

PRESENTACIÓN SOBRE FRAUDE

Carlos Sanz

III FORO REGIONAL DE PAGOS INSTANTÁNEOS
29 y 30 de mayo de 2025

DEPARTAMENTO DE SISTEMAS DE PAGO





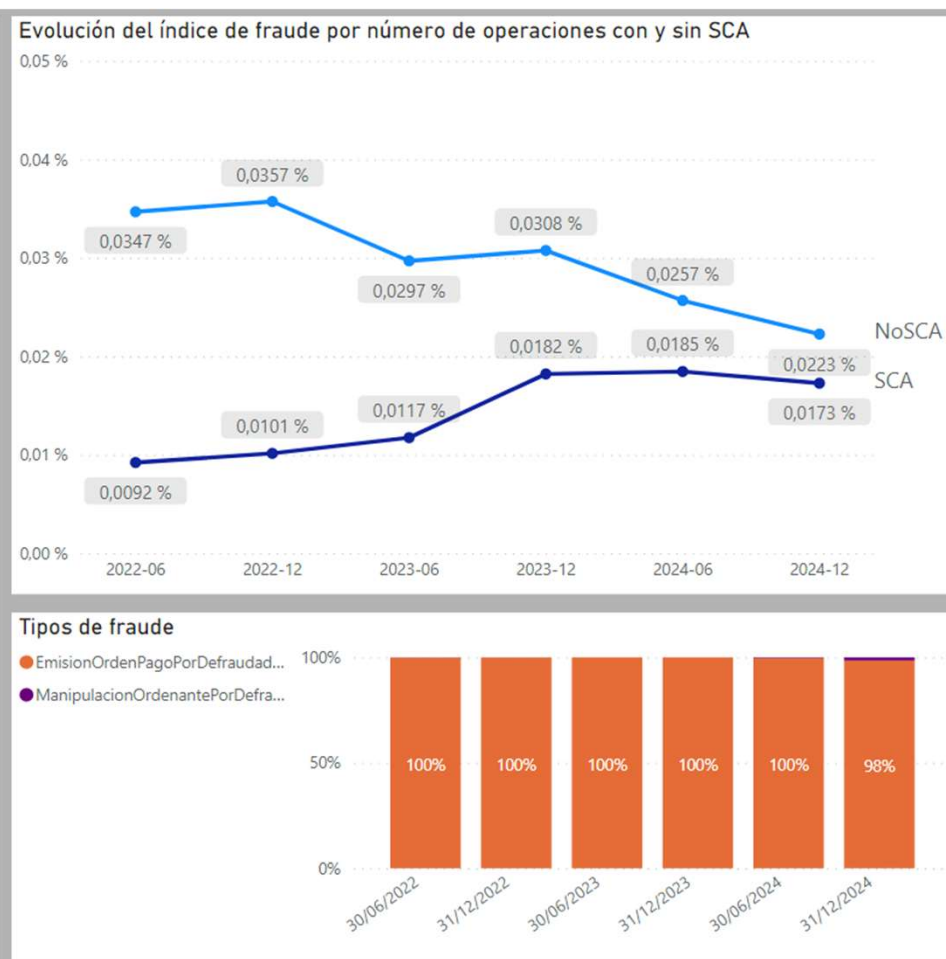
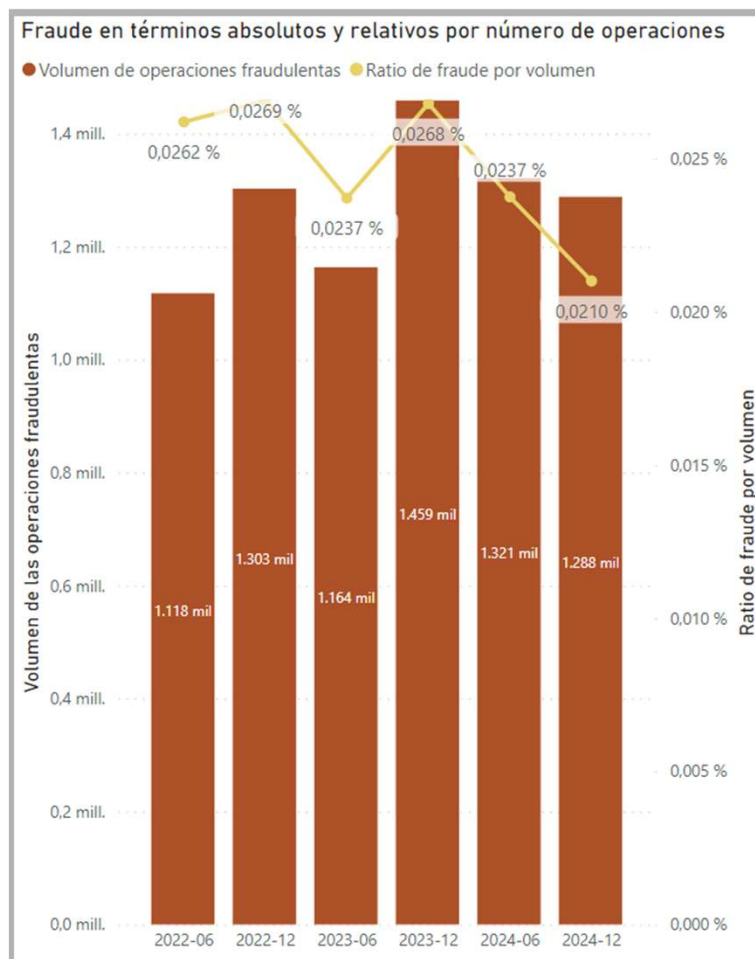
ÍNDICE

