TREBALL DE FI DE GRAU

Grau en Estadística

Títol: Detecció de frau en targetes de crèdit/dèbit.

Autor: Àngel Reig Miralles

Director: Hector Rufino Alcalde

Departament: Econometria, Estadística i Economia Aplicada

Convocatòria: Juny 2023

:

UNIVERSITAT DE BARCELONA

UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Facultat de Matemàtiques i Estadística

AGRAÏMENTS

En primer lloc, m'agradaria agrair al meu tutor, l'Hector Rufino Alcalde, per acompanyar-me en tot el projecte. La seva dedicació i disposició ha estat fonamental per aconseguir els objectius que ens havíem plantejat en el poc temps que teníem. També vull agrair a l'equip de l'entitat financera per confiar en mi i permetrem participar en el projecte, va ser molt important la seva col·laboració i van posar a la meva disposició totes les facilitats possibles perquè el projecte tirés endavant.

ABSTRACT

The importance of fraud detection has increased over the last years, which is why companies, especially banks, are looking for a solution in this regard. This final degree project focuses on the detection of anomalies in banking transactions with the aim of preventing fraud. A methodology based on Machine learning has been applied using data from a real bank. An unsupervised model based on the Isolation Forest algorithm has been developed to identify anomalous patterns in the transaction logs. The project also includes the implementation of the model in the bank, contributing to the improvement of fraud prevention strategies in the bank.

Key words: bank, credit risk, merchant, fraud, unsupervised models, anomaly, Machine Learning

American Mathematical Society (AMS) classification:

- 65C20 Models, numerical methods
- 91G40 Credit risk
- 97M30 Financial and insurance mathematics

ÍNDEX

1. INTRODUCCIÓ

En els darrers anys hem vist un augment significatiu en les pràctiques fraudulentes que han impactat negativament a les empreses i als particulars. Això es deu al desenvolupament tecnològic, que ha permès als estafadors buscar maneres més sofisticades per a dur a terme el frau. També es deu als canvis en els hàbits de consum de la gent, on les compres en línia han augmentat exponencialment generant un escenari propici a l'aparició de noves formes de frau. Per a reduir les pèrdues derivades del frau, les empreses busquen maneres de poder-lo detectar i prevenir, per això, destinen recursos per a trobar models d'aprenentatge automàtic que els ajudin a detectar patrons anòmals.

Des del moment on havia de començar a pensar en el tema del treball, la meva idea era poder fer-lo en col·laboració amb una entitat financera, així podria aplicar els coneixements adquirits a la universitat en el món real. Aleshores em vaig posar en contacte amb un banc, i la primera resposta que vaig rebre, va ser que en aquell moment no tenien cap projecte on pogués col·laborar. No va ser fins a mitjans d'abril, on el mateix banc va contactar amb mi per a dir-me que els hi havia sortit un problema, i que ara sí que els aniria bé la meva ajuda. Quan m'ho van comunicar vam arribar a un acord, on jo ajudaria a solucionar el problema i ho utilitzaria com a tema per a fer el treball. També vam acordar que el nom del banc seria anònim durant tot l'informe.

Es va escollir la detecció de frau com a tema d'aquest treball després de parlar amb el banc i que em comentessin que en els últims mesos, estaven tenint el problema que alguns establiments rebien atacs de transaccions fraudulentes. Aleshores vam decidir que podia col·laborar amb l'entitat i utilitzar les seves dades per a desenvolupar un model que detectes aquests atacs. Aquesta oportunitat m'ha permès resoldre un problema real mentre faig el treball sobre dos dels camps que em van semblar més interessants durant la carrera, la programació i les finances.

El principal objectiu és desenvolupar un model que sigui útil per a l'entitat financera. Per aconseguir aquest objectiu hem de treballar i transformar les dades que ens donen, fer un model no supervisat que sigui ràpid i que detecti les anomalies. Amb això, obtindríem una resposta més ràpida i eficaç davant els fraus i millorarem la confiança dels clients amb l'entitat.

La metodologia emprada consisteix en l'anàlisi de les transaccions d'un banc i la implantació de tècniques d'aprenentatge automàtic no supervisades per a detectar anomalies. El principal llenguatge de programació amb el qual es treballarà és Python i s'utilitzarà l'algoritme *Isolation Forest* per a resoldre el problema.

