VISIONAMOS

Comité operativo
Prevención del fraude

Marzo 2026

PCI CERTIFICADO DSS

ISO 27001 SGS

CO19/9022

Agenda

1. Objetivo
2. ¿Qué es un fraude?
3. Modalidades de fraudes más comunes
4. ¿Qué hacer cuando un asociado es víctima de fraude?
5. ¿Cómo radicar un caso de presunto fraude en Visionamos?
6. Alertas y notificaciones
7. Nuevo monitoreo transaccional (Próximamente)
8. Mecanismo de seguridad
9. Recomendaciones para reducir el riesgo de fraude

visionamos

Objetivo

Brindar a las entidades participantes pautas y recomendaciones para fortalecer sus procedimientos y políticas internas, permitiendo una atención clara y oportuna frente a eventos reportados como presuntos fraudes o transacciones no reconocidas.

VISIONAMOS

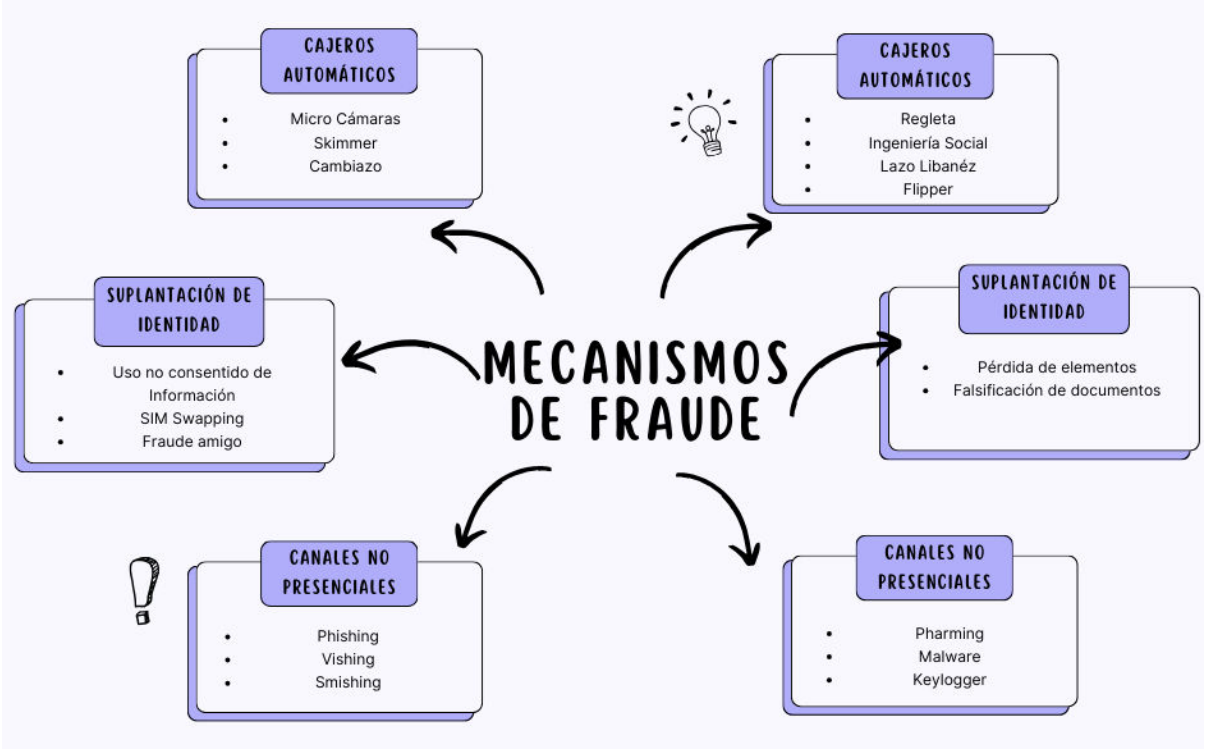
¿Qué es un fraude?

Actividad ilegal en la que se manipula información o recursos financieros para obtener ganancias indebidas, causando un perjuicio económico a un tercero. Puede incluir falsificación de documentos, manipulación de datos o suplantación de identidad.

