



FRAUDE FINANCIERO

Análisis de Riesgo y Métodos de Pago

AUTOR: LUIS ARBIO

ÍNDICE

CONTENIDO

2. DESCRIPCIÓN DEL PROYECTO: RESUMEN GENERAL DEL CASO, CONTEXTO Y PROBLEMÁTICA A RESOLVER.
3. HIPÓTESIS: PLANTEAMIENTO DE HIPÓTESIS ANALÍTICAS RELACIONADAS CON EL COMPORTAMIENTO FRAUDULENTO.
4. OBJETIVO, ALCANCE Y USUARIOS FINALES DEL TABLERO: DEFINICIÓN DEL PROPÓSITO DEL ANÁLISIS, SUS LÍMITES Y QUIÉN UTILIZARÁ LOS RESULTADOS.
5. EXPLICACIÓN DE LAS TABLAS: DETALLE DE LAS TABLAS UTILIZADAS, SU ORIGEN Y RELACIÓN CON EL ANÁLISIS.
6. LISTADO DE COLUMNAS: ENUMERACIÓN DE LOS CAMPOS CLAVE POR TABLA Y SU FUNCIÓN EN EL MODELO.
7. TRANSFORMACIONES REALIZADAS: EXPLICACIÓN DE LOS PASOS DE LIMPIEZA, COMBINACIÓN Y NORMALIZACIÓN DE DATOS.
8. MEDIDAS CALCULADAS (DAX): LISTADO Y DESCRIPCIÓN DE LAS MEDIDAS MÁS IMPORTANTES CREADAS PARA EL ANÁLISIS.
9. TABLAS AUXILIARES: DESCRIPCIÓN DE TABLAS ADICIONALES CREADAS PARA FACILITAR EL MODELADO O LOS ANÁLISIS.
10. DIAGRAMA ENTIDAD - RELACIÓN (ERD): REPRESENTACIÓN GRÁFICA DEL MODELO DE DATOS Y RELACIONES ENTRE TABLAS.
- .

TABLEROS Y VISUALIZACIONES

11. PORTADA: PRESENTACIÓN INICIAL CON BRANDING, TÍTULO Y AUTORES DEL PROYECTO.
12. OVERVIEW: RESUMEN GENERAL DE INDICADORES CLAVE Y VOLUMEN DE FRAUDE.
13. ANÁLISIS POR TICKET, CIUDAD Y RUBRO: EXPLORACIÓN GEOGRÁFICA Y POR INDUSTRIA DE LOS FRAUDES, CON ANÁLISIS DE MONTOS.
14. INDICADORES CRÍTICOS: INDICADORES DE RIESGO Y COMPORTAMIENTO, COMO REINCIDENCIAS, FALLOS Y DÍAS CRÍTICOS.
15. GLOSARIO: DEFINICIÓN DE MÉTRICAS, VARIABLES Y TÉRMINOS CLAVE UTILIZADOS EN EL DASHBOARD.

PERSPECTIVAS FUTURAS

16. FUTURAS LÍNEAS DE MEJORA: PROPUESTAS DE EVOLUCIÓN DEL MODELO

DESCRIPCION DEL PROYECTO

En la era digital, el fraude financiero representa un desafío significativo para las instituciones bancarias, comercios y usuarios. Con el crecimiento del comercio electrónico y los pagos digitales, es fundamental comprender los patrones de fraude y las variables que influyen en su ocurrencia.

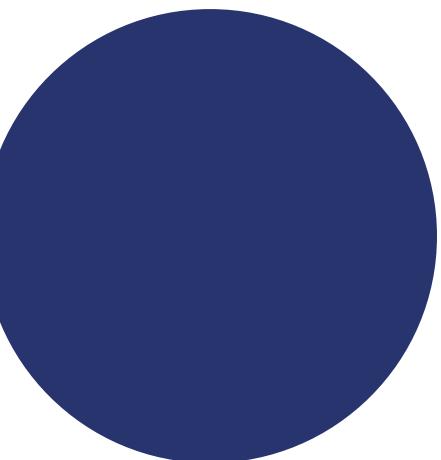
Este proyecto tiene como objetivo analizar un dataset de transacciones financieras para identificar factores clave asociados al fraude. Se buscará responder preguntas como:

¿Qué métodos de pago presentan mayor riesgo de fraude?

¿Cuáles son las características comunes en transacciones fraudulentas?

Áreas geográficas, dispositivos y patrones de autenticación, ¿influyen el fraude?

El análisis se llevará a cabo mediante el procesamiento y exploración de datos, aplicando estadísticas descriptivas y visualización de datos para identificar correlaciones entre variables.



HIPÓTESIS



Para guiar el análisis, se plantean las siguientes hipótesis:

El fraude está correlacionado con el método de pago utilizado. Algunos métodos de pago, como tarjetas de crédito, podrían ser más susceptibles a fraude en comparación con pagos por transferencia o billeteras digitales.

Las transacciones realizadas desde diferentes dispositivos tienen mayor probabilidad de ser fraudulentas.

Los usuarios con historial de transacciones fallidas tienen una mayor probabilidad de estar involucrados en actividades fraudulentas.

El fraude ocurre con mayor frecuencia los fines de semana .

Las transacciones con montos atípicos tienen una mayor probabilidad de ser fraudulentas.

1

Objetivo del Proyecto

El objetivo principal de este proyecto es identificar patrones y factores de riesgo asociados a transacciones financieras fraudulentas, a fin de mejorar los mecanismos de prevención y detección de fraude.

Se pretende, además, proporcionar información útil para el diseño de políticas de seguridad y estrategias de mitigación, utilizando datos históricos y análisis cuantitativo como base para la toma de decisiones.

2

Alcance

El análisis se centra en transacciones financieras individuales registradas en una plataforma digital. El alcance del proyecto incluye:

- Análisis exploratorio de variables transaccionales y de usuario.
- Identificación de correlaciones entre características y eventos de fraude.
- Evaluación del riesgo de fraude por método de pago, ubicación, dispositivo y comportamiento del usuario.

