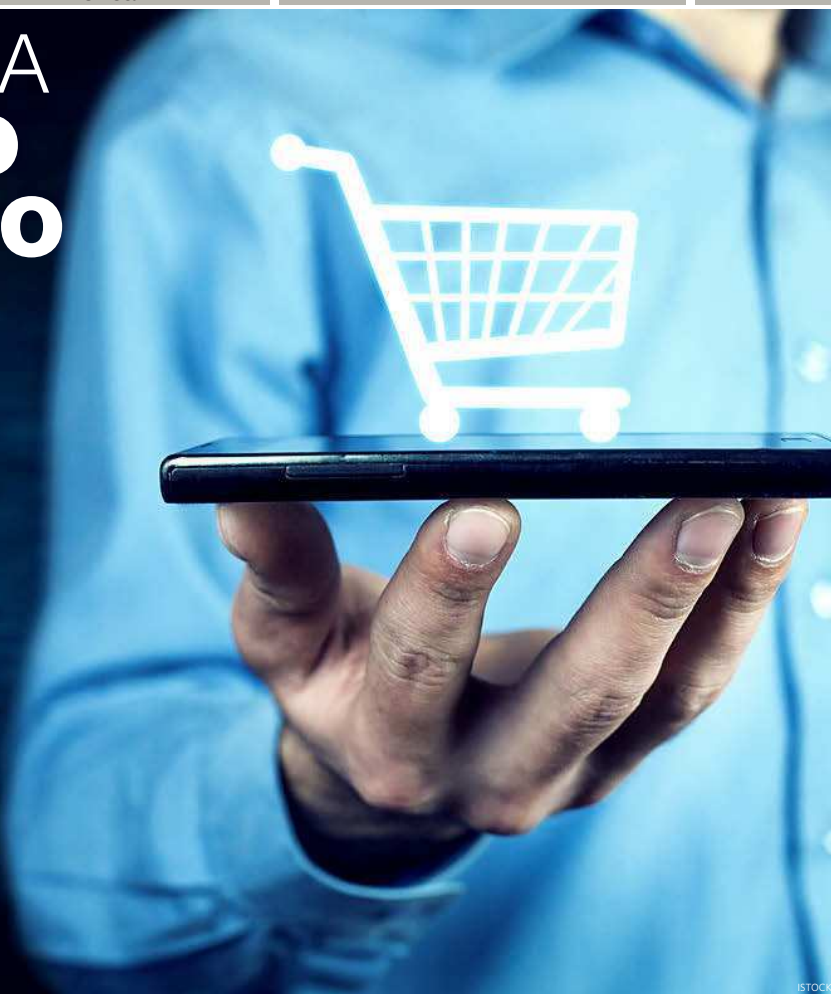


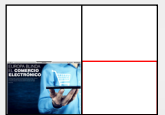


EUROPA BLINDA EL **COMERCIO** **ELECTRÓNICO**

Ya está en vigor la Directiva europea de Servicios de Pago, conocida como PSD2, que trae uno de los mayores cambios en años en la industria bancaria y financiera desde el punto de vista digital

IGNACIO FAES





Cambia la forma en la que los consumidores compran por Internet. Ha entrado ya en vigor las medidas de la Directiva europea de Servicios de Pago, conocida como PSD2, que trae uno de los mayores cambios en años en la industria bancaria y financiera y, en concreto, desde el punto de vista digital y de las aplicaciones móviles.

"Los consumidores se beneficiarán de un entorno de pagos en línea más seguro y fácil", señala la Comisión Europea en un comunicado. El Gobierno ya adaptó esta directiva con el Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera, que se publicó en el BOE el sábado 24 de noviembre de 2018. Entre otras cosas, este nuevo servicio facilitará la ejecución de los pagos en toda Europa y permitirá ofrecer un servicio bancario adaptado a las nuevas tecnologías, especialmente desde el punto de vista móvil.

Aplicaciones móviles

Las principales beneficiadas de esta Directiva son las nuevas operadoras que ofrecen servicios financieros a través de aplicaciones para el teléfono móvil, conocidas como *fintech*. La normativa permite a terceros acceder a la infraestructura de los bancos. De este modo, la norma comunitaria obliga a las entidades bancarias a abrir sus sistemas a terceras partes o TPP (*Third Party Payment Service Providers*), acción que se denomina *open banking*.

Esto permitirá que terceras partes accedan a la cuenta del cliente y así puedan realizar pagos en su nombre, previo consentimiento del titular de la cuenta. Esta apertura conlleva un aumento en la competencia que provocará la aparición de nuevas empresas, ya que hasta ahora las restricciones



GETTY

Los bancos deberán permitir a las aplicaciones 'fintech' el acceso a las cuentas

impuestas a los TPP lo hacían muy complicado. Eso sí, deberán cumplir con la misma reglamentación que los servicios de pago tradicionales.

En cuanto a los pagos por Internet, serán mucho más rápidos. Si el cliente ha autorizado a un TPP el acceso a su información bancaria, el cobro de un determinado producto o servicio será inmediato, de manera similar a como se realiza una transferencia bancaria.

Los titulares de la cuenta deberán dar permiso para que sus datos sean accedidos por un tercero que tenga licencia para ofrecer servicios de pago. Con estas premisas, podría parecer que la eliminación de intermediarios que





ahora son innecesarios hace más vulnerables los pagos en línea. Sin embargo, nada más lejos de la realidad.

