INFORME FINAL: WALLAPOP FRAUD RADAR

Proyecto: Hunting Scams on Wallapop

Autores: Iván Ciudad y Víctor Carbajo

Fecha: 6 de Diciembre, 2025

---

1. Introducción y Selección de Categoría

Este proyecto se enmarca dentro de un trabajo práctico universitario dedicado a detectar fraude en Wallapop.

1.1. Categoría Seleccionada: Smartphones (iPhone)

Hemos seleccionado la categoría de Telefonía Móvil, centrándonos específicamente en la marca Apple (iPhone).

Justificación: Los productos de Apple presentan el mayor riesgo de fraude en plataformas de segunda mano debido a su alta liquidez, alto valor unitario y demanda constante.

1.2. Análisis de Patrones de Fraude

Durante la fase de investigación del dominio, identificamos los siguientes vectores de ataque comunes en esta categoría:

1. **Estafa de Pago Externo:** Vendedores que solicitan pagos vía **Bizum** o transferencia inmediata para evitar la protección de la plataforma ("Wallapop Envíos").
2. **Dispositivos Bloqueados:** Venta de terminales robados o encontrados con bloqueo de iCloud o IMEI.
3. **Falsificaciones (Réplicas):** Venta de clones chinos (Android con skin de iOS) anunciados como originales.
4. **Precios Gancho:** Terminales de última generación (ej: iPhone 15 Pro) a precios irrisorios (<200€) para captar víctimas rápidamente.

---

2. Arquitectura del Pipeline de Datos

Para monitorizar estos riesgos, hemos implementado un pipeline completo de ingestión y análisis (Opción A.1).

2.1. Estrategia de Recolección (Poller)

Desarrollamos un script en Python (poller.py) que interactúa con la API pública de Wallapop (/api/v3/search).

- **Frecuencia:** Ejecución cada 5 minutos orquestada por monitor.py para detectar amenazas en tiempo casi real.
- **Filtrado:** Uso de time_filter=today y palabras clave específicas para obtener solo ítems relevantes.
- **Salida:** Generación de un archivo diario wallapop_master.json con formato NDJSON.

2.2. Ingestión en Elasticsearch

Utilizamos un script de ingestión manual (bulk_ingest.py) que lee el archivo maestro y envía los documentos a Elasticsearch utilizando la **Bulk API** sobre HTTPS.

- **Índice:** wallapop-items con política de rotación ILM.
- **Deduplicación:** Se utiliza el item_id de Wallapop como _id de Elasticsearch para evitar duplicados y permitir actualizaciones de precios.

---

3. Lógica de Sospecha y Scoring (Suspicion Logic)

El núcleo del sistema es nuestro algoritmo de **Risk Scoring** (0-100), implementado directamente en la fase de recolección. A diferencia de un enfoque simple basado en medias globales, hemos implementado una **Segmentación por Modelo**.

3.1. Señales de Sospecha (Signals)

Hemos clasificado los indicadores en dos niveles de severidad:

Tipo de Señal	Indicadores (Keywords/Comportamiento)	Impacto en Score
Crítico	bizum, transferencia, whatsapp, réplica, clon, bloqueo	**+50-60 puntos**
Sospechoso	urgente, sin factura, no negociable, viaje	**+15 puntos**

Técnico	Vendedor masivo (>3 anuncios/día), Descripción muy corta	**+10-30 puntos**

3.2. Innovación: Segmentación de Precios

Para reducir falsos positivos (evitar marcar un iPhone X barato como estafa), el sistema utiliza un diccionario de referencia:

- Si detecta "iPhone 15 Pro", aplica un precio de referencia de 750€.
- Si el precio real es < 40% de la referencia, se dispara el riesgo (**+95 puntos**).
- Esto permite distinguir "chollos" legítimos de "estafas imposibles".

Ejemplo de cálculo real:

