# Revisar

El módulo de Review es un sistema de análisis manual que permite a los asesores y analistas de seguridad del banco evaluar, clasificar y proporcionar retroalimentación sobre sesiones que han sido reportadas por clientes o escaladas por los sistemas automáticos. Su función principal es realizar una investigación humana detallada de casos sospechosos, confirmar o descartar alertas de fraude, y documentar hallazgos para mejorar los algoritmos de detección automática.

## Objetivos Principales

| Objetivo | Descripción | Aplicación |
|---|---|---|
| **Clasificación Manual de Casos** | Permitir evaluación humana experta de sesiones sospechosas | Confirmación de fraude o falsos positivos |
| **Retroalimentación al Sistema** | Proporcionar datos de entrenamiento para algoritmos ML | Mejora continua de detección automática |
| **Investigación Detallada** | Análisis profundo de casos complejos | Identificación de nuevos vectores de ataque |
| **Documentación de Hallazgos** | Registro detallado de evidencia y conclusiones | Soporte legal y auditoría |
| **Escalación de Casos** | Identificar casos que requieren intervención especializada | Gestión de incidentes críticos |

## Arquitectura del Sistema

## Componentes Principales

| Componente | Función | Descripción |
|---|---|---|
| **Panel de Clasificación** | Selección de tipo de caso | Opciones predefinidas de categorización |
| **Área de Comentarios** | Documentación detallada | Campo de texto libre para observaciones |
| **Sistema de Envío** | Procesamiento de decisiones | Botón de confirmación y envío |
| **Base de Conocimiento** | Referencia de tipos de fraude | Guías para clasificación consistente |

## Panel de Clasificación - Tipos de Casos

El panel de clasificación presenta una lista comprehensiva de categorías predefinidas que cubren todos los tipos posibles de actividad, desde casos legítimos hasta diferentes variantes de fraude.

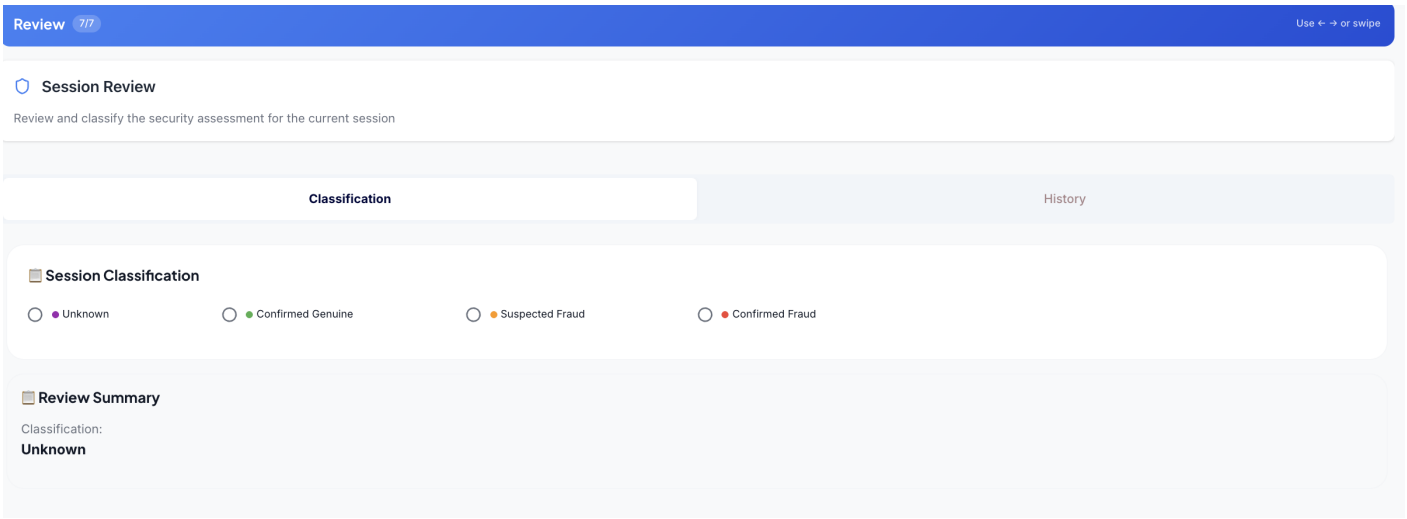
Permite selección múltiple para casos que involucran varios vectores de ataque simultáneamente.

