Ficha informativa SCA

¿Qué es? SCA es un procedimiento de verificación de la identidad del cliente para las operaciones de pago, que deberá incluir dos o más factores de autenticación de las siguientes categorías:

- Conocimiento: algo que sabe.
- Posesión: algo que tiene.
- Inherencia: algo que es (biometría).

Obligatoriedad: desde el 14 septiembre de 2019, la normativa europea de pagos exige requisitos de seguridad más rigurosos para las operaciones de pago electrónico, que deberán realizarse con autenticación reforzada de clientes. Para los pagos con tarjeta en comercio electrónico se ha concedido cierta flexibilidad temporal para permitir que todos los actores involucrados (comercios electrónicos, emisores y titulares de tarjetas), puedan adoptar los cambios necesarios para aplicar la autenticación reforzada.

Confianza y sencillez: como consecuencia, los pagos con tarjeta en comercio electrónico serán aún más seguros e igualmente sencillos.

¿Qué va a cambiar? Hoy en la web del comercio se solicitan detalles de la tarjeta (nº + fecha + caducidad +CVV) y si se usan soluciones de comercio seguro (3DS) se requiere además un código adicional (SMS remitido al móvil, palabra clave, otros…).

- Según los nuevos requerimientos, todas las transacciones deberán efectuarse con soluciones de comercio seguro (3DS), pero los detalles de la tarjeta no constituyen un factor de verificación válido. Esto obliga a adoptar alternativas para obtener el doble factor de autenticación (o uno cuando se pueda aplicar una exención).

¿Cuándo? En la medida en que las entidades emisoras desplieguen los nuevos factores de autenticación y los comercios adopten las soluciones de comercio electrónico seguro, se requerirá el uso de estos códigos.

¿Qué códigos utilizar? Dependiendo de las circunstancias:

- durante el proceso de compra el titular de la tarjeta podrá ser redirigido a la aplicación o banca electrónica de la entidad donde se autenticará por el procedimiento habitual.
- en otras ocasiones el titular dispondrá de una clave personal (CIP o PIN u otra) y/o podrá recibir un SMS con un código para verificar el pago.

Facilidad de uso: para facilitar la experiencia de compra, se podrá requerir un único factor de autenticación en función del nivel de riesgo detectado, en operaciones de escasa cuantía o en transacciones recurrentes, etc.

Seguridad: conviene siempre operar de manera consciente y responsable. Comprobar que las claves se introducen en los sitios de banca electrónica o en páginas seguras de sitios oficiales evitando siempre acceder a través de enlaces en correos electrónicos que pueden llevar a portales o aplicaciones fraudulentas.