenticación y soluciones de cifrado para proteger sus datos en la nube.

PAGOS EN COMPRAS ONLINE

Gran parte del auge y éxito del comercio electrónico (*e-commerce* en inglés) hoy en día se debe a la confianza que sienten los clientes al momento de realizar un pago en línea. Y es que el *e-commerce* ha mejorado la experiencia de compra, brindando una amplia variedad de métodos de pagos seguros y accesibles.

Con todo lo anterior y como consecuencia de la entrada en vigor de la Directiva 2015/2366 sobre servicios de pago en el mercado interior o *PSD2*, cabe preguntarse, ¿qué pasos serán entonces necesarios para realizar una compra online?

Pasos que marca la *PSD2* para una compra online:

- Acceder a la web del comercio en el que se desean adquirir ciertos productos.
- Solicitar la realización del pago del contenido del nuestro carrito de la compra -que incluirá los productos anteriormente seleccionados-.

- En este momento deben activarse los mecanismos de autenticación reforzada de clientes - SCA- aplicable a los pagos por internet iniciados por el cliente dentro de Europa, lo que incluye la mayoría de los pagos con tarjeta y todas las transferencias bancarias:
 - La operación de pago podrá iniciarse por un PISP o resultar necesaria la introducción de un medio de pago como, por ejemplo, una tarjeta bancaria.
 - Durante el proceso de pago resultará necesario autenticarse ante la entidad bancaria correspondiente.

Actualmente, la forma más común de autenticar un pago con tarjeta por Internet es mediante el protocolo *3D Secure v2*, un estándar de autenticación basado en XML, implementado en 2019 para cumplir con los requisitos de SCA que marca la PSD2, y aceptado por la gran mayoría de las tarjetas europeas. Por lo general, al utilizarse este protocolo se añade un paso extra posterior a la compra, en el que el banco del titular de la tarjeta solicita al cliente información adicional para completar un pago -por ejemplo, un código de único uso que se envía a su teléfono o autenticación por huella digital desde el móvil a través de la aplicación del banco-.

Otros métodos de pago con tarjeta como *Apple Pay* o *Google Pay* ya aceptan flujos de pago con una capa integrada de autenticación (biométrica o con contraseña).

- Una vez realizados los pasos anteriores, el proceso finaliza con la vuelta a la web del comercio para comprobar que la operación se ha realizado con éxito.



The image shows a smartphone screen with a clock at 06:12 and the heading "PAGO SEGURO:". Below the heading are three numbered steps: 1. Access the bank app, 2. Review payment data and authorize, and 3. Return to the merchant's website to verify completion.

¿CÓMO FUNCIONA?

En el momento de efectuar el pago tu banco te pedirá que realices los siguientes pasos:

1. Accede a la Aplicación o web de tu Banco
2. Revisa los datos de pago y autoriza la compra
3. Vuelve a la web del comercio y podrás comprobar que la operación se ha realizado con éxito.

Figura 13. Pasos de la SCA establecidos por la PSD2 para la compra online.

Como hemos visto, hay que tener en cuenta que, para la realización del primer paso anterior *Acceso a la Aplicación o web de tu banco*, resulta necesaria la autenticación del cliente ante dicha entidad bancaria, haciendo efectiva los mecanismos de SCA o autenticación reforzada que la PSD2 hace obligatoria.

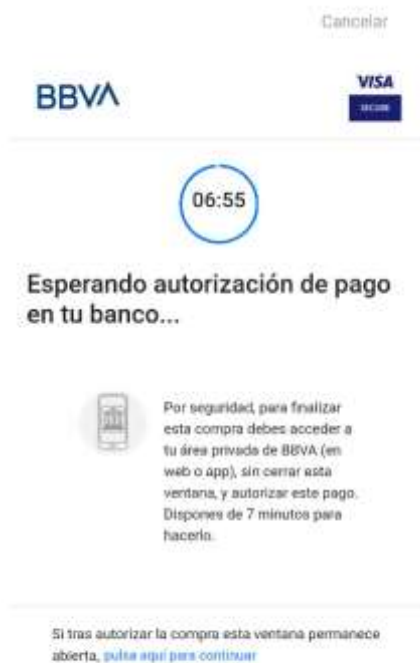


Figura 14. Autenticación necesaria para compra online.