3

Usuario Final y Nivel de Aplicación del Análisis

Usuario Final: Analistas de riesgo, equipos de ciberseguridad, desarrolladores de soluciones antifraude, y tomadores de decisiones en instituciones financieras y fintechs.

Nivel de Aplicación:

- Operativo: Detección de transacciones anómalas en tiempo real y análisis de casos sospechosos.
- Táctico: Desarrollo de reglas de negocio y segmentación de usuarios según el nivel de riesgo.
- Estratégico: Definición de políticas de seguridad, inversión en tecnología antifraude y gestión de riesgos organizacionales a largo plazo.

EXPLICACIÓN DE LAS TABLAS

Users (Usuarios), Cards (Tarjetas) y Card_Type (bandera de la tarjeta)

Contiene información sobre los usuarios registrados en la plataforma, incluyendo:

- User_ID: Identificador único del usuario.
- Name: Nombre del usuario.
- Lastname: Apellido del usuario.
- CardID: Identificador único de tarjeta.
- Previous_Fraudulent_Activity: Historial de actividades fraudulentas.
- Card_Type_ID: Tipo de tarjeta asociada al usuario.
- Card_Age: Antigüedad de la tarjeta en meses.

Transactions (Transacciones)

Registra todas las transacciones realizadas, con atributos como:

- Transaction_ID: Identificador único de la transacción.
- User_ID: Usuario que realizó la transacción.
- Transaction_Amount: Monto de la transacción.
- Transaction_Type_ID: Tipo de transacción (Online, ATM, etc.).
- Timestamp: Fecha y hora de la transacción.
- Risk_Score: Puntuación de riesgo de fraude.
- Fraud_Label: Indicador de fraude (0 = No, 1 = Sí).

Transaction_Aggregates (Datos Agregados de Transacciones)

Guarda información sobre los patrones de transacción a nivel diario:

- Transaction_Aggregates_ID: Identificador único de transaction_Aggregate
- User_ID: Usuario asociado.
- Date: Fecha de agregación de datos.
- Daily_Transaction_Count: Cantidad de transacciones realizadas ese día.
- Avg_Transaction_Amount_7d: Promedio de transacciones en los últimos 7 días.
- Failed_Transaction_Count_7d: Cantidad de transacciones fallidas en los últimos 7 días.

Métodos de Pago, Dispositivos, Ubicación, Calendario, Días, Perfil de Fraude, Medidas y Fraudes Grupos Usuarios

Tablas auxiliares que incluyen:

- Transaction_Types: Tipos de transacciones.
- Device_Types: Tipos de dispositivos utilizados.
- Locations: Ubicaciones geográficas de las transacciones.
- Merchant_Categories: Categorías de comercio.
- Authentication_Methods: Métodos de autenticación empleados.
- Actualización



LISTADO DE COLUMNAS

Tabla: Cards			
Tipo de Clave	Campo	Tipo de Dato	Descripción
PK	CardID	INT	Clave primaria, identificador único
FK	User_ID	INT	FK a tabla Users
	Previous_Fraudulent_Activity	INT	Cantidad de fraudes previos del usuario
FK	Card_Type_ID	INT	FK a tabla Card_Types
	Card_Age	INT	Edad de la tarjeta en meses

Tabla: Users			
Tipo de Clave	Campo	Tipo de Dato	Descripción
	Cantidad_de_fraudes_users	INT	Suma la cantidad de fraudes por usuario
	Fraudulento	INT	Indica si el usuario cometió fraude
	Last_Name	INT	Apellido del usuario
	Name	INT	Nombre del usuario
PK	User_ID	INT	Clave primaria, identificador único

Tabla: Transactions			
Tipo de Clave	Campo	Tipo de Dato	Descripción
	Account_Balance	FLOAT(10,2)	Saldo antes de la transacción
FK	Authentication_Method_ID	INT	FK a Authentication_Methods
FK	Card_ID	INT	FK a Cards
FK	Card_Type_ID	INT	FK a Card Types
FK	Device_Type_ID	INT	FK a Device_Types
	Fraud_Label	BOOLEAN	Indicador de fraude (0 o 1)
	IP_Address_Flag	BOOLEAN	IP sospechosa (0 = no, 1 = sí)
	Is_Weekend	BOOLEAN	Si ocurrió en fin de semana
FK	Location_ID	INT	FK a Locations
FK	Merchant_Category_ID	INT	FK a Merchant_Categories
	Risk_Score	FLOAT(10,2)	Valor numérico del riesgo
	Timestamp	DATE	Fecha y hora de la transacción
	Transaction_Amount	FLOAT(10,2)	Monto de la transacción
	Transaction_Distance	FLOAT(10,2)	Distancia al lugar habitual del usuario
PK	Transaction_ID	INT	Clave primaria, identificador único
FK	Transaction_Type_ID	INT	FK a Transaction_Types
FK	User_ID	INT	FK a tabla Users

Tabla: Transaction_Aggregates			
Tipo de Clave	Campo	Tipo de Dato	Descripción
PK	Transaction_Aggregates_ID	INT	Clave primaria, identificador único
FK	User_ID	INT	FK a Users
	Date	DATE	Fecha del resumen
	Daily_Transaction_Count	INT	Cantidad de transacciones ese día
	Avg_Transaction_Amount_7d	FLOAT(10,2)	Promedio últimos 7 días
	Failed_Transaction_Count_7d	INT	Intentos fallidos últimos 7 días

Tabla: Transaction_Types			
Tipo de Clave	Campo	Tipo de Dato	Descripción
PK	Transaction_Type_ID	INT	PK
	Transaction_Type_Name	VARCHAR2(50)	Ej: "Online", "ATM", "In-Store"

