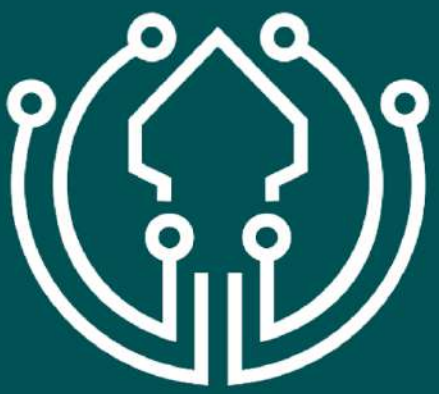
FRAUD DETECTION

Detección del Fraude basado en localización,
el enfoque de seguridad que su empresa necesita.

www.ironchip.com

by



IRONCHIP

TABLA DE CONTENIDO

1. INTRODUCCIÓN

La manera más eficiente de prevenir las situaciones de fraude es anticipándose a ellas, y la clave está en predecir el comportamiento humano. La localización como parámetro para identificar a las personas (usuarios) y dispositivos no es algo que no se haya pensado hasta el momento. A comienzos de la pasada década ya había estudios que demostraban que el 95% de los usuarios son identificables conociendo **4 puntos espacio-temporales frecuentes**; es decir, conocer cuatro lugares habituales en unos tiempos concretos bastaría para identificar al 95% de los individuos.

Así, al identificar a los usuarios, y junto a ello, al predecir su comportamiento, se les puede ofrecer una experiencia de producto completamente personalizada, logrando definir estrategias de negocio que realmente satisfagan sus necesidades.

No solo se trata de prevenir el fraude, sino de obtener la información correcta y oportuna de los usuarios basada en su localización, la cual apoyé la toma de decisiones de ventas asertivas a través de: los volúmenes de transacciones históricas y en real-time, las densidades segmentadas por regiones o zonas, las tendencias estacionales o renovables, etc.

En sí, desde ofrecerle al usuario servicios de seguridad bancaria personalizados, hasta préstamos y seguros transmitidos por geolocalización (zonas universitarias, industriales, residenciales, rurales, carreteras, etc.), donde cada dato procesado contribuya con la buena reputación y el adecuado reconocimiento que su negocio se merece.

1.1. Identidad por Comportamiento

La verificación de la identidad de los usuarios es un desafío que se ha encaminado hacia el estudio de su comportamiento a través del análisis de datos y la ponderación de una extensa gama de pruebas/factores de identidad asociadas a sus dispositivos. Cada usuario manifiesta un comportamiento el cual es expresado a través del uso de sus dispositivos, generando una gran cantidad de datos e información, lo que permite con la ayuda de una inteligencia artificial, analizar, verificar y determinar la identidad de dicho usuario, es decir, si es realmente o no el individuo que dice ser, o se piensa es.

Actualmente existe una gran cantidad de tipos de pruebas de identidad relacionada con el comportamiento del usuario: la manera en la que se escribe, las aplicaciones que se tiene instaladas, el pulso que tenemos, la posición de la pantalla del dispositivo, la voz, etc., por lo que, dentro de esta gran variedad de pruebas para verificar la identidad, se pueden diferenciar principalmente dos grupos: las pruebas biométricas y las pruebas asociadas a los dispositivos.

El nuevo paradigma de seguridad basado en localización y comportamientos habituales nos abre la puerta para buscar la manera de localizar el lugar en el cual se encuentra un usuario comprobando con mayor certeza su identidad, lo cual es clave para permitirnos no solo identificar al 95% de los usuarios de manera que no se puedan suplantar, sino que nos da la capacidad de detectar comportamientos que no se ajusten a identidades reales de los usuarios detectando eficientemente a usuarios maliciosos en tiempo real, e incluso en un futuro, a través del aprendizaje de nuestra inteligencia artificial, localizarlos con una excelente precisión.