PAGOS CON EL MÓVIL

No cabe duda que, si tuviéramos que citar un objeto que, hoy en día, está continuamente con nosotros, ese sería el teléfono móvil *-smartphone-*. Por ese motivo, esos dispositivos han pasado de ser teléfonos que nos permitían simplemente hablar y comunicarnos, a ser elementos que nos ayudan en un sinnúmero de tareas cotidianas: en el seguimiento de nuestra actividad física y deportiva, como agendas digitales, permitiendo nuestra presencia en redes sociales, realizando compras online, etc. De esa forma, no resulta extraño que los móviles se hayan convertido también en medios de pago.



Figura 15. El móvil como medio de pago y para sacar dinero en cajeros.

En cualquier caso, resulta importante aclarar que cuando hablamos de pagos con el móvil no nos estamos refiriendo al proceso de pago de las compras en tiendas online desde un teléfono móvil o *smartphone* a través de internet, ya que entendemos eso como compras online y utilizan las plataformas de pago anteriormente descritas, que pueden usarse desde cualquier dispositivo electrónico, como *smartphone*, tableta u ordenador. En estos casos, estamos hablando del uso del móvil para el pago, en sustitución de la tarjeta bancaria, en establecimientos físicos.

En este sentido, ya resulta posible pagar con el móvil en prácticamente la totalidad de los establecimientos en los que, hasta ahora, resultaba posible pagar con tarjeta bancaria. Y no cabe duda, dada la enorme presencia de los dispositivos móviles en nuestra vida cotidiana, que se trata de una práctica al alza, no resultando descabellado pensar que se convertirá en mayoritaria frente al uso de tarjetas bancarias en un no muy prolongado espacio de tiempo.

