MNRAS 000, 1–6 (2023) Preprint 20 May 2023 Compiled using MNRAS LATEX style file v3.0

Detección de anomalias para identificar fraude financiero

Carlos A. Rico Martínez★

Mayo 2023

ABSTRACT

This work attempts to show the results of multiple machine learning models applied over a credit card transaction data set wich aim to identify anomalies that indicate likely fraudulent.

Key words: anomaly – fraud – detection –supervisaded – learning – regression – clasification – knn

1 OBJETIVO

El objetivo de este proyecto es realizar la implementación de diversos modelos tanto de aprendizaje supervisado como no supervisado, de matera que se puedan comparar los resultados obtenidos en cada uno de llos. Logrando asi identificar aquel que ayude a clasificar de manera más adecuada aquellas posibles transacciones que pudieran ser tipificadas como fraudulentas. Para dicha estimación (ya sea un "score" o una clasificación) se hará uso de un conjunto de transacciones de tarjetas de crédito.

2 INTRODUCCIÓN

Se entiende por anomalia, valor atípico u outlier por su término anglosajón, eventos raro o desviación dentro del conjunto de datos a: "aquella observación que se desvía tanto de las otras observaciones que despierta sospechas de que fue generada por un mecanismo diferente" (Hawkins, 1980). En otras palabras, la detección de anomalías es la tarea de encontrar aquellas observaciones que difieren significativamente del resto de los datos. En la mayoría de los casos, los datos son creados por un proceso generador el cual es el resultado ya sea de un reflejo de la actividad en algún sistema o de observaciones recolectadas de las entradas a este. Cuando el resultado presenta un comportamiento inusual, la capacidad de reconocerlo permite la generación de información muy útil en diversas industrias. Dicha información resultará en la capacidad de emitir una respuesta planificada lo cual permitirá ahorrar tiempo, costos y clientes a las empresas. Por lo tanto, la detección de anomalías ha encontrado diversas aplicaciones en una variedad de dominios, incluidos análisis de TI, análisis de intrusión de red, diagnósticos médicos, protección contra fraudes financieros, control de calidad de fabricación, análisis de marketing y redes sociales, y más.

La detección de anomalías en el ámbito financiero, específicamente en la detección de fraudes, es un desafío constante para las organizaciones. Con el aumento de transacciones electrónicas y el avance tecnológico, los delincuentes han encontrado formas cada vez más audaces de cometer fraudes financieros. Existen diversas modalidades de fraudes financieros, electrónicos y no electrónicos. Dentro de los fraudes electrónicos los ciberdelincuentes utilizan la red para realizar operaciones monetarias ilícitas. De acuerdo a La Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF), El incremento a partir de 2020 en el número de transacciones digitales ha provocado que el fraude cibernético sea más sofisticado cada vez, al grado de que, hacer un depósito, cobrar un cheque, retirar dinero de un cajero automático, solicitar un crédito, pagar con la tarjeta o realizar compras en línea, se ha convertido en un riesgo y de no adoptar medidas preventivas, puede llevarnos a ser víctimas de un algún fraude. De 2020 a finales del 2022 se han registrado 391 mil 182 controversias por posible fraude, teniendo su mayor crecimiento en el fraude cibernético.
Tan solo, durante 2022, el 62.3 porciento de las controversias correspondieron a la banca múltiple (134,433). De esa cifra, 30.5 porciento fueron asuntos presentados por personas adultas mayores (41,051) y de éstos, el 50.5 por ciento (20,745) se originaron por un posible fraude.

Estos delitos por sus características se han clasificado en cuatro tipos:

2.0.1 Correo Basura (Spam)

Suelen ser mensajes de carácter publicitario con información no solicitada que puede incluir un enlace fraudulento.

2.0.2 Smishing

Consiste en el envío de mensajes de texto con un vínculo, para que entres a esa página fraudulenta y te roben tus datos.

2.0.3 Phishing

Es un tipo de estafa que tiene como objetivo obtenerla obtención de datos privados a través de internet, especialmente para acceder a sus cuentas o datos bancarios.

2.0.4 Pharming

Son usualmente ventanas emergentes presentes en los sitios web, ocultos en botones principales que pretenden redigirigir al usuario a

★ E-mail: carlos.2302@hotmail.com

sitios que roban información personal.

