

# Módulo Sessions

El **Módulo de Sesiones** constituye el núcleo operacional del sistema ADO-STS, proporcionando una interfaz completa para el monitoreo, análisis y gestión de todas las sesiones de usuario en tiempo real. Este módulo integra datos de múltiples fuentes para ofrecer una vista unificada del comportamiento del usuario y los riesgos asociados.

## Sistema de Filtros Avanzados - Configuración Técnica

### Filtros Primarios (Barra Superior)

Brand

User Group

Device Source

Ip Country

Indicators

All Context

Refresh

OR

Search...

Search

Reset Search

IP ISP

MUID

Platform

UA Device Brand

IP City

Date range

Export

Filtro Técnico	Tipo de Datos	Descripción Técnica	Interpretación de Uso	Algoritmo Subyacente
Brand	Enum de fabricantes	Filtrado por marca del dispositivo (Apple, Samsung, Google, etc.)	Análisis de patrones por fabricante, detección de cambios abruptos de marca	Matching exacto con base de datos de dispositivos
User Group	Categoría segmentada	Clasificación del tipo de usuario (Business, Personal, Premium, etc.)	Segmentación de riesgo por tipo de usuario, aplicación de políticas específicas	Clasificación basada en metadatos de cuenta
Device Source	Origen de adquisición	Fuente de donde proviene el dispositivo (Organic, Referral, Direct, etc.)	Tracking de procedencia para detectar dispositivos comprometidos	Análisis de cadena de referencia
IP Country	ISO 3166-1 Alpha-2	Código de país basado en geolocalización IP	Filtrado geográfico, detección de accesos desde países de riesgo	GeoIP database con actualización diaria
Indicators	Array de flags	Tipos específicos de alertas e indicadores de riesgo activados	Filtrado por señales específicas de fraude o comportamiento anómalo	Bitmap de indicadores con OR lógico
AI Context	Nivel de procesamiento	Profundidad del análisis de IA aplicado (Basic, Standard, Advanced, Deep)	Control del nivel de análisis, balance entre precisión y performance	Configuración de pipelines de ML
IP ISP	String del proveedor	Proveedor de servicios de Internet específico	Análisis por ISP, detección de granjas de bots o proxies comerciales	Lookup en bases de datos ASN/WHOIS
MUID	Hash único	Machine Unique Identifier para búsqueda específica	Tracking directo de dispositivos específicos	SHA-256 hash de características hardware

Filtro Técnico	Tipo de Datos	Descripción Técnica	Interpretación de Uso	Algoritmo Subyacente
Platform	OS/Browser combo	Combinación de sistema operativo y plataforma de acceso	Análisis por plataforma, detección de emuladores	User-Agent parsing con validación
UA Device Brand	User-Agent parsing	Marca del dispositivo extraída del User-Agent	Comparación con brand real para detectar spoofing	Cross-validation entre fuentes
IP City	Geolocalización granular	Ciudad específica basada en IP con precisión metropolitana	Análisis local de patrones, detección micro-geográfica	GeoIP con precisión de ciudad (95%+ accuracy)
Date Range	Timestamp range	Selector de rango temporal con precisión de minutos	Análisis temporal de tendencias, investigación de incidentes	Índices temporales optimizados

Filtros Secundarios (Chips/Tags Contextuales)

Filtro Contextual	Descripción Técnica	Casos de Uso	Implementación
IP Location Risk	Evaluación automática del riesgo geográfico	Alto/Medio/Bajo basado en historial de fraude de la ubicación	Modelo ML entrenado con datos geográficos de fraude
User Group Business	Segmentación automática de usuarios corporativos	Aplicación de políticas específicas para usuarios empresariales	Clasificación basada en dominio de email y metadatos

