

**Implementación de la Carta Circular 019 de 2024**  
**Actualización en SAC-E para casos de fraude**  
**Capacitación interna**  
**Dirección Servicio al Cliente**  
**Julio 2025**



## ¿Qué es la Carta Circular 019 de 2024?

La Superintendencia Financiera de Colombia establece lineamientos específicos para el tratamiento y reporte de eventos relacionados con fraude a través de los sistemas de atención al consumidor.

Esta mejora en la solución digital Smartsupervision es para optimizar el monitoreo, seguimiento y supervisión de las quejas y reclamos asociadas a fraudes.



¿Qué cambia a partir del 1 de julio? 📅 Nuevos campos en SAC-EA partir del 1 de julio de 2025 se implementan dos cambios principales en los formularios de gestión:

Nuevo campo: ✅ "Relacionado con fraude"

- ♦ Esta casilla se marcará automáticamente cuando la causal del caso corresponda a un evento de fraude.
- ♦ Esta información será enviada automáticamente a la SFC a través de Smartsupervision.

The screenshot displays the 'Integr@ Colocaciones V2.0' application window. The main form is titled 'Solicitud v3' and contains various fields for user and case information. A red box highlights the 'Relacionada con fraude?' checkbox, which is checked. The form includes sections for 'Datos Generales', 'Eventos', and 'Productos'. The 'Eventos' section shows a list of events, with 'Id Causal' set to 3981. The 'Productos' section shows a list of products, with 'Producto Super' set to 215. The 'Relacionada con fraude?' checkbox is located in the 'Eventos' section, next to the 'Id Causal' field.

Id Canal	Id Prodserv	Id Causal	nit Origen	Proceso	Agencia
16	31	3981	890927034	M6P4	

Producto Super	Causal Super	Canal Super	Escalamiento	Cond Especial	Ente control	Tipo MarcaSuper	Estado super	Pto recep SUPER	Instan .recepción	Tipo Admisión Super	desistimiento Super	Estado acepta Super	Rectificación Super	Tipo Identificación Super	sexoSuper	DiviCiudad super	Divi Dpto super	Ult Fe envío a Sup	Ult Fecha Gestión Sup	Ult Fecha Int m3 Sup
215	940	14	No				1	1	2	9	2			1	1	5088	5			





Si se te asigna un caso marcado como fraude:

- ◆ Debes diligenciar los campos específicos del análisis relacionados con el tratamiento de fraudes.
- ◆ Estos campos son obligatorios para cerrar el análisis.

Integr@ Colocaciones V2.0 <colmd20.fmx> [LUI5GALI@cliente-unico] - [Análisis de Servicios :SER20020 <SER20020>] [LUI5GALI@cliente-unico]

Archivo Edición Parametros Transacciones PProcesos RepOrtes Utilitarios Herramientas ? Window

Consulta Servicio | Documentos Cliente | **Análisis** | Detalles Seg Análisis | Reasignar | log Reversion

Nro Solicitud: 301243 # Registro: 2025/06/27 Tipo Seguimiento: 1 INICIO INVESTIGACIÓN Y ANÁLISIS

Responsable: 1037583996 JULIANA ANDREASANCHEZ MEJIA

Fecha Vto: 2025/07/03 Vencido Tiempo Rta Análisis: 3 Tiempo Rta Adicional:

Explicación \*\* Explicar qué pasó, cuándo, por qué...

Corrección \*\* Corrección implementada y plan de acción para que no vuelva a ocurrir, esto solo si es a favor del cliente.

No. Sac TI / Procesos:

Observación:

R/ta Tiempo adicional:

Tipo Solicitud: RECLAMOS Producto: 31 - TARJETA CRÉDITO

Proceso: M6P4-Gestión de Medios de Pago Fecha Solución:

Código Riesgo Pronus\* Este campo se llena si el caso es a favor del cliente

Nombre Originador: COLTEFINANCIERA SA

\*\* Campos que deben ser diligenciados, en caso de evidencia

Seguimiento: 440033 Usuario Crea: LUI5GALI

Estado:

codigo pronus:

Tipo fraude:

Tipo fraude: 2

Tipo fraude: 1

Tipo Fraude

Find: %

Id Tipo Fraude Super	Descripción
1	Interno
2	Externo

Find OK Cancel

Uso. Mod:

nto reclamo: 250.000

nto reconocido: 250.000



Consulta Servicio | Documentos Cliente | **Análisis** | Detalles Seg Análisis | Reasignar | log Reversion