Dentro de los mas comunes se encuentra el Phising, este delito consiste en la suplantación de identidad y el objetivo es hacerse pasar por una persona frente a una institución para cometer fraudes a su nombre. Esto representa fuertes implicaciones tanto a las personas clientas de instituciones financieras como a las propias entidades, es por eso que para contrarrestar esta amenaza, se han desarrollado técnicas y algoritmos sofisticados de detección de anomalías que permiten identificar patrones sospechosos y comportamientos anómalos en los datos financieros.

La detección de anomaliass en el ambito financiero consiste en identificar transacciones fraudulentas o comportamientos atípicos que puedan indicar actividades ilícitas. Esto incluye detectar actividades como el robo de identidad, el lavado de dinero, las estafas con tarjetas de crédito y otros tipos de fraude financiero. La detección temprana de estas anomalías es crucial para minimizar el impacto financiero y reputacional en las organizaciones, así como para proteger a las personas clientes y evitar pérdidas. Para contrarrestar esta corriente delictiva, se han implementado diferentes enfoques y técnicas en la detección de anomalías financieras. Una de las estrategias más comunes es el uso de algoritmos de aprendizaje automático, tales como el aprendizaje supervisado y no supervisado. Estos algoritmos se entrenan utilizando conjuntos de datos históricos que contienen transacciones tanto legítimas como fraudulentas. A través del análisis de estas muestras, los algoritmos aprenden a identificar patrones y características distintivas asociadas con el fraude.

2.1 Aprendizaje supervisado

En el caso del aprendizaje supervisado, los algoritmos se entrenan utilizando datos etiquetados, esto quiere decir, transacciones previamente clasificadas como legítimas o ilícitas. Estos algoritmos luego se aplican a nuevos conjuntos de datos para predecir si una transacción dada es sospechosa o no.

2.2 Aprendizaje no supervisado

En este tipo de aprendizaje se utiliza cuando no se dispone de etiquetas en los datos de entrenamiento. Los algoritmos analizan los datos en busca de patrones inusuales o agrupaciones anómalas que puedan indicar la presencia de operaciones ilícitas y fraudulentas. Además de los algoritmos de aprendizaje automático, también se emplean otras técnicas en la detección de anomalías financieras. Esto incluye el uso de reglas de negocio, que establecen criterios específicos para identificar transacciones sospechosas basadas en condiciones predefinidas. Asimismo, se utilizan técnicas de minería de datos para descubrir patrones ocultos y relaciones entre los datos financieros que puedan ser indicativos de fraude.

La detección de anomalías en el ámbito financiero es un campo de investigación y desarrollo en constante evolución. Con el fin de proteger los activos financieros y la integridad de las entidades, imperativo la implementación de estrategias efectivas de detección en cuestión fraudes, esto a través de tener medido el comportamiento de sus usuarios, de manera que sea notorio cuando una operación es ilegitima. Al combinar algoritmos de aprendizaje automático, reglas de negocio y técnicas de minería de datos, las entidades pueden fortalecer sus sistemas de detección de anomalías y reducir el riesgo de fraude financiero.

RECLAMACIONES RELACIONADAS CON UN POSIBE FRAUDE EN LA CIUDAD DE MÉXICO, SECTOR BANCARIO

CAUSAS	Enero - Agosto				
	2019	2020	2021	Var. (%) 2021-2020	Var. (%) 2021-2019
TOTAL BANCA MÚLTIPLE	25,876	15,769	22,782	44.5	-12.0
POSIBLE FRAUDE	15,334	8,242	10,078	22.3	-34.3
POSIBLE FRAUDE/ TOTAL BM	59%	52%	44%	-	-
Consumos no reconocidos	7,751	3,568	3,206	-10.1	-58.6
Transferencia electrónica no reconocida	1,376	1,240	2,909	134.6	111.4
Cargos no reconocidos en la cuenta	1,431	799	1,227	53.6	-14.3
Disposición de efectivo en cajero automático no reconocida por el Usuario, cliente y/o socio	1,481	990	820	-17.2	-44.6
Consumos vía internet no reconocidos	239	258	523	102.7	118.8
Otras	3,056	1,387	1,393	0.4	-54.4

Figure 1. En la CDMX, del total de reclamaciones presentadas en contra de los bancos, el 44 porciento estuvieron relacionadascon un posible fraude, fundamentalmente originadas por llamadas telefónicas, acceso a páginas apócrifas y en cajeros automáticos.Al respecto, destaca el incremento de estos asuntos porlos Consumos no reconocidos y las Transferencias electrónicas no reconocidas, por ello es muy importante que las y los usuarios no den información por teléfono(muchas veces a través de llamadas realizadas supuestamente de su banco), no accedan a páginas que les llegan a través de redes sociales o den sus claves o datos personales, si no iniciaron ellos mismos algún tipo de consulta.

