MÁS SEGURIDAD PARA LOS PAGOS

¿Qué es la PSD2?

La PSD2 son las siglas en inglés por las que habitualmente se hace referencia a la segunda directiva de servicios de pago comunitaria.

La PSD2, aplicable desde 2018, tiene por objeto promover la transparencia, la innovación y una mayor seguridad en los servicios de pago: además de introducir nuevos servicios de pago, establece requerimientos adicionales de seguridad en las transacciones de pago electrónicas y en los accesos a las cuentas a través de internet.

Nuevas medidas de seguridad

El 14 de septiembre entrará en vigor la normativa técnica aplicable en materia de seguridad, -Reglamento Delegado (UE) 2018/389 de la Comisión (conocido como RTS en SCA & CSC)- que establece las obligaciones de la autenticación reforzada.

A partir de esta fecha las operaciones de pago electrónico deberán hacerse con autenticación reforzada salvo que pueda aplicarse alguna exención.

Su aplicación implicará algunos cambios en la experiencia de pagos en los clientes, no solo en la banca electrónica y aplicaciones bancarias para dispositivos móviles, sino también en los pagos con tarjeta, tanto para el comercio electrónico como para el comercio presencial.

¿Qué es la autenticación reforzada?

La autenticación reforzada de clientes es un procedimiento de verificación de la identidad del cliente en el entorno electrónico. De acuerdo con la nueva normativa, esta identificación deberá incluir dos o más factores de autenticación de las siguientes categorías:

- Posesión (algo que solo posee el usuario)
- Inherencia (algo que es el usuario)
- Conocimiento (algo que solo conoce el usuario)

¿Qué implica la aplicación de autenticación reforzada?

En la práctica los pagos electrónicos cuentan ya con niveles de seguridad elevados, sin embargo, la aplicación de la nueva normativa requiere que en ocasiones se deberán introducir elementos adicionales de autenticación en pagos para los que hasta ahora no se requerían.

A modo de ejemplo, puede que además de los habituales códigos (algo que el usuario conoce) puedan enviar un código a un dispositivo (algo que el usuario posee), o pueden introducir factores biométricos (algo que el usuario es).

Cada banco, de manera individual, comunicará a sus clientes cómo la autenticación reforzada afectará a la operativa bancaria. En este sentido, los bancos trabajan para que la incorporación de la autenticación reforzada en dicha operativa se haga adoptando un equilibrio adecuado entre la seguridad y las necesidades de facilidad de uso y accesibilidad de los pagos electrónicos.

Consejos básicos de seguridad en internet

Los requerimientos adicionales reforzarán la seguridad en las operaciones electrónicas, no obstante, conviene recordar algunos consejos básicos para los usuarios de los servicios bancarios a la hora de operar de manera consciente y responsable:

- Comprobar que las claves se introducen en la banca electrónica o aplicación móvil del banco y no en portales o aplicaciones fraudulentas.
- El banco nunca pedirá información sobre los códigos y elementos de seguridad para operar en canales remotos ni por teléfono, ni por correo electrónico.
- No compartir con nadie las contraseñas de acceso a la banca electrónica, banca móvil ni las de las tarjetas.
- Ser precavidos y nunca instalar programas que se reciban por correo electrónico sino únicamente webs oficiales.
- No introducir datos privados en redes "wifi" públicas.
- Ante cualquier duda contactar con el banco.

Más información sobre medidas de seguridad disponible en este enlace.