Acerca de este Manual

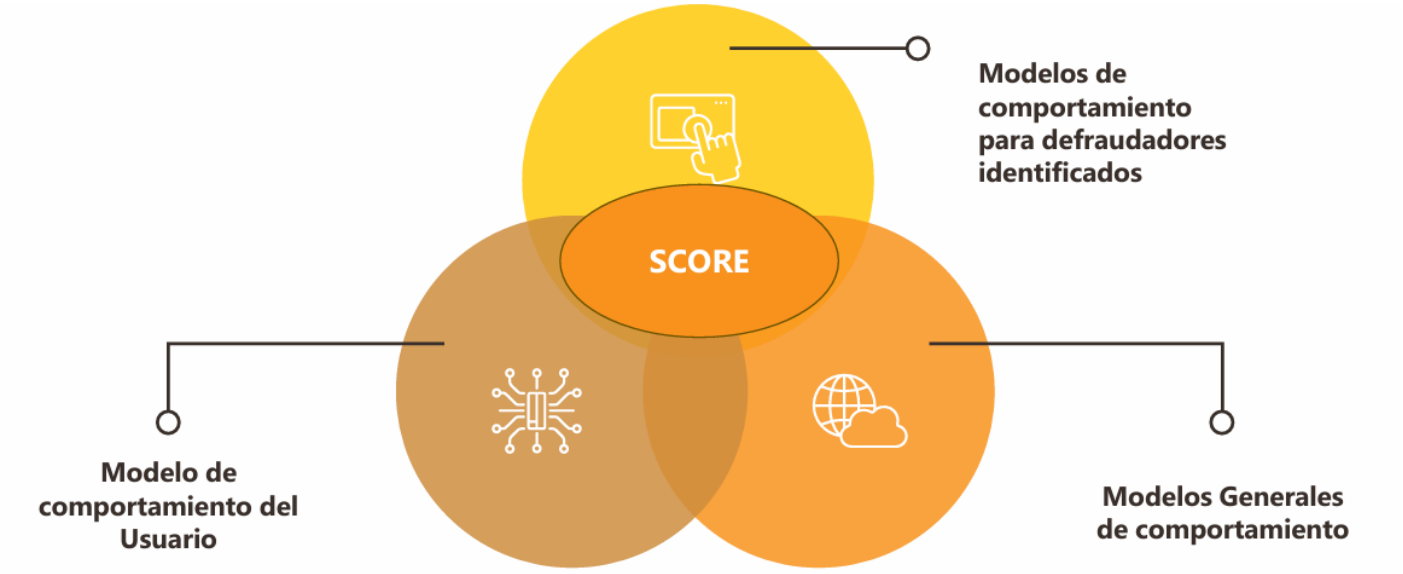
Este manual ha sido diseñado para proporcionar una comprensión integral del Módulo de Detección de Fraude (FDM), una solución tecnológica avanzada que protege las transacciones digitales y la integridad de las plataformas en línea. A través de este documento, los usuarios encontrarán información detallada sobre el funcionamiento, características y beneficios del sistema, así como guías prácticas para su implementación y uso efectivo.

Información de Contacto Importante

Para obtener información sobre esta API y otras soluciones de nuestro catálogo, por favor comuníquese con nuestra área financiera para su evaluación al correo **julian@ado-tech.com**. Todas las claves de acceso, URLs de endpoints y demás elementos de acceso solo serán proporcionados una vez se haya alcanzado un acuerdo formal entre ambas partes.

> **Importante:**
> El alcance y los límites de la recolección de datos dependen en gran medida del tipo de implementación realizada durante la integración de nuestra solución, así como de los límites y capacidades definidos en la contratación actual.
> Algunos módulos o soluciones podrían no estar activos. En caso de que se identifique alguna funcionalidad no disponible, se recomienda validar con nuestro equipo del área financiera, quien proporcionará toda la información necesaria sobre estas limitaciones.

Propósito del Sistema



El propósito fundamental del FDM es proporcionar una capa de seguridad invisible pero altamente efectiva que proteja tanto a las organizaciones como a sus usuarios finales. El sistema ha sido diseñado para:

1. **Detectar amenazas en tiempo real:** Identificar intentos de fraude en el momento en que ocurren, permitiendo una respuesta inmediata que minimice el impacto potencial.
2. **Reducir falsos positivos:** Mediante el análisis sofisticado de múltiples variables, el sistema distingue con precisión entre comportamientos legítimos inusuales y verdaderas amenazas de seguridad.
3. **Adaptarse continuamente:** El sistema aprende constantemente de nuevos patrones y evoluciona para enfrentar amenazas emergentes sin requerir actualizaciones manuales frecuentes.
4. **Mantener la experiencia del usuario:** Operar de manera transparente para los usuarios legítimos, evitando interrupciones innecesarias en sus actividades normales.

¿Qué es el Módulo de Detección de Fraude?

El Módulo de Detección de Fraude (FDM) es una plataforma integral de seguridad digital que utiliza tecnologías de vanguardia para identificar, prevenir y mitigar actividades fraudulentas en tiempo real. A diferencia de los sistemas tradicionales de seguridad que se basan únicamente en credenciales estáticas como contraseñas o tokens, el FDM implementa un enfoque multidimensional que analiza el comportamiento del usuario, las características ambientales y las relaciones contextuales para crear un perfil de seguridad dinámico y adaptativo.

Tipos de Datos Recolectados

Capacidad de Recolección de Datos según el **Alcance del Servicio Contratado**

La capacidad de recolección de datos depende directamente del tipo de servicio contratado y de lo establecido en el contrato. Todos los datos recolectados se obtienen a partir de una integración completa y eficiente con nuestra solución.

En caso de contar únicamente con una **integración simple**, el sistema seguirá siendo funcional; sin embargo, es posible que **algunos datos no estén disponibles** o no se reflejen en la información mostrada, debido a las limitaciones propias de ese tipo de implementación.

INFORMACIÓN DE BIOMETRÍA COMPORTAMENTAL

Esta categoría es fundamental porque permite identificar inmediatamente cuando una persona diferente al propietario legítimo está utilizando el dispositivo. Los patrones biométricos comportamentales son únicos como las huellas dactilares, pero más difíciles de falsificar porque son inconscientes y automáticos. El sistema puede detectar cambios en estos patrones desde los primeros segundos de interacción, proporcionando evaluación de riesgo en tiempo real.