1.2.Detección del Fraude por Comportamiento Anómalo

Mediante esta **solución**, IRONCHIP proporciona a sus clientes una herramienta que les permite conocer si un usuario de su plataforma (aplicación) está teniendo un comportamiento anómalo o sospechoso. Dicho comportamiento está basado en datos del usuario, dispositivo asociado al mismo y la localización; esta última siendo obtenida a partir de las ondas radioeléctricas circundantes en un lugar específico en tiempo-real y asociadas a los lugares habituales del usuario. Por tanto, estos tres parámetros: usuario, dispositivo asociado y localización real/habitual, determinan de manera muy precisa y oportuna los comportamientos de los individuos, permitiendo perfilarlos como sospechosos o fraudulentos, logrando así, generar la información adecuada para tomar decisiones rápidas y asertivas.

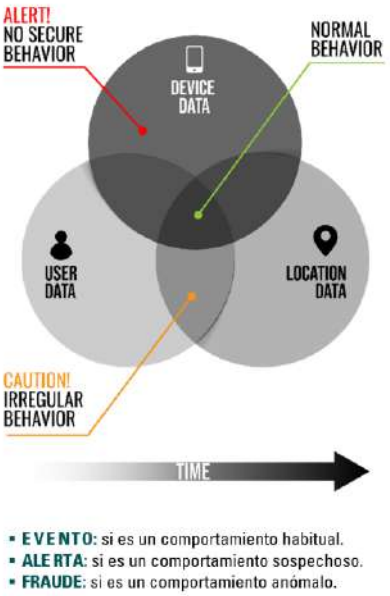
De manera eficaz, la tecnología de IRONCHIP interpreta e identifica los comportamientos naturales de los usuarios, los cuales comúnmente utilizan sus dispositivos habituales para interactuar con sus aplicaciones desde las zonas que frecuentemente permanecen o visitan, e identifica las conductas irregulares o sospechosas, donde ni el dispositivo con el cual se está accediendo a la aplicación, ni el lugar desde donde se encuentra el usuario son los habituales, detectándose un posible caso de fraude, debido a que, obviamente la relación entre ambas informaciones no coincide.

La solución de **Fraud Detection** de IRONCHIP cruza las 3 tipologías de datos: datos de los usuarios, datos de sus dispositivos y datos de sus localizaciones para verificar, certificar y garantizar la identidad de los usuarios al realizar cualquier tipo de operación en las aplicaciones de nuestros clientes, alertando sobre situaciones sospechosas o anómalas, cuando las operaciones sean realizadas desde lugares en los cuales sus usuarios habitualmente no permanecen o frecuentemente no visitan.

La inteligencia artificial desarrollada por IRONCHIP le permite a **Fraud Detection** aprender y mejorar la calidad de sus detecciones a medida que

trabajamos en equipo con nuestros clientes, identificando con mucha certeza situaciones de fraude:

- **SIM Swapping**, también conocido como "SIM jacking" o "SIM hijacking". Los delincuentes al recopilar información personal de la víctima convencen al proveedor de servicios de telefonía móvil para que se transfiera el número de teléfono de la víctima a una nueva SIM controlada por ellos, robando el número de teléfono y la identidad de ella.
- **Location Swapping**, o intercambio de ubicación. Este término se refiere a cuando se produce un cambio en la ubicación de un usuario fuera de su zona segura o habitual, y no necesariamente implica actividad fraudulenta.
- **Location Fraud**, también conocido como Fraude de Ubicación. Este tipo de fraude ocurre cuando los delincuentes manipulan los datos de ubicación transmitidos por un dispositivo, creando una discrepancia entre la ubicación real del dispositivo y la ubicación reportada por el sistema de GPS y las ondas electromagnéticas.
- **Device Swapping**, o cambio de dispositivo. Los delincuentes transfieren información y datos de un dispositivo a otro, tomando el control de la cuenta de la víctima al transferir el número de teléfono y la información del dispositivo a otro dispositivo bajo su control.
- **Device Rooted**, o acceso completo al sistema operativo. Aunque en sí mismo el proceso de rootear un dispositivo no es ilegal, los delincuentes lo utilizan para eludir las medidas de seguridad, obteniendo acceso no autorizado a cuentas y datos de la víctima a través de la instalación de aplicaciones maliciosas o modificaciones en el sistema operativo.
- **Device Debugged**, es una técnica que implica el uso de herramientas especializadas por los delincuentes para alterar o "depurar" el software y/o hardware de un dispositivo, a pesar de no poder hacerse modificaciones en el sistema operativo, si se puede acceder a toda la información, logrando falsificar los datos que se envían desde el dispositivo depurado.
- **Device Emulated**, un emulador es un software que imita el comportamiento de un dispositivo específico de manera precisa a nivel de hardware y software. Los delincuentes utilizan emuladores para que cualquier programa o sistema operativo diseñado para ese dispositivo funcione maliciosamente de manera virtualizada.
- **Red VPN**, los delincuentes utilizan la red VPN para obtener anonimato y privacidad en línea al realizar sus operaciones maliciosas. Aunque es una herramienta legal para proteger la privacidad, puede ser utilizada para actividades malintencionadas al ocultar la identidad y ubicación del usuario.
- **Red TOR**, empleada tanto por usuarios legítimos como delincuentes para resguardar su privacidad y anonimato en línea. Aunque es una herramienta legal para proteger la privacidad, puede ser utilizada para actividades malintencionadas al ocultar la identidad y ubicación del usuario.
- **New User**, o Nuevo Usuario, se refiere a alguien que accede por primera vez a la plataforma de Fraud Detection de Ironchip. Este término no indica necesariamente actividad fraudulenta, simplemente destaca que el usuario es nuevo en el sistema, pero muy útil para que el sistema este atento al comportamiento del usuario respectivo.
- **Unknown Location**, o Ubicación Desconocida, se da cuando la plataforma IRONCHIP no puede determinar la ubicación precisa del usuario, ya sea porque está conectado únicamente por IP o debido a discrepancias entre distintos proveedores de ubicación. No necesariamente indica actividad sospechosa, solo una falta de información geolocalizada precisa, pero muy útil para que el sistema este atento al comportamiento del usuario respectivo.



1.1.1. ¿Cómo IRONCHIP sabe si es un lugar habitual?

Por repetición, si ya se ha realizado **más de una transacción correcta** desde ese lugar se considerará un lugar habitual para ese usuario/dispositivo. Cada usuario puede llegar a tener entre 3-10 lugares seguros/habituales, necesitando al menos dos transacciones desde un mismo lugar para catalogarlo como habitual. De esta manera, si tenemos estos tres datos correctamente correlacionados, verificaríamos que el usuario es quien dice ser.

1.1.2. ¿Qué es una Zona Segura?

Es una zona desde la que el usuario suele operar. Una operación fraudulenta tiende a realizarse desde un lugar alejado de las zonas seguras. Esta dimensión se añade a los sistemas de detección del fraude sin que se viole la privacidad del cliente, ya que este sistema no permite la localización inversa.

El concepto de Zona Segura también se complementa con el sistema de reconocimiento de dispositivos IRONCHIP, asignando una huella digital vinculada a un dispositivo único y anónimo.

2. FRAUD DETECTION

El producto **Fraud Detection** de IRONCHIP es el más completo sistema integrado de alertas, monitorización y seguimiento para prevenir el Fraude, el cual se integra con cualquier tipo de aplicación y plataforma de software gracias al desarrollo innovador de sus versátiles interfaces de programación.