1. Tendencias recientes, evolución y tipología
2. Cambios normativos pasados y previstos (PSD2 / PSD3)
3. Herramientas para la mitigación del fraude



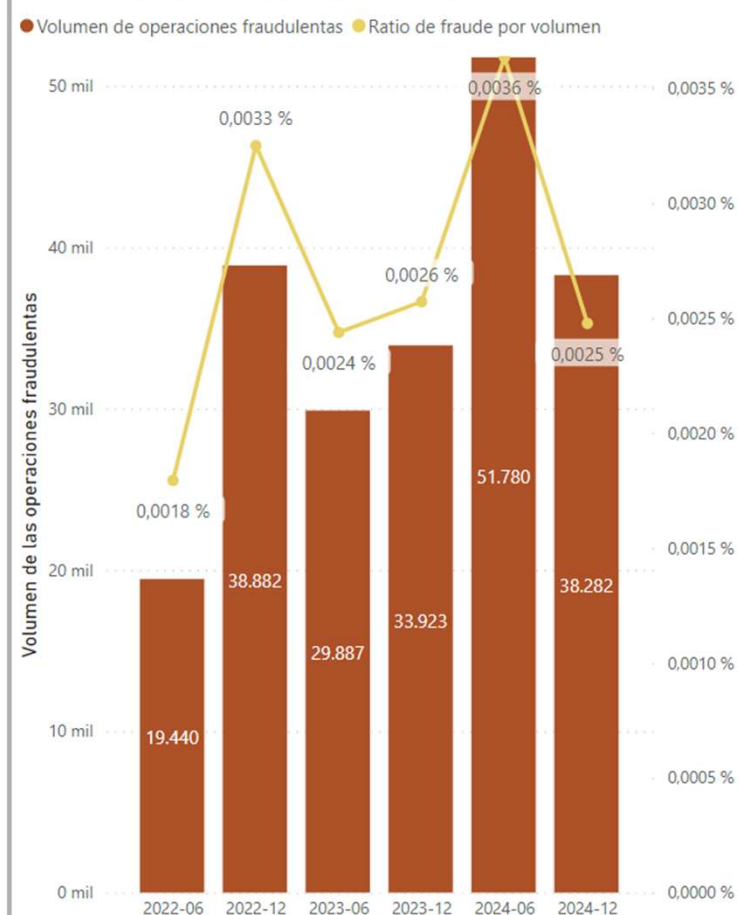
1. TENDENCIAS RECIENTES, EVOLUCIÓN Y TIPOLOGÍA