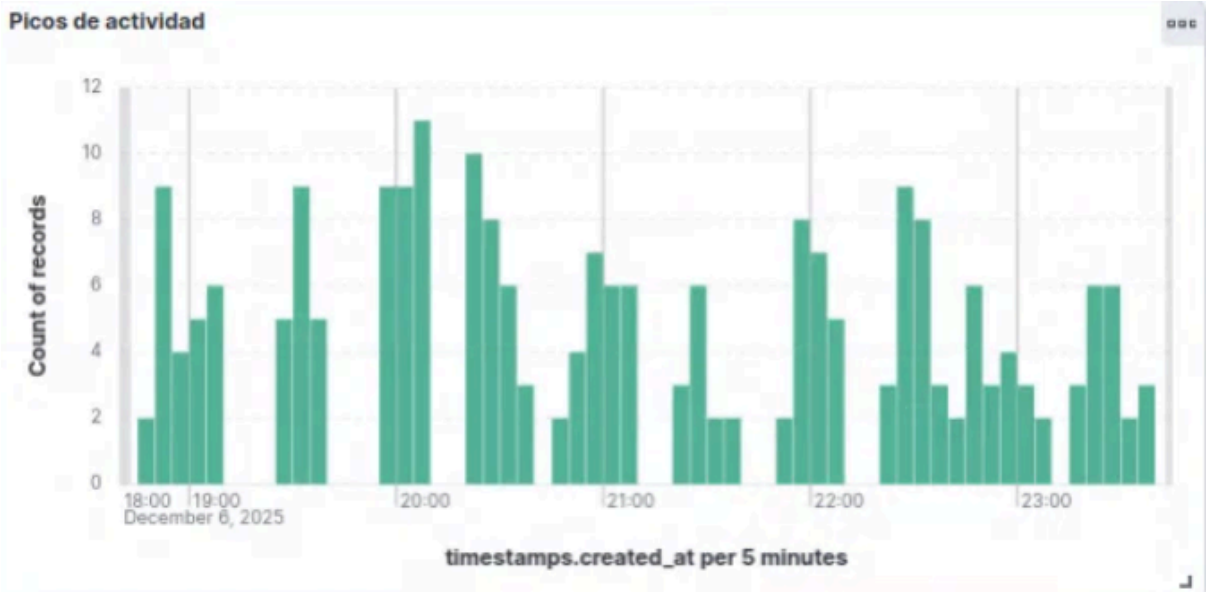
> Ítem: "iPhone 15 Pro Max Nuevo" a 150€.
>
> Lógica: Detectado modelo "15 Pro Max" (Ref: 850€). Precio (150€) es el 17% del valor.
>
> Resultado: Risk Score 100 (Alerta Crítica).

---

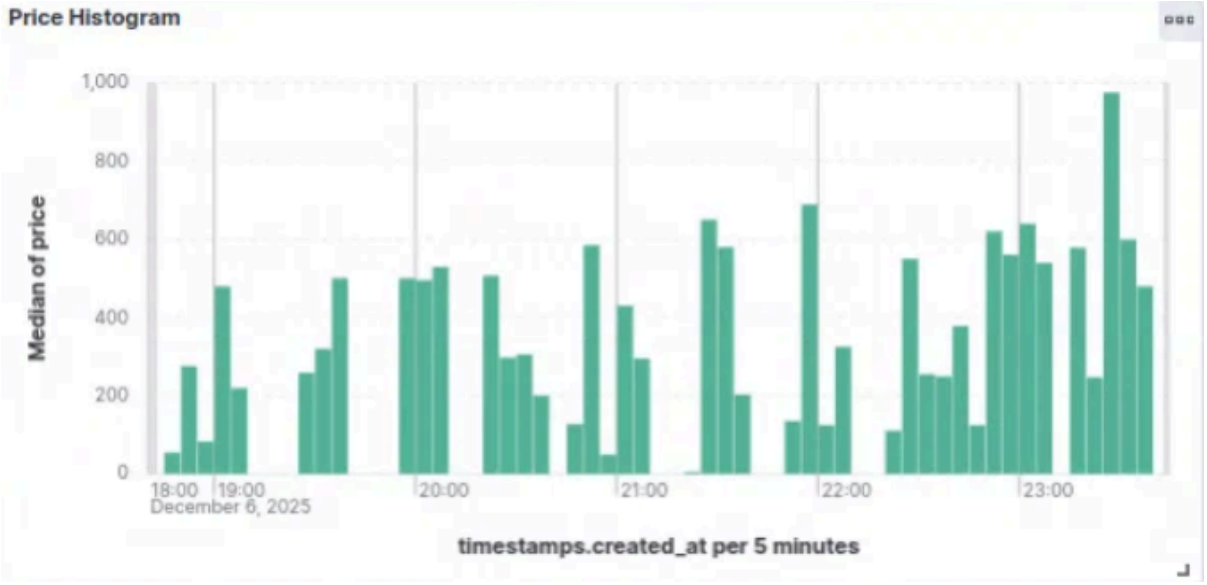
4. Visualización Operacional (Kibana Dashboard)

El panel de control "Wallapop View" permite a los analistas visualizar la actividad del mercado en tiempo real.