Estructura de Columnas - Análisis Técnico Detallado

Columnas de Identificación y Control

Columna	Tipo de Dato	Descripción Técnica	Interpretación de Riesgo	Algoritmo de Análisis
TRY	Integer (1-∞)	Número secuencial de intentos de la sesión	>3 intentos indican comportamiento sospechoso, >5 es crítico	Contador incremental con timeout de reset
DATE	Timestamp UTC	Fecha y hora exacta de inicio de sesión con precisión de milisegundos	Análisis de patrones temporales, detección de actividad fuera de horarios	Índice temporal para consultas de rango
SCORE	Float (0-1000)	Puntuación de riesgo calculada por el motor de IA	0-199: Bajo, 200-499: Medio, 500-799: Alto, 800+: Crítico	Ensemble de 12 modelos ML con weighted average

Columna	Tipo de Dato	DescripciónTécnica	Interpretación de Riesgo	Algoritmo de Análisis
USER	Hash/ID único	Identificador único del usuario en el sistema	Tracking de comportamiento histórico del usuario	Hash irreversible de PII
CSID	UUID v4	Client Session Identifier único por sesión	Correlación de eventos dentro de la misma sesión	UUID generado por cliente, validado por servidor

## Columnas de Contexto Temporal y Operacional

Columna	Tipo de Dato	Descripción Técnica	Interpretación de Riesgo	Algoritmo de Análisis
DURATION	Integer (segundos)	Duración total de la sesión desde inicio hasta último evento	<30s o >3600s son anómalos según el tipo de operación	Análisis estadístico de distribución temporal
BRAND	Enum normalizado	Marca del dispositivo normalizada (Apple, Samsung, Xiaomi, etc.)	Cambios frecuentes de marca (>1/semana) incrementan score	Análisis de estabilidad de dispositivo
CHANNEL	String categorizado	Canal de acceso (Mobile App, Web, API, etc.)	Canales inusuales para el perfil del usuario	Análisis de consistencia de canal
CONTEXT	JSON estructurado	Información contextual adicional de la operación	LOGIN, LOGOUT, TRANSFER, etc. afectan interpretación del riesgo	Parsing de contexto operacional

## Columnas de Análisis de Red e Infraestructura

Columna	Tipo de Dato	Descripción Técnica	Interpretación de Riesgo	Algoritmo de Análisis
ISP	String del proveedor	Nombre del proveedor de servicios de Internet	Cambios frecuentes de ISP sin roaming legítimo	Análisis de estabilidad de conectividad
IP	IPv4/IPv6	Dirección IP pública desde la cual se origina la conexión	IPs de TOR, VPN, proxies conocidos incrementan riesgo	Blacklists y análisis de reputación IP
IP AGE	Integer (días)	Edad de la primera vez que esta IP fue vista en el sistema	IPs nuevas (edad 0) tienen mayor riesgo inherente	Tracking temporal de IPs
IP COUNTRY	ISO Alpha-2	Código de país de dos letras basado en geolocalización IP	Países en listas de riesgo incrementan score automáticamente	GeoIP con validación de coherencia

## Columnas de Análisis de Dispositivo y Usuario

Columna	Tipo de Dato	Descripción Técnica	Interpretación de Riesgo	Algoritmo de Análisis
KNOWN DEVICE	Boolean/Enum	Estado de reconocimiento del dispositivo (0=Nuevo, 1=Conocido)	Dispositivos nuevos requieren verificación adicional	Fingerprinting multi-dimensional
USERS ON DEVICE TW	Integer	Número de usuarios únicos que han usado este dispositivo en ventana temporal	>1 usuario por dispositivo es indicador de riesgo	Análisis de multiplicidad de usuarios
DEVICE USED	Integer	Número de veces que este dispositivo específico ha sido utilizado	Muy poco uso (<5) o uso excesivo (>100/día) es sospechoso	Análisis de frecuencia de uso
USER AGE	Integer (días)	Antigüedad del usuario en el sistema desde su primer registro	Usuarios muy nuevos (<7 días) tienen score de riesgo elevado	Cálculo de antigüedad con factor de confianza