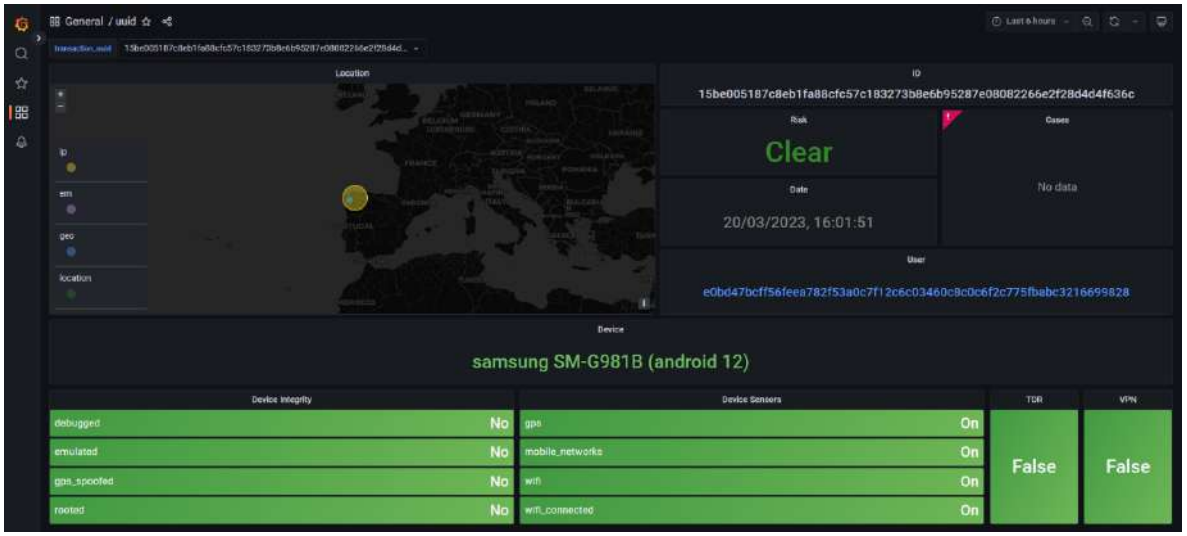
El sistema combina la inteligencia artificial de IRONCHIP con tecnología espacial de última generación para identificar las **Zonas Seguras** de los usuarios de nuestros clientes mediante la geolocalización (GPS), la localización por ondas electromagnéticas (EM) y otros elementos posicionales, así como los comportamientos habituales de ellos a través del uso de sus dispositivos, garantizando la comprobación de su identidad en cada momento.

2.1.Alertas

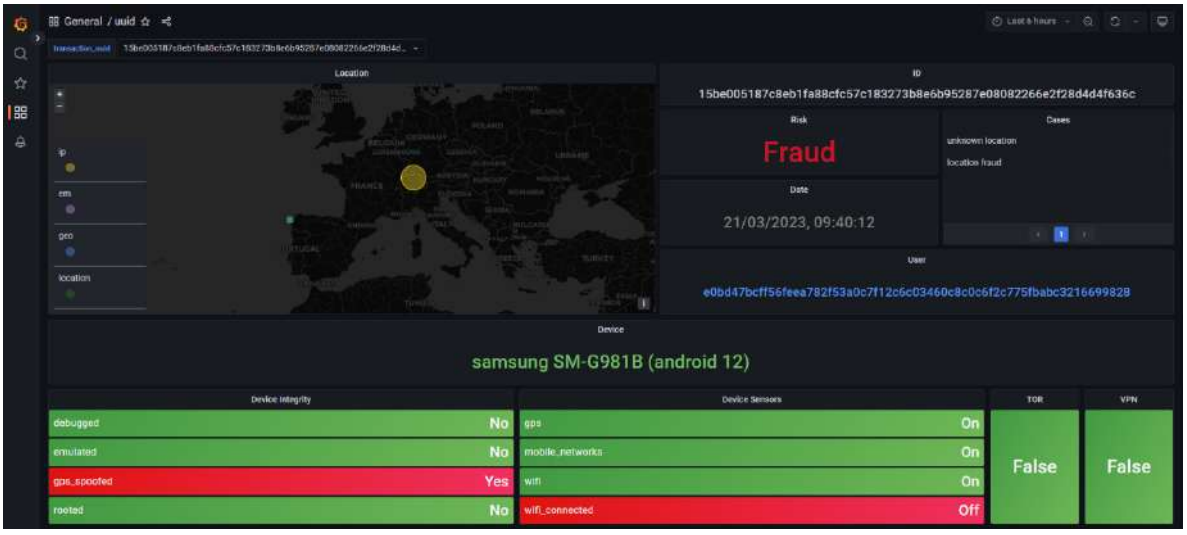
Al combinar los conceptos de Identidad por Comportamiento, Lugares Habituales, Zonas Seguras y Comportamientos Anómalos, la inteligencia artificial de IRONCHIP alerta sobre situaciones sospechosas o de riesgos que no coinciden con los comportamientos habituales de los usuarios de los clientes.