Trimestre	Compras autorizadas		% de solicitudes	Contracargos en compras autorizadas		% de contracargos
	Monto*	Número		Monto*	Número	
2021Q1	112,474	197,811,526	64%	787	968,639	0.49%
2021Q2	120,181	209,672,655	64%	761	1,043,089	0.50%
2021Q3	117,968	204,486,392	62%	575	906,582	0.44%
2021Q4	149,549	228,329,597	64%	749	1,031,063	0.45%
2022Q1	142,913	216,587,642	63%	676	891,683	0.41%

Figure 2. Compras y contracargos registrados durante el 2021 y 2022.

2.3 Panorama del fraude en México

En el primer trimestre de 2022 se realizaron 1,019 millones de pagos con tarjetas en comercios electrónicos, representando el 21.3 porciento del total de pagos con tarjeta. Del total de compras en comercios electrónicos, 69.9 porciento de ellas se hicieron con tarjetas de débito y el 30.1 porciento con tarjeta de crédito.

De acuerdo a El Financiero, México ocupa el primer lugar de América Latina de los países donde se registran más fraudes en línea. Esto ha traido como implicación que las autoridades traigan en la mira invertir en ciberseguridad. Esto a través de empujar la aprobación de la Ley de Ciberseguridad ya que al tener una mejor regulación de las transacciones que se realizan en los {*e-commerce*. Tal es la frecuencia de fraudes eléctronicos en nuestro país que un grupo de senadores han considerado esta problemática como un problema en materia de Seguridad Nacional. De acuerdo con la CONDUSEF, durante los primeros cinco meses del año 2021 hubo un aumento del 89 porciento en materia de delitos cibernéticos, en comparación con 2020. En contraste, durante el primer trimestre de 2022, se cometieron 463 delitos cibernéticos en operaciones por comercio electrónico y banca móvil cada hora.

3 DETECCIÓN DE ANOMALIAS

La detección de anomalías con Machine Learning en la prevención de fraudes es un campo de investigación y aplicación que busca identificar patrones y comportamientos inusuales en los datos financieros con el fin de prevenir y mitigar actividades fraudulentas. Este enfoque se basa en el uso de algoritmos de aprendizaje automático para analizar grandes cantidades de datos y detectar transacciones sospechosas o anómalas que podrían indicar la presencia de fraude. El marco teórico de detección de anomalías con Machine Learning en la prevención de fraudes se sustenta en diferentes técnicas y conceptos clave:

3.1 Aprendizaje supervisado

Este enfoque utiliza datos etiquetados que contienen ejemplos de transacciones fraudulentas y legítimas para entrenar modelos de Machine Learning. Estos modelos aprenden a reconocer patrones característicos del fraude y, posteriormente, se utilizan para clasificar nuevas transacciones como legítimas o sospechosas. El aprendizaje supervisado es un enfoque para crear inteligencia artificial (IA), donde un algoritmo se entrena con datos de entrada que han sido etiquetados para una salida en particular. El modelo se entrena hasta que puede detectar los patrones subyacentes y las relaciones entre los datos de entrada y las etiquetas de salida, lo que le permite producir resultados de etiquetado precisos cuando se presentan con datos nunca antes vistos.

El aprendizaje supervisado es bueno en problemas de clasificación y regresión, como determinar a qué categoría pertenece un artículo de noticias o predecir el volumen de ventas para una fecha futura determinada. En el aprendizaje supervisado, el objetivo es dar sentido a los datos dentro del contexto de una pregunta de negocio específica.

3.1.1 Regresión Logística

La regresión logística es un algoritmo de aprendizaje supervisado que nos permite modelar un evento dicotómico en forma probabilística donde p representa la probabilidad de éxito. Dependiendo del contexto, “éxito” puede interpretarse de manera relativa, en nuestro estudio nos referiremos a “éxito” por aquellos casos de representan una característica de interés (tomar un producto, incumplir un préstamo, enfermar, etc.). El complemento de p se denota por q = 1 - p , en ocasiones, es útil el cociente p = p / (1-p) denominado momio (odd’s) que representa cuánto más probable es el éxito que el fracaso.