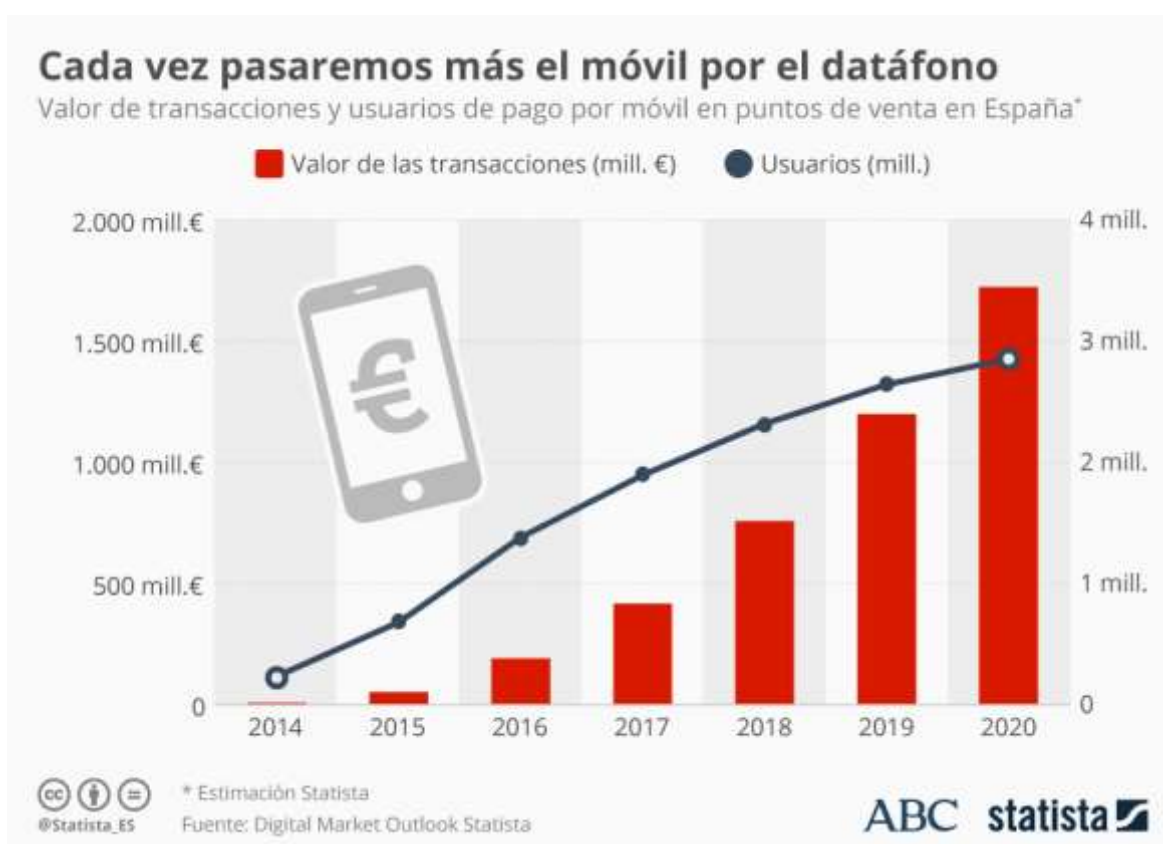


Figura 16. Evolución anual del móvil como medio de pago.

En cualquier caso, como otro gran número de tecnologías emergentes, su adopción está resultando más acelerada en aquellos países que ya contaban con un avance tecnológico mayor previo.



Figura 17. Evolución del móvil como medio de pago por países.

REQUISITOS DE FUNCIONAMIENTO

A continuación, describimos lo que, más allá de, lógicamente, disponer de un dispositivo móvil, resulta necesario para realizar pagos con el móvil ante un establecimiento físico, como sustitutivo de las tradicionales tarjetas bancarias:

- Instalar una aplicación de pagos y configurarla de tal forma que carguemos en ella las tarjetas bancarias compatibles que deseemos utilizar. Dada la extensión actual de este tipo de soluciones, no resulta esperable que existan problemas de compatibilidad en este sentido.

En la mayoría de los casos, estas apps requerirán de un factor biométrico -como por ejemplo la huella dactilar- o de conocimiento -ya sea un patrón o un código *PIN* -personal identification number- por ejemplo, para acceder a la utilización de su contenido.

De esta forma, estas aplicaciones contendrán una copia digital o virtual de tu tarjeta de crédito y serán las encargadas de comprobar la veracidad y la seguridad de la transacción y, si todo es correcto, autoriza el pago de la compra.

Como más adelante enumeraremos algunas de las principales *apps* en este campo son las de las propias entidades bancarias (*BBVA, Banco Santander o Caixa Banc*), *Google Pay, Amazon Pay, Apple Pay o Samsung Pay*.

- Disponer de un móvil que cuente con la tecnología inalámbrica de corto alcance *NFC* (*Near Field Communication*), que permite transmitir datos entre dos dispositivos que se encuentren muy próximos entre sí.

El funcionamiento es similar al de *RFID* para las tarjetas *contactless* -sin contacto- y, al igual que con estas, resulta suficiente con acercar el móvil al datafono o terminal de venta al público -*TPV*- para efectuar el pago.



Figura 18. NFC: Near Field Communication.

Los estándares de *NFC* cubren protocolos de comunicación y formatos de intercambio de datos, y están basados en *ISO 14443 -RFID, radio-frequency identification-*. Los estándares incluyen *ISO/IEC 180922* y los definidos por el *NFC Forum*, fundado en 2004, por Nokia, Philips y Sony, y que hoy suma más de 170 miembros.

NFC se comunica mediante inducción en un campo magnético, en donde dos antenas de espiral son colocadas dentro de sus respectivos campos cercanos. Trabaja en la banda de los 13,56 MHz, lo que hace que no se aplique ninguna restricción no sea requerida ninguna licencia para su uso.

