



25

RED FLAGS DEL FRAUDE DIGITAL

Las señales que todo analista y profesional del riesgo debe reconocer

The signals every risk professional must recognize

ÍNDICE DE CONTENIDOS

TABLE OF CONTENTS

01

IDENTIDAD / IDENTITY

Red Flags 01-05

Señales relacionadas con datos de registro, emails y dispositivos

03

TRANSACCIONAL / TRANSACTIONAL

Red Flags 10-14

Velocidad de compra, card testing y triangulación de pagos

05

PROMOCIONAL / PROMOTIONAL

Red Flags 18-20

Abuso de promociones, wardrobing digital y redes organizadas

07

TÉCNICO / TECHNICAL

Red Flags 24-25

IPs de alto riesgo, proxies, Tor, user agent spoofing y automatización

02

ACCESO / ACCESS

Red Flags 06-09

Patrones de login, cambios de credenciales y geolocalización

04

COMPORTAMENTAL / BEHAVIORAL

Red Flags 15-17

Interacción con el sitio, patrones de navegación y bots

06

INTERNO / INTERNAL

Red Flags 21-23

Insider threats, acceso a datos y separación de funciones

• CAPÍTULO 01 / CHAPTER 01

IDENTIDAD

Señales de alerta relacionadas con la identidad del usuario

Identity-related warning signals

5 Red Flags

RF 01 - 05



IDENTIDAD / IDENTITY

Red Flags 01 – 03

01

CRÍTICO

Datos de registro inconsistentes

Inconsistent registration data

Nombre, email y teléfono **sin coherencia geográfica**. El dominio del email no coincide con el país de registro.

Name, email and phone with no geographic coherence. Email domain doesn't match registration country.

💡 **Ejemplo:** Nombre español + email @gmail.ru + teléfono de Colombia

02

ALTO

Velocidad de registro anómala

Anomalous registration speed

Formulario completado en **menos de 30 segundos**. Un humano real necesita tiempo para leer y escribir.

Form completed in under 30 seconds. A real human needs time to read and type.

💡 **Detección:** Timestamp de inicio vs. timestamp de submit

03

CRÍTICO

Múltiples cuentas desde el mismo dispositivo

Multiple accounts from same device

El mismo **fingerprint aparece en más de 2 registros** distintos en poco tiempo. Señal clásica de fraude de identidad múltiple.

Same device fingerprint in more than 2 different registrations. Classic multi-identity fraud signal.

💡 **Indicador:** Device fingerprint, cookies, canvas fingerprinting

IDENTIDAD / IDENTITY

Red Flags 04 - 05

04

CRÍTICO

Email de un solo uso detectado

Disposable email detected

Dominios como **mailinator.com** o **tempmail.com** indican que el usuario no quiere ser contactado ni rastreado.

Domains like mailinator.com or tempmail.com indicate the user doesn't want to be contacted or tracked.



Lista negra recomendada: 10minutemail, guerrillamail, throwawaymail

05

ALTO

Identidad sintética parcial

Partial synthetic identity

Datos reales mezclados con inventados: nombre real + dirección de otra ciudad + teléfono de otro país.

Real data mixed with fabricated: real name + address from another city + phone from another country.



Verificación cruzada: Validar consistencia entre nombre, dirección y teléfono



Resumen del Capítulo 1

5 señales de identidad: 3 CRÍTICAS + 2 ALTAS | Enfoque en inconsistencias geográficas y velocidad

• CAPÍTULO 02 / CHAPTER 02

ACCESO



Señales de alerta en patrones de acceso a cuentas

Access pattern warning signals

4 Red Flags

RF 06 - 09



ACCESO / ACCESS

Red Flags 06 - 09

06

CRÍTICO

Cambio de contraseña y email simultáneo

Simultaneous password and email change

Cuando ambos campos se modifican en la **misma sesión**, la cuenta ha sido tomada. El atacante aísla al titular legítimo.

When both fields are modified in the same session, the account has been taken over.

 **Acción:** Bloquear cuenta y requerir verificación adicional

07

CRÍTICO

Login desde país nunca antes visto

Login from never-seen-before country

Sin contexto previo, un acceso desde un **país nuevo** en una cuenta con historial señala compromiso de credenciales.

Without prior context, access from a new country signals credential compromise.

 **Contexto:** Verificar si hay viaje programado o VPN

08

ALTO

Múltiples fallos seguidos de éxito

Multiple failures followed by success

X intentos fallidos + 1 exitoso describe credential stuffing. El éxito tras fallo sistemático es ataque, no recuperación.

X failed attempts + 1 success describes credential stuffing.

