Diseño de flujo de ingesta en streaming para detección de fraudes en tiempo real

**1. Objetivo del flujo**

* **Eventos capturados**: Transacciones financieras realizadas por clientes en tiempo real desde la app móvil, sitio web y terminales bancarios.
* **Propósito**: Detectar patrones sospechosos como transacciones duplicadas, montos inusuales, ubicaciones geográficas inconsistentes o intentos de acceso no autorizados. Generar alertas inmediatas para prevenir fraudes.}

**2. Herramienta principal seleccionada**

Apache Kafka + Apache Flink

Justificación:

Kafka permite la ingesta distribuida y confiable de eventos en tiempo real.

Flink ofrece procesamiento de eventos con baja latencia, detección de patrones complejos y tolerancia a fallos.

Ambos se integran fácilmente y escalan horizontalmente.

**3. Esquema general del flujo**

**🔹 Origen de datos**

* API de pagos
* App móvil de clientes
* Sistemas bancarios internos

**🔹 Plataforma de mensajería**

* Apache Kafka
* Topics: transacciones-clientes, alertas-fraude

**🔹 Procesamiento**

* Apache Flink:
  + Validación de estructura de datos
  + Enriquecimiento con datos históricos
  + Detección de patrones sospechosos (CEP - Complex Event Processing)
  + Limpieza y normalización

**🔹 Destino final**

* Sistema de alertas en tiempo real (correo, SMS, dashboard)
* Base de datos operativa para auditoría
* Dashboard de monitoreo para el equipo de seguridad

**4. Beneficios del streaming frente al batch**

* **Detección inmediata** de fraudes, evitando pérdidas económicas.
* **Mayor capacidad de reacción** ante eventos críticos, mejorando la experiencia del cliente y la seguridad.
* **Procesamiento continuo** sin necesidad de esperar acumulación de datos.

**5. Flujo paso a paso**

[1] Captura de eventos desde API de pagos, app móvil y sistemas bancarios

     ↓

[2] Envío de eventos a Kafka → Topic: transacciones-clientes

     ↓

[3] Procesamiento en Flink:

     - Validación de datos

     - Enriquecimiento con historial

     - Detección de patrones sospechosos

     ↓

[4] Generación de alertas → Topic: alertas-fraude

     ↓

[5] Envío a:

     - Dashboard de monitoreo

     - Sistema de alertas (correo/SMS)

     - Base de datos operativa