Elemento Recolectado	Descripción	Aplicación Antifraude
Forma de uso del celular	Patrón individual de interacción con el dispositivo, incluyendo forma de sostener, manipular y orientar el dispositivo durante el uso	Detecta cuando una persona no familiarizada usa el dispositivo, generando movimientos compensatorios atípicos, cambios en la estabilidad del agarre y patrones de movimiento inconsistentes
Uso de la pantalla táctil	Ritmo, presión, trayectorias al tocar o deslizar, patrones de gestos y área de contacto específica	Identifica diferencias en la presión ejercida, patrones de deslizamiento únicos, y detecta variaciones en el tamaño del área de contacto que indican diferencias físicas entre usuarios
Uso del teclado	Velocidad de tipeo, presión, combinación de teclas, patrones de pausas entre caracteres y dinámicas de escritura específicas	Revela si el usuario está escribiendo información conocida (flujo natural) o consultando datos externos (pausas prolongadas superiores a 2 segundos, indicativo de búsqueda externa)

Elemento Recolectado	Descripción	Aplicación Antifraude
Uso del mouse	Movimiento del cursor, velocidad, patrones de aceleración, clics y micro-movimientos naturales	Distingue entre movimientos humanos naturales con entropía natural y patrones automatizados de bots que presentan consistencia temporal inhumana
Uso de atajos	Detección de teclas rápidas, combinaciones comunes utilizadas y familiaridad con navegación avanzada	Identifica si el usuario conoce los atajos habituales del sistema y navega con experiencia, o si muestra patrones de navegación inexpertos inconsistentes con el perfil del usuario
Tamaño del dedo y huella	Dimensiones inferidas a partir de la interacción táctil, área de contacto y presión característica	Detecta cambios físicos significativos que indican que otra persona está usando el dispositivo, con rangos típicos de 0.00-0.40 para usuarios legítimos vs. 0.50-1.00 para usuarios fraudulentos
Movimiento del dispositivo	Análisis de estabilidad, inclinación, patrones de acelerómetro durante el uso y vibraciones características	Revela nerviosismo, falta de familiaridad o situaciones de estrés durante el uso, detectando movimientos erráticos que indican manipulación por personas no autorizadas

INFORMACIÓN DE CONTEXTO Y PREFERENCIAS DEL USUARIO

> Esta información permite identificar cuando el acceso proviene de un entorno tecnológico inconsistente con el perfil establecido del usuario legítimo. Los cambios súbitos en preferencias, contexto de uso o ecosistema tecnológico son indicadores altamente confiables de actividad fraudulenta, especialmente cuando se presentan múltiples discrepancias simultáneamente.

Elemento Recolectado	Descripción	Aplicación Antifraude
Preferencias del tema	Configuraciones personalizadas como esquemas de color, fuente, tamaño de texto, contraste, modo claro/oscuro, y otras personalizaciones visuales del sistema	Detecta accesos desde dispositivos que no han sido personalizados por el usuario legítimo, revelando uso de dispositivos genéricos o recién configurados por defraudadores
Tipo de dispositivo	Sistema operativo específico (Android o iOS), fabricante, modelo exacto, versión de software y configuración de hardware	Identifica cambios súbitos de ecosistema tecnológico que pueden indicar dispositivos robados, comprometidos o emulados para evadir otras medidas de seguridad
Navegador utilizado	Navegador web predeterminado, versión específica, configuraciones de privacidad y extensiones instaladas	Revela si el acceso proviene del navegador habitual y configurado del usuario, o de un navegador diferente que sugiere acceso desde dispositivo no autorizado

Elemento Recolectado	Descripción	Aplicación Antifraude
Operador móvil	Proveedor de red celular específico, tipo de plan, configuraciones de red y características del servicio	Detecta cambios de operador que pueden indicar uso de dispositivos clonados, SIM swapping, o tarjetas prepagadas utilizadas por defraudadores
Aplicaciones instaladas	Lista completa de aplicaciones activas e instaladas, versiones específicas, patrones de actualización y configuraciones de aplicaciones	Identifica dispositivos que no contienen el ecosistema personalizado de aplicaciones del usuario, revelando dispositivos genéricos o recientemente comprometidos
Ubicación de uso	Entornos recurrentes y patrones geográficos desde los que se accede habitualmente (hogar, trabajo, ubicaciones frecuentes, rutas habituales)	Detecta accesos desde ubicaciones geográficamente anómalas, físicamente imposibles en el tiempo transcurrido, o inconsistentes con los patrones de movilidad establecidos del usuario

INFORMACIÓN GENERAL DEL DISPOSITIVO

> Permite identificar discrepancias significativas entre el dispositivo habitual del usuario y el dispositivo desde el cual se está intentando realizar el acceso. Los defraudadores raramente pueden replicar todas las configuraciones técnicas específicas y personalizaciones del dispositivo legítimo, especialmente las configuraciones internas y los permisos específicos que el usuario ha otorgado a lo largo del tiempo.

Elemento Recolectado	Descripción	Aplicación Antifraude
Zona horaria e idioma	Configuración regional del sistema, preferencias de idioma principal y secundarios, formato de fecha y hora, y configuraciones de localización	Detecta accesos desde ubicaciones geográficas inconsistentes con el perfil del usuario, identificando discrepancias entre la configuración del dispositivo y la ubicación real
Marca, modelo y sistema operativo	Identificación técnica completa del hardware, versión específica del software, número de compilación y características técnicas del dispositivo	Identifica cambios de dispositivo que pueden indicar robo, clonación, acceso no autorizado, o uso de emuladores para evadir otras medidas de seguridad
Configuraciones de usuario	Personalizaciones específicas realizadas por el usuario a nivel del sistema operativo, preferencias de accesibilidad, configuraciones de pantalla y ajustes personales	Revela si el dispositivo ha sido genuinamente personalizado por el usuario legítimo durante un período extenso, o si es un dispositivo genérico sin historial de personalización