1. OPERACIONES CON TARJETAS



1. TRANSFERENCIAS

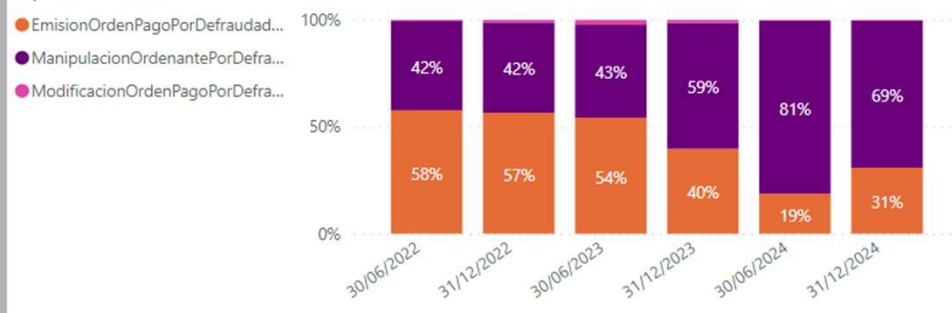
Fraude en términos absolutos y relativos por número de operaciones



Evolución del índice de fraude por número de operaciones con y sin SCA



Tipos de fraude





2. CAMBIOS NORMATIVOS PASADOS Y PREVISTOS (PSD2 / PSD3)

Propuesta PSD3/PSDR

➤ Alcance

- La actual PSD2 se dividirá en una **directiva (PSD3)** y un **reglamento (PSR)**. Este último pretende un mayor alineamiento de los estados miembros, precisando los derechos y obligaciones de los distintos participantes.
- Fusiona las directivas sobre prestación de servicios de pago y emisión de dinero electrónico, que pasa a considerarse un servicio más.

➤ Principales modificaciones en relación al fraude y autenticación reforzada

Las nuevas técnicas de defraudación basadas en la manipulación del cliente (ej. fraudes basados en ingeniería social/Phising), **han mostrado que la SCA no es suficiente**, por sí sola, para la eliminación del fraude.

Se introducen **disposiciones adicionales**:

- **Se fomenta la colaboración entre actores participantes en el mercado de pagos:**
 - Se establece una base jurídica que permite el **intercambio de información sobre el fraude entre PSP**.
 - Los **proveedores de servicios de comunicaciones electrónicas** tendrán obligación de colaborar con los PSP.
 - Los **proveedores de servicios técnicos** que se encarguen de proporcionar y verificar los elementos de la autenticación reforzada de cliente serán responsables de los perjuicios que puedan causar al beneficiario o PSP.
- Se asigna la **responsabilidad al PSP** en el caso de que un usuario de sus servicios de pago (PSU) haya sido **manipulado por un tercero (defraudador) haciéndose pasar por empleado**.
- Se añade una nueva disposición por la que se exige a los PSP que dispongan de **mecanismos de monitorización de las operaciones en tiempo real**.
- Obligación de realizar campañas de sensibilización sobre las tendencias y los riesgos del fraude dirigidos a los clientes y empleados.
- Se introducen aclaraciones sobre las operaciones excluidas en **ventas por correspondencia o telefónicas (MOTO)**, y exenciones en **operaciones iniciadas por el comerciante (MIT)**, dado que se entendían de manera divergente siendo objeto de abuso.
- Se incorporan **requisitos de accesibilidad en la autenticación reforzada** para facilitar la inclusión de grupos vulnerables.



3. HERRAMIENTAS PARA LA MITIGACIÓN DEL FRAUDE

➤ **Uso de IA y Machine Learning**

- Evaluación del riesgo e identificación del fraude en tiempo real
- Modelización y análisis predictivo **detección de operaciones sospechosas y anomalías basadas en patrones**
- Monitorización de amenazas
- Mecanismos de conocimiento y evaluación (scoring) del cliente
- Automatización de alertas y notificaciones al cliente

➤ **Educación al cliente**

- Campañas de información sobre riesgos y tipos comunes de fraude
- Comunicación activa al cliente sobre los procedimientos de la entidad

GRACIAS POR SU ATENCIÓN