El teléfono, fundamental

La Directiva ha establecido un conjunto de elementos de seguridad, aunque algunos de ellos no serán vinculantes hasta septiembre de 2019 para dar tiempo a los bancos y firmas de tecnología para que puedan ajustar su tecnología. La verificación se realizará a través de dos factores, entre los cuales se encuentran una contraseña, código PIN, el número de la tarjeta, el teléfono móvil e incluso el escaneo del iris o la huella digital.

Además, al regularse el acceso a las cuentas bancarias del consumidor por parte de terceros, se evitan algunas tecnologías como el Screen Scraping, que realizan un rastreo de los datos de los clientes haciéndose pasar por un usuario normal y después utiliza esta información para facilitar los accesos o reducir el tiempo de comprobación y análisis al, por ejemplo, conceder un préstamo. Todos los elementos seleccionados deberán ser independientes. De esta forma, aunque uno de los factores sea robado, no se podrá tener acceso al resto de los elementos.

Por otra parte, hasta ahora, para acceder a una cuenta corriente por Internet bastaba un usuario y una contraseña o, en su lugar, algún tipo de información biométrica como la lectura de la huella dactilar o el reconocimiento del iris. Sin embargo, ahora el usuario necesitará un teléfono inteligente y, en algunos casos, tener instalada la *app* de su banco.

En realidad, el sistema de doble autenticación no es totalmente nuevo. Por ejemplo, cuando se abona una compra en un comercio, se combina una tarjeta con un código pin o cuando se abona una compra por Internet, muchos comercios solicitan un código recibido por SMS para confirmar la

operación. En cuanto a los comercios *online*, la entrada en vigor supondrá acciones mínimas en aquellos que, actualmente, ya tengan implementado un sistema de autenticación reforzada o de doble factor de autenticación. En cualquier caso, el Incibe recomienda contactar con la entidad que facilita la pasarela de pago para ver que se cumple la norma.

Por el contrario, aquellos negocios *online* que no cuenten con un sistema de autenticación reforzada en sus pagos deberán adaptar la pasarela de pago a la nueva Directiva, y así provocar que sea obligatoria la autenticación reforzada. Para ello, deberán ponerse en contacto con el proveedor de la pasarela de pago y realizar el proceso de migración hacia este nuevo sistema más seguro y de obligado cumplimiento.

Existen varias excepciones a la hora de implementar métodos de autenticación reforzada que la pasarela de pago deberá contemplar, entre ellas las operaciones cuyo pago se ha iniciado por teléfono o correo electrónico o pagos realizados con tarjetas prepago anónimas.

Cómo acceder al banco

Desde HelpMyCash han hecho una lista de algunos de los principales bancos. En el caso de los clientes de Banco Santander y de Openbank se necesitará su clave de acceso más un código recibido por SMS para acceder a la banca *online*. BBVA ha optado por la misma opción y ya ha notificado a sus clientes que a partir de septiembre el "móvil será imprescindible para acceder" a los canales digitales. Colonya y las cajas rurales combinarán los datos de acceso habituales (usuario, NIF y contraseña o bien huella y reconocimiento facial) con un código recibido por SMS.

Algunas entidades están aprovechando la entrada en vigor de la normativa PSD2 para eliminar la tarjeta de coordenadas. Laboral Kutxa ha avisado que





"la actual tarjeta de firmas para operar en banca *online* será sustituida por claves que recibirás por SMS".

¿Qué hacer si ese es de ING? La entidad quiere licenciar la tarjeta de coordenadas; sin embargo, en lugar de recurrir al popular SMS, enviará notificaciones a través de su app, por lo que a partir de este mes sus clientes estarán obligados a tenerla instalada en su móvil si quieren operar con normalidad a través de la web. ING avisa que antes del 10 de septiembre era necesario cumplir estos tres requisitos: descargar la app o actualizarla a la versión 2.5 o superior, activar las notificaciones y dar de alta la validación móvil, que sustituirá a la tarjeta de coordenadas.

A la hora de acceder a una cuenta de ING a través del ordenador (se podrá seguir operando por la web, aunque la app sea obligatoria), el cliente recibirá una notificación en su móvil para verificar su identidad. La app también será necesaria para validar operaciones realizadas desde el ordenador. En esos casos, el cliente recibirá una notificación en su smartphone que deberá aceptar y luego introducir una contraseña.

Pero ING no es el único banco que quiere que todos sus clientes tengan su app instalada. Targobank también quiere sustituir los mensajes de texto: "El servicio de Confirmación Móvil reemplaza el envío del SMS por una validación realizada directamente desde su smartphone y totalmente integrada en la aplicación de Targobank".

Obligar al cliente a operar a través de una notificación integrada en una app en lugar de enviarle un SMS implica que solo podrá operar cuando el smartphone tenga acceso a Internet. Asimismo, será necesario disponer de un terminal que soporte las últimas versiones de las aplicaciones bancarias y que tenga espacio suficiente para instalarlas, explican los expertos. Para agilizar el proceso, la doble autenticación no será necesaria siempre que se



GETTY

acceda a la banca *online*, sino que los bancos que lo consideren oportuno podrán dar una tregua de 90 días a sus clientes durante los cuales estarán exentos de usar la SCA. Según el Reglamento Delegado 2018/389, solo será necesario introducir el segundo factor de seguridad la primera vez que se acceda a una cuenta *online* y cuando hayan transcurrido más de 90 días desde la última vez que se solicitara la autenticación reforzada. Las cajas rurales, Colonya, Openbank e ING han avisado de que solo se solicitará el segundo factor la primera vez que se acceda a la banca electrónica a partir del 14 de septiembre y luego cada 90 días.