Elemento Recolectado	Descripción	Aplicación Antifraude
Configuraciones internas	Parámetros operativos internos del sistema, configuraciones de desarrollador, ajustes avanzados y modificaciones técnicas del dispositivo	Detecta modificaciones técnicas, rooteo, jailbreak, o alteraciones que pueden indicar dispositivos comprometidos, emulados o preparados específicamente para actividades fraudulentas
Permisos otorgados	Accesos específicos habilitados por el usuario para aplicaciones (ubicación, cámara, micrófono, contactos, almacenamiento), historial de decisiones de permisos	Identifica patrones de permisos inconsistentes con el comportamiento y preferencias de privacidad habituales del usuario, detectando configuraciones atípicas
Fuentes instaladas	Tipografías personalizadas presentes en el sistema operativo, paquetes de idiomas adicionales y recursos de localización instalados	Detecta dispositivos que no han sido utilizados por el usuario legítimo durante tiempo suficiente para acumular personalizaciones típicas de uso prolongado

ESTADO DEL DISPOSITIVO

> Esta información es crucial para identificar situaciones inusuales que pueden indicar fraude, como dispositivos utilizados de manera atípica, condiciones operativas anómalas, o patrones de uso que sugieren acceso no autorizado. Los defraudadores no pueden controlar fácilmente estos aspectos técnicos del dispositivo, especialmente cuando operan remotamente.

Elemento Recolectado	Descripción	Aplicación Antifraude
Estado y nivel de batería	Carga actual del dispositivo, estado de carga activa, patrones históricos de carga y gestión de energía características del usuario	Detecta patrones inusuales de uso de batería que pueden indicar actividad automatizada continua, uso prolongado anómalo por parte de defraudadores, o dispositivos manipulados
Tiempo de actividad	Tiempo transcurrido desde el último reinicio o encendido del dispositivo, frecuencia de reinicios y patrones de uso continuo	Identifica dispositivos recién reiniciados que pueden haber sido comprometidos, manipulados técnicamente, o que han sido objeto de modificaciones para evadir detección
Tamaño de pantalla	Resolución específica, dimensiones físicas exactas del display, densidad de píxeles y características técnicas de la pantalla	Detecta accesos desde dispositivos con características físicas diferentes al dispositivo habitual, identificando intentos de acceso desde emuladores o dispositivos clonados

Elemento Recolectado	Descripción	Aplicación Antifraude
Compartición de pantalla	Estado activo de transmisión del contenido del dispositivo, aplicaciones de control remoto en ejecución y conexiones de pantalla externa	Identifica posibles ataques de ingeniería social donde la pantalla está siendo compartida con defraudadores, o situaciones de control remoto no autorizado del dispositivo

SENSORES AMBIENTALES

> Los datos ambientales son virtualmente imposibles de replicar artificialmente por defraudadores, lo que los convierte en indicadores extremadamente confiables de la ubicación y contexto real del dispositivo. Son especialmente valiosos para detectar fraudes que involucran cambios de ubicación geográfica, uso de emuladores, o accesos remotos que intentan enmascarar la ubicación real.

Elemento Recolectado	Descripción	Aplicación Antifraude
Cantidad de luz	Nivel específico de luminosidad detectado en el ambiente inmediato, variaciones naturales de luz y patrones de iluminación característicos del entorno	Detecta discrepancias críticas entre la ubicación geográfica declarada y las condiciones reales de iluminación (ejemplo: horario nocturno local vs. alta luminosidad detectada, indicando ubicación real diferente)
Presión barométrica	Medición precisa de presión atmosférica útil para determinar altitud exacta, condiciones meteorológicas locales y características del entorno físico	Identifica cambios súbitos e imposibles de altitud que revelan viajes no reportados, uso del dispositivo en ubicaciones geográficamente inconsistentes, o discrepancias con la ubicación declarada

INFORMACIÓN DE UBICACIÓN

> La ubicación constituye uno de los indicadores más poderosos y definitivos de actividad fraudulenta, ya que permite detectar accesos desde ubicaciones físicamente imposibles de alcanzar, geográficamente improbables según los patrones históricos, o completamente inconsistentes con los patrones de movilidad y rutinas establecidas del usuario legítimo.

Elemento Recolectado	Descripción	Aplicación Antifraude
Ubicación aproximada	Estimación geográfica basada en triangulación de redes móviles y Wi-Fi disponibles, proporcionando contexto regional general	Proporciona validación inicial del contexto geográfico general para evaluar la coherencia básica del acceso y detectar discrepancias regionales significativas

Elemento Recolectado	Descripción	Aplicación Antifraude
Ubicación precisa	Coordenadas exactas obtenidas mediante GPS de alta precisión y triangulación avanzada de múltiples redes, con precisión métrica	Detecta ubicaciones específicas anómalas, identifica viajes físicamente imposibles en el tiempo transcurrido entre accesos, y valida la coherencia geográfica detallada
Ubicación basada en IP	Geolocalización aproximada determinada mediante análisis de la dirección IP del dispositivo y rutas de red utilizadas	Identifica discrepancias críticas entre la ubicación física real del dispositivo y la ubicación aparente de la conexión de red, detectando uso de VPN, proxies o redes comprometidas

INFORMACIÓN DE SIM Y TELEFONÍA

> Esta categoría es crítica para detectar uno de los vectores más comunes y peligrosos de fraude móvil moderno: el SIM swapping, la clonación de tarjetas, y la manipulación de identidad telefónica. También permite identificar dispositivos que han sido técnicamente comprometidos o están siendo utilizados de manera deliberadamente anómala para actividades fraudulentas organizadas.

Elemento Recolectado	Descripción	Aplicación Antifraude
Número de teléfono	Número telefónico actualmente asociado al dispositivo, verificando disponibilidad y consistencia en el sistema	Verifica la consistencia crítica entre el número históricamente asociado al usuario y el número actual del dispositivo, detectando cambios no autorizados
ID de SIM y operador	Identificación única técnica del chip SIM físico y información específica del proveedor de servicios asociado	Detecta cambios de tarjeta SIM que pueden indicar SIM swapping exitoso, clonación de tarjetas, o transferencias fraudulentas de números telefónicos
Número de SIMs activas	Cantidad total de tarjetas SIM funcionando simultáneamente en el dispositivo y configuración de conectividad múltiple	Identifica configuraciones técnicas anómalas que pueden indicar dispositivos específicamente preparados para fraude masivo o actividades de phishing organizadas
Estado de llamadas	Estado operativo actual del dispositivo en relación a llamadas telefónicas: activa, timbrando, o inactiva	Detecta situaciones críticas donde el usuario puede estar siendo coercionado activamente durante una llamada telefónica por parte de ingenieros sociales o extorsionistas

CONECTIVIDAD DE RED

> Las redes y la infraestructura de conectividad constituyen elementos que los defraudadores no pueden controlar ni manipular fácilmente, especialmente cuando operan remotamente desde ubicaciones diferentes. Esta información permite detectar accesos desde infraestructuras de red anómalas, proveedores no habituales, o configuraciones técnicas asociadas con actividades fraudulentas conocidas y documentadas.