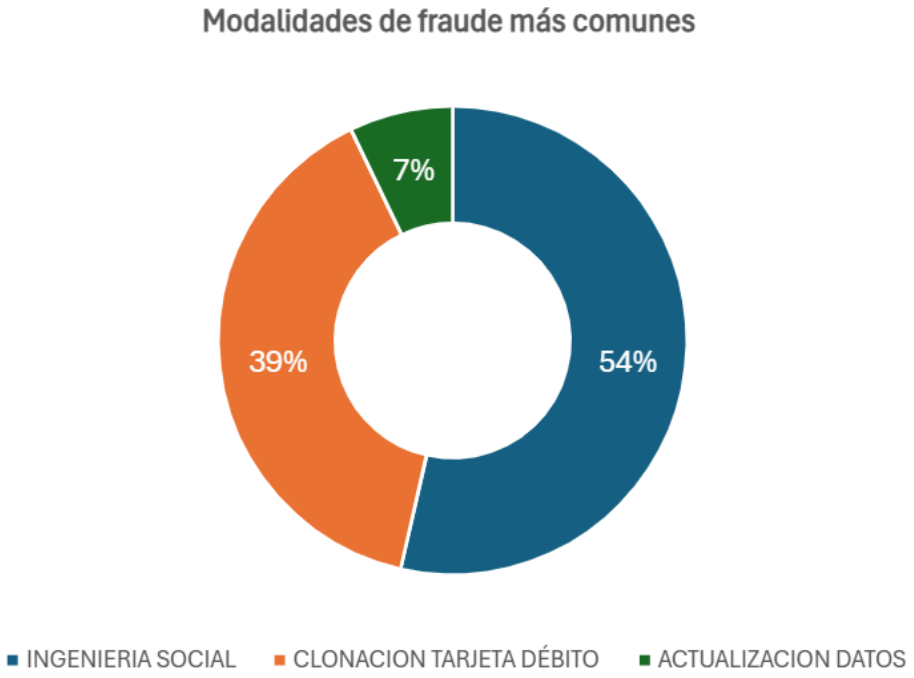
Elementos para identificarlo a tiempo:

- Transacciones o comportamientos inusuales.
- Movimientos no reconocidos en canales transaccionales.
- Solicitudes inusuales o urgentes que buscan saltar controles internos.
- Alertas del sistema de monitoreo.

Mecanismos de fraudes



Modalidad más frecuente
ultimo trimestre del 2025



¿Qué hacer cuando un asociado es víctima de fraude?

Cuando un asociado reporte a su entidad que ha sido víctima de fraude, la entidad deberá ejecutar **acciones inmediatas de seguridad**, de acuerdo con el tipo de producto afectado (fraude físico o virtual).

A continuación, se presentan pautas clave para el acompañamiento y la gestión adecuada del reporte de fraude por parte del asociado.

Fraude con tarjeta física

- Realizar el bloqueo inmediato de la tarjeta débito Red Coopcentral y la clave del asociado.

- Indagar al asociado si sufrió pérdida o robo de su tarjeta débito.

Medios para bloquear la Tarjeta Débito física

Autogestión asociado

El asociado/cliente tendrá a su disposición los siguientes canales para realizar el bloqueo de su tarjeta:

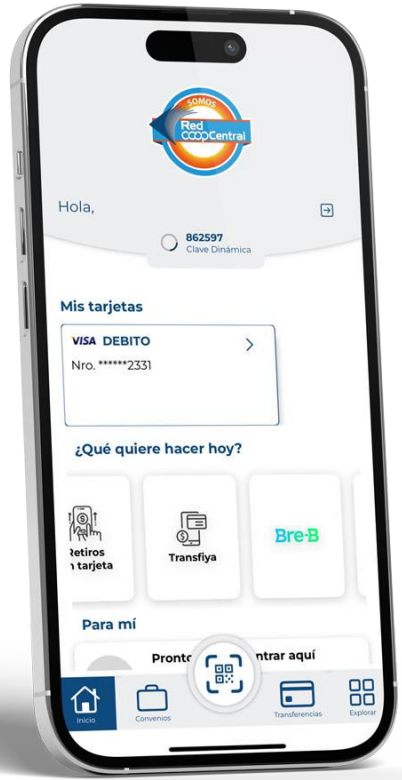
➢**Autogestión IVR: 01 8000 521124**

➢**Aplicación Móvil:** Explorar – bloquear tarjeta

➢**Portal natural:** Seguridad – tarjetas débito y crédito, bloquear tarjetas

Gestión entidad participante

- **Administrativo Web:** Administrativas – Cambiar Estado de Tarjeta
- **Entidades en Línea:** bloqueo de la cuenta y/o tarjeta a través de su core financiero/contable