Tabla: Device_Types			
Tipo de Clave	Campo	Tipo de Dato	Descripción
PK	Device_Type_ID	INT	PK
	Device_Type_Name	VARCHAR2(50)	Ej: "Mobile", "Desktop"

Tabla: Locations			
Tipo de Clave	Campo	Tipo de Dato	Descripción
PK	Location_ID	INT	PK
	City	VARCHAR2(100)	Ciudad
	Country	VARCHAR2(100)	País

LISTADO DE COLUMNAS

Tabla: Calendario			
Tipo de Clave	Campo	Tipo de Dato	Descripción
	Dia de la semana	INT	Día de la semana en numeros (1-7)
	Fecha	INT	Fecha calendario (dd-mm-aaaa)
	Mes	INT	Mes en formato numero
	Nombre del dia	INT	Nombre del dia de la semana
	Nombre del mes	INT	Nombre del mes calendario
PK	Timestamp	INT	Fecha completa de origen y horario

Tabla:Medidas			
Tipo de Clave	Campo	Tipo de Dato	Descripción
	% Fraude	INT	Porcentaje de fraude sobre facturacion
	\$ Fraude	INT	Monto total en \$ de fraude
	AVG Fraude	INT	Promedio de fraude
	Cantidad_Usuarios_Fraudulentos	INT	Cantidad de usuarios fraudulentos
	Ciudad Mayor Fraude	INT	Ciudad con mayor cantidad de fraudes
	Día Mayor Fraude	INT	Dia con mayor cantidad de fraudes
	Dispositivo_Mayor_Fraude	INT	Dispositivo con mayor cantidad de fraude
	Mediana_Fraude	INT	Mediana de ticket de fraude
	Medio cobro mas fraude	INT	Medio de cobro con mayor cantidad de fraude
	Mes Mayor Fraude	INT	Mes con mayor cantidad de fraude
	Moda_Ticket_Fraude	INT	Moda del ticket de fraude
	Objetivo fraude	INT	Objetivo anual de fraude total en %
	Prom_Fallos_7D_Usuarios_1Frau	INT	AVG de operaciones fallidas grupo 1 fraude
	Promedio_Reincidentes	INT	Promedio de fraude en reincidentes
	Rubro_Mayor_Fraude	INT	Rubro con mayor cantidad de fraudes
	Score_Promedio_Fraude	INT	Score promedio de users fraude
	Tarjeta_Mayor_Fraude	INT	Tarjeta con mayor cantidad de fraudes
	Ticket_Max_Fraude	INT	Ticket Maximo de fraude
	Ticket_Promedio_Fraude_Reincid	INT	Ticket promedio en \$ de reincidentes
	Ticket_Promedio_No_Fraude	INT	Ticket promedio de usuarios no fraude
	Users Reincidentes	INT	Cantida de usuarios reincidentes

Tabla: Merchant_Categories			
Tipo de Clave	Campo	Tipo de Dato	Descripción
PK	Merchant_Category_ID	INT	PK
	Merchant_Category_Name	VARCHAR(100)	Ej: "Retail", "Food", "Travel"

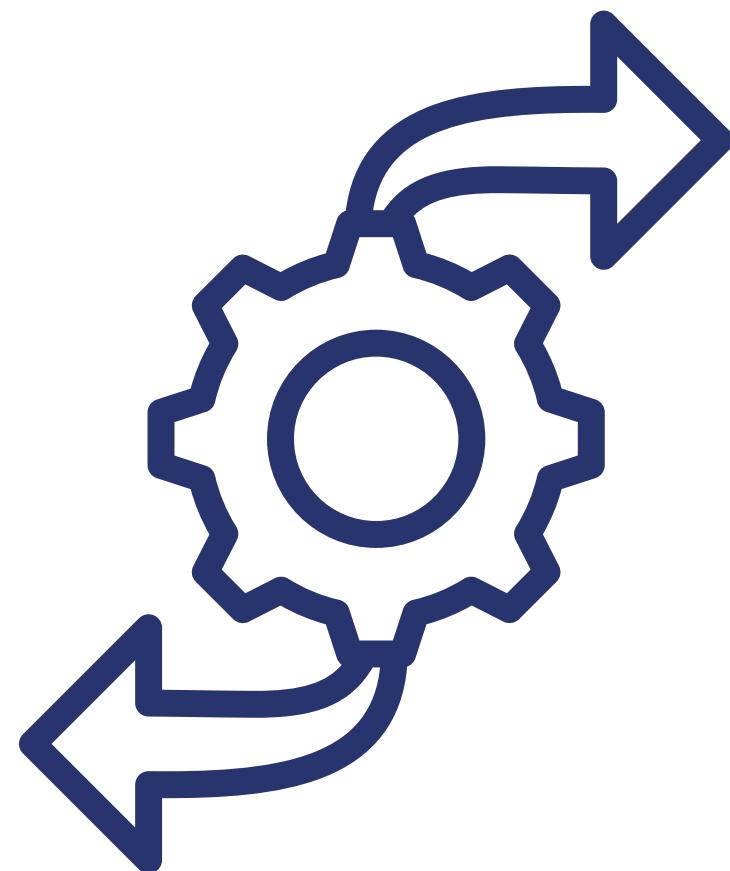
Tabla: Authentication_Methods			
Tipo de Clave	Campo	Tipo de Dato	Descripción
PK	Authentication_Method_ID	INT	PK
	Method_Name	VARCHAR(50)	Ej: "PIN", "Biometric", "OTP"

Tabla: Card_Types			
Tipo de Clave	Campo	Tipo de Dato	Descripción
PK	Card_Type_ID	INT	PK
	Card_Type_Name	VARCHAR(50)	Ej: "Credit", "Debit", "Prepaid"

Tabla: Fraud_Grupos_Usuarios (tabla auxiliar)			
Tipo de Clave	Campo	Tipo de Dato	Descripción
	Cantidad_de_fraudes_users	INT	Suma cantidad de fraudes por grupo
	Monto Total Fraude	INT	Suma el monto total de fraude por grupo
	Ticket Promedio	INT	Ticket promedio por fraude por grupo
	Usuarios	INT	Agrupa usuarios por cantidad de fraudes

Tabla: Actualización			
Tipo de Clave	Campo	Tipo de Dato	Descripción
	Última actualización	INT	Última actualización de los datos del tablero

TRANSFORMACIONES



Tras comenzar con el armado de las medidas, fue necesario realizar algunos cambios en el dataset original y adaptar algunas tablas para poder obtener indicadores clave que permitan profundizar el análisis.