Elemento Recolectado	Descripción	Aplicación Antifraude
Red celular y Wi-Fi actual	Nombre específico, tipo técnico, configuración de seguridad y características de las redes actualmente conectadas	Detecta conexiones desde redes desconocidas, no verificadas, o históricamente asociadas con actividades fraudulentas documentadas en bases de datos de amenazas
Historial de redes Wi-Fi	Registro completo de redes utilizadas previamente por el dispositivo, incluyendo timestamps y duración de conexiones	Identifica si el dispositivo ha sido utilizado consistentemente en ubicaciones coherentes con el perfil geográfico del usuario legítimo a lo largo del tiempo
Redes Wi-Fi escaneadas	Lista completa de redes inalámbricas disponibles detectadas en el entorno inmediato durante el escaneo activo	Proporciona contexto geográfico adicional altamente específico y detecta ubicaciones anómalas mediante análisis de la infraestructura de red local
Dirección MAC e IP	Identificadores únicos de red del dispositivo a nivel de hardware y software, incluyendo configuraciones específicas	Detecta cambios en identificadores fundamentales que pueden indicar dispositivos clonados, emulados, o que han sido objeto de manipulación técnica
Adaptadores y cifrado	Información técnica detallada de adaptadores de conectividad, protocolos de seguridad utilizados y configuraciones de cifrado	Identifica configuraciones de red técnicamente anómalas o inseguras que pueden indicar dispositivos comprometidos o preparados para actividades maliciosas
Encabezados de red y proveedor	Información específica de protocolo de comunicación y datos del proveedor de servicios de Internet (ISP) utilizado	Detecta proveedores de servicios geográficamente inconsistentes con el perfil del usuario, o ISPs asociados con actividades fraudulentas o servicios de anonimización

DISPOSITIVOS CERCANOS

> Los dispositivos cercanos proporcionan validación adicional crítica de la ubicación real y el contexto auténtico del usuario. Los defraudadores que operan remotamente, desde ubicaciones diferentes, o utilizando dispositivos comprometidos no pueden replicar el ecosistema específico de dispositivos tecnológicos que caracteriza el entorno habitual del usuario legítimo.

Elemento Recolectado	Descripción	Aplicación Antifraude
Dispositivos Wi-Fi cercanos	Equipos específicos visibles en la red inalámbrica del entorno, incluyendo routers, dispositivos IoT, y equipos conectados habituales	Valida de manera definitiva si el usuario se encuentra en su entorno tecnológico habitual (hogar, oficina) mediante detección de dispositivos conocidos y familiares
Dispositivos Bluetooth cercanos	Equipos con conectividad Bluetooth disponibles o emparejados previamente en proximidad física inmediata	Detecta la presencia de dispositivos personales habituales del usuario (auriculares, smartwatch, dispositivos wearables) que confirman la identidad y ubicación real

METADATOS ADICIONALES DEL DISPOSITIVO

>

> Estos datos técnicos adicionales proporcionan capas extra de verificación y validación que son especialmente útiles para detectar dispositivos emulados, clonados, modificados técnicamente, o que han sido específicamente preparados para evadir otros sistemas de detección de fraude más básicos.

Elemento Recolectado	Descripción	Aplicación Antifraude
Datos clave de configuración	Información técnica adicional específica utilizada para identificación contextual avanzada y verificación de autenticidad	Proporciona verificación técnica adicional y detallada para confirmar la autenticidad del dispositivo y detectar manipulaciones técnicas sofisticadas
Lista de redes Wi-Fi disponibles	Inventario completo de redes inalámbricas detectadas durante escaneos activos del entorno	Confirma la ubicación geográfica específica mediante verificación cruzada de redes características del entorno, detectando inconsistencias geográficas
Dirección MAC del dispositivo	Identificador único de red del hardware a nivel físico (cuando está técnicamente disponible y no ha sido enmascarado)	Detecta dispositivos clonados, emulados, o que utilizan identificadores duplicados o técnicamente falsificados para evadir detección

> Gracias a la recopilación de estos datos nos ayuda a calcular nuestro **sistema de puntuación unificado** mediante el procesamiento inteligente de todas las variables mencionadas. La integración de estos múltiples vectores de información permite crear un perfil completo y único de cada usuario, estableciendo patrones de comportamiento normal que sirven como línea base para la detección de anomalías.

El sistema de recolección opera de manera completamente pasiva y transparente para el usuario, capturando información contextual sin interrumpir la experiencia de uso normal. Esta metodología de recolección continua permite la construcción de modelos de comportamiento robustos que se adaptan a los cambios legítimos en los patrones de uso del usuario a lo largo del tiempo, mientras mantienen la sensibilidad necesaria para detectar actividades fraudulentas.

La arquitectura de recolección está diseñada para operar en tiempo real, procesando y analizando los datos de manera simultánea durante cada interacción del usuario con el dispositivo. Esta capacidad de análisis en tiempo real es fundamental para proporcionar evaluaciones de riesgo inmediatas que permiten tomar decisiones de seguridad apropiadas sin demoras que puedan afectar la experiencia del usuario o permitir que actividades fraudulentas se completen exitosamente.

Modelos de análisis y detección

Este modelo crea un perfil único y personalizado para cada usuario, basado en su forma habitual de interactuar con el dispositivo. Al conocer sus patrones normales de uso, el sistema puede detectar cualquier comportamiento inusual que podría indicar que otra persona está accediendo al sistema sin autorización.