Fraude por canales virtuales (App – Portal Natural)

Realizar el bloqueo inmediato del usuario de acceso al **Portal Natural o App**, para impedir el ingreso a estos canales.

Medios para bloquear los canales virtuales

Autogestión asociado

El asociado/cliente tendrá a su disposición los siguientes medios para realizar el bloqueo de los canales virtuales:

- **Aplicación Móvil:** Explorar – Bloquear servicios.
- **Portal Natural:** Seguridad – Servicios y notificaciones – Bloquear y desbloquear
- Llamando a su entidad para realizar el bloqueo.

Gestión entidad participante

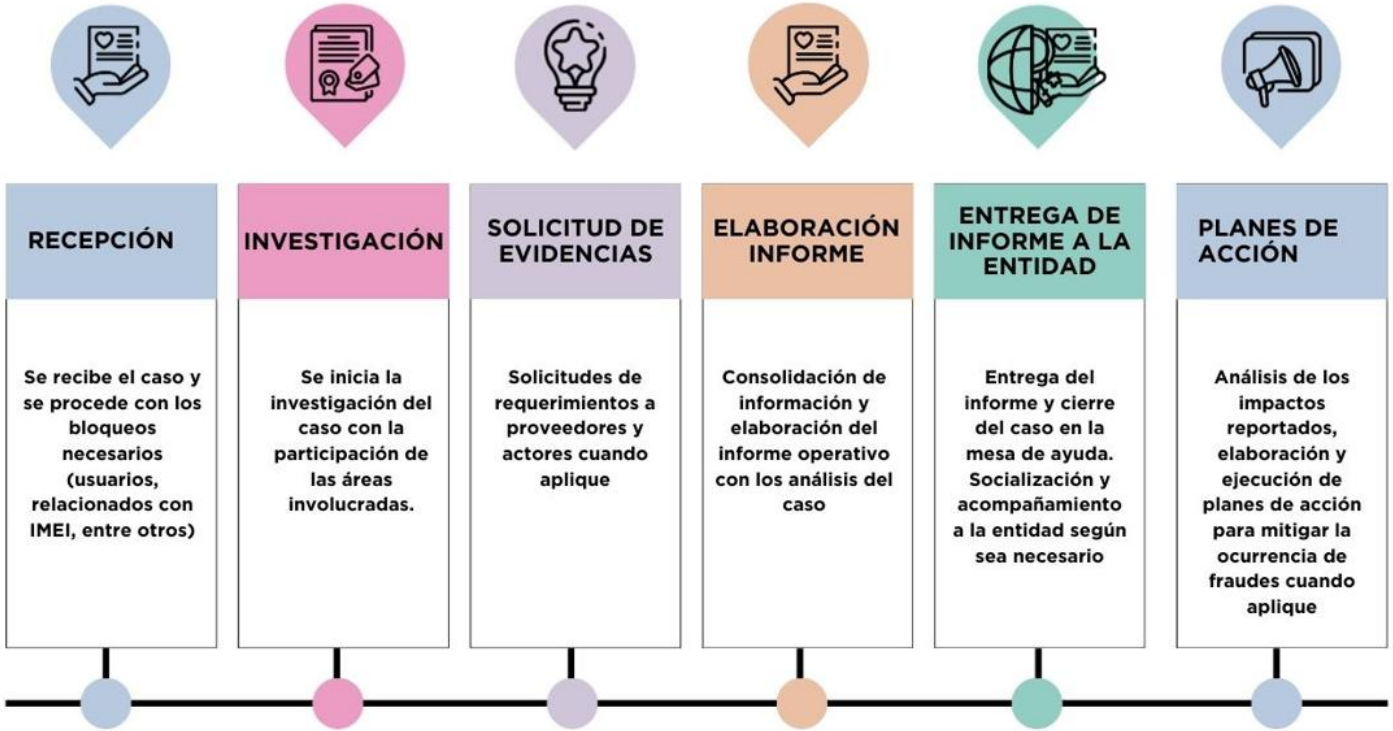
La entidad podrá realizar el bloqueo desde el **Centro de soluciones**:

Portal Natural – App – Bloqueo de usuarios

¿Cómo radicar un caso de presunto fraude?