Todos los dispositivos del estándar *NFCIP-1* deben soportar los dos modos de funcionamiento existentes:

- Activo, en el que ambos dispositivos que se comunican generan su propio campo electromagnético, que utilizarán para transmitir sus datos.
- Pasivo, cuando solo un dispositivo genera el campo electromagnético y el otro se aprovecha de la modulación de la carga para poder transferir los datos. El iniciador de la comunicación es el encargado de generar dicho campo electromagnético.

El protocolo *NFCIP-1* puede funcionar a diversas velocidades como 106, 212, 424 u 848 Kbit/s. Según el entorno en el que se trabaje, las dos partes pueden ponerse de acuerdo -suele hablarse de negociación- de a qué velocidad trabajar y reajustar el parámetro en cualquier instante de la comunicación.

- Que la tienda disponga de un *TPV* -Terminal de venta al público- o datafono *contactless* -sin contacto-. Como decíamos, el cumplimiento de este requisito suele ser habitual en la práctica totalidad de los establecimientos hoy en día.

De esta forma, cuando todos los requisitos anteriores son correctos, basta con acercar el móvil al datafono o terminal de punto de venta -TPV-, para que, tras realizar las comprobaciones configuradas correspondientes -factores biométricos, patrones o códigos PIN como mecanismos de acceso y uso de las tarjetas bancarias virtuales-, pueda efectuarse el pago desde el móvil. De una forma similar, adicionalmente, mediante los dispositivos móviles también resulta posible sacar dinero en efectivo de aquellos cajeros automáticos que cuenten con tecnologías que los habiliten para ello.

PRINCIPALES APLICACIONES PARA PAGAR CON EL MOVIL

Para hacer realidad lo anteriormente explicado, lo habitual es hacer uso de aplicaciones móviles que han sido desarrolladas, principalmente, bien por entidades bancarias o por actores del sector que cuenta con una extensión de uso muy alta entre los consumidores habituales del comercio online.

Dichas aplicaciones, serán las encargadas de alojar y gestionar los medios de pago que luego utilizarán los usuarios para realizar sus pagos:

- Las aplicaciones móviles de las propias entidades bancarias. Hoy en día, aunque sea en diferentes formatos, la práctica totalidad de las aplicaciones móviles de los bancos suelen contar con secciones de cartera o *wallet* digital, con la que configurar los pagos móviles. El dónde está dependerá de cada una, pero por lo general es uno de los servicios que ofrecen los principales bancos -BBVA, Caixa Bank, Banco Santander, etc. son sólo algunas de las entidades que cuentan con este tipo de soluciones o funcionalidades en sus aplicaciones de banca online-.
- *Google Pay*. Se trata de la aplicación de pagos móviles creada para *Google* y compatible tanto con los dispositivos Android como con iOS. Lo único que necesario es instalarla e identificarte utilizando la cuenta de Google que, habitualmente, ya tendrás en tu móvil con Android, para, posteriormente, registrar las tarjetas de bancos compatibles. Sirve también para los pagos online en tiendas de Google.
- *Amazon Pay*. Se trata de un servicio de pago online de *Amazon* que puede integrarse con sitios web, para apoyarles en la gestión de sus pagos. Además, está optimizado para móvil, de modo que los compradores pueden pagar desde su propio dispositivo.

