# Requerimientos necesarios para la utilización de EDITRAN bajo PSD2

En ASSET queremos compartir con vosotros un tema de especial relevancia y actualidad, relativo al procesamiento de operaciones de pago mediante el protocolo EDITRAN, en el marco del artículo 17 del Reglamento delegado (UE) 2018/389 de la CE relativo a las normas técnicas de regulación para la autenticación reforzada de clientes (SCA).

Según hemos confirmado con las entidades financieras y siguiendo recomendaciones al respecto del Banco de España, EDITRAN se considera que es un protocolo de pago corporativo seguro que garantiza al menos un nivel de seguridad equivalente a los previstos en la Directiva (UE) 2015/2366 siempre que se den ciertas condiciones, para ello EDITRAN debe estar actualizado a las últimas versiones y configurado adecuadamente.

Dado que el nivel de seguridad depende de manera decisiva tanto de la versión de EDITRAN instalada como de la configuración específica (el nivel de flexibilidad permitido a nivel de configuración es muy grande), el Banco de España instruye que se sigan las siguientes indicaciones:

- Se aconseja actualizarse a la última versión disponible EDITRAN siempre que sea posible. Debido a las mejoras de seguridad que introduce se recomienda tener instalada al menos la versión 5.2

- Los envíos de ficheros que contengan datos relativos a servicios de pago dentro del ámbito de la Payment Service Directive 2 (PSD2) deben ir firmados. En el caso de que no sea posible debe disponerse de mecanismos de autentificación alternativos equiparables.

- En cuanto al cifrado de datos, destacamos los siguientes aspectos:

a) Se debe aplicar un cifrado seguro que utilice técnicas reforzadas y ampliamente reconocidas.
El cifrado de datos debe estar siempre activado. Cuando sea posible podrá añadirse algún elemento adicional de seguridad (ej. túneles VPN).

b) La conexión e intercambio de claves simétricas se debe realizar utilizando preferentemente algoritmos seguros como RSA (preferencia por longitudes de clave de 2048 o 4096 bits frente a 1024 bits).
No debe utilizarse el algoritmo DES, salvo que existan medidas de seguridad adicionales que eliminen los riesgos asociados al uso de dicho algoritmo, tales como la implementación de una VPN.

c) Algoritmos de cifrado de datos utilizables:

* DES cifrado DES con clave simple: No debe utilizarse salvo que existan medidas de seguridad adicionales que eliminen los riesgos asociados al uso de dicho algoritmo, tales como la implementación de una VPN.
* TD2 cifrado Triple DES con clave doble: No es recomendado, debe evitarse siempre que sea posible en nuevas instalaciones y/o actualizaciones y migrar a algoritmos recomendados.
* TD3 cifrado Triple DES con clave triple: No recomendado, debe evitarse siempre que sea posible en nuevas instalaciones y/o actualizaciones y migrar a algoritmos recomendados.

* AES cifrado AES-128: Recomendado.
* AE2 cifrado AES-192: Recomendado.
* AE3 cifrado AES-256: Recomendado y preferido.

Las entidades están realizando los ajustes oportunos a la mayor brevedad y enviarán una comunicación a los clientes afectados en esta línea próximamente. En ella se indicará la necesidad de que los clientes contacten con su proveedor habitual del servicio, que también están al tanto, y hará una comunicación equivalente a los usuarios. Las entidades además facilitarán datos de contacto para que las empresas puedan dirigirse a ellos con el objetivo de planificar la actualización del sistema, definición de sesiones y pruebas y, por supuesto, en caso de duda o consulta.