Nro Solicitud: 301243 F Registro: 2025/06/27 Tipo Seguimiento: 1 INICIO INVESTIGACIÓN Y ANÁLISIS

Responsable: 1037583996 JULIANA ANDREASANCHEZ MEJIA

Fecha Vto: 2025/07/03 ☐ Vencido Tiempo Rta Análisis: 3 Tiempo Rta Adicional:

**Explicación \***  
Explicar qué pasó, cuándo, por qué...

**Corrección \*\***  
Corrección implementada y plan de acción para que no vuelva a ocurrir, esto solo si es a favor del cliente.


No. Sac TI / Procesos:

Observación:

R/ta Tiempo adicional:

Tipo Solicitud: RECLAMOS Producto:

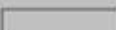
Proceso: M6P4-Gestión de Medios de Pago

Código Riesgo Pronus\*: 

Nombre Originador: COLTEFINANCIERA SA


**\*\* Campos que deben ser diligenciados, en caso de evidenciar que...**


Seguimiento: 440033 Usuario Crea: LUISGALI Fecha:

Estado: 

codigo prunus:

**Fraude**

Tipo fraude: 

Tipo modalidad fraude: 1 

**Modalidad Fraude**

Find: %

Id Modalidad Super	Descripcion
1	Suplantación de
2	Sim Swapping
3	Vulneración de c
4	Phishing
5	Vishing
6	Smishing
7	Pharming
8	Enumeración
9	Malware
10	Skimming
11	Ataque BIN

Find OK Cancel





Consulta Servicio

Documentos Cliente

**Análisis**

Detalles Seg Análisis

Reasignar

log Reversion

Nro Solicitud: 301243 F Registro: 2025/06/27 Tipo Seguimiento: 1 INICIO INVESTIGACIÓN Y ANÁLISIS

Responsable: 1037583996 JULIANA ANDREASANCHEZ MEJIA

Fecha Vto: 2025/07/03 ☐ Vencido Tiempo Rta Análisis: 3 Tiempo Rta Adicional:

Explicación \* Explicar qué pasó, cuándo, por qué...

Corrección \*\* Corrección implementada y plan de acción para que no vuelva a ocurrir, esto solo si es a favor del cliente.

No. Sac TI / Procesos

Observación

R/ta Tiempo adicional

Tipo Solicitud: RECLAMOS Producto: 31 - TARJETA CRÉDITO

Proceso: M6P4-Gestión de Medios de Pago Fecha Solución:

Código Riesgo Pronus\*

Nombre Originador: COLTEFINANCIERA SA

**\*\* Campos que deben ser diligenciados, en caso de evidenciar que se generó un error de parte de Coltefinanciera**

**Datos Sistema**

Seguimiento: 440033 Usuario Crea: LUISGALI Fecha Crea: 2025/06/27 F. Mod: Usu. Mod:

Estado:

codigo prunus

**Fraude**

Tipo fraude: 2 Exemo

Tipo modalidad fraude: 1 Suplantación de identidad

Monto reclamo

250,000

Monto reconocido

250,000

Aquí se pone el valor que el cliente reclama en la petición

Aquí se pone el valor que reconoció Coltefinanciera, de lo contrario es \$0.



**IMPORTANTE:** No se permite el cierre parcial ✅ El análisis solo podrá cerrarse cuando haya una respuesta definitiva. 📅 Si se cumple el plazo normativo de 15 días hábiles sin respuesta final, se deberá solicitar prórroga a la SFC.



## Tipo de fraude

Código	Tipología queja fraude	Descripción
1	Interno	Registre sí el evento identificado ocurrió por acciones de empleados o colaboradores de la entidad.
2	Externo	Registre sí el evento identificado ocurrió por acciones de externos y que resulte en la materialización de un fraude bajo alguna de las modalidades relacionadas en la hoja "modalidad de fraude"