Modificaciones en tablas

Tabla Users: se agregaron dos nuevos campos (Cantidad users fraude y Fraudulentos)

Nuevas tablas

Calendario

Medidas

Fraudes Grupos Usuarios (aux)

Actualización

MEDIDAS CALCULADAS

Medidas	Fórmula
% Fraude	% Fraude = DIVIDE([\$ Fraude], SUM(Transactions[Transaction_Amount]))
\$ Fraude	\$ Fraude = CALCULATE(SUM(Transactions[Transaction_Amount]), Transactions[Fraud_Label] = 1)
AVG Fraude	AVG Fraude = CALCULATE(AVERAGE(Transactions[Transaction_Amount]), Transactions[Fraud_Label] = 1)
Cantidad_Usuarios_Fraudulentos	Cantidad_Usuarios_Fraudulentos = CALCULATE(DISTINCTCOUNT(Transactions[User_ID]), Transactions[Fraud_Label] = 1)
Ciudad Mayor Fraude	Ciudad Mayor Fraude = CALCULATE(MAXX(TOPN(1, SUMMARIZE(Locations, Locations[Location], "TotalFraude", CALCULATE(COUNTROWS(Transactions), Transactions[Fraud_Label] = 1)), [TotalFraude]), Locations[Location])))
Día Mayor Fraude	Día MayorFraude = CALCULATE(MAXX(TOPN(1, SUMMARIZE('Calendario', 'Calendario'[Nombre del día], "TotalFraude", CALCULATE(COUNTROWS(Transactions), Transactions[Fraud_Label] = 1)), [TotalFraude]), 'Calendario'[Nombre del día])))
Objetivo fraude	Objetivo fraude = 0.2

Medidas	Fórmula
Dispositivo_Mayor_Fraude	Dispositivo_Mayor_Fraude = CALCULATE(MAXX(TOPN(1, SUMMARIZE('Device_Types', 'Device_Types'[Device_Type], "TotalFraude", CALCULATE(COUNTROWS(Transactions), Transactions[Fraud_Label] = 1)), [TotalFraude]), 'Device_Types'[Device_Type])))
Mediana_Fraude	Mediana_Fraude = MEDIANX(FILTER(Transactions, Transactions[Fraud_Label] = 1), Transactions[Transaction_Amount])
Medio cobro mas fraude	Medio cobro mas fraude = CALCULATE(MAXX(TOPN(1, SUMMARIZE(Transaction_Types, Transaction_Types[Transaction_Type], "TotalFraude", CALCULATE(COUNTROWS(Transactions), Transactions[Fraud_Label] = 1)), [TotalFraude], DESC), Transaction_Types[Transaction_Type])))
Mes Mayor Fraude	Mes Mayor Fraude = VAR TablaFraudesPorMes = ADDCOLUMNS (SUMMARIZE ('Calendario', 'Calendario'[Nombre del mes]), "TotalFraude", CALCULATE (COUNTROWS (Transactions), Transactions[Fraud_Label] = 1)) VAR MaxFraude = MAXX (TablaFraudesPorMes, [TotalFraude]) RETURN MAXX (FILTER (TablaFraudesPorMes, [TotalFraude] = MaxFraude), 'Calendario'[Nombre del mes]))

MEDIDAS CALCULADAS

Medidas	Fórmula
Moda_Ticket_Fraude	<pre> Moda_Ticket_Fraude = VAR TablaAgrupada = ADDCOLUMNS(SUMMARIZE(FILTER(Transactions, Transactions[Fraud_Label] = 1), Transactions[Transaction_Amount]), "Cantidad", COUNTROWS(FILTER(Transactions, Transactions[Fraud_Label] = 1 && Transactions[Transaction_Amount] = EARLIER(Transactions[Transaction_Amount])))) VAR TopFrecuencia = TOPN(1, TablaAgrupada, [Cantidad], DESC) RETURN MAXX(TopFrecuencia, Transactions[Transaction_Amount]) </pre>
Prom_Fallos_7D_Usuarios_1Fraude	<pre> Prom_Fallos_7D_Usuarios_1Fraude = CALCULATE(AVERAGE(Transaction_Aggregates[Failed_Transaction_Count_7d]), FILTER(Users, Users[Cantidad_de_fraudes_users] = 1)) </pre>
Promedio_Reincidentes	<pre> Promedio_Reincidentes = DIVIDE(516, -- cantidad de reincidentes 2814, -- cantidad de usuarios con al menos 1 fraude 0) </pre>
Rubro_Mayor_Fraude	<pre> Rubro_Mayor_Fraude = CALCULATE(MAXX(TOPN(1, SUMMARIZE(Merchant_Categories, Merchant_Categories[Merchant_Category], "TotalFraude", CALCULATE(COUNTROWS(Transactions), Transactions[Fraud_Label] = 1)), [TotalFraude]), Merchant_Categories[Merchant_Category])) </pre>