Una forma interesante de comprobar las horas puntas es saber cuándo se publican muchos anuncios. Por ello registramos la actividad horaria de cuando se publican estos anuncios.

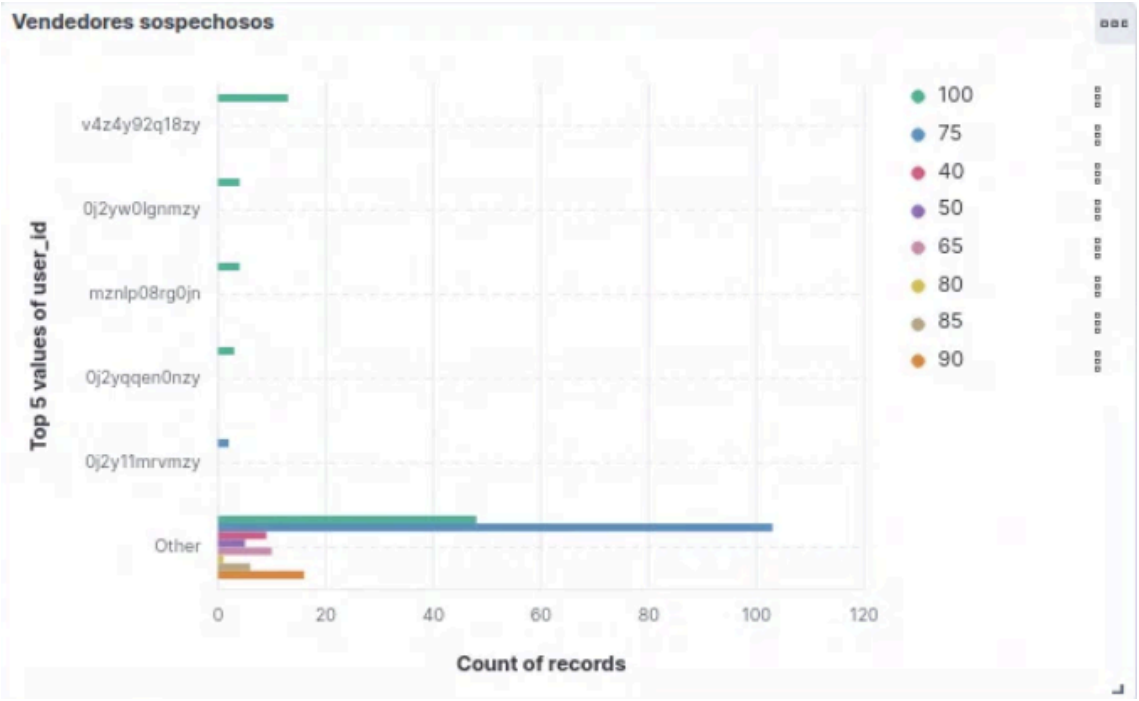


4.1. Análisis de Precios (Price Histogram)



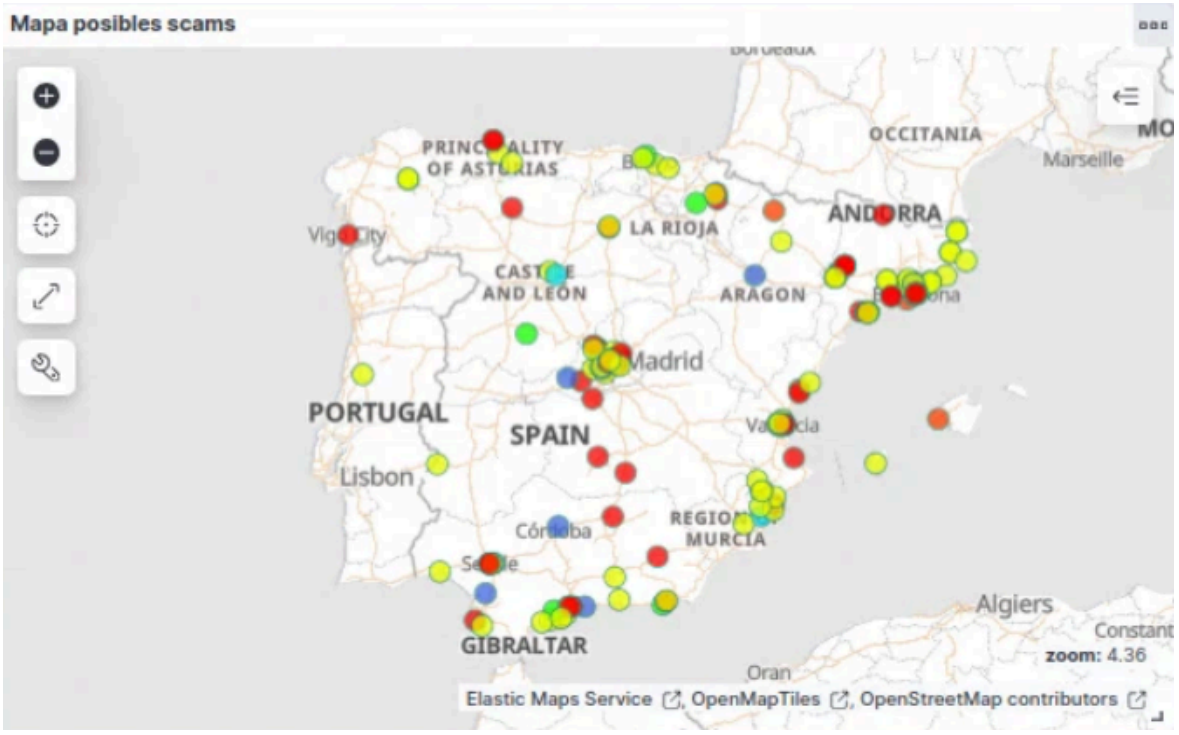
Análisis: Este histograma permite identificar la "zona de fraude" (precios anormalmente bajos a la izquierda) frente a la distribución normal del mercado.