Información Recolectada del Usuario

> Comportamiento del Usuario

- **Uso del dispositivo celular:** Forma específica de manipulación
- **Forma de sostener el celular:** Patrones únicos de agarre
- **Uso del teclado:** Velocidad, ritmo y presión de escritura

> Información de Ubicación

- **Ubicación del usuario:** Coordenadas GPS y ubicación aproximada
- **Red utilizada:** Conectividad celular y Wi-Fi
- **Redes Wi-Fi:** Historial y redes cercanas disponibles

> Información del Dispositivo

- **Tamaño de pantalla:** Resolución y configuración
- **Preferencias de tema:** Color, tamaño de fuente, configuraciones visuales
- **Modelo y marca:** Especificaciones técnicas del dispositivo
- **Identificadores únicos:** Metadatos del dispositivo

Análisis Biométrico Comportamental

Enfoque Estricto

- **Uso de pantalla táctil:** Patrones de deslizamiento y presión
- **Uso del mouse:** Movimientos y clics característicos
- **Uso del teclado:** Dinámicas de escritura y atajos
- **Velocidad de escritura:** Ritmo y pausas personalizadas

- **Uso de atajos:** Preferencias de navegación
- **Tamaño de huella dactilar:** Biometría física única
- **Tamaño del dedo:** Área de contacto en pantalla
- **Movimiento del celular:** Patrones de acelerómetro durante uso

Enfoque Amplio

- **Preferencias de tema:** Configuraciones de color y tamaño de fuente
- **Ubicación de uso:** Patrones geográficos habituales
- **Tipo de dispositivo:** Android o iOS, preferencias de ecosistema
- **Navegador utilizado:** Preferencias de software
- **Operador celular:** Proveedor de servicios habitual
- **Aplicaciones instaladas:** Ecosistema de software personal

Modelos Generales de Comportamiento

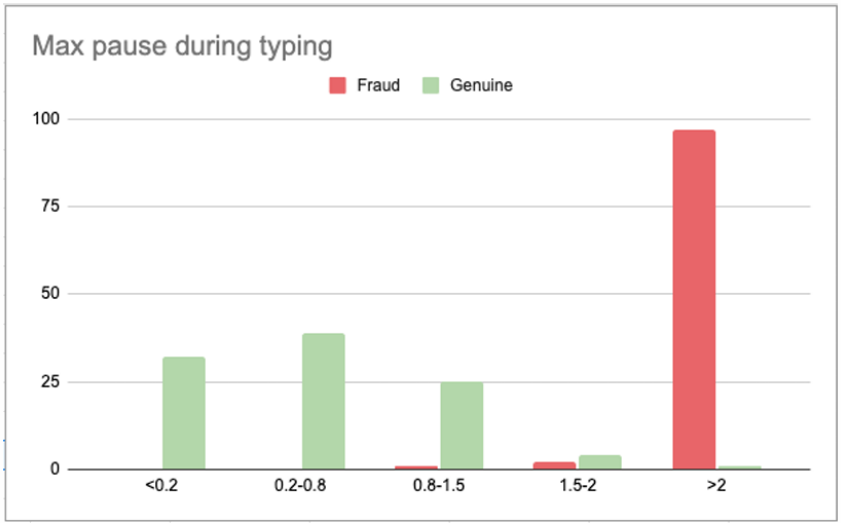
Contamos con modelos entrenados con millones de interacciones reales que ayudan a diferenciar entre comportamientos típicos de usuarios legítimos y aquellos que son característicos de acciones fraudulentas. Esto permite identificar comportamientos sospechosos, incluso si nunca antes se habían visto en el sistema.

Análisis Comparativo de Comportamientos

Patrón de Interacción	Comportamiento Fraudulento	Comportamiento de Usuario Legítimo
Alternar entre aplicaciones	Múltiples veces	Nunca
Ingreso de DNI/ID	Pegar texto / Tipeo alternado	Tipeo manual normal
Navegación en formularios	Uso de teclado	Uso de mouse

Ejemplo: Análisis de Pausas Durante Escritura

Gráfico de Pausas Máximas Durante Escritura del DNI



Interpretación:

- **Usuarios Legítimos:** Pausas distribuidas naturalmente
- **Usuarios Fraudulentos:** 95% presenta pausas extremas (>2 segundos), indicativo de consulta externa

Análisis de Uso de DNI con Pegar/Copiar

Gráfico de Detección de Pegado de DNI

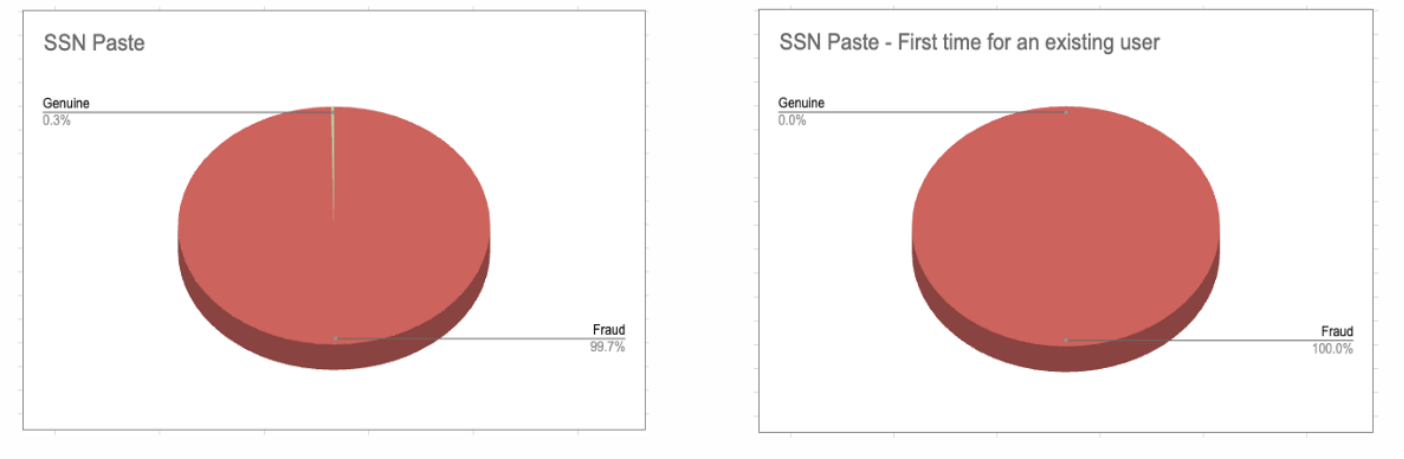


Gráfico Izquierdo - "SSN Paste" (Pegado de SSN):