El sistema de **Fraud Detection** ha sido diseñado para identificar los comportamientos normales/habituales y anómalos de los usuarios según los siguientes niveles de riesgo:

- **Clear:** Comportamiento normal/habitual del usuario. Realización de operaciones en el *dispositivo del usuario* a través de la aplicación o plataforma del cliente en lugares frecuentes, es decir, en **Zonas Seguras**.
- **Low:** Comportamiento sospechoso del usuario. Realización de operaciones en un *dispositivo diferente al del usuario* a través de la aplicación o plataforma del cliente en lugares frecuentes, es decir, en **Zonas Seguras**.
- **High:** Comportamiento anómalo del usuario. Realización de operaciones en un *dispositivo diferente al del usuario* a través de la aplicación o plataforma del cliente en lugares desconocidos, es decir, en **Zonas NO Seguras**.
- **Fraud:** Comportamiento fraudulento del usuario. Realización de operaciones en un *dispositivo corrupto y/o diferente al del usuario* a través de la aplicación o plataforma del cliente en lugares desconocidos o improbables, es decir, en **Zonas NO Seguras e Imposibles**.

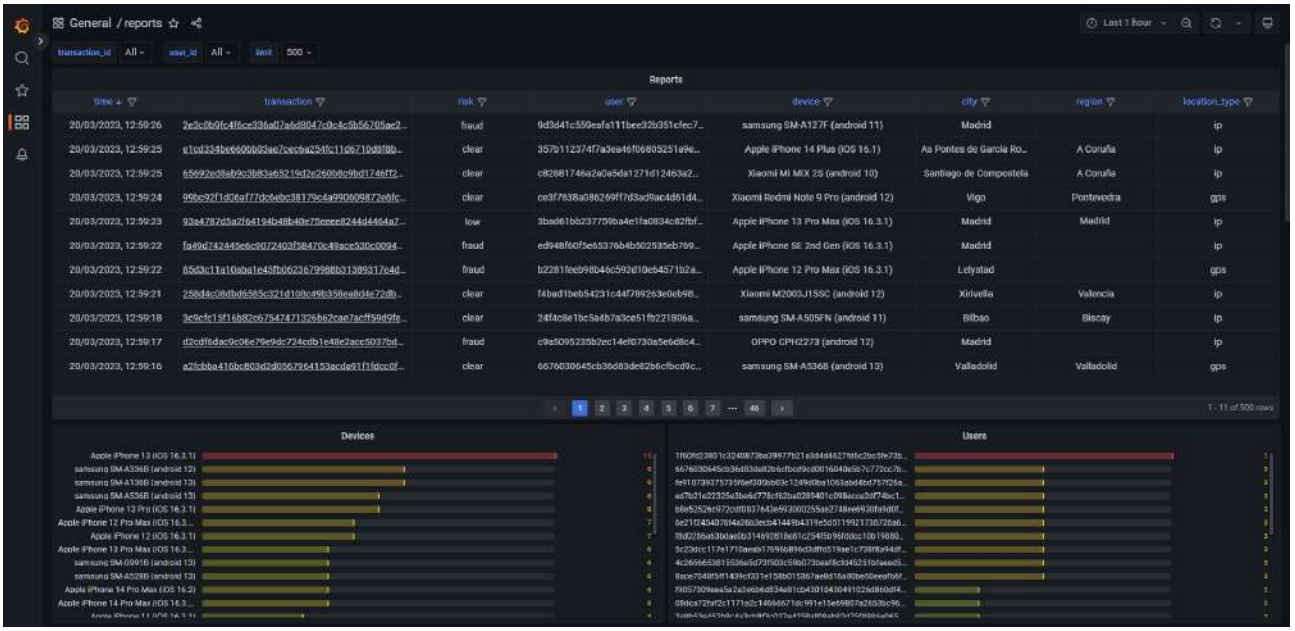


Así, la inteligencia artificial de IRONCHIP desarrolla la capacidad para detectar comportamientos que no se ajusten a identidades reales de los usuarios, alertando sobre comportamientos sospechosos o fraudulentos de aquellos usuarios maliciosos que utilizan las aplicaciones o plataformas de nuestros clientes.