# Categorías de Clasificación

| Categoría | Descripción | Nivel de Riesgo | Acción Posterior |
|---|---|---|---|
| **Unknown** | Caso sin clasificar o información insuficiente | N/A | Requiere investigación adicional |
| **Confirmed Genuine** | Actividad legítima confirmada | Ninguno | Marcar como falso positivo |
| **Suspected Fraud** | Indicios de fraude sin confirmación total | Medio-Alto | Monitoreo intensivo |
| **Confirmed Fraud** | Fraude confirmado con evidencia | Crítico | Bloqueo inmediato y escalación |

# Tipos Específicos de Fraude

| Tipo de Fraude | Descripción Técnica | Indicadores Típicos | Acción Recomendada |
|---|---|---|---|
| **ATO Fraud** | Account Take Over - Compromiso de cuenta | Cambio de patrones, nueva ubicación, dispositivo desconocido | Bloqueo de cuenta, verificación de identidad |
| **Malware Fraud** | Fraude mediante software malicioso | Comportamiento automatizado, keyloggers, RATs | Limpieza de dispositivo, cambio de credenciales |
| **Social Engineering Fraud** | Ingeniería social y manipulación | Usuario reporta presión externa, transferencias inusuales | Educación del usuario, revisión de transacciones |
| **Remote Access Fraud** | Acceso remoto no autorizado | Software de control remoto, actividad desde múltiples ubicaciones | Verificación de dispositivos autorizados |
| **Digital Fraud** | Fraude mediante canales digitales | Manipulación de aplicaciones, bypass de controles | Fortalecimiento de seguridad digital |
| **Phishing** | Suplantación de identidad digital | Links maliciosos, sitios falsos, credenciales comprometidas | Educación, cambio de contraseñas |
| **Cell Phone Theft** | Robo de dispositivo móvil | Acceso desde dispositivo robado | Bloqueo de dispositivo, verificación de identidad |
| **SIM Swap** | Intercambio fraudulento de tarjeta SIM | Pérdida de control del número telefónico | Verificación con operadora, método alternativo |
| **New Device** | Actividad desde dispositivo nuevo | Primer acceso desde dispositivo desconocido | Verificación adicional de identidad |
| **Owner Device** | Dispositivo propio del usuario | Actividad desde dispositivo registrado | Monitoreo estándar |




El área de comentarios proporciona un espacio de texto libre donde los analistas pueden documentar sus hallazgos, evidencias específicas, metodología de investigación y recomendaciones detalladas.

# Estructura de Documentación Recomendada

| Sección | Contenido | Propósito | Ejemplo |
|---|---|---|---|
| **Resumen del Caso** | Descripción breve del incidente | Contexto inicial | "Usuario reporta transferencias no autorizadas desde dispositivo conocido" |
| **Evidencia Encontrada** | Datos específicos que apoyan la clasificación | Sustento técnico | "Detectado keylogger en análisis de dispositivo, logs muestran captura de credenciales" |
| **Metodología de Análisis** | Pasos seguidos en la investigación | Reproducibilidad | "Análisis de logs de sesión, verificación cruzada con datos de ubicación" |
| **Conclusiones** | Determinación final del analista | Decisión fundamentada | "Confirmo compromiso por malware, dispositivo requiere limpieza completa" |
| **Recomendaciones** | Acciones sugeridas | Pasos siguientes | "Bloqueo temporal, educación sobre seguridad, instalación de antivirus" |

Revision #3
Created 30 June 2025 14:54:01 by roger de avila
Updated 25 August 2025 16:06:59 by roger de avila