3.1.2 Árboles de decisión

Un árbol de decisión (empírico) representa una segmentación de un conjunto de datos, la cual se traduce en simples reglas que deciden la etiqueta (target estimada) de cada observación. Un árbol de decisión tiene la siguiente estructura: **Nodo raíz:** representa toda la población o muestra y esta se divide en dos o más conjuntos. Nodo de decisión: cuando un subnodo se divide en otros subnodos, se denomina nodo de decisión. **Nodo Hoja/ Terminal:** Los nodos que no se dividen se denominan nodo Hoja o Terminal. **Rama / Subárbol:** una subsección de todo el árbol se denomina rama o subárbol. **Rama / Subárbol:** un nodo, que se divide en subnodos, se denomina nodo padre de subnodos, mientras que los subnodos son hijos de un nodo padre.

3.1.3 Support Vectorial Machine

En este algoritmo el objetivo principal es encontrar un hiperplano en un espacio de alta dimensión que pueda separar de manera óptima las diferentes clases de datos.
SVM tiene base en la idea de que dicho hiperplano maximice el margen entre las clases de datos, lo que se conoce como el "margen máximo". Los puntos de datos que se encuentran más cerca del hiperplano se denominan vectores de soporte. De manera que por ssu construcción, este algoritmo es capaz de realizar clasificaciones lineales y no lineales con ayuda del uso del kernel haciendo una transformación del espacioauno de mayor dimensión.

3.2 Aprendizaje no supervisado

En ausencia de etiquetas en los datos ingresados de entrenamiento, se recurre al aprendizaje no supervisado. Este enfoque se basa en identificar patrones o agrupaciones anómalas en los datos sin una categorización predefinida. Los algoritmos no supervisados, como el clustering o detección de anomalías, pueden revelar comportamientos inusuales que merecen una mayor atención para su posterior análisis y verificación.

3.3 Selección y extracción de características

La calidad y relevancia de las características utilizadas en el modelado de detección de anomalías son fundamentales. Se emplean técnicas de selección y extracción de características para identificar aquellas variables que tienen un mayor impacto en la detección de fraudes. Esto puede incluir atributos relacionados con el tiempo, ubicación, cantidad de transacciones, patrones de gasto, entre otros.

3.4 Modelos de clasificación y detección de anomalías

Se pretemde emplear diversos modelos de machine learning para clasificar las transacciones en legítimas o fraudulentas, o para identificar aquellas que difieren significativamente del comportamiento normal. Los modelos que se pretende usar son K-Means, Árboles de decisión, redes neuronales, regresión, algoritmos de detección de anomalías y DBSCAN (Density-Based Spatial Clustering of Applications with Noise.

3.5 Validación y evaluación del modelo

Una vez aplicados los modelos, se evaluará el rendimiento y la precisión del modelo de detección de anomalías. Se utilizarán técnicas como la validación cruzada, la matriz de confusión y medidas de evaluación como la precisión, el recall y la F1-score para determinar la eficacia del modelo en la identificación de fraudes y su capacidad para minimizar los falsos positivos y falsos negativos.

3.6 Actualización y adaptabilidad del modelo

El entorno financiero y las técnicas de fraude están en constante evolución. Por lo tanto, es esencial que el modelo de detección de anomalías se actualice y se adapte regularmente a medida que surjan nuevas técnicas de fraude y cambien los patrones de comportamiento de los delincuentes financieros. Esto implica el monitoreo constante de los resultados del modelo yhttps://www.overleaf.com/project/6466b3d2bf57a2244f445601 la

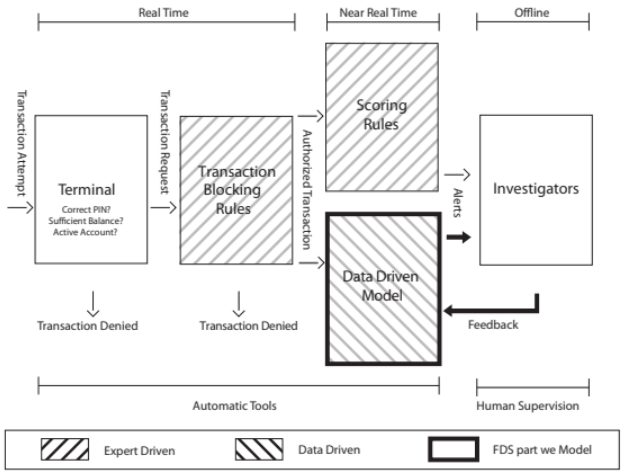

Figure 3. Identificación de una operación fraudulenta

incorporación de nuevos datos y características relevantes. En resumen, la detección de anomalías con machine learning en la prevención de fraudes se basa en la aplicación de algoritmos y técnicas de aprendizaje automático para identificar patrones y comportamientos anómalos en los datos financieros. Este enfoque ofrece una forma eficiente y efectiva de detectar y prevenir fraudes, permitiendo a las organizaciones proteger sus activos y mantener la integridad de sus sistemas financieros.

