# **INFORME EJECUTIVO**

# **Inteligencia de Negocios para Detección y Prevención de Fraude Transaccional**

Fecha: Septiembre de 2025  
Elaborado por: Área de Analítica y Prevención de Fraude

## **📊 1. Resumen Ejecutivo**

El análisis de inteligencia de negocio realizado sobre el conjunto de datos transaccionales revela que, si bien la tasa de fraude en volumen de transacciones es baja (0.063%), el impacto económico es significativo ($319.83 mil USD). Este informe consolida hallazgos clave, KPIs críticos y recomendaciones operativas priorizadas para mitigar riesgos, optimizar controles y sentar las bases para un sistema predictivo de fraude.

## **📈 2. KPIs Principales**

| Métrica | Valor |
| --- | --- |
| Total de transacciones | 13,000,000 |
| Total de fraudes | 82 |
| Tasa de fraude | 0.063% |
| Monto total transaccional (USD) | $571.84 millones |
| Monto defraudado (USD) | $319.83 mil |
| Ticket medio por transacción | $3,900 |
| Ticket medio por fraude | $3,900 |

Interpretación: Aunque los fraudes son escasos en frecuencia, su impacto económico es alto en relación con el ticket promedio, lo que exige un enfoque basado en el impacto económico además de la frecuencia.

## **🔍 3. Hallazgos Clave**

### **3.1. Comportamiento Temporal**

* Los fraudes se concentran en días laborables (martes a viernes).
* Se observan picos en horarios fuera de oficina en ciertas ciudades.
* Recomendación: Implementar reglas temporales (ej. autenticación reforzada en horarios críticos) y entrenar modelos con variables temporales.

### **3.2. Comportamiento Geográfico**

* Alta concentración de fraudes en Estados Unidos, especialmente en la costa este y regiones centrales.
* Ciudades específicas presentan mayor monto defraudado.
* Recomendación: Establecer controles geográficos dinámicos y monitoreo en tiempo real para transacciones atípicas.

### **3.3. Señales y Vulnerabilidades**

* Visa y Mastercard concentran la mayoría de fraudes.
* Las tarjetas sin chip presentan mayor incidencia de fraude.
* Flags relevantes: card\_on\_dark\_web, has\_error, use\_chip\_flag.
* Recomendación: Integrar feeds de dark web, reforzar autenticación en transacciones sin chip y priorizar el reemplazo de tarjetas vulnerables.

## **📲 4. Dashboard de Monitoreo – Vista General**

### **4.1. Vista de Transacciones Totales**

* Filtros activos: por día, mes, año.
* Transacciones por edad, género y tipo de tarjeta.
* Monto total transaccional: $571.84 millones.

### 

### **4.2. Vista de Fraudes**

* Cantidad de fraudes: 82
* Monto defraudado: $319.83 mil
* Promedio por fraude: $3.9 mil
* Distribución por ciudad, día de la semana, género y edad.

## **🛡️ 5. Recomendaciones Operativas Priorizadas**

### **5.1. Corto Plazo (Inmediato)**

* Implementar step-up authentication para transacciones > $2,000 o con card\_on\_dark\_web = True.
* Reforzar verificación en transacciones sin chip (bloqueo o solicitud de CVV + OTP).
* Monitoreo en tiempo real para ciudades críticas.

### **5.2. Mediano Plazo (2-3 sprints)**

* Integrar feeds de dark web y servicios de verificación de identidad.
* Establecer reglas dinámicas por horario y ubicación.
* Desarrollar playbooks para el equipo de operaciones.

### **5.3. Largo Plazo (ML y Automatización)**

* Entrenar modelo predictivo (XGBoost/LightGBM) con variables clave.
* Implementar scoring en tiempo real y sistema híbrido (reglas + ML).
* Establecer un ciclo de retroalimentación continua con outcomes reales.

## **🗓️ 6. Roadmap de Implementación**

| Fase | Acciones Clave |
| --- | --- |
| Fase 1: Rápida | Activación de reglas temporales y step-up, dashboards de monitoreo y alertas. |
| Fase 2: Datos | Mejora de calidad de datos, integración con dark web, trazabilidad. |
| Fase 3: Modelado | Construcción y validación de modelo ML, pruebas A/B con reglas híbridas. |
| Fase 4: Operación | Despliegue en pasarela de pagos y retroalimentación continua. |

## **📋 7. Métricas de Seguimiento**

* Reducción del monto defraudado (objetivo: -20% en 3 meses).
* Tasa de falsos positivos (< 1.5%).
* Tiempo medio de resolución de alertas.
* Cobertura de flags (dark web, device fingerprinting).
* Precisión y recall del modelo ML.

## **🔧 8. Apéndice Técnico**

### **Heurística de Fraude**

text

fraud\_score = 0.5\*(amount > 3000) + 0.3\*card\_on\_dark\_web + 0.2\*has\_error

is\_fraud = 1 si fraud\_score >= 0.5

### **Columnas Principales Utilizadas**

* is\_fraud, amount, date, hour, merchant\_city, mcc, use\_chip\_flag, has\_error, card\_on\_dark\_web, credit\_limit, account\_age\_days.

### **Calidad de Datos Asegurada**

* Normalización de montos y fechas.
* Validación de coordenadas geográficas.
* Deduplicación por transaction\_id.
* Integración transaccional con datos de tarjetas y usuarios.

## **✅ 9. Conclusión**

El presente informe proporciona una base sólida para la toma de decisiones operativas y estratégicas en la prevención de fraude. La implementación de las recomendaciones aquí detalladas permitirá reducir significativamente el impacto económico del fraude y sentar las bases para un sistema de detección proactivo y escalable.