**Reporte Normativo sobre la Generación de Informes**

Directrices y Procedimientos para la Elaboración de Reportes Efectivos

06/05/2025

# 1. Executive Summary

* Ejecutivo: Reporte sobre la Generación de Informes de Actividad de Fraude\*\*

Este informe establece los requisitos de presentación y cumplimiento para los emisores de Visa en la región de ALC en relación con la actividad fraudulenta. Se exige que todos los emisores informen al menos el 95% del fraude detectado y clasifiquen correctamente el 90% de dicha actividad, limitando el fraude misceláneo a un máximo del 5%. Los informes deben ser presentados dentro de los 60 días posteriores a la detección y dentro de los 30 días tras la notificación de controversia por parte del tarjetahabiente. El incumplimiento de estos requisitos puede resultar en auditorías a cargo del emisor, recargos por incumplimiento y la introducción de una cuota del programa FRECOP a partir del 12 de abril de 2025. Se recomienda a los emisores consultar la guía del Sistema de Reporte de Fraude (FRS) para obtener instrucciones detalladas sobre el cumplimiento normativo.

# 2. Alcance

## Alcance del Informe

Este informe tiene como propósito establecer un marco normativo claro y detallado sobre la generación de informes de actividad de fraude en el ecosistema de pagos de Visa, específicamente para los emisores en la región de América Latina y el Caribe (ALC). El alcance del informe se define de la siguiente manera:

## 1. Propósito

## El informe busca

* Proporcionar directrices claras sobre las obligaciones de los emisores de Visa en relación con la detección, clasificación y reporte de actividades fraudulentas.
* Establecer criterios específicos que deben cumplirse para asegurar la integridad y precisión de los informes de fraude.
* Informar sobre las consecuencias que pueden derivarse del incumplimiento de los requisitos establecidos.

## 2. Límites

## El informe se limita a

* Aplicar únicamente a los emisores de Visa en la región de ALC, excluyendo otras regiones o entidades que no estén bajo esta normativa.
* Enfocarse exclusivamente en la actividad fraudulenta relacionada con transacciones procesadas a través de la red de Visa, sin abordar otros tipos de fraudes que no estén directamente vinculados a esta red.
* Detallar los requisitos de presentación y no incluir procedimientos operativos internos o medidas de mitigación de fraude que los emisores puedan implementar más allá de lo estipulado en este informe.

## 3. Audiencia

## Este informe está dirigido a

* Ejecutivos y personal responsable de la gestión de riesgos y cumplimiento normativo en instituciones emisoras de Visa.
* Equipos de auditoría interna y externa que supervisan el cumplimiento de las normativas de fraude.
* Cualquier parte interesada que requiera información sobre las obligaciones de reporte de fraude en el ecosistema de Visa.

## 4. Exclusiones

## No se incluyen en este informe

* Detalles sobre las herramientas tecnológicas o sistemas específicos que los emisores pueden utilizar para detectar o reportar fraude.
* Información sobre el tratamiento de datos personales o regulaciones de privacidad que puedan ser relevantes en el contexto de la actividad fraudulenta.

Este alcance establece un marco claro para la interpretación y aplicación de las directrices contenidas en el informe, asegurando que todas las partes interesadas comprendan sus responsabilidades y los límites de la normativa.

# 3. Análisis Regulatorio

## Análisis Regulatorio sobre la Generación de Informes de Actividad de Fraude en el Ecosistema de Pagos de Visa

## 1. Principales Requisitos Normativos Identificados

## 1.1. Obligaciones Generales

Los emisores de Visa en la región de América Latina y el Caribe (ALC) tienen la obligación de informar toda actividad fraudulenta, sin importar el estatus de la transacción. Esta obligación es fundamental para mantener la integridad del sistema de pagos y proteger a los tarjetahabientes.

## 1.2. Criterios de Presentación

## Los emisores deben cumplir con criterios específicos en la presentación de informes de fraude

* \*\*Cobertura de Fraude\*\*: Se requiere que al menos el \*\*95%\*\* de toda la actividad fraudulenta detectada sea reportada.
* \*\*Clasificación de Fraude\*\*: Al menos el \*\*90%\*\* de la actividad fraudulenta debe ser clasificada correctamente, lo que implica un manejo adecuado de los datos y una comprensión clara de las categorías de fraude.
* \*\*Limitación de Tipos de Fraude\*\*: No más del \*\*5%\*\* de las denuncias puede ser registrado como tipo de fraude 05 (Misceláneo), lo que sugiere la necesidad de una clasificación precisa y rigurosa.