3.7 Estado de Arte

En este apartado, se encuentra a modo de resumen un recontexto de los trabajos que se han hecho previamente con respecto identificación de anomalías. Los trabajos que han aportado en mayor medida a esta investigación han sido los siguientes:

3.7.1 "A Survey of Outlier Detection Methodologies." de Hodge and Austin, 2004

En este artículo se proporciona una revisión exhaustiva de las metodologías de detección de valores atípicos. Se abordan varios aspectos relacionados con la detección de anomalías, incluyendo técnicas de preprocesamiento de datos, algoritmos de detección de anomalías, métricas de evaluación y aplicaciones prácticas.

Los autores presentan una clasificación de las metodologías de detección de anomalías en diferentes categorías, como enfoques basados en reglas, métodos estadísticos, métodos de aprendizaje automático y enfoques híbridos. Se discuten las ventajas y limitaciones de cada categoría, así como ejemplos de algoritmos y técnicas comunes dentro de cada una.

Además, el artículo analiza las métricas utilizadas para evaluar la calidad de las detecciones de anomalías, como la precisión, la exhaustividad y la puntuación F. Se destacan los desafíos y las consideraciones importantes al evaluar y comparar diferentes métodos de detección de anomalías. Este artículo resulta relevante ya que es útil en en comprender y aplicar técnicas de detección de anomalías, además proporciona una visión general completa de las metodologías existentes y ofrece información útil para orientar la selección y evaluación de métodos de detección de anomalías en diversas aplicaciones.

3.7.2 "Anomaly detection: A survey. " de Chandola et al, 2009

En este artículo escrito por Chandola, Banerjee y Kumar se ofrece una revisión amplia de las técnicas y enfoques utilizados en la detección de anomalías. Trata de tanto métodos tradicionales como técnicas más avanzadas y se centra en diversos aspectos de la detección de anomalías, incluyendo definiciones, desafíos, enfoques de modelado y evaluación.

Los autores proporcionan una definición de anomalía y discuten las características y propiedades de las anomalías en los datos. Se exploran los desafíos asociados con la detección de anomalías, como el desequilibrio de clases, la escalabilidad y la interpretación de los resultados.

El artículo también presenta una clasificación de los métodos de detección de anomalías en diferentes categorías, como métodos basados en enfoques estadísticos, enfoques basados en aprendizaje automático, técnicas basadas en proximidad y enfoques basados en conocimiento. Para cada categoría, se describen ejemplos de algoritmos y técnicas comunes.

También se discuten las métricas y técnicas de evaluación utilizadas para evaluar la efectividad de los métodos de detección de anomalías. Se exploran enfoques como la validación cruzada, la matriz de confusión y las curvas de precisión-recuperación. Este trabajo es relevante ya que proporciona una visión general exhaustiva de las técnicas de detección de anomalías. Es una buena referencia para comprender las metodologías existentes y las consideraciones clave en la detección de anomalías en diferentes dominios de aplicación.

3.7.3 "Outlier Analysis" de Aggarwal, 2013

En este libro se aborda a detalle el campo de análisis de valores atípicos (outliers). Donde se proporciona una visión completa de las técnicas, métodos y aplicaciones relacionados con el análisis de valores atípicos.

El autor comienza definiendo y conceptualizando los valores atípicos, así como discute los desafíos y las características de los datos con valores atípicos. Luego, se adentra en una variedad de técnicas y algoritmos utilizados para detectar y tratar los valores atípicos en diferentes contextos. Este trabajo cubre una amplia variedad de temas, incluyendo técnicas estadísticas clásicas, enfoques basados en aprendizaje automático, métodos basados en distancias y enfoques basados en modelos probabilísticos. También se discuten técnicas avanzadas como detección de anomalías en datos en streaming, detección de anomalías en datos de alto rendimiento y detección de anomalías en datos de redes sociales.

Además de las técnicas de detección de valores atípicos, se adbordan aplicaciones prácticas en diversas áreas, como detección de fraudes, detección de intrusiones, análisis de datos biomédicos y análisis de datos ambientales. Este libro es relevante porque es una obra de referencia completa que cubre los fundamentos teóricos, los métodos y las aplicaciones del análisis de valores atípicos.