## Columnas de Identificadores Técnicos

Columna	Tipo de Dato	Descripción Técnica	Interpretación de Riesgo	Algoritmo de Análisis
MUID	Hash SHA-256	Machine Unique Identifier basado en características hardware	Cambios de MUID indican nuevo dispositivo o manipulación	Hashing de componentes hardware únicos
SID	UUID v4	Session Identifier único generado por el sistema	Utilizado para correlación de eventos y debugging	UUID generado server-side

## Interpretación de Códigos de Color en el Dashboard

### Sistema de Semáforo Visual

Color	Rango de Score	Interpretación	Acción Automática	Revisión Requerida
Verde	0-299	Riesgo Bajo - Comportamiento normal	Procesamiento automático	No
Amarillo	300-599	Riesgo Medio - Anomalías menores detectadas	Logging adicional	Revisión opcional

Color	Rango de Score	Interpretación	Acción Automática	Revisión Requerida
Naranja	600-799	Riesgo Alto - Múltiples indicadores sospechosos	Verificación automática	Revisión recomendada
Rojo	800-949	Riesgo Crítico - Patrón fraudulento probable	Bloqueo temporal	Revisión obligatoria
Rojo Intenso	950-1000	Riesgo Extremo - Fraude casi confirmado	Bloqueo inmediato	Escalamiento

## Funcionalidades Avanzadas del Módulo

### Sistema de Búsqueda y Filtrado

#### Motor de Búsqueda:

- **Elasticsearch backend** para consultas complejas
- **Índices optimizados** por timestamp, score, usuario e IP
- **Búsqueda fuzzy** para identificadores parciales
- **Agregaciones en tiempo real** para estadísticas dinámicas

#### Filtros Combinados:

- **Operadores lógicos** (AND, OR, NOT) entre filtros
- **Filtros temporales relativos** (última hora, último día, última semana)
- **Filtros geográficos** con mapas interactivos
- **Filtros por rangos** para scores y métricas numéricas

### Exportación y Reporting

Formato	Descripción	Casos de Uso
CSV	Datos tabulares para análisis en Excel/Python	Análisis estadístico offline
JSON	Estructura completa de datos para integración	APIs y sistemas automatizados
PDF	Reportes formateados para presentación	Documentación de incidentes
Excel	Hojas de cálculo con gráficos automáticos	Análisis ejecutivo

### Alertas y Notificaciones Configurables

#### Tipos de Alertas:

- L. Monitoreo Proactivo:** Revisar scores >600 en tiempo real

2. **Análisis de Tendencias:** Usar filtros temporales para identificar patrones
3. **Correlación de Datos:** Combinar múltiples filtros para investigaciones
4. **Documentación de Casos:** Exportar evidencia para análisis forense

## Configuraciones Recomendadas por Industria

### Sector Bancario:

- Threshold de alerta: 400
- Revisión manual obligatoria: 600+
- Bloqueo automático: 800+

### E-commerce:

- Threshold de alerta: 500
- Revisión manual obligatoria: 700+
- Bloqueo automático: 850+

### Sector Gobierno:

- Threshold de alerta: 300
- Revisión manual obligatoria: 500+
- Bloqueo automático: 700+

## Análisis Relacional

### Grafos de Conexión

El sistema visualiza relaciones entre:

- **Usuarios → Dispositivos**
- **Dispositivos → Ubicaciones**
- **Ubicaciones → Redes**
- **Redes → ISPs**
- **Usuarios → Patrones de Comportamiento**

### Indicadores de Alerta en Análisis Relacional

- **Mismo Wi-Fi → Distintos Usuarios:** Posible uso compartido malicioso
- **Mismo Patrón de Comportamiento → Distintos Dispositivos:** Posible bot
- **Mismos Dispositivos BT → Diferentes Ubicaciones:** Dispositivo móvil sospechoso
- **Mismo ISP → Diferentes Cuentas:** Granjas de fraude