- **Fraud (Fraude): 99.7%** - Representado en color rojo oscuro
- **Genuine (Genuino): 0.3%** - Representado en color rojo claro/rosado
- Muestra que cuando se detecta pegado de número de identificación, casi la totalidad de los casos (99.7%) son fraudulentos

Gráfico Derecho - "SSN Paste - First time for an existing user" (Pegado de SSN - Primera vez para usuario existente):

- **Fraud (Fraude): 100.0%** - Representado completamente en color rojo
- **Genuine (Genuino): 0.0%** - Sin representación visual
- Muestra que cuando un usuario existente utiliza "pegar" por primera vez, el 100% de los casos son fraudulentos

Modelos de Comportamiento para Defraudadores Identificados

A través del análisis histórico, se han identificado patrones comunes en personas que previamente han intentado realizar fraudes. Estos modelos almacenan y actualizan de forma continua esta información, lo que permite detectar cuando un intento de acceso o transacción se asemeja al comportamiento de estos defraudadores conocidos.

Indicadores Específicos para Estafas de Transferencia

Indicador	Valor	Prevalencia Relativa	Prevalencia en Fraude	Fuerza de Indicación
Transferencia de cuenta limpia	Sí	0.4%	98.7%	67
Múltiples cambios posición teléfono-oído	Sí	1.5%	67.7%	58
Nuevo beneficiario	Sí	0.24%	98.7%	46
Estado de llamada durante login	EN CURSO	2.3%	68.3%	35
Usuario senior	Verdadero	17.2%	93.2%	18

Indicadores de Teléfono Robado

Indicador	Valor	Prevalencia Relativa	Prevalencia en Fraude	Fuerza de Indicación
Nombre Wi-Fi	Azizi 423	0%	64.2%	999
Señal Bluetooth	46542342134	0%	34.7%	999
ID de ubicación	642547854652321	0.05%	34.2%	750
Nuevo ISP	Verdadero	0.4%	88.3%	574
Estado SIM	No SIM detectada	0.03%	64.7%	67
Nueva ubicación	Verdadero	4%	66.7%	65
Nuevo beneficiario	Sí	0.24%	98.7%	46

Modelos Adicionales

Detección de Malware

Permite identificar comportamientos que podrían estar siendo generados por software malicioso instalado en el dispositivo.

Indicadores Técnicos:

- Patrones de automatización perfecta
- Timing inhumano en interacciones
- Secuencias repetitivas de acciones
- Acceso a recursos del sistema sin intervención del usuario

Detección de Bots

Diferencia entre un humano y un sistema automático, lo que es clave para prevenir fraudes automatizados.

Características de Detección:

- Análisis de entropía en movimientos
- Patrones de timing demasiado consistentes
- Ausencia de micro-movimientos naturales
- Secuencias de acciones predecibles

Análisis de Riesgo por Actividad

Evalúa el riesgo de una acción específica (como una transferencia o un inicio de sesión) considerando el contexto en el que se realiza.

Factores Contextuales:

- Horario de la transacción
- Monto involucrado
- Tipo de beneficiario
- Historial de transacciones similares

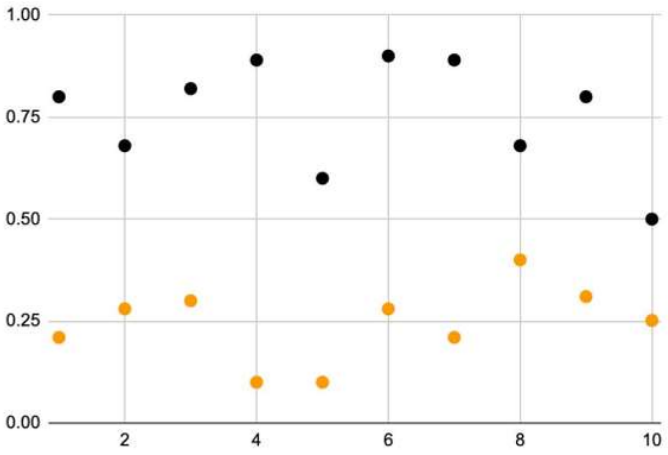
Análisis de Conexiones

Analiza las relaciones entre usuarios, dispositivos y redes para detectar patrones organizados de fraude.

Métricas de Conexión:

- Usuarios compartiendo infraestructura de red
- Dispositivos utilizados por múltiples identidades
- Patrones temporales coordinados
- Ubicaciones físicas compartidas

ANÁLISIS DE DIFERENCIAS EN TAMAÑO DE HUELLA DACTILAR



El gráfico presenta un análisis de dispersión que mide el tamaño de la huella dactilar detectada durante el uso del dispositivo móvil. Esta métrica biométrica permite identificar si el usuario actual corresponde al propietario legítimo del dispositivo.

Características del Gráfico:

- Título: "Finger size"
- Eje X: Secuencia temporal de mediciones (escala de 2 a 10)
- Eje Y: Tamaño relativo de la huella dactilar (escala de 0.00 a 1.00)
- Puntos Negros: Representan sesiones identificadas como fraudulentas
- Puntos Naranjas: Representan sesiones de usuarios legítimos

Interpretación de Patrones

Sesiones de Usuarios Legítimos (Puntos Naranjas)

Rango de valores: 0.00 - 0.40 Características observadas:

- Consistencia en el tamaño de huella a lo largo de toda la sesión
- Variación mínima entre mediciones sucesivas
- Agrupación de valores en rangos específicos que corresponden al usuario registrado
- Estabilidad temporal que refleja el uso natural del dispositivo

Significado: Los usuarios legítimos mantienen un tamaño de huella constante porque utilizan consistentemente los mismos dedos y con la misma presión habitual.