 **Patrón:** 5+ fallos en 2 minutos + 1 éxito

09

CRÍTICO

Sesión activa en múltiples geolocalizaciones

Session from multiple simultaneous geolocations

Físicamente imposible. Actividad desde Madrid y Moscú en el mismo minuto: una sesión es fraudulenta.

Physically impossible. Activity from Madrid and Moscow in the same minute.

 **Umbral:** 500+ km de distancia en <1 hora

• CAPÍTULO 03 / CHAPTER 03

TRANSACCIONAL

Señales de alerta en actividad transaccional

Transactional activity warning signals

5 Red Flags

RF 10 - 14



WHAT TO LOOK FOR

TRANSACCIONAL / TRANSACTIONAL

Red Flags 10 - 12

10

CRÍTICO

Primera transacción de alto valor en cuenta nueva

High-value first transaction on new account

Una cuenta de **menos de 48 horas** intentando una transacción elevada no tiene historial de comportamiento legítimo.

An account less than 48 hours old attempting a high-value transaction has no legitimate behavior history.



Regla: Cuentas <48h → límite de €100 en primera transacción

11

CRÍTICO

Card testing detectado

Card testing detected

Múltiples transacciones de €0.01–€1.00 en secuencia rápida. El atacante valida tarjetas robadas antes del golpe real.

Multiple €0.01–€1.00 transactions in rapid sequence. Attacker validates stolen cards.



Patrón: 3+ transacciones <€5 en 10 minutos desde nueva cuenta

12

MEDIO

Dirección de envío diferente a la de facturación

Shipping address different from billing address

Solo es señal en **combinación** con cuenta nueva + instrumento nuevo + horario nocturno. En aislamiento: riesgo medio.

Only a signal combined with new account + new payment instrument + late-night timing.



Contexto: Regalos legítimos vs. fraude con AVS mismatch

TRANSACCIONAL / TRANSACTIONAL

Red Flags 13 - 14

13

ALTO

Velocidad de compra anómala

Anomalous purchase velocity

10 transacciones en 5 minutos no es comportamiento humano. Indica automatización para agotar saldo robado.

10 transactions in 5 minutes is not human behavior. Indicates automation to exhaust stolen balance.

Umbral crítico: >5 transacciones/minuto

Patrón: Mismo producto, cantidades altas

14

CRÍTICO

Triangulación de pagos

Payment triangulation

Compra con tarjeta robada para revender. El producto llega al comprador real; el cargo fraudulento al titular de la tarjeta.

Purchase with stolen card to resell. Product reaches real buyer; fraudulent charge reaches the card holder.



Complejidad: Difícil de detectar - el comprador final es legítimo



Resumen del Capítulo 3

5 señales transaccionales: 3 CRÍTICAS + 1 ALTA + 1 MEDIA | Enfoque en velocidad y validación

RED FLAGS RESTANTES / REMAINING RED FLAGS

Red Flags 15 – 25: Comportamental, Promocional, Interno y Técnico

04 COMPORTAMENTAL

15 ALTO

Sesión sin scroll ni interacción real

Session with no scroll or real interaction

16 ALTO

Patrones idénticos entre cuentas

Identical usage patterns across accounts

17 MEDIO

Ausencia de comportamiento post-conversión

Absence of post-conversion behavior

05 PROMOCIONAL

18 CRÍTICO

Concentración temporal de uso de promoción

Temporal concentration of promotion usage

19 CRÍTICO

Múltiples cuentas con mismo método de pago

Multiple accounts sharing same payment method

20 ALTO

Devolución sistemática post-promoción

Systematic post-promotion return

06 INTERNO

21 ALTO

Acceso a datos fuera de horario sin justificación

Data access outside usual hours without justification

22 CRÍTICO

Descarga masiva de datos antes de una salida

Massive data download before departure

23 CRÍTICO

Operaciones aprobadas por quien las inicia

Operations approved by the initiating user

07 TÉCNICO

24 ALTO

IP de alto riesgo conocida

Known high-risk IP

Proxies, Tor, hosting de bajo coste, blacklists

25 ALTO

Discrepancia entre user agent y comportamiento

Discrepancy between user agent and real behavior

Chrome declarado pero comportamiento de bot

 FORMACIÓN ESPECIALIZADA

¿LISTO PARA DOMINAR EL ANÁLISIS DE FRAUDE?

Programa completo de metodología operativa, casos reales y frameworks profesionales



Analistas
Analysts



Investigadores
Investigators



Directivos de Riesgo
Risk Executives

Precio de lanzamiento

€397



THE FRAUD DESK
thefrauddesk.com