4.2. Actividad Temporal y Vendedores (Top Sellers)



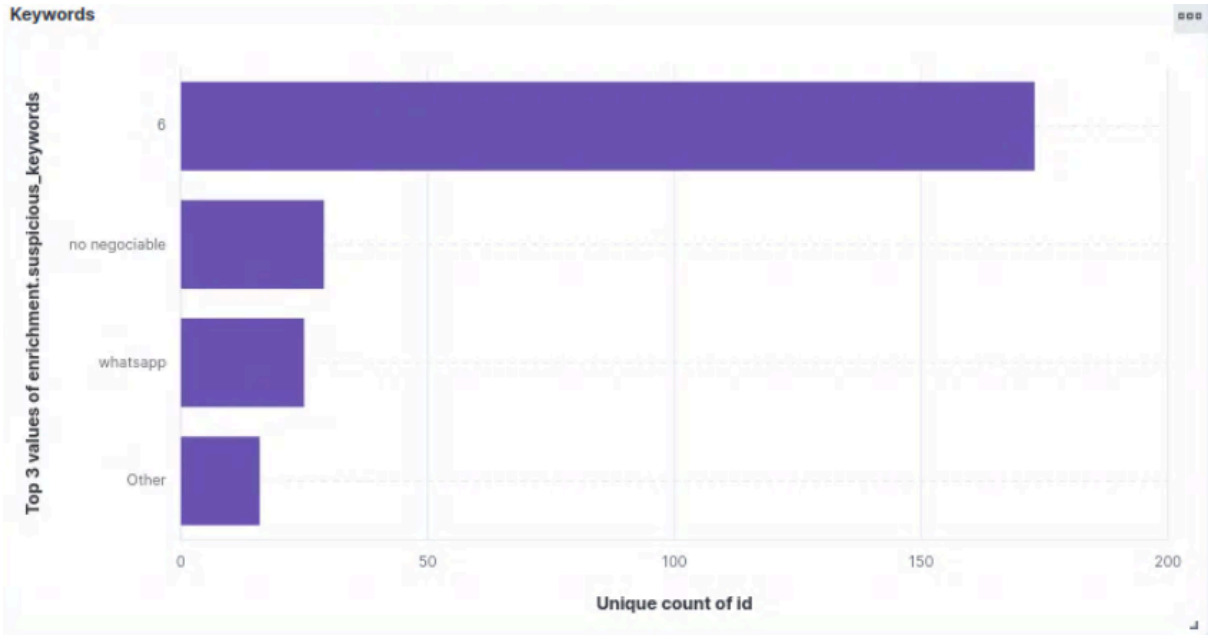
Análisis: El gráfico de barras horizontales revela usuarios con actividad masiva (posibles bots). El código de colores (verde para riesgo alto) ayuda a identificar actores maliciosos rápidamente.

4.3. Mapa de Riesgo (Geo Map)



Análisis: Geolocalización de anuncios. Los puntos rojos indican ubicaciones donde se concentran los anuncios de alto riesgo.