2.2.Monitoring: Monitoreo y Seguimiento

El panel de monitoreo y seguimiento de **Fraud Detection** ha sido diseñado para que *de manera fácil e intuitiva* nuestros clientes puedan conocer en tiempo real el riesgo de cada una de las transacciones que se generen por las operaciones de sus usuarios en sus aplicaciones o plataformas. A través de este práctico panel, nuestros clientes pueden conocer la información de cada uno de los dispositivos de sus usuarios, los niveles de riesgo asociados a sus **Zonas Seguras**, las horas, fechas, ciudades y regiones donde se están generando las interacciones con sus aplicaciones o plataformas, e incluso, los tipos de localización predominantes detectados por nuestra inteligencia artificial para identificar identidades reales, comportamientos normales/habituales, dispositivos saludables (no corruptos), entre otros aspectos de interés.



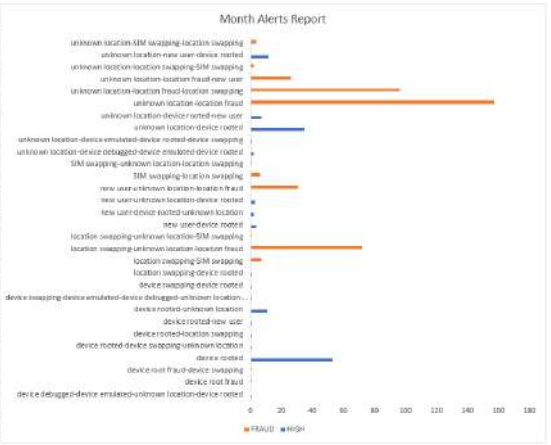
Además, gracias al diseño visual del mapa interactivo, se pueden realizar seguimientos detallados de cada una de las ubicaciones donde los usuarios de nuestros clientes están interactuando con sus aplicaciones o plataformas.

2.3.Reporting: Analytics y Reportes

Con el objetivo de darle el mejor apoyo visual estadístico a nuestros clientes para facilitarles la interpretación de la información procesada por la inteligencia artificial de IRONCHIP, **Fraud Detection** cuenta con una serie de paneles gráficos con los cuales se describe la información de las tasas de los niveles de riesgos, los tipos de localizaciones predominantes y las densidades regionales de interacción asociadas a los comportamientos de sus usuarios en tiempo real.

Junto a ello, y considerando las necesidades de nuestros clientes, periódicamente se envían reportes históricos relacionados con la información más relevante relacionada con los datos procesados por la inteligencia artificial de IRONCHIP.

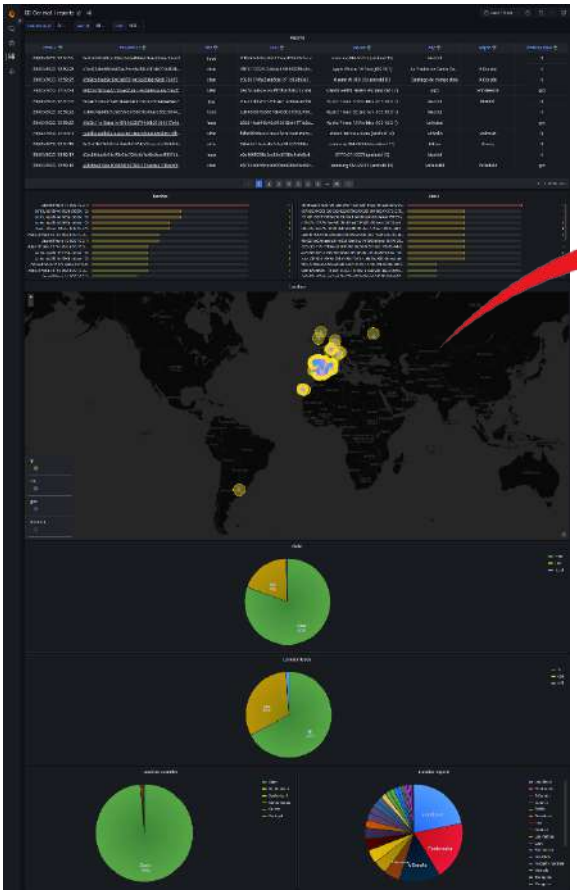
ALERT TYPES	HIGH	FRAUD	TOTAL
device debugged-device emulated-unknown location-device rooted	1		1
device root fraud		1	1
device root fraud-device swapping		1	1
device rooted	53		53
device rooted-device swapping-unknown location	1		1
device rooted-location swapping	1		1
device rooted-new user	1		1
device rooted-unknown location	11		11
device swapping-device emulated-device debugged-unknown location-device rooted	1		1
device swapping-device rooted	1		1
location swapping-device rooted	1		1
location swapping-SIM swapping		7	7
location swapping-unknown location-location fraud		72	72
location swapping-unknown location-SIM swapping		1	1
new user-device rooted	4		4
new user-device rooted-unknown location	2		2
new user-unknown location-device rooted	3		3
new user-unknown location-location fraud		31	31
SIM swapping-location swapping		6	6
SIM swapping-unknown location-location swapping		1	1
unknown location-device debugged-device emulated-device rooted	2		2
unknown location-device emulated-device rooted-device swapping	1		1
unknown location-device rooted	35		35
unknown location-device rooted-new user	7		7
unknown location-location fraud		157	157
unknown location-location fraud-location swapping		96	96
unknown location-location fraud-new user		20	20
unknown location-location swapping-SIM swapping		2	2
unknown location-new user-device rooted	12		12
unknown location-SIM swapping-location swapping		4	4
Total	137	405	542