Medidas	Fórmula
Score_Promedio_Fraude	<pre> Score_Promedio_Fraude = CALCULATE(AVERAGE(Transactions[Risk_Score]), Transactions[Fraud_Label] = 1) </pre>
Tarjeta_Mayor_Fraude	<pre> Tarjeta_Mayor_Fraude = CALCULATE(MAXX(TOPN(1, SUMMARIZE('Card Types', 'Card Types'[Card_Type], "TotalFraude", CALCULATE(COUNTROWS(Transactions), Transactions[Fraud_Label] = 1)), [TotalFraude]), 'Card Types'[Card_Type])) </pre>
Ticket_Max_Fraude	<pre> Ticket_Max_Fraude = CALCULATE(MAX(Transactions[Transaction_Amount]), FILTER(Transactions, Transactions[Fraud_Label] = 1)) </pre>
Ticket_Promedio_Fraude_Reincidentes	<pre> Ticket_Promedio_Fraude_Reincidentes = AVERAGEX(FILTER(Transactions, Transactions[Fraud_Label] = 1 && CALCULATE(COUNTROWS(Transactions), ALLEXCEPT(Transactions, Transactions[User_ID]), Transactions[Fraud_Label] = 1) > 1), Transactions[Transaction_Amount]) </pre>
Ticket_Promedio_No_Fraude	<pre> Ticket_Promedio_No_Fraude = AVERAGEX(FILTER(Transactions, Transactions[Fraud_Label] = 0), Transactions[Transaction_Amount]) </pre>
Users Reincidentes	<pre> Users Reincidentes = CALCULATE(DISTINCTCOUNT(Transactions[User_ID]), FILTER(VALUES(Transactions[User_ID]), CALCULATE(COUNTROWS(Transactions), Transactions[Fraud_Label] = 1) > 1)) </pre>

TABLAS AUXILIARES

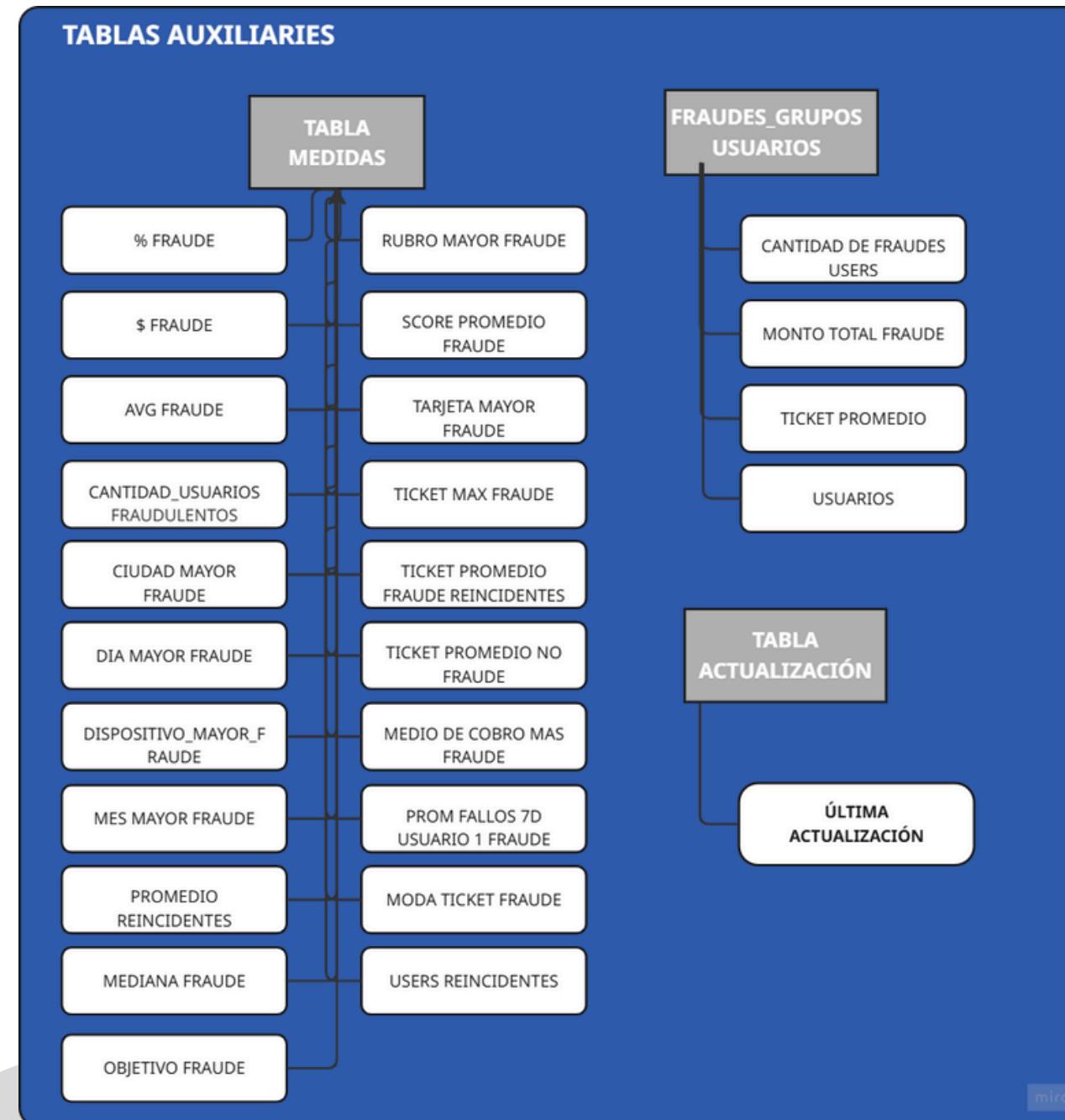


Tabla Medidas

- % Fraude: porcentaje de fraude sobre el total
- \$ Fraude: Monto total de fraude
- AVG fraude: Ticket promedio de fraude
- Cantidad de usuarios fraudulentos
- Ciudad Mayor Fraude
- Día Mayor Fraude
- Dispositivo Mayor Fraude
- Mes mayor Fraude
- Promedio reincidentes
- Mediana fraude
- Rubro mayor fraude
- Score promedio fraude:
- Tarjeta mayor fraude
- Ticket max fraude
- Ticket promedio fraude reincidentes
- Ticket promedio no fraude
- Medio de cobro mas fraude
- Prom fallos 7D usuarios 1 fraude
- Moda ticket fraude
- Users reincidentes
- Objetivo fraude