4 METODOLOGÍA

4.1 KDD – Knowledge Discovery in Databases

Proceso iterativo no-trivial. Depende la interacción para la toma de decisiones Consta de un número resumido y bien definido de pasos.

Knowledge Discovery in Databases (KDD) se utiliza en la detección de anomalías para descubrir patrones y relaciones ocultas en conjuntos de datos. Aquí hay un resumen conciso de cómo se usa:

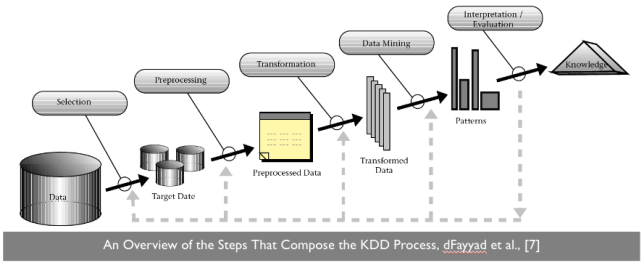

Figure 4. Metodología KDD

Recopilación de datos: Se recopilan datos relevantes, como registros de transacciones, mediciones de sensores o datos de comportamiento.

Preprocesamiento de datos: Los datos se limpian y se les aplica transformaciones necesarias, como normalización, eliminación de valores atípicos o manejo de datos faltantes.

Selección de características: Se seleccionan las características o variables más relevantes para el análisis de anomalías, con el objetivo de reducir la dimensionalidad y mejorar la eficiencia del proceso.

Aplicación de algoritmos de detección de anomalías: Se aplican algoritmos de aprendizaje automático o estadísticos, como detección de valores atípicos, clustering o detección de desviaciones, para identificar patrones anómalos en los datos.

Validación y evaluación: Se valida la calidad de las anomalías detectadas y se evalúa el rendimiento del modelo utilizando métricas adecuadas, como precisión, exhaustividad o puntuación F.

Interpretación de resultados: Se interpretan los resultados de la detección de anomalías para comprender la naturaleza y el impacto de las anomalías detectadas.

Es importante destacar que KDD en la detección de anomalías es un proceso iterativo y puede requerir ajustes en cada etapa para mejorar la precisión y la eficacia de la detección.

El aprendizaje supervisado es un enfoque para crear inteligencia artificial (IA), donde un algoritmo informático se entrena con datos de entrada que han sido etiquetados para una salida en particular. El modelo se entrena hasta que puede detectar los patrones subyacentes y las relaciones entre los datos de entrada y las etiquetas de salida, lo que le permite producir resultados de etiquetado precisos cuando se presentan con datos nunca antes vistos.

El aprendizaje supervisado es bueno en problemas de clasificación y regresión, como determinar a qué categoría pertenece un artículo de noticias o predecir el volumen de ventas para una fecha futura determinada. En el aprendizaje supervisado, el objetivo es dar sentido a los datos dentro del contexto de una pregunta de negocio específica.

5 SECCIÓN

5.1 Subsección

DATA AVAILABILITY

REFERENCES

[1] D.M. Hawkins. 1980. Identification of outliers. Springer, Heidelberg, Germany.

[2] Condusef contenido. (s. f.). https://www.condusef.gob.mx/?p=contenido

[3] Condusef estadisticas. (s. f.). https://www.condusef.gob.mx/?p=estadisticas

[4] Victoria Hodge Jim Austin. (2004). A Survey of Outlier Detection Methodologies. Recuperado de: https://link.springer.com/article/10.1023/B:AIRE.0000045502.10941.a9

[5] Chandola, et al. (2009). Anomaly detection: A survey. Recuperado de: https://dl.acm.org/doi/10.1145/1541880.1541882

[6] Charu C. Aggarwal. (2013). Outlier Analysis. Recuperado de: https://sadbhavnapublications.org/research-enrichment-material/2-Statistical-Books/Outlier-Analysis.pdf

[7] Usama Fayyad y Evangelos Simoudis. (1997). Data Mining and Knowledge Discovery in Databases.

[8] Hilal, Gadsden Yawney. (2022). Finanacial Fraud: A Reviwe of Anomaly Detection Techniques and Recent Advances. Recuperado: https://www.sciencedirect.com/science/article/pii/S0957417421017164.

APPENDIX A: ANÁLISIS EXXPLORATORIO

Aquí van los gráficos

APPENDIX B: DICCIONARIO DE DATOS

This paper has been typeset from a TEX/LATEX file prepared by the author.