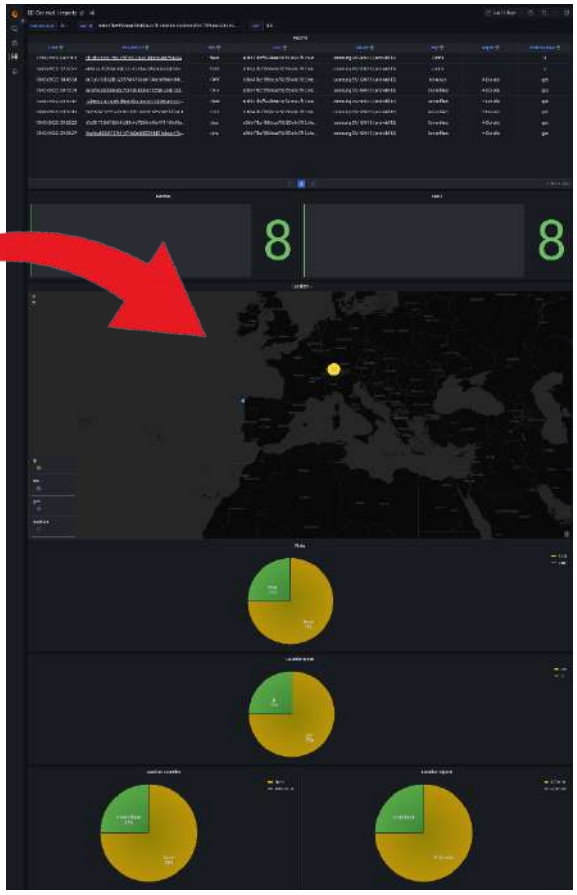
2.4.Dashboard de Control

Fraud Detection es un producto de vanguardia, pensado para darle a nuestros clientes el mejor apoyo en la toma de decisiones relacionadas con la detección de situaciones sospechosas o fraudulentas. Por ello, a continuación, se presentan las vistas integradas del producto: en la de la izquierda se encuentra la información general y en la de la derecha se encuentra la información de un usuario seleccionado:

VISTA GENERAL: Varios Usuarios

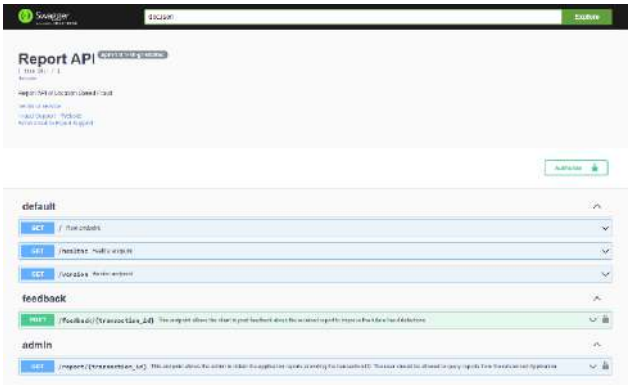


VISTA DETALLADA: 1 Usuario



3. FUNCIONAMIENTO E IMPLEMENTACIÓN

El producto **Fraud Detection** es un sistema que funciona y se integra con cualquier tipo de aplicación o plataforma gracias a sus versátiles piezas de código, las cuales permiten a diferentes aplicaciones comunicarse entre sí, compartiendo información y funcionalidades de manera dinámica. El procesamiento de la información de las transacciones realizado por la inteligencia artificial de IRONCHIP, así como el reporte y comunicación de ella a los sistemas de nuestros clientes, se genera a través de las interfaces de programación de aplicaciones (APIs) desarrolladas por el equipo técnico de IRONCHIP.