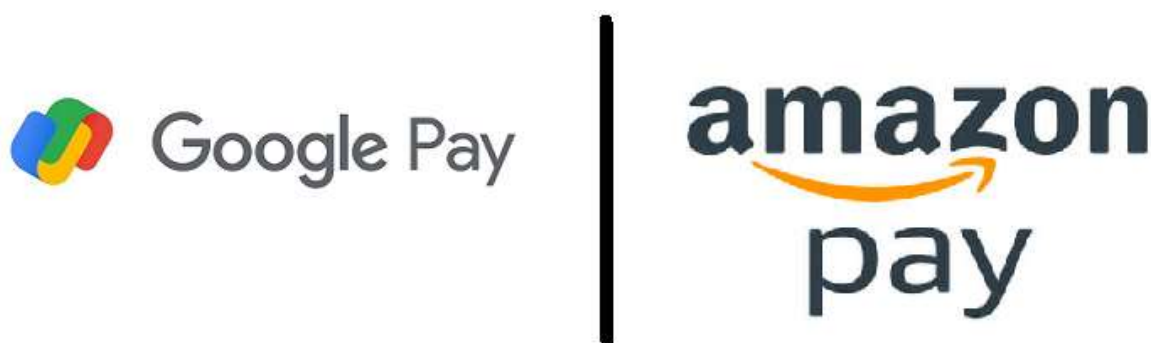


Figura 19. Google Pay y Amazon Pay, ejemplo de algunas de las principales app de pago con el móvil.

- *Apple Pay*: Se trata del sistema de pagos móviles creado por Apple para todos los dispositivos móviles propios a partir de los modelos de *smartphones iPhone SE* e *iPhone 6*. No es compatible con Android, y además de tarjetas bancarias también puede alojar tarjetas de fidelidad compatibles, aunque hasta el momento no son demasiadas.
- *Samsung Pay*: El fabricante coreano Samsung también cuenta con su propio sistema de pagos pensado para sus dispositivos, y que destaca por la inclusión de un sistema de puntos y recompensas por utilizarlo. Aunque en el mundo *Android* resulta complicado competir con la aplicación genérica de Google, la *app* móvil de Samsung cuenta también con bastante importancia en el sector.
- Adicionalmente existen muchas otras aplicaciones móviles con una cuota de mercado o visibilidad menor, que permiten el pago con dispositivos móviles. Entre estas aplicaciones pueden citarse, entre otras, *Orange Bank*, *Vodafone Wallet* o *FitbitPay*.

FUNCIONALIDADES ADICIONALES ASOCIADAS DE LAS APPS DE PAGO MÓVIL

En cualquier caso, no cabe duda de que no debemos entender el pago con el móvil como una simple sustitución de las tarjetas bancarias por su equivalente virtual en los terminales móviles. Dado que estos dispositivos son más activos y más avanzados tecnológicamente, las aplicaciones anteriormente listadas suelen ofrecer servicios adicionales, asociadas a estas funcionalidades de las tecnologías móviles.

De esa forma, en general, las aplicaciones móviles que gestionan medios de pago, podrían acceder, para la prestación de ciertas funcionalidades adicionales asociadas, a los servicios nativos que ofrece el sistema operativo del dispositivo que las aloja -ya sea *Android* o *iOS* en el caso del fabricante *Apple*-, como podría ser, por ejemplo, los servicios de localización GPS del dispositivo móvil, la gestión de datos biométricos y algunos otros similares.

De una forma más concreta, algunas de dichas funcionalidades añadidas ventajosas son las siguientes:

- Uno de los beneficios más directos del pago con el móvil, pasa por la comodidad que supone la eliminación de la cartera/billetera, lo que hace que el procedimiento de pago no solo sea más seguro, si no más rápido -el dispositivo móvil siempre lo tenemos a mano-.
- Ofrece una mayor seguridad, ya que, de manera asociada, y en contraposición a las tarjetas bancarias, resulta posible añadir un factor que requiera identificación táctil o mediante un PIN. Además, durante la transacción, se generan códigos de seguridad individuales temporales, de forma que los datos de la tarjeta bancaria realmente no viajan desde el móvil hasta el *datafono*.
- Otra de las ventajas es la privacidad, dado que, aunque estés en presencia de terceras personas, nadie sabe a qué entidad bancaria pertenece el medio de pago que estás utilizando. Por decirlo de alguna forma, con un símil físico, la tarjeta nunca es expuesta a ojos de terceras personas.