Aquest treball es divideix en dues parts: la part teòrica i la part pràctica. En la part teòrica s'explica els conceptes necessaris per a conèixer els riscos financers i els tipus de frau amb

targetes de crèdit. També es mostren estadístiques per a poder entendre l'efecte del frau en les empreses i, en últim lloc, s'explica un model per a la detecció d'anomalies. En la part pràctica és mostra com es treballen les dades, com s'aplica un algoritme i els respectius resultats, i finalment, s'explica com s'ha aplicat l'algoritme en l'entitat financera.

2. METODOLOGIA

La base de dades utilitzada ha estat proporcionada pel banc. Aquesta ens mostra les transaccions que s'han dut a terme a través de targetes del banc entre el 23 de desembre del 2022 fins al 23 d'abril de 2023. Cada dia de les dades estava guardat en un fitxer de text on cada línia hi havia una transacció amb la informació en format JSON. A partir d'aquests fitxers de text, s'ha construït una base de dades estructurada per a poder-hi treballar millor. És important destacar que la informació emprada ha estat tractada amb la deguda confidencialitat i seguint les polítiques de privacitat i protecció de dades del banc.

La metodologia usada ha sigut l'algoritme d'aprenentatge automàtic *Isolation Forest*, aquest mètode és una tècnica de detecció d'anomalies que es pot fer servir en casos no supervisats com el nostre.

Per a dur a terme el cas pràctic s'ha utilitzat el llenguatge de programació de Python i les principals llibreries utilitzades per a manipular les dades i aplicar els algoritmes han sigut *Pandas*, *NumPy*, *Scikit-learn* i *Plotly*. Primer hem construït la base de dades amb totes les transaccions juntes usant *Pandas* i *Json*. En la següent part fem un bucle que s'executa cada 10 minuts on en cada iteració fem un càlcul per acabar obtenint els valors que emprarem en el model, en aquesta part hem emprat *Numpy* per a fer els càlculs i *Pandas* per guardar les dades en una taula. Per la part de fer els gràfics dels valors de les sèries hem fet servir *Plotly*. Finalment, per a crear l'algoritme hem fet ús de *Scikit-learn*. Quan hem decidit aplicar la manipulació de dades i l'algoritme en temps real en el banc hem treballat agafant les dades d'Elasticsearch fent servir la llibreria *elasticsearch*.

3. CONCEPTES BÀSICS

3.1. Tipus de riscs financers

El risc financer és un factor molt important que cal tenir en compte quan s'analitza una inversió. Es refereix a la probabilitat que es produeixi un esdeveniment negatiu que provoqui pèrdues financeres en una empresa. En qualsevol inversió que es vulgui dur a terme és crític quantificar els riscos per a poder decidir si fer la inversió o no. El risc acostuma a estar relacionat amb la rendibilitat, com major sigui el risc major serà la rendibilitat que s'obtindrà en cas que surti bé.

Existeixen diferents tipus de riscos financers que poden afectar a les empreses, els principals són:

- Risc de crèdit: és aquell que està relacionat amb la possibilitat que una part involucrada en la transacció no compleixi les seves obligacions de pagament.

- Risc de mercat: es refereix a les fluctuacions en els mercats financers que poden afectar el valor dels actius i les inversions. Aquest tipus de risc financer inclou el risc de tipus d'interès, el risc de tipus de canvi i el risc de matèries primeres, aquests riscos els veure'm amb més detall en un apartat posterior.

- Risc operacional: està associat amb els processos interns, inclou riscos com possibles errors en els sistemes tecnològics, erros humans, frau intern o l'incompliment de regulacions.

Cada un d'ells presenta característiques úniques que s'han d'avaluar i gestionar correctament.

La gestió del risc financer és un procés que implica identificar, mesurar, controlar i mitigar els riscos per protegir els interessos de l'empresa i maximitzar-ne el valor per als accionistes. Això inclou desenvolupar estratègies de diversificació de carteres, l'ús d'instruments financers derivats per cobrir posicions i la implementació de polítiques de gestió de riscos.

En resum, entendre i gestionar el risc financer és essencial per a qualsevol empresa que busqui prendre decisions d'inversió informades i protegir la salut financera a llarg termini. Quantificar els riscos i avaluar-ne l'impacte potencial en la rendibilitat ajudarà a implementar estratègies de gestió efectives.

A continuació exposaré una explicació més detallada dels diferents tipus de risc financers amb la finalitat d'entendre les seves característiques, els desafiaments que planteja cada un d'ells i les estratègies per a gestionar-los.