## 1.3. Plazos para el Reporte

## Los emisores deben cumplir con plazos estrictos para la presentación de informes

* Informar sobre la actividad fraudulenta a más tardar \*\*60 días\*\* desde su detección.
* Reportar casos en un plazo de \*\*30 días\*\* tras la notificación de controversia por parte del tarjetahabiente.

## 2. Obligaciones para las Entidades Reguladas

## 2.1. Responsabilidad de Reporte

Los emisores son responsables de asegurar que todos los informes de fraude se presenten de manera oportuna y precisa, cumpliendo con los criterios establecidos por Visa. Esto incluye la implementación de sistemas internos que faciliten la detección y clasificación del fraude.

## 2.2. Capacitación y Recursos

Se espera que los emisores proporcionen capacitación adecuada a su personal sobre los procedimientos de reporte de fraude y utilicen recursos como la \*\*guía Fraud Reporting System (FRS)—User’s Guide\*\* para garantizar el cumplimiento normativo.

## 2.3. Consulta con Representantes de Visa

Los emisores deben mantener una comunicación constante con sus representantes de Visa para recibir asesoría y asegurarse de que sus prácticas de reporte estén alineadas con las normativas vigentes.

## 3. Procesos de Cumplimiento Necesarios

## 3.1. Implementación de Sistemas de Detección

Los emisores deben establecer sistemas robustos para la detección de fraude que permitan identificar y clasificar las transacciones fraudulentas de manera efectiva y eficiente.

## 3.2. Auditorías Internas

Es recomendable que los emisores realicen auditorías internas periódicas para evaluar la efectividad de sus procesos de reporte y asegurarse de que cumplen con los requisitos establecidos por Visa.

## 3.3. Documentación y Registro

Es esencial mantener una documentación detallada de todas las actividades relacionadas con el fraude, incluyendo la detección, clasificación y reporte, para facilitar auditorías y revisiones.

## 4. Riesgos y Consecuencias del Incumplimiento

## 4.1. Auditorías y Costos Asociados

Si un emisor no cumple con los requisitos de presentación de informes, Visa puede llevar a cabo auditorías en el lugar. Los costos de estas auditorías serán asumidos por el emisor, lo que puede representar una carga financiera significativa.

## 4.2. Recargos por Incumplimiento

Los emisores que no cumplan con los estándares de presentación de informes estarán sujetos a recargos por incumplimiento, lo que afectará su rentabilidad y reputación en el mercado.

## 4.3. Cuota FRECOP

A partir del \*\*12 de abril de 2025\*\*, se introducirá una cuota del programa de Control e Informes de Fraude (FRECOP) para emisores que no informen el fraude con exactitud. Esta cuota puede representar un costo adicional significativo para los emisores que no cumplan con las normativas.

## 5. Conclusiones

El cumplimiento de los requisitos de presentación de informes de actividad fraudulenta es esencial para la sostenibilidad del ecosistema de pagos de Visa. Los emisores deben adoptar un enfoque proactivo para mejorar sus procesos de reporte, no solo para evitar sanciones, sino también para contribuir a la reducción del fraude a nivel global. La implementación de sistemas adecuados, la capacitación del personal y la consulta con representantes de Visa son pasos críticos para garantizar el cumplimiento normativo.

## 6. Información de Contacto

Para más información, se recomienda visitar la [página de ayuda de Visa](https://www.visa.com/support) o comunicarse directamente con el soporte regional de Visa.

# 4. Conclusiones

## Conclusiones Clave sobre la Normativa de Informes de Actividad de Fraude en el Ecosistema de Pagos de Visa

1. \*\*Importancia del Cumplimiento Normativo\*\*: El cumplimiento de los requisitos de presentación de informes de actividad fraudulenta es fundamental para la integridad del ecosistema de pagos de Visa. Los emisores deben reconocer que la transparencia y la precisión en el reporte no solo son obligaciones legales, sino también prácticas que fomentan la confianza de los tarjetahabientes y la sostenibilidad del sistema.

2. \*\*Criterios de Presentación Rigurosos\*\*: Los criterios establecidos, como la obligación de reportar al menos el 95% de la actividad fraudulenta y clasificar correctamente el 90% de los casos, subrayan la necesidad de un manejo meticuloso de los datos. Esto implica que los emisores deben invertir en tecnología y capacitación para asegurar que sus procesos de detección y clasificación sean efectivos.