- Por otro lado, estas tecnologías pueden suponer una oportunidad para los pequeños y medianos negocios, ya que facilita y acelera el pago, aprovechando para interactuar con los clientes mediante el proceso -fidelizando al cliente a base de su conocimiento, enviándoles ofertas y cupones de descuento, etc.-.
- La centralización en un único punto del conjunto de medios de pago disponibles, suele producir ahorros a los usuarios de este tipo de aplicaciones. Dado que pueden alojar desde tarjetas bancarias hasta tarjetas regalo o prepago pasando por cupones, resulta más difícil que estos medios de pago se caduquen y, por tanto, dejen de tener validez. De esa forma, incluso se podría llegar a pensar en que la aplicación lanzara alertas al usuario con aquellas fechas asociadas a sus medios de pago con una caducidad cercana en el tiempo.
- Como ya se ha comentado, las aplicaciones de pagos móviles permiten realizar un seguimiento personalizado de las necesidades del usuario, integrando programas de fidelización o envío de ofertas y cupones de descuento, basándose, de manera proactiva, en los patrones de uso previos del usuario.

PAGOS ONLINE ENTRE PARTICULARES: BIZUM Y TWIP

Los medios de pago que hemos visto hasta ahora son, casi en su totalidad, utilizados en compras *online* o en pagos con el móvil ante establecimientos físicos que lo permiten. En cualquier caso, dado que la tecnología inunda hoy en día todos los aspectos de nuestra vida, también existen aplicaciones o soluciones que permiten los pagos o intercambios económicos online entre los propios particulares.

De esta forma, preguntas tradicionales como ¿quién paga la cuenta de la cena?, o prácticas tan típicas como la puesta en común de botes de dinero en las reuniones de amigos, quedadas, comidas o similares, parecen, cada día más, cosa del pasado.

BIZUM

La aplicación *Bizum* es una solución de pagos a través del móvil, impulsada por la banca española, instantánea, rápida, cómoda y universal. Actualmente, permite realizar pagos entre particulares, donaciones a Organizaciones No Gubernamentales -ONG- y pagar en aquellos comercios online asociados. Adicionalmente, dado que se trata de una tecnología en expansión es previsible una ampliación de estos servicios en las próximas fechas.



Figura 20. Bizum

El hecho de que se trate de una iniciativa de la banca española, hace que cuente con el respaldo de la gran mayoría de los bancos del país -la práctica totalidad de las principales entidades bancarias están asociadas a este servicio-. De esa forma, para utilizar *Bizum* basta con disponer de cuenta bancaria -*International Bank Account Number o IBAN*- en España con cualquiera de las entidades que ofrecen el servicio y de un número de teléfono móvil asociado; descargando de manera previa la aplicación de la entidad bancaria y dando de alta el servicio.

Con todo esto, para transferir dinero, no resulta necesario conocer ni recordar el *IBAN* u otros trámites complejos, tan solo necesitarás el número de móvil de la persona a la que quieres enviarle o solicitar el dinero, y todo con las máximas medidas de seguridad y con el respaldo de los principales bancos españoles.

¿Cómo usar Bizum con tu banco?




| | | |
|---|---|---|
|  |  |  |
| Selecciona tu banco | Descárgate su app | Entra a la app y ¡actívalo! |
| Consulta el listado de bancos que trabajan con Bizum, encuentra el tuyo y pincha el logo. | Una vez en la web de tu banco, sigue las instrucciones para descargarte la app. | Busca la opción enviar y recibir dinero con Bizum. Elige a uno de tus contactos y activa el servicio. |

Figura 21. Modo de uso y funcionamiento de Bizum.

En cuanto a la seguridad, dado que *Bizum* es un servicio íntegramente ofrecido por los canales bancarios, está totalmente respaldado por sus sistemas de seguridad, de tal forma que la transferencia siempre la ordena tu banco y son ellos los que se encargan de autentificarte.