3.1.1. Risc de crèdit

El risc de crèdit és la possibilitat que té un creditor de tenir pèrdues derivades d'un impagament dels crèdits concedits als seus clients i deutors en una operació financera, normalment aquest incompliment sorgeixen per motius d'insolvència produint pèrdues en el prestador, en aquest cas el banc.

Aquest tipus de risc està directament relacionat amb els problemes que puguin presentar els deutors de l'operació financera de forma individual, en canvi, altres riscs com el de mercat, el qual veurem posteriorment, tenen un component de risc sistemàtic, aquest deriva de la incertesa global del mercat que afecta tots els actius existents en l'economia.

Hi ha 3 formes del risc de crèdit:

- Risc d'incompliment: és quan l'emissor d'un bo o el deutor d'un préstec no compleix amb les obligacions contractuals. Quan l'impagament és parcial, una part del deute emès és recuperada, en canvi, quan és total el deutor no paga res de la quantitat que es deu.

- Ris de rebaixa creditícia: és la possibilitat que una agència de qualificació redueixi la qualitat creditícia d'un actiu o emissor.

- Risc de *spread* de crèdit: aquest risc mesura un augment en la diferència de la rendibilitat d'un actiu de referència respecte a la rendibilitat d'un actiu lliure de risc i amb un venciment semblant. Un augment en l'*spread* ens indica que l'actiu de referència ho està fent pitjor que l'actiu lliure de risc, això és perquè que augmenta la rendibilitat de l'actiu de referència aquest cau en preu, ja que el preu i la rendibilitat d'un bo es mouen inversament.

Per a mesurar el risc de crèdit s'utilitza la pèrdua esperada (PE), la qual es pot calcular a partir de la fórmula següent:

$$PE = PD * EAD * LGD$$

On la probabilitat d'incompliment (PD), en angles *probability of default*,és la probabilitat que el prestatari no compleixi amb les seves obligacions contractuals, s'expressa en forma de percentatge. L'exposició a l'incompliment (EAD), en angles *exposure at default*, és la quantitat total de la posició que resta per pagar en el moment de l'incompliment. La pèrdua

en cas d'incompliment (LGD), en angles *loss given default*, és la part del total de l'exposició a l'incompliment (EAD) que no es recupera després que el deutor hagi incomplert el pagament i ja s'hagi dut a terme un procés de recuperació d'actius, s'expressa en forma de percentatge. És important tenir en compte que la PD, EAD i la LGD són unes estimacions i estan subjectes a canvis, per tant, és important que les entitats financeres realitzin un seguiment i les actualitzin periòdicament per assegurar-se que és precís el risc creditici que assignen a cada deutor, així poden gestionar correctament el risc creditici.

Algunes de les accions que es poden prendre per a reduir el risc creditici són les següents:

- Invertir en capacitació de personal, l'equip de gestors ha de tenir la capacitat de reconèixer els riscos associats a les operacions de crèdit.
- Facilitar la comunicació directa i eficaç entre els clients i l'àrea de crèdit.
- Automatitzar el flux d'informacions i processos, així les decisions es poden prendre més ràpidament.

Per a minimitzar els problemes causats per al risc d'impagament, els creditors poden contractar assegurances de crèdit, les quals són oferits per asseguradores que cobreixen les pèrdues derivades de l'impagament de l'operació, a canvi d'aquesta protecció el creditor paga una prima a l'asseguradora.

3.1.2. Risc de mercat:

El risc de mercat és la probabilitat de variacions en el preu d'un actiu financer com podrien ser bons, accions, divises, matèries primeres i altres instruments financers. Fa referència al risc de possibles pèrdues de valor d'un actiu associat a la fluctuació i les variacions en el mercat. Aquest risc és provocat per la volatilitat i imprevistos que afecten el valor dels actius.

Els principals components del risc de mercat són:

- Risc de tipus d'interès: fa referència a la possibilitat que la variació dels tipus d'interès afecti el valor d'actius financers, principalment dels bons. Quan les taxes d'interès augmenten, el preu dels bons disminueix, això pot portar pèrdues latents dels bonistes si volen vendre el bo a mercat en lloc d'esperar a venciment, on l'import que havien pagat del bo es tornarà íntegrament sempre que l'emissor del bo no hagi fet fallida. Altrament, quan les taxes d'interès s'abaixen, el preu dels bons augmenta, això pot portar guanys als bonistes. Un altre efecte de l'augment dels tipus d'interès és l'encariment del finançament d'empreses amb deute variable, això es traslladarà en més despeses per l'empresa reduint els beneficis.