3. \*\*Plazos Estrictos y Responsabilidad\*\*: Los plazos de 60 y 30 días para la presentación de informes son exigentes y requieren que los emisores establezcan protocolos internos eficientes. La responsabilidad recae en los emisores para garantizar que se cumplan estos plazos, lo que puede requerir una revisión y mejora continua de sus sistemas de reporte.

4. \*\*Riesgos Financieros por Incumplimiento\*\*: Las consecuencias del incumplimiento, que incluyen auditorías costosas, recargos y la futura cuota del programa FRECOP, representan riesgos financieros significativos. Esto resalta la necesidad de que los emisores adopten un enfoque proactivo para evitar sanciones que puedan afectar su rentabilidad y reputación.

5. \*\*Capacitación y Recursos como Claves del Éxito\*\*: La capacitación del personal y el uso de recursos como la guía FRS son esenciales para asegurar que todos los empleados comprendan los procedimientos de reporte de fraude. La inversión en formación no solo mejora el cumplimiento, sino que también fortalece la capacidad de la organización para detectar y prevenir el fraude.

6. \*\*Comunicación Continua con Visa\*\*: Mantener una comunicación constante con los representantes de Visa es crucial para que los emisores se mantengan actualizados sobre las normativas y reciban asesoría sobre las mejores prácticas. Esta colaboración puede facilitar la adaptación a cambios normativos y mejorar la efectividad de los procesos de reporte.

7. \*\*Implementación de Sistemas de Detección Efectivos\*\*: La creación de sistemas robustos para la detección y clasificación de fraude es un aspecto crítico que los emisores deben priorizar. La tecnología adecuada puede ayudar a minimizar errores en el reporte y a cumplir con los criterios establecidos por Visa.

8. \*\*Auditorías Internas como Herramienta de Mejora\*\*: La realización de auditorías internas periódicas permitirá a los emisores evaluar la efectividad de sus procesos de reporte y detectar áreas de mejora. Esta práctica no solo asegura el cumplimiento, sino que también puede contribuir a la optimización de recursos y procesos.

En resumen, los emisores de Visa en América Latina y el Caribe deben adoptar un enfoque integral y proactivo para cumplir con las normativas de reporte de fraude. Esto no solo les permitirá evitar sanciones, sino que también contribuirá a un ecosistema de pagos más seguro y eficiente.

# 5. Recomendaciones

A continuación, se presentan recomendaciones prácticas y accionables para que los emisores de Visa en América Latina y el Caribe cumplan con la normativa de informes de actividad de fraude:

## Recomendaciones Prácticas

## 1. \*\*Desarrollo de un Plan de Cumplimiento Normativo\*\*

* \*\*Establecer un equipo dedicado\*\*: Formar un equipo de cumplimiento normativo que se encargue de supervisar y gestionar todos los aspectos relacionados con la normativa de informes de fraude.
* \*\*Definir roles y responsabilidades\*\*: Asignar responsabilidades claras a cada miembro del equipo para asegurar que todos comprendan su papel en el proceso de reporte.

## 2. \*\*Inversión en Tecnología\*\*

* \*\*Implementar soluciones de detección de fraude\*\*: Adoptar tecnologías avanzadas, como inteligencia artificial y aprendizaje automático, para mejorar la detección y clasificación de actividades fraudulentas.
* \*\*Automatizar procesos de reporte\*\*: Utilizar software que facilite la recopilación y el análisis de datos para cumplir con los criterios de presentación establecidos por Visa.

## 3. \*\*Capacitación Continua\*\*

* \*\*Programas de formación regular\*\*: Establecer un programa de capacitación continua para el personal involucrado en la detección y reporte de fraude, asegurando que estén al tanto de las últimas normativas y mejores prácticas.
* \*\*Simulaciones de fraude\*\*: Realizar ejercicios prácticos que simulen situaciones de fraude para que el personal pueda practicar la identificación y el reporte de estos casos.

## 4. \*\*Establecimiento de Protocolos Internos\*\*

* \*\*Crear un manual de procedimientos\*\*: Documentar todos los procesos de detección y reporte de fraude en un manual accesible para el personal.
* \*\*Definir un flujo de trabajo claro\*\*: Establecer un flujo de trabajo que detalle cada paso desde la detección de un posible fraude hasta la presentación del informe a Visa.