La entidad participante deberá generar un requerimiento ante la Mesa de Ayuda, anexando el **formato Reporte de Fraudes Confirmados-02**, en caso de que sean más de 3 transacciones detallando lo sucedido.

Gestión del caso desde Visionamos



Alertas y notificaciones enviadas al asociado y a la entidad

ALERTAS PARA EL ASOCIADO

- **Notificación vía SMS:** Mensajes al móvil sobre transacciones.
- **Notificación por correo electrónico:** Información al correo registrado.
- **Llamadas de monitoreo:** Verificación telefónica de transacciones sospechosas.
- **Bloqueo de canales:** Evitar fraude al bloquear acceso a otras entidades.

ALERTAS PARA LA ENTIDAD

- Se enviará correos electrónicos por el área de monitoreo transaccional para la gestión oportuna con el asociado.
- Si no logran contactar al asociado afectado de manera oportuna, se procederá con el bloqueo de manera preventiva.

Nuevo monitoreo transaccional (próximamente)

- ✓ Plataforma moderna para gestionar alertas sospechosas.
- ✓ Perfil transaccional personalizado y bloqueos inmediatos ante riesgos.
- ✓ Operativo en BRE-B y en pruebas para otros canales.
- ✓ Tecnología con IA, Machine Learning y biometría de comportamiento para detectar fraudes en tiempo real.

Beneficios para la prevención del fraude

- ✓ Prevención temprana de fraudes y riesgos operativos.
- ✓ Reducción significativa de falsos positivos.
- ✓ Cumplimiento regulatorio y fortalecimiento del control interno.
- ✓ Plataforma escalable para soportar el crecimiento transaccional.
- ✓ Alta disponibilidad del servicio **(99.99%).**
- ✓ Mayor confianza y seguridad para los usuarios finales.

Mecanismos de seguridad

- ✓ Activar o desactivar tarjeta desde la app.
- ✓ Control de IMEI.
- ✓ Seguridad biométrica (nueva app).
- ✓ Preguntas de seguridad para recuperación de usuario y contraseñas, cambio de equipo celular.
- ✓ Monitoreo transaccional.

Recomendaciones para reducir el riesgo de fraude

1. Supervisa regularmente tus cuentas bancarias y tarjetas de crédito en busca de actividades sospechosas.
2. Utiliza contraseñas fuertes y únicas para cada cuenta en línea, y cámbialas periódicamente.
3. Nunca compartas información confidencial por teléfono, correo electrónico o mensajes de texto no seguros.
4. No divulgues información personal o financiera en sitios web no verificados.
5. Verifica la autenticidad de las solicitudes de información personal antes de responder.
6. No permitas que terceros te asistan en transacciones en cajeros automáticos.
7. Cubre el teclado al ingresar tu PIN al pagar en establecimientos.

Recomendaciones para reducir el riesgo de fraude

8. Accede al portal transaccional de tu entidad a través de su página oficial, no por enlaces sospechosos.
9. Bloquea tu teléfono celular perdido y notifica a tu entidad para bloquear usuarios y claves.
10. Durante el proceso de la transacción, se debe verificar constantemente que la URL se mantenga sin cambios y que no redireccione el pago a otra entidad o comercio.
11. Informa a los asociados sobre cómo bloquear canales virtuales y tarjetas físicas.
12. Mantén tus tarjetas débito de la Red Coopcentral y créditos del Banco Cooperativo Coopcentral apagadas.
13. Actualiza regularmente la seguridad de tus dispositivos y programas.
14. Capacitación constante a los asociados al buen manejo de sus datos personales.
15. Mantente informado sobre las tácticas de fraude comunes, como el phishing por correo electrónico y las llamadas fraudulentas.

¡Muchas gracias!

VISIONAMOS