  Per a intentar contrarestar l'efecte dels tipus d'interès hi ha diverses vies:

- Si contractem un tipus d'interès fix, pagarem un interès més alt que el que pagaríem si agaféssim l'opció variable, però ens dona més seguretat davant de possibles futures pujades de tipus d'interès.

- També es pot intentar contrarestar l'efecte de les possibles pujades de tipus d'interès invertint en productes que augmentin de preu quan augmenten els tipus d'interès, eliminant així els efectes negatius de les pujades de tipus.

Una altra opció més complexa per a mitigar aquest risc és el dels futurs sobre taxes d'interès, aquests contractes són una cobertura sobre actius els quals el seu preu depèn únicament del nivell dels tipus d'interès. El propòsit és tenir un mecanisme que et permeti fixar de manera anticipada la taxa d'interès reals i cobrir la volatilitat causada pels moviments de la inflació. El funcionament d'aquests futurs és que qui els ven es compromet a entregar una quantitat de títols de deute amb un període de vigència, a un preu pactat i una data futura, per l'altra part, el comprador es compromet a rebre els títols i pagar el preu pactat. Els guanys d'ambdues parts al venciment sorgeix de la diferència en la taxa d'interès entre la pactada i la que existeix en el mercat quan el contracte venç.

- Risc de tipus de canvi:

Aquest risc fa referència a la possibilitat que canviïn els tipus de canvi entre diferents divises, ja que el seu preu fluctua constantment en el mercat de divises. Aquests moviments principalment són causats per canvis en les condicions econòmiques i polítiques, anuncis de política monetària dels bancs centrals, esdeveniments geopolítics i fluxos de capital internacionals, entre altres.

Per exemple, si comprem un fons d'inversió estatunidenc en dòlars, una depreciació del dòlar contra l'euro perjudicaria la rendibilitat dels fons per a un inversor europeu.

Un altre exemple habitual, és les empreses manufactureres, aquestes compren matèries primeres de diferents llocs del món, per tant, treballen amb monedes diferents, algunes d'elles amb països poc estables tant econòmicament com socialment, i això implica un risc per l'empresa.

Un recurs molt utilitzat per a minimitzar aquest risc és la cobertura de tipus de canvi, això consisteix a fixar el tipus de canvi futur al qual es vendrà una divisa, en el cas que s'ha comentat anteriorment del fons d'inversió, consistiria a vendre dòlars, així eliminaríem l'exposició a possibles fluctuacions en el tipus de canvi. En el cas que el dòlar es depreciés respecte a l'euro, obtindríem una plusvàlua amb el tipus a futur, donat que prèviament havíem fixat un preu a futur superior a l'actual, el qual

compensaria la caiguda del valor dels actius en euros derivat de la depreciació del dòlar.

Per a determinar la diferència entre el tipus de canvi a futur i l'actual es té en compte el diferencial de tipus d'interès entre els respectius països, això vol dir que la cotització futura de la moneda del país amb els tipus d'interès més elevats ha de ser rebaixada respecte a la moneda amb els tipus d'interès més baixos, així s'evita la possibilitat d'arbitratge.

El que ens costaria cobrir el risc d'aquesta manera seria el corresponent al diferencial de tipus d'interès entre les dues monedes, en aquest cas, entre el tipus d'interès dels Estats Units i Europa.

Per a avaluar com és d'important cobrir el tipus de canvi hem de tenir en compte diferents factors. El primer factor seria la classe d'actiu en la que invertim, ja que si es tracta d'actius amb una baixa volatilitat, el risc de no cobrir la divisa té un pes més rellevant en el risc de la inversió. El segon factor és l'horitzó temporal de la inversió, donat que a llarg termini les fluctuacions s'acostumen a anul·lar i no compensa assumir el cost de la cobertura, en canvi, en inversions a curt i mitjà termini la cobertura pot ser una bona opció per a gestionar el risc. Per acabar, és necessari tenir una visió a futur de la divisa, ja que si creiem que aquesta s'apreciarà més que el cost de la cobertura, la cobertura no estaria justificada.

- Risc de les matèries primeres:

Aquest risc fa referència a les pèrdues financeres que poden ocórrer tant al consumidor com al productor quan hi ha un canvi de preus en els productes bàsics. Un risc per als compradors és que els preus de les matèries primeres pugin, fent que es redueixi el seu marge de benefici si mantenen intacte el preu del producte final, si volen mantenir el marge, hauran d'incrementar el preu del producte final.

Aquest risc afecta principalment als productors, incloent-hi agricultors, empreses mineres, empreses petrolieres i fabricants d'automòbil, ja que la variació de preu en matèries primeres afecta directament als seus *inputs* de producció.

També afecta els consumidors perquè un augment dels preus de les matèries primeres s'acaba traslladant als productes finals que requereixen aquestes matèries en la seva fase de producció.

Alguns dels factors que afecten en aquest risc són els següents:

- Per la part de la política es poden imposar aranzels a les matèries primers. Un exemple per a entendre les conseqüències d'aquest factor és en la guerra comercial entre els EUA i Xina, on en el 2018 EUA va imposar aranzels a les importacions de l'acer i alumini de Xina com a represàlia del que consideraven practiques comercials deslleials per part de Xina. Aleshores, Xina va respondre imposant aranzels a les importacions de productes agrícoles, automòbils i altres productes dels EUA. A conseqüència dels aranzels, els consumidors estatunidencs van veure un augment en els preus dels productes que depenien de l'acer i l'alumini. Els agricultors nord-americans es van trobar amb barreres en el mercat xinès per als seus productes agrícoles, això va provocar una disminució de les exportacions i la caiguda de preu dels productes agrícoles dels EUA. Per l'altra part, la disminució d'exportacions de Xina als EUA va tenir un impacte negatiu en l'economia xinesa i les empreses que depenien del mercat nord-americà.

- Un altre factor important és les condicions climàtiques, ja que en períodes de secada o d'inundació les collites es veuen perjudicades fent que augmenti el preu de productes que requereixen les matèries primeres afectades.

- La innovació tecnològica juga un paper important. Un exemple és quan aquesta innovació permet descobrir i accedir a nous jaciments de matèries primeres, això pot tenir un impacte significatiu augmentant l'oferta de les matèries i influint en el seu preu. Un altre cas on es veu l'efecte de la tecnologia és en l'augment de l'eficiència en el processament de les matèries aconseguint una producció més eficient i econòmica, això pot augmentar l'oferta i disminuir els preus. Quan es desenvolupen tecnologies alternatives poden afectar la demanda d'algunes matèries, un exemple que està en ple creixement és el de les energies renovables, on la solar i l'eòlica poden reduir la demanda de combustibles fòssils. En últim lloc, un efecte indirecte és que la tecnologia pot influir en la demanada de matèries primeres a través de modificar els patrons de consum, això ho veiem en l'augment en la demanda de dispositius electrònics, incrementant la demanda de les matèries que s'utilitzen per a fabricar els components dels dispositius.

Per a fer front a les fluctuacions dels preus causades per la gran diversitat de factors que acabem de veure, existeixen les cobertures de futurs per a protegir tant als consumidors com als productors contra els moviments de preu. El productor té el risc que els preus baixin, i els consumidors tenen el risc que els preus augmentin.

3.1.3. Risc de concentració

Aquest terme es refereix al nombre de préstecs que un banc ha concedit i que encara estan pendents de pagament, en relació amb la quantitat i el tipus de persones o entitats que han rebut aquests préstecs. Els bancs utilitzen l'avaluació d'aquest risc financer per a mantenir un equilibri entre els dipòsits i el valor dels préstecs.

Aquest risc també té en compte la naturalesa dels préstecs, això inclou la identificació de si un percentatge significatiu dels préstecs tenen un propòsit similar, com per exemple, hipoteques o prestes al consum.

Classificar els prestes i determinar el percentatge que es té de cada classe pot ajudar a determinar el nivell de risc de concentració que té el banc en un sector determinat.

Per a mantenir el risc baix a vegades això s'aconsegueix assegurant-se que els tipus de préstecs amb més risc no superin un cert percentatge dels préstecs totals que estan actualment actius.

Si el banc perd clients, la seva capacitat de generar ingressos i administrar els préstecs es veurà compromesa, el que pot fer que augmenti el risc de concentració, si el risc es torna massa alt i el banc no té suficients actius en balanç per a protegir la quantitat total dels préstecs en dificultats, podria córrer el risc de fer fallida.

3.1.4. Risc operacional

El risc operacional és tota possible contingència que pugui provocar pèrdues a una empresa, en aquest cas entitats bancàries, causades d'errors humans, error tecnològics, de processos interns defectuosos o fallits, o arran d'esdeveniments externs com fraus.

Aquest tipus de risc és inherent a tots els sistemes i processos realitzats per