## 5. \*\*Monitoreo y Evaluación de Desempeño\*\*

* \*\*Implementar indicadores de desempeño\*\*: Definir KPIs (indicadores clave de desempeño) que midan la efectividad de los procesos de detección y reporte de fraude.
* \*\*Revisiones periódicas\*\*: Realizar revisiones trimestrales de los informes de fraude para evaluar la precisión y la puntualidad de los mismos.

## 6. \*\*Auditorías Internas\*\*

* \*\*Programar auditorías regulares\*\*: Establecer un calendario de auditorías internas para evaluar la efectividad de los procesos de reporte y detectar áreas de mejora.
* \*\*Informes de auditoría\*\*: Generar informes de auditoría que incluyan recomendaciones específicas para mejorar los procesos y asegurar el cumplimiento normativo.

## 7. \*\*Comunicación Proactiva con Visa\*\*

* \*\*Establecer un canal de comunicación\*\*: Designar un punto de contacto dentro de la organización para mantener una comunicación constante con Visa.
* \*\*Participar en foros y capacitaciones\*\*: Asistir a eventos y capacitaciones organizados por Visa para mantenerse actualizado sobre cambios normativos y mejores prácticas.

## 8. \*\*Gestión de Riesgos\*\*

* \*\*Realizar un análisis de riesgos\*\*: Evaluar los riesgos asociados con el incumplimiento normativo y desarrollar estrategias para mitigarlos.
* \*\*Plan de contingencia\*\*: Crear un plan de contingencia para abordar posibles incidentes de fraude y garantizar que se sigan los procedimientos adecuados en caso de incumplimiento.

## Implementación de las Recomendaciones

* \*\*Cronograma de Implementación\*\*: Desarrollar un cronograma detallado para la implementación de estas recomendaciones, asignando plazos y responsables para cada acción.
* \*\*Revisión y Ajuste\*\*: Establecer un proceso de revisión y ajuste de las recomendaciones implementadas, asegurando que se adapten a cambios en la normativa o en el entorno del mercado.

Al adoptar estas recomendaciones, los emisores de Visa no solo cumplirán con la normativa de informes de actividad de fraude, sino que también fortalecerán su capacidad para prevenir y gestionar el fraude, contribuyendo a un ecosistema de pagos más seguro y eficiente.

# 6. Referencias

Para un análisis normativo como el que has presentado, es importante incluir referencias a documentos oficiales, normativas y fuentes relevantes que sustenten los requisitos y obligaciones mencionados. A continuación, se sugieren algunas referencias que podrían ser relevantes para incluir en una sección de referencias:

## Referencias

## 1. \*\*Reglamento de la Red de Pagos de Visa\*\*

* Documento que establece las normas y procedimientos que deben seguir los emisores y adquirentes en relación con las transacciones de pago y la gestión de fraude.

## 2. \*\*Políticas de Prevención de Fraude de Visa\*\*

* Directrices específicas sobre cómo los emisores deben manejar y reportar la actividad fraudulenta, incluyendo criterios de clasificación y plazos de reporte.

## 3. \*\*Normativa de la Autoridad de Supervisión Financiera\*\*

* Regulaciones locales o regionales que rigen la actividad de los emisores de tarjetas y la gestión del fraude en el sector financiero.

## 4. \*\*Estándares de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS)\*\*

* Normativa que establece requisitos de seguridad para proteger la información de tarjetas de pago y prevenir el fraude.

## 5. \*\*Guía de Reporte de Actividades Sospechosas (SAR)\*\*

* Documentación que detalla los procedimientos para reportar actividades sospechosas a las autoridades competentes, en caso de que se identifique fraude.

## 6. \*\*Informes Anuales de Fraude de Visa\*\*

* Informes que proporcionan estadísticas y análisis sobre la actividad fraudulenta en el ecosistema de pagos, que pueden servir como referencia para los emisores.

## 7. \*\*Legislación Local sobre Fraude y Protección al Consumidor\*\*

* Leyes que regulan la actividad fraudulenta y protegen a los consumidores en el ámbito de los pagos electrónicos.

## 8. \*\*Manual de Procedimientos de Gestión de Fraude de Visa\*\*

* Documento que detalla los pasos a seguir por los emisores para la detección, gestión y reporte de fraude.

Incluir estas referencias en la sección correspondiente del informe ayudará a proporcionar un marco normativo claro y a respaldar los requisitos establecidos en el reporte sobre la generación de informes de actividad de fraude.