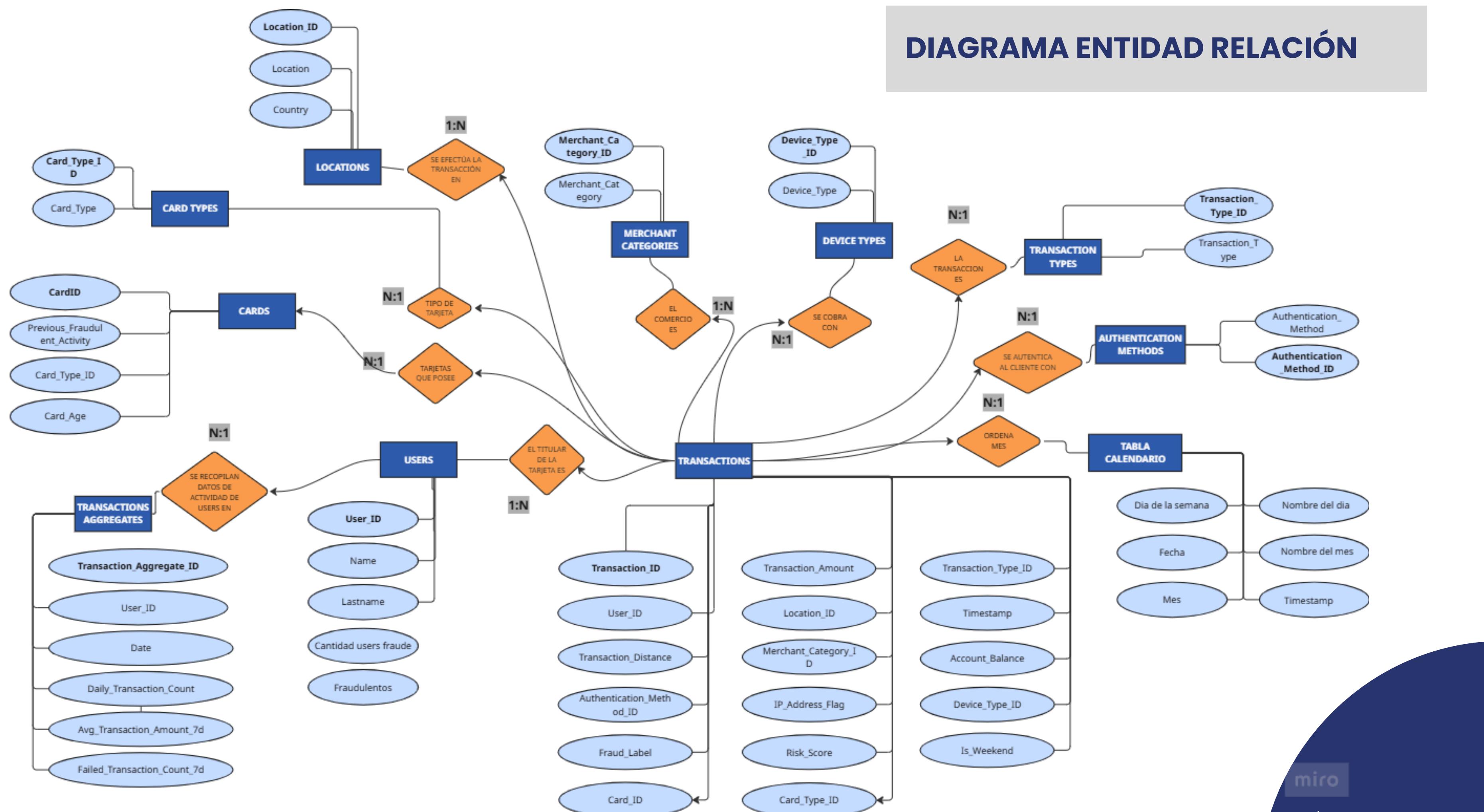
Tabla Fraudes Grupos Usuarios

- Cantidad de Fraudes Users: cantidad de fraudes por usuario
- Monto total fraude: Monto total de fraude por usuario
- Ticket promedio: ticket promedio por usuario.
- Usuario

Tabla Actualización

- Última Actualización

DIAGRAMA ENTIDAD RELACIÓN



PORTADA



La portada cuenta de cuatro accesos a los diferentes análisis:

- Overview
- Análisis de Ticket - Ciudad - Rubro
- Indicadores Críticos
- Glosario

También cuenta con un menú para desplazarse entre las distintas páginas del tablero.

Por último muestra información de la última actualización de los datos en formato de fecha y hora.