---

## Parámetros de Filtrado

## Filtros Temporales

Parámetro	Opciones	Uso Recomendado
Date Range	Selector de fechas	Análisis de tendencias y patrones temporales
Time of Day	Franjas horarias	Detección de actividad fuera de horarios normales

## Filtros Geográficos

Parámetro	Opciones	Uso Recomendado
IP Country	Lista de países	Identificación de accesos desde países de riesgo
IP City	Ciudades específicas	Análisis local de patrones
Location Risk	Alto, Medio, Bajo	Filtrado por nivel de riesgo geográfico

## Filtros de Dispositivo

Parámetro	Opciones	Uso Recomendado
Device Brand	Apple, Samsung, etc.	Análisis por fabricante
OS Family	iOS, Android, Windows	Segmentación por sistema operativo
Device Age	Nuevo, Conocido, Frecuente	Estado del dispositivo en el sistema
Device Source	Orgánico, Referido, etc.	Origen del dispositivo

## Filtros de Red

Parámetro	Opciones	Uso Recomendado
ISP	Proveedores específicos	Análisis por proveedor de Internet
Connection Type	Móvil, Wi-Fi, Ethernet	Tipo de conexión utilizada
VPN Detection	Sí, No, Probable	Identificación de uso de VPN

## Filtros de Comportamiento

Parámetro	Opciones	Uso Recomendado
User Behavior	Normal, Sospechoso, Anómalo	Filtrado por patrón comportamental
Session Duration	Rangos de tiempo	Identificación de sesiones atípicas
Activity Pattern	Múltiples criterios	Análisis de patrones de actividad

## Filtros de Riesgo



Parámetro	Opciones	Uso Recomendado
Risk Score	Rangos 0-1000	Filtrado por nivel de riesgo
Fraud Indicators	Lista de indicadores	Búsqueda por señales específicas
Alert Type	Categorías de alertas	Filtrado por tipo de alerta

## Casos de Uso y Ejemplos

### Caso 1: Detección de Fraude por Copiar/Pegar DNI

**Indicadores Detectados:**

- Patrón de escritura: Paste vs Manual typing
- Pausas máximas durante el tecleo >2 segundos
- Navegación por teclado vs mouse

**Interpretación:** Los usuarios legítimos escriben su DNI manualmente, mientras que los fraudadores suelen copiarlo y pegarlo.

### Caso 2: Detección de Dispositivos Robados

**Indicadores Clave:**

- **Wi-Fi Name:** Cambio abrupto de red doméstica
- **BT Sign:** Dispositivos Bluetooth desconocidos
- **Location ID:** Nueva ubicación sin patrón de viaje
- **New ISP:** Cambio de proveedor de Internet
- **SIM Status:** "No SIM detected"
- **New Location:** Ubicación nunca antes vista

### Caso 3: Análisis de Usuario Múltiple en Dispositivo

**Patrones Detectados:**

- Diferentes tamaños de huella dactilar
- Variaciones en movimientos del acelerómetro
- Pausas máximas en actividad inconsistentes
- Múltiples usuarios en ventana de 4 horas

### Caso 4: Detección de Estafas (Account Move Scam)

**Indicadores Específicos:**

- **Is clean account money transfer:** 98.7% prevalencia en fraude

- **Multiple switch phone position ear-eye:** Comportamiento nervioso
- **Is new payee:** 98.7% prevalencia en fraude
- **Call status during login:** "ON GOING" - llamada activa durante login
- **Is senior user:** Target demográfico común para estafas

## Caso 5: Análisis de Edad de Ubicación

### Patrón Normal vs Fraudulento:

- **Usuarios Legítimos:** Consistencia en ubicaciones (edad >14 días)
- **Sesiones Fraudulentas:** Concentración en ubicaciones nuevas (edad 0-1 días)

---

Revision #11

Created 29 June 2025 02:39:26 by roger de avila

Updated 30 June 2025 14:16:42 by roger de avila