4.5. Nube de Términos Sospechosos (Bar Horizontal)



Análisis: Visualización de los términos más usados en fraudes. Destacan palabras como "whatsapp", "no negociable" o intentos de contacto externo.

---

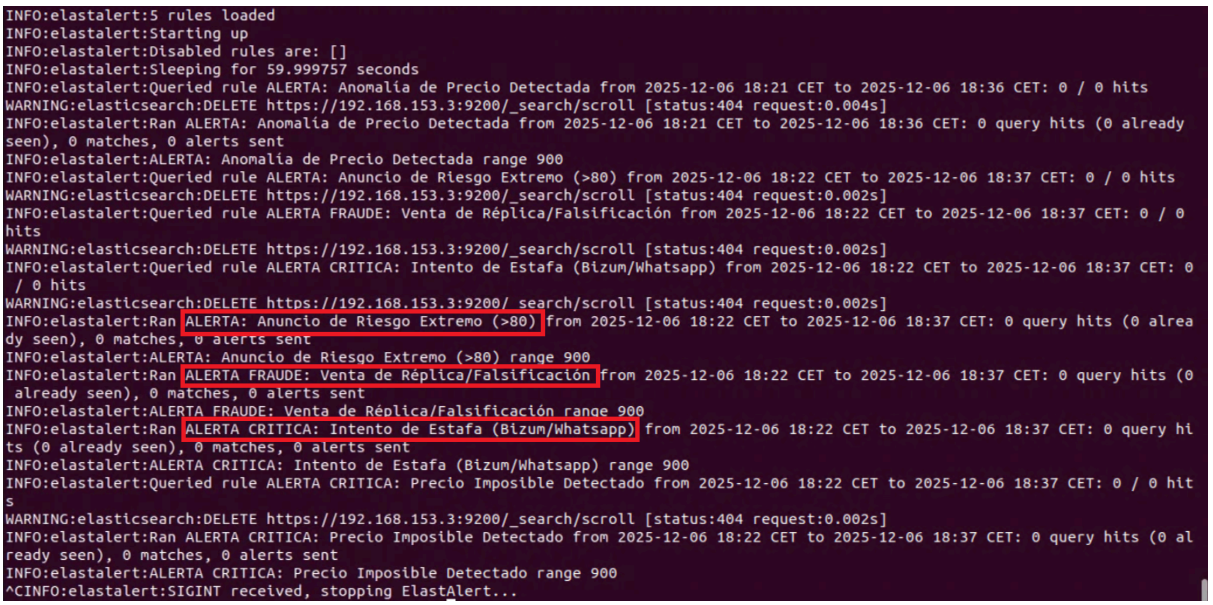
5. Sistema de Alertas (Elastalert2)

Se ha desplegado Elastalert2 para la vigilancia continua.

5.1. Reglas Implementadas

1. **alert_pagos.yaml**: Detecta intentos de pago fuera de plataforma (Keywords: Bizum, WhatsApp).
2. **low_price.yaml**: Detecta anomalías de precio basadas en nuestra segmentación por modelos.
3. **high_risk.yaml**: Dispara alerta si risk_score > 80.

5.2. Evidencia de Alerta



Descripción: Captura de una alerta real disparada durante la fase de pruebas, demostrando la capacidad de reacción del sistema ante un anuncio fraudulento inyectado.

---

6. Plan de Experimentación y Validación

Según lo requerido en la sección 10.7, se ejecutó el siguiente plan:

1. **Periodo de Recolección:** Monitorización continua durante 5 horas.
2. **Volumen de Datos:** >200 ítems recolectados e ingestados.
3. **Validación de Hipótesis:**
    - *Hipótesis:* Los estafadores usan precios psicológicos bajos y piden contacto externo.
    - *Resultado:* Confirmado por las alertas de "Bizum" y el histograma de precios bajos.
4. **Limitaciones:** La API de Wallapop limita el número de peticiones, por lo que se ajustó el polling a 30 minutos para evitar bloqueos.

7. Conclusiones

El sistema "Wallapop View" ha demostrado ser efectivo para:

1. **Automatizar** la recolección de inteligencia en un mercado volátil.
2. **Filtrar el ruido** (fundas, accesorios) gracias a la lógica de exclusión.
3. **Identificar amenazas** concretas (pagos externos y réplicas) mediante reglas de negocio específicas.

Mejoras Futuras: Usar modelos de ML para Anomalías. Sustituir los umbrales fijos de precio por modelos de *Unsupervised Learning* (como Isolation Forest) permitiría detectar fraudes dinámicos que se adaptan a las reglas estáticas.