OVERVIEW FRAUDE



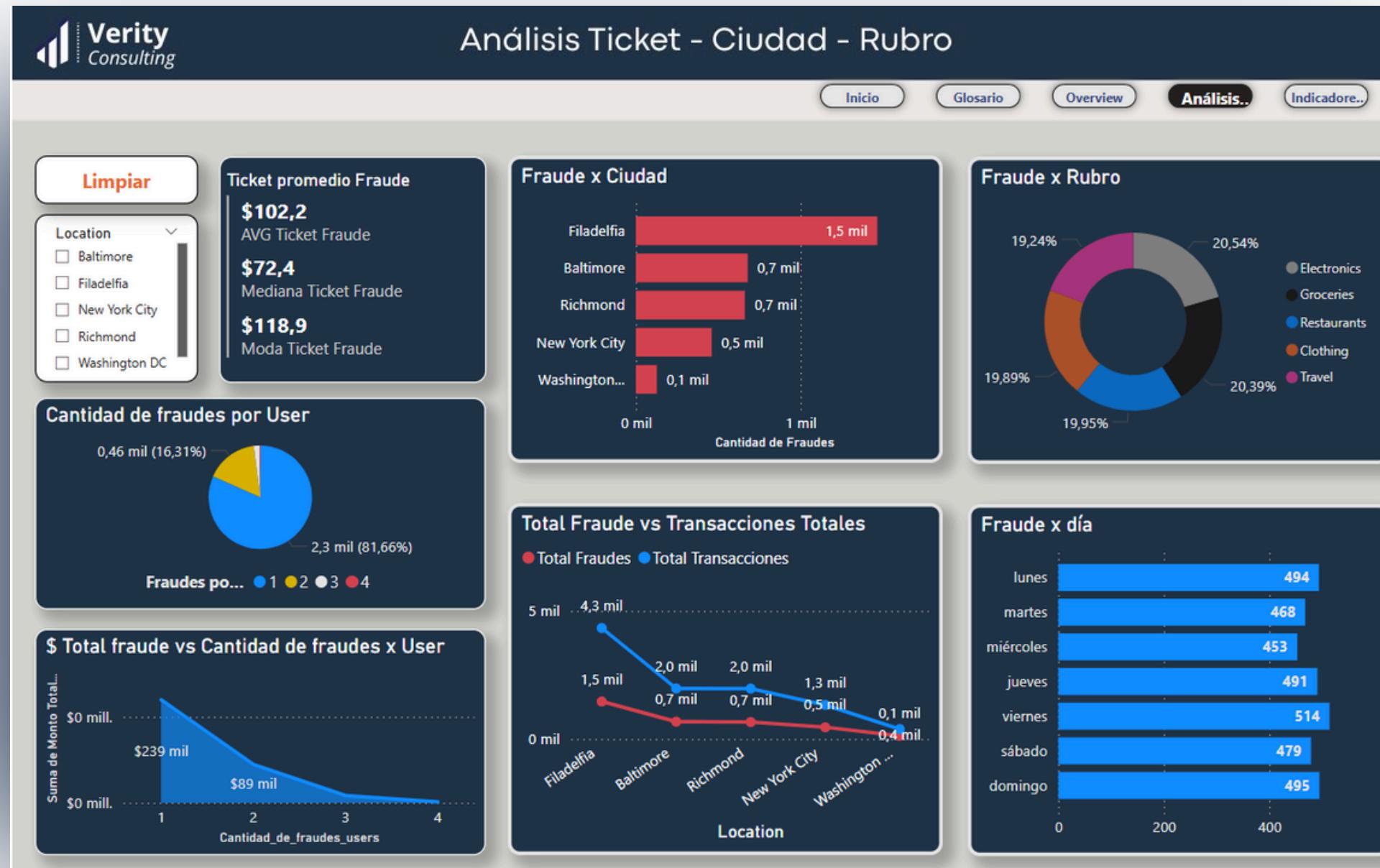
Esta página aborda los principales indicadores que permiten un primer análisis visual de los aspectos más relevantes y de mayor impacto.

- KPI
- \$ Fraude
- Usuarios afectados
- Transacciones
- Ticket promedio donde se compara con el total de transacciones.
- Fraude x Tarjeta
- Fraude por Medio de cobro
- Fraude por Dispositivos utilizados
- Funnel de usuarios fraudulentos
- Línea de tiempo con Fraudes x Mes.

Además cuenta con segmentadores y un marcador para eliminar cualquier segmentación aplicada y volver los indicadores al punto inicial.

Por último muestra un menú para desplazarse entre las distintas páginas del tablero.

ANÁLISIS TICKET - CIUDAD - RUBRO



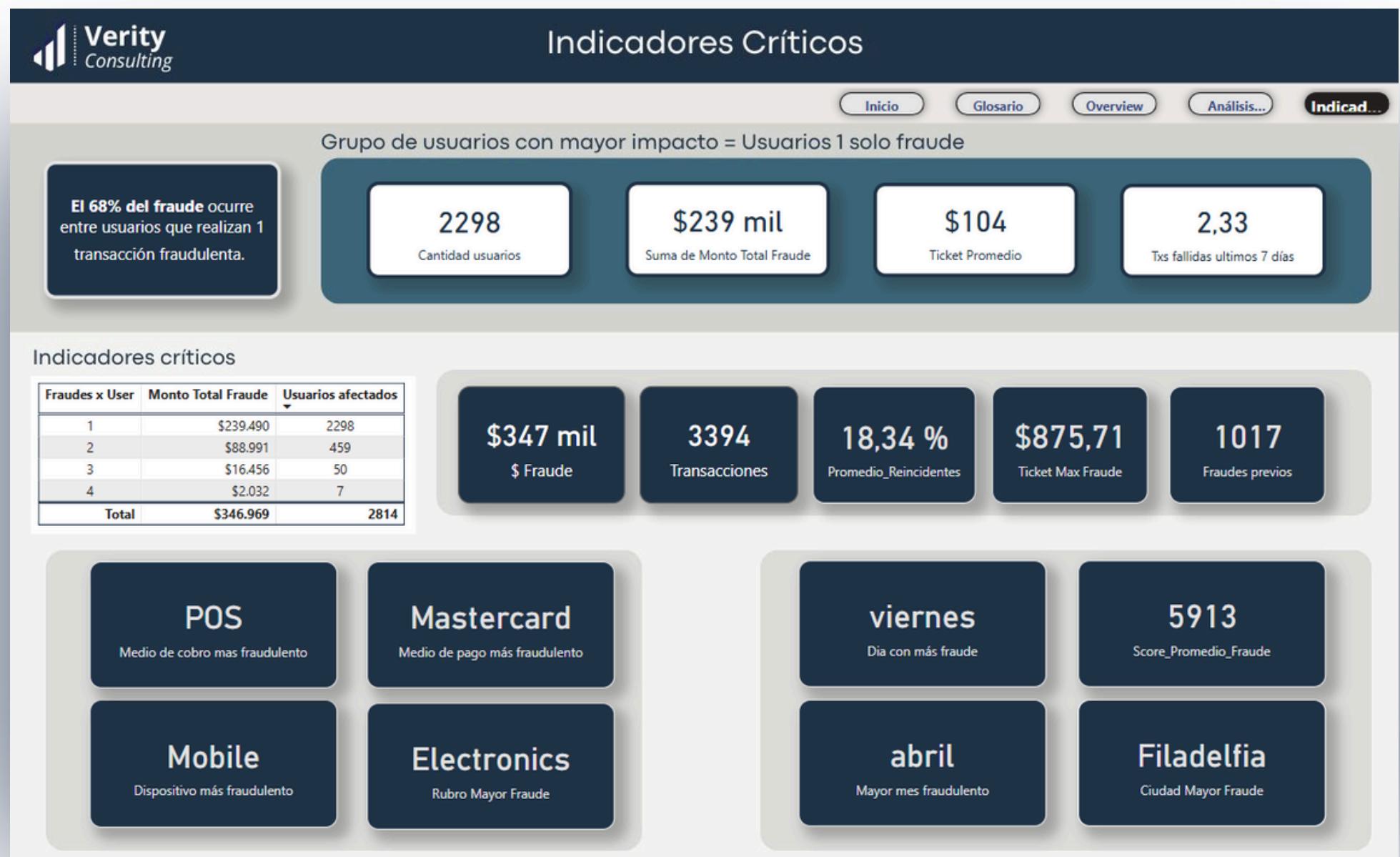
Esta página continúa con el análisis profundizando en aspectos adicionales como el ticket, la ciudad y el rubro afectado