Adicionalmente, debes tener en cuenta las siguientes consideraciones a la hora de utilizar la aplicación *Bizum*:

- Resulta posible tener más de un teléfono configurado contra la misma cuenta bancaria - *International Bank Account Number o IBAN*-.
- En cambio, un número de teléfono tan sólo puede estar asociado a una determinada cuenta bancaria -*International Bank Account Number o IBAN* -.
- En cualquier caso, pese a la restricción de asociación anterior, ésta puede cambiarse tantas veces como se desee, haciéndolo incluso entre cuentas bancarias que sean de diferentes entidades.
- Ciertas restricciones de uso, como por ejemplo en el caso de uso de menores de edad, dependen de las consideraciones que apliquen cada una de las entidades bancarias a ese respecto.

- Los canales para la baja del servicio son los mismos que para el alta, esto es, a través de la aplicación o página web mediante la que tu entidad ofrece los servicios bancarios online.

TWYP

La aplicación de la entidad bancaria *ING*, *Twyp*, está basada en la creación de tarjetas virtuales prepago que pueden ser utilizadas en compras, suscripciones online y, en general, como medio de pago.

De manera general, este servicio tiene como principales características, las siguientes:

- Al tratarse de una tarjeta virtual de prepago, no es necesario que esté asociada a una cuenta bancaria -*International Bank Account Number o IBAN*-.
- Se recarga desde una cuenta de cualquier entidad bancaria -no siendo necesario ser cliente de *ING*- cuando y con el importe que se desee.
- Al tratarse de una tarjeta digital o virtual, puede apagarse con un *clic* en el momento en que lo necesites, lo que le aporta una mayor seguridad contra usos fraudulentos.
- Estas tarjetas virtuales pueden cargarse, para su uso posterior, en las aplicaciones de pago con el móvil anteriormente enumeradas -*Google Pay, Amazon Pay, etc.*- De esa forma, pueden utilizarse como medios de pago de carácter general.
- Permite obtener dinero en los comercios asociados, convirtiendo en efectivo el saldo que necesites de la tarjeta virtual. Esto puede resultar muy útil para los casos en que se necesita disponer de efectivo para realizar compras o pagos de pequeño importe.
- *Twyp* permite el envío de dinero entre diferentes tarjetas virtuales de la plataforma -lo que equivale al intercambio económico entre particulares que actúan como usuarios de *Twyp*-.
- Se trata de un servicio seguro, dado que los mecanismos y sistemas de seguridad utilizados son los mismos que utiliza *ING* para ofrecer el resto de los servicios bancarios online.



Figura 22. Logotipo de la app Twyp.

Todas estas características anteriores han hecho que *Twyp* tenga su principal grupo de uso entre jóvenes con una franja de edad comprendida entre los 14 y los 17 años. Como hemos visto, mediante su utilización, los padres de dichos jóvenes pueden poner a su disposición una cantidad de dinero limitada, de forma segura y con garantías.



Figura 23. Twyp para jóvenes

CONCLUSIONES Y TENDENCIAS FUTURAS

En cuanto a los servicios de pago, no cabe duda que nos encontramos ante un escenario sin precedentes, lleno de cambios, innovaciones, cuestionamientos y, sobre todo, retos. Un escenario que también plantea incertidumbres, pero que sin duda es prometedor e ilusionante tanto para el sector financiero o bancario -ya sea el tradicional o el tecnológico más avanzado-, como para los ciudadanos y usuarios de sus servicios. Un escenario que nos muestra un entorno global y diverso donde la transparencia, la observación de las necesidades del usuario y la integración segura de los avances tecnológicos se convierten en retos imprescindibles.

De esa forma, los clientes de estos servicios son cada vez más exigentes, más expertos en tecnologías de la información y, por ello, demandan una mayor atención y unos servicios bancarios con un mayor grado de ajuste y personalización a sus necesidades. En este ámbito, como en muchos otros, los servicios que se presten deben estar completamente orientados a los usuarios que van a consumirlos.