- **Transaction API:** Es la encargada de la recepción de datos relativos a información de cuentas, localización y deviceID desde los móviles de los usuarios de los clientes.
- **Report API:** Es la encargada de enviar los reportes de fraude al BPM o SIEM cuando sean requeridos.

3.1.Elementos Clave

IRONCHIP proporciona información a sus clientes que les permite conocer si los usuarios de sus sistemas están teniendo un comportamiento normal/habitual o anómalo en tiempo real. Dichos comportamientos están basados en datos de los usuarios, sus dispositivos asociados y su localización. Para garantizar la calidad de la información suministrada se deben considerar los siguientes elementos:

3.1.1. Permiso de localización

Las peticiones de permisos de localización son un requisito indispensable y definir los flujos de llamadas a ellas es parte fundamental para la integración. Al habilitarse los permisos de localización en los dispositivos de los usuarios, la tecnología de IRONCHIP puede detectar los comportamientos de los usuarios con mayor precisión y comunicar las alertas con mayor cantidad de información útil para el cliente.

3.1.2. Integración de la API

Contemplamos varias maneras de proporcionar la información a los usuarios de nuestros clientes:

- Integración en la lógica de negocio del BPM o SIEM vía API Rest HTTP.
- Creando un canal de stream para recibir datos en tiempo real.

3.1.3. SDK/librería móvil

Una librería instalada en la aplicación móvil de la entidad distribuida de manera natural una vez la aplicación solicite alguna actualización. Esta librería es la encargada de proporcionar los datos, cuenta y localización de los usuarios cuando el cliente considere que es oportuno hacer la petición.

3.2.Etapas de Implementación

El sistema de **Fraud Detection** presenta una arquitectura de software basada en microservicios, por lo que gracias a sus versátiles interfaces de programación, se requieren de 5 etapas de integración para disfrutar de los servicios brindados por la inteligencia artificial de IRONCHIP.

3.2.1. Instalación SDK

A través de un Kit de Desarrollo de Software (SDK) se genera la integración de **Fraud Detection** a la aplicación o plataforma móvil de nuestros clientes proporcionándose una librería nativa de iOS (.framework) y Android (.aar).

3.2.2. Integración BPM | API (BATCH) or Stream (REALTIME)

Esta integración puede realizarse de dos maneras diferentes o de ambas; Batch o streaming.

- **Batch:** Este modelo consiste en la integración por medio de una API Rest que se podrá consultar los reportes siempre que se quiera, incluso para reportes del pasado.
- **Streaming:** Este modelo consiste en un Websocket conectado constantemente y reportará información en tiempo real, notificando en caso de que consideremos que una interacción que se está realizando es fraudulenta.

3.2.3. Pruebas de Integraciones

Se realizará un despliegue controlado a un grupo concreto de usuarios del cliente y se realizan unas pruebas de medición de resultados. Con ello, se verifica que todo está funcionando como debería, para detectar correctamente los comportamientos anómalos y medir los datos relativos a tiempos de respuesta.

3.2.4. Análisis de resultados y ajustes

Las pruebas de estrés son realizadas de acuerdo con las validaciones que se hayan definido previamente con el cliente, generando la suficiente cantidad de información para estructurar KPIs que identifiquen e informen sobre las situaciones anómalas y/o riesgos para la detección de fraudes.

3.2.5. Puesta en Producción

Finalmente, se realizará la actualización completa de la aplicación, junto con la documentación correspondiente, y se transmitirá el conocimiento del funcionamiento de la tecnología proporcionada para su correcto uso por parte del personal indicado por el cliente.