# Modalidad de fraude

Código	Modalidad de Fraude	Descripción
1	Suplantación de identidad	Consiste en usurpar la identidad de un consumidor financiero con el ánimo de obtener productos, servicios o recursos en su nombre. Transacciones repudiadas por el cliente, donde se incluyan presuntos eventos de fraude o uso no autorizado de sus productos financiero y situaciones de suplantación que permitan transacciones (transferencias, pagos, descuentos) que el consumidor no reconoce.
2	Sim Swapping	Consiste en aprovechar la capacidad de un proveedor de servicios de telefonía móvil para transferir un número de teléfono a un dispositivo que contiene una tarjeta SIM diferente.
3	Vulneración de cuenta o producto	Consiste en aprovechar la vulnerabilidad en un control o en un proceso, permitiendo el acceso a los productos y/o recursos de un consumidor financiero.
4	Phishing	Consiste en la emisión masiva de correos electrónicos a usuarios. Estos correos suplantán a entidades de confianza y persiguen el engaño del consumidor financiero y la consecución de información.
5	Vishing	Consiste en la suplantación de entidades de confianza a través de llamadas telefónicas, persiguiendo el engaño del consumidor financiero y la consecución de información.
6	Smishing	Consiste en el envío masivo de mensajes de texto a usuarios. Estos mensajes suplantán a entidades de confianza y persiguen el engaño del consumidor financiero y la consecución de información.



	7	Pharming	Es un tipo de ataque informático cuyo objetivo es el robo de información sensible. Para ello, los ciberdelincuentes realizan un ataque al DNS (Domain Name Server) con el que consiguen redirigir a los consumidores financieros a una página web falsa, que cuenta con el nombre de dominio oficial.
	8	Enumeración	Consiste en identificar nombres de usuarios u otros datos válidos a través de diferentes técnicas con la finalidad de usarlos irregularmente.
	9	Malware	Software malicioso diseñado para alterar o extraer información de cualquier dispositivo, servicio o red. Se incluyen, Ransomware, Keyloggers, etc.
	10	Skimming	Consiste en tomar información de la banda magnética de la tarjeta bancaria con fines de duplicarla, por medio de dispositivos modificados conocidos como "skimmer", conectado a un ATM.
	11	Ataque BIN	Es un ataque de fuerza bruta que busca identificar en un comercio una combinación válida de PAN, fecha de vencimiento y CVC.
	12	Fraude amigable	Aquel en el que un titular de un producto presenta un reclamo asociado, a veces con el conocimiento de que recibió el servicio el propio consumidor financiero o sabiendo que personas diferentes a él (por ejemplo familiares) han tenido acceso a sus productos y servicios.



13	Cambiado	Consiste en cambiar la tarjeta débito o crédito de la víctima por otra falsa.
14	Falsificación	Consiste en la creación o modificación de documentos, timbres, sellos, firmas, etc, con el fin de hacerlos parecer como verdaderos.
15	Pérdida de elementos (como Tarjetas, chequeras, tokens)	Consiste en el que un titular extravíe alguno de los elementos (como tarjetas, chequeras, tokens, documentos de identidad, dispositivos electrónicos con información financiera, entre otros).
16	Suplantación de elementos suministrados por la entidad (como QRs de pagos, correspondientes, datafonos)	Consiste en alterar los códigos QR de pagos en los correspondientes bancarios y puntos de pago de los comercios, cambiándolos por códigos de otro destinatario, el cual no corresponde al comercio.
17	Estafa	Consiste en provocar un perjuicio patrimonial a alguien mediante engaño. Por ejemplo, compras en comercios inexistentes, entre otros.
18	Errores operativos de la entidad que hayan propiciado o facilitado el fraude	Consiste en errores operativos identificados o no identificados, que hayan propiciado o facilitado eventos de fraude.
19	Otras técnicas de ingeniería social	Ingrese la modalidad "Otras técnicas de ingeniería social" ÚNICAMENTE en caso de que no se encuentre cobijada bajo las siguientes modalidades: phishing, vishing, smishing, cambiado y estafa. Favor tener en cuenta las definiciones.
90	Otras	Ingrese la modalidad de fraude ÚNICAMENTE en caso de que no se encuentre cobijada en las opciones propuestas. No deberán reportarse "taquillazos", ni actos de violencia en contra de la entidad.







¡Muchas gracias!





# Coltefinanciera

## ¡Contáctanos!

Línea Gratuita Nacional 01800 01800 40  
[coltefinanciera@coltefinanciera.com.co](mailto:coltefinanciera@coltefinanciera.com.co)  
[www.coltefinanciera.com.co](http://www.coltefinanciera.com.co)