De acuerdo con esto y aunque resulta difícil predecir el futuro en un entorno que cambia tan rápidamente, algunos expertos apuntan a que, entre las tendencias venideras, pueden citarse las siguientes:

- Generalización del uso de pagos basados en el contexto. Esta forma de pago no requiere que haya una interacción directa entre el cliente y el comerciante, dado que una plataforma intermediaria se encarga de poner en contacto a ambos. Ejemplos actuales de esto son los casos de *Uber* o *Airbnb*, en los que es la propia aplicación o web de la empresa la que actúa como intermediario entre las dos partes actuantes en la transacción, encargándose de que se realice la transferencia económica correspondiente al pago por el servicio prestado.
- *Weareables* como medios de pago. Se trata de dispositivos o *gadgets* electrónicos que se incorporan en alguna parte de nuestro cuerpo, interactuando de forma continua con el usuario y con otros dispositivos electrónicos de su entorno. Algunos dispositivos *weareables* que podrían actuar como medios de pago serían los relojes inteligentes, las pulseras de actividad, los cascos o las gafas electrónicas o, incluso, anillos con capacidad de conectividad.



Figura 24. Los dispositivos wearables como medios de pago (Iberdrola).

- Biometría. No es casualidad que la práctica totalidad de los nuevos modelos de *smartphones* incluyan desde hace algún tiempo modos de desbloqueo y otras funcionalidades basadas en nuestras particularidades biométricas, como pueden ser las huellas dactilares, el reconocimiento facial o algún otro rasgo corporal. Este tipo de sistemas tiene un gran potencial, pues hace que el dispositivo solamente pueda ser manejado por una determinada persona -su propietario-. Es esta cualidad, asociada a la seguridad, la razón que hace que se espere que se convierta en un elemento importante de las formas de pago del futuro.

Finalmente, incluso existen perspectivas que llegan a afirmar que el momento, el acto, del pago tenderá a desaparecer en muchos casos en un futuro relativamente próximo. Tecnologías como la inteligencia artificial están cada vez más presentes en nuestras vidas y seguirán evolucionando para facilitarnos las cosas en este ámbito de los servicios de pago y en muchos otros. De esa forma, existirán sistemas de seguridad y de encriptación, que permitirán identificar al usuario para poder determinar que es el propietario de una cuenta o una tarjeta -o cualquier otro medio de pago- y simplemente verificar, de esa forma, que la compra que se ha realizado es válida. Hoy en día, este tipo de situaciones nos pueden parecer poco menos que ciencia ficción, pero, en cambio, están más cerca de lo que parece.

REFERENCIAS

| | |
|--------------|---|
| UE | https://ec.europa.eu/info/policies/single-market_es https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32015L2366 |
| MINECO | https://www.mineco.gob.es/ |
| BBVA | https://www.bbva.com/es/lo-saber-la-psd2/ https://www.bbva.com/es/4-claves-para-entender-por-fin-el-mundo-de-las-apis/ https://www.bbva.com/wp-content/uploads/2017/10/cibbva-ebook-empresas-tecnologias-financieras.pdf |
| B. SANTANDER | https://www.bancosantander.es/espacio-psd2 |
| XAKATA | https://www.xataka.com |
| ComputerHoy | https://computerhoy.com/listas/tecnologia/cual-mejor-forma-pagar-movil-2019-505221#Primero |
| AndaluciaLab | https://www.andalucialab.org/blog/6-ventajas-del-pago-movil/ |
| OCU | https://www.ocu.org/tecnologia/telefono/noticias/pagar-con-el-movil |
| Bizum | https://bizum.es/ |
| Twyp | https://www.twyp.com/ |
| Bankinter | https://www.bankinter.com/blog/empresas/fintech-que-tipos |
| Wikipedia | https://es.wikipedia.org/wiki/Near_field_communication https://es.wikipedia.org/wiki/3D_Secure |
| Stripe | https://stripe.com/es/guides/strong-customer-authentication |