Sesiones Fraudulentas (Puntos Negros)

Rango de valores: 0.50 - 1.00 Características observadas:

- Mayor variabilidad en el tamaño de huella
- Valores significativamente diferentes al perfil biométrico registrado
- Inconsistencia entre mediciones dentro de la misma sesión
- Tendencia hacia valores más altos que sugieren diferencias físicas

Significado: Los defraudadores presentan huellas de tamaño diferente al usuario legítimo, lo que indica que se trata de una persona física distinta utilizando el dispositivo.

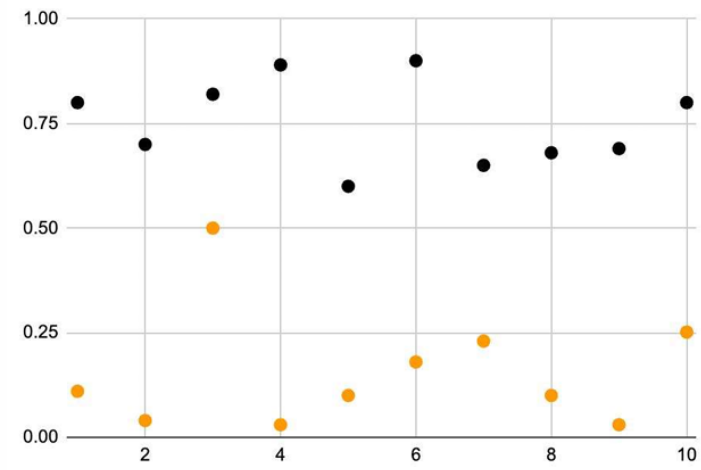
Aplicación Práctica

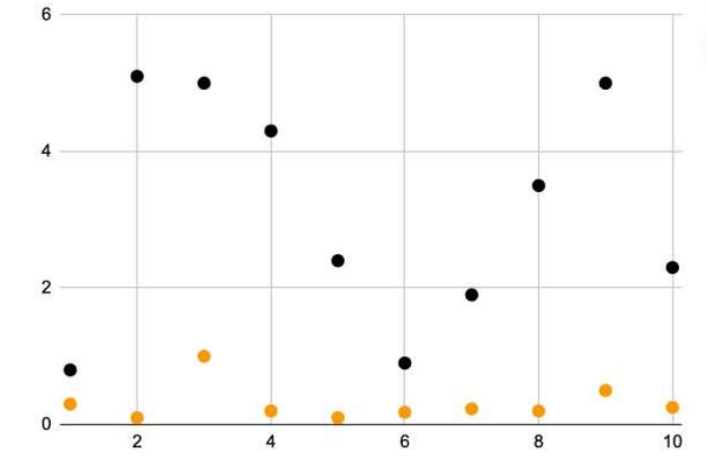
Detección de Uso No Autorizado: El sistema puede identificar inmediatamente cuando una persona diferente al propietario registrado está utilizando el dispositivo, basándose en las diferencias anatómicas naturales entre individuos.

Casos de Detección:

- Dispositivos robados siendo utilizados por terceros
- Acceso no autorizado por familiares o conocidos
- Uso fraudulento después de pérdida del dispositivo
- Suplantación de identidad con dispositivos comprometidos

ANÁLISIS DE MOVIMIENTOS DEL CELULAR





La forma en que las personas sostienen y mueven sus dispositivos móviles durante el uso constituye una firma biométrica única y personal. Estos patrones de movimiento reflejan hábitos motores inconscientes que son extremadamente difíciles de replicar por personas no autorizadas.

Gráfico 1: Acelerómetro Durante Toque de Botón

Este gráfico analiza las lecturas del acelerómetro del dispositivo específicamente en los momentos cuando el usuario realiza toques en botones de la interfaz.

Estructura del Gráfico:

- Medición: Intensidad de movimiento captada por sensores de aceleración
- Eje Temporal: Secuencia de eventos de toque (2 a 10)
- Eje de Intensidad: Magnitud del movimiento (0.00 a 1.00)
- Diferenciación: Puntos negros para fraude, naranjas para usuarios legítimos

Usuarios Legítimos:

- Rango de movimiento: 0.00 - 0.50
- Patrón característico: Movimientos controlados y predecibles
- Estabilidad: Variaciones mínimas entre toques sucesivos
- Explicación: Los usuarios familiares con su dispositivo desarrollan patrones motores automáticos que resultan en movimientos económicos y precisos

Usuarios Fraudulentos:

- Rango de movimiento: 0.50 - 1.00
- Patrón característico: Movimientos erráticos e impredecibles
- Inestabilidad: Gran variación entre diferentes acciones
- Explicación: La falta de familiaridad con el dispositivo genera movimientos compensatorios, nerviosismo y patrones motores atípicos

Gráfico 2: Pausa Máxima de Actividad Durante Sesión

Este análisis mide los intervalos de inactividad más prolongados que ocurren durante una sesión de uso del dispositivo, proporcionando información sobre los procesos cognitivos del usuario.

Estructura del Gráfico:

- Medición: Duración de pausas en segundos
- Eje Temporal: Progresión de la sesión (2 a 10)
- Eje de Duración: Tiempo de pausa máxima (0 a 6 segundos)
- Diferenciación: Puntos negros para fraude, naranjas para usuarios legítimos

Análisis de Comportamientos Cognitivos

Usuarios Legítimos:

- Rango de pausas: 0 - 1.5 segundos
- Características: Flujo continuo y natural de interacción
- Procesamiento: Acceso inmediato a información personal memorizada
- Navegación: Conocimiento intuitivo de la interfaz y procesos

Usuarios Fraudulentos:

- Rango de pausas: 1.5 - 6+ segundos
- Características: Interrupciones prolongadas y frecuentes
- Procesamiento: Necesidad de búsqueda, verificación o consulta externa
- Navegación: Incertidumbre sobre procedimientos y datos requeridos

Casos Especiales y Excepciones

Situaciones Atípicas en Usuarios Legítimos

El sistema está diseñado para reconocer circunstancias excepcionales donde el propietario legítimo puede exhibir patrones anómalos:

Condiciones de Estrés:

- Situaciones de emergencia que alteran comportamiento motor
- Presión temporal que afecta patrones habituales
- Circunstancias de riesgo que generan nerviosismo

Condiciones Físicas:

- Lesiones temporales en manos o dedos
- Efectos de medicación que afectan coordinación
- Fatiga extrema que altera precisión motora

Condiciones Ambientales:

- Uso durante transporte que introduce vibraciones externas
- Condiciones climáticas que afectan manipulación del dispositivo
- Iluminación deficiente que requiere mayor concentración

Detección Inmediata: El análisis de movimientos proporciona evaluación de riesgo en tiempo real desde los primeros segundos de interacción, sin requerir completar transacciones o procesos específicos.