- Ticket promedio Fraude
- Fraude por ciudad
- Fraude por rubro
- Cantidad de fraudes por User agrupados en 1,2,3 o 4 fraudes.
- \$ Total de fraude por Users agrupados en 1,2,3 o 4 fraudes.
- Total Fraude vs Transacciones totales según ciudad.
- Fraudes por día para evaluar en que día de la semana ocurren la mayor cantidad de fraudes.

Además cuenta con segmentadores y un marcador para eliminar cualquier segmentación aplicada y volver los indicadores al punto inicial.

Por último muestra un menú para desplazarse entre las distintas páginas del tablero.

INDICADORES CRÍTICOS



"Esta página del tablero NO cuenta con segmentadores ya que muestra los indicadores más máximos o críticos de todo el período analizado"

Esta página reúne los indicadores críticos con los datos hallados en el dataset, mostrando el análisis en dos partes:

Grupo de usuarios de mayor impacto negativo

- Cantidad de usuarios afectados
- Monto total de fraude de este grupo
- Ticket promedio del grupo
- Transacciones fallidas promedio de los usuarios del grupo

Indicadores críticos totales de fraude, donde se muestran todos los máximos de cada variable analizada.

- Fraude x user
- Monto Total de fraude
- Usuarios afectados por grupo (cantidad de fraudes)
- \$ Total de fraude
- Total de transacciones fraudulentas
- Promedio de usuarios reincidentes
- Cantidad de fraudes previos de los usuarios afectados
- Medio de cobro más fraudulento
- Medio de pago más fraudulento
- Dispositivo utilizado con más fraudes
- Rubro donde se encontraron más fraudes.
- Día de la semana con mayor fraude
- Mes de mayor fraude
- Ciudad de mayor fraude
- Score promedio de usuarios fraudulentos

Estos valores complementan el análisis realizado en las primeras hojas, dando un marco en que puntos principales se deberán tomar medidas para corregir o mejorar estos problemas detectados.

GLOSARIO

The screenshot shows a dark-themed dashboard with a navigation bar at the top featuring five items: 'Inicio', 'Glosario' (which is highlighted in black), 'Overview', 'Análisis...', and 'Indicadore...'. The main content area is titled 'GLOSARIO' in large white letters. Below the title, there is a list of terms with their definitions:

- Objetivo:** porcentaje de fraude definido como aceptable en este tablero.
- Fraude:** transacciones realizadas por usuarios con el objetivo de estafar al comercio o banco emisor
- Usuarios o Users:** universo de usuarios que transaccionaron.
- Usuarios afectados:** usuarios que tienen 1 transacción identificada como fraude.
- Usuarios reincidentes:** usuarios que han tenido mas de 1 transacción identificada como fraude
- Tarjetas:** universo de tarjetas que se encuentran identificadas por marca (Amex, Mastercard, Visa, Discover)
- Medio de cobro:** se refiere al medio utilizado para realizar el cobro de la transacción. (POS, Online, Bank Transfer, ATM)
- Dispositivos utilizados:** son los dispositivos electrónicos utilizados al momento de realizar la transacción (mobile, laptop, tablet)
- Average (AVG):** es el promedio aplicado a las diferentes variables.
- Ticket:** monto de cada transacción
- Ciudad:** lugar geográfico donde se localizó la transacción fraudulenta.
- Transacciones (Tx):** corresponde a cada operación realizada por los usuarios
- Transacciones fallidas:** corresponde a la cantidad de intentos de compra que fallaron y no se concretaron.
- Score fraude:** es el puntaje que se otorga a los usuarios en función de su historial de transacciones.

El glosario muestra todas las palabras técnicas utilizadas en este tablero, lo que permite el entendimiento de toda la terminología relacionada con el análisis del sector.

También cuenta con un menú para desplazarse entre las distintas páginas del tablero.

PERSPECTIVAS FUTURAS

El modelo actual permite identificar patrones de fraude mediante análisis descriptivos y visualizaciones interactivas, aportando valor al negocio en términos de detección y monitoreo. Sin embargo, existen diversas oportunidades para evolucionar este enfoque hacia un modelo más predictivo y automatizado, con los siguientes ejes de desarrollo:

- Incorporación de Algoritmos de Machine Learning
- Segmentación Avanzada de Usuarios
- Enriquecimiento del Dataset

Esto permitirá el día de mañana identificar con mayor precisión a usuarios fraudulentos y prevenir casos de fraude, así como anticiparse a los comportamientos de usuarios que intenten realizar transacciones fraudulentas.