Invisibilidad para el Usuario: La recopilación de datos biométricos de movimiento ocurre de manera transparente durante el uso normal, sin generar fricción adicional en la experiencia del usuario.

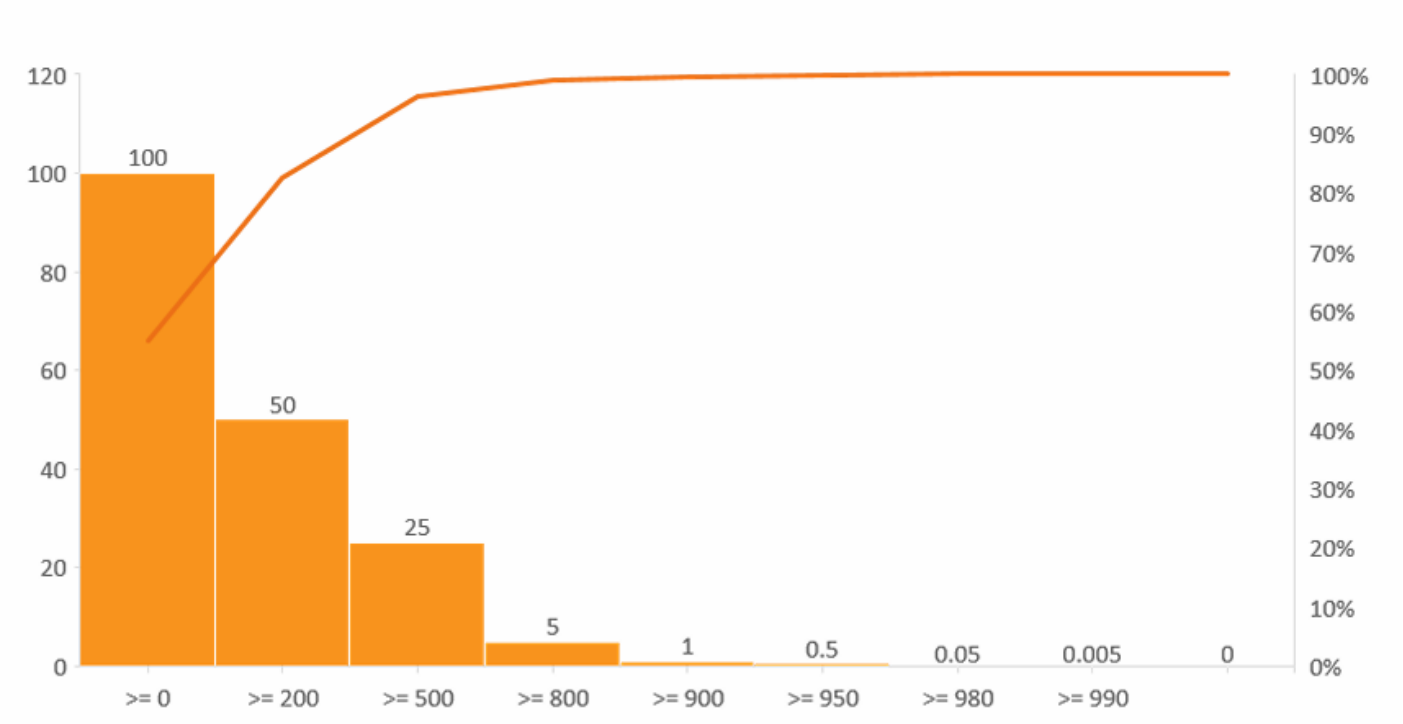
Resistencia a Falsificación: Los patrones de movimiento son resultado de años de desarrollo motor personal, haciéndolos extremadamente difíciles de replicar conscientemente por actores maliciosos.

Adaptabilidad Contextual: El sistema aprende y se adapta a las variaciones naturales del usuario legítimo, mejorando su precisión con el tiempo mientras mantiene sensibilidad para detectar uso no autorizado.

Cálculo del score de riesgo

Toda la información recolectada se integra en una arquitectura basada en inteligencia artificial que analiza tanto modelos individuales como patrones colectivos en tiempo real. Como resultado de este análisis, se genera un **score unificado de riesgo**, que va de **0 a 1000**, e indica con alta precisión la **probabilidad de que una sesión o acción sea legítima o fraudulenta**. A mayor puntuación, mayor es el nivel de riesgo identificado.

Este score se convierte en un **indicador clave** para la toma de decisiones, ya sean **automatizadas o asistidas**, sobre accesos, transacciones o actividades dentro de plataformas digitales. De esta manera, se **elevan los niveles de seguridad sin comprometer la experiencia del usuario**.



Descripción: Este gráfico muestra la distribución de los scores de riesgo calculados por el sistema de IA que integra todos los modelos de detección de fraude.

Explicación detallada:

- **Eje X:** Rangos de scores de riesgo (≥0, ≥200, ≥500, ≥800, ≥900, ≥950, ≥980, ≥990)
-

- **Eje Y izquierdo:** Cantidad de casos (hasta 120)
- **Eje Y derecho:** Porcentaje acumulativo (hasta 100%)
- **Barras naranjas:** Muestran la cantidad de sesiones en cada rango de score
- **Línea naranja:** Representa el porcentaje acumulativo

Interpretación: La mayoría de las sesiones (100 casos) tienen scores bajos (≥0), indicando comportamiento normal. Conforme aumenta el score, disminuye drasticamente el número de casos, siendo muy pocas las sesiones con scores altos (≥980, ≥990) que indican alto riesgo de fraude.

Rango	Nivel de Riesgo	Acción Recomendada
0 - 200	Muy bajo	Monitoreo estándar
201 - 400	Bajo	Monitoreo estándar
401 - 600	Medio	Verificación
601 - 800	Alto	Autenticación reforzada
801 - 1000	Muy alto	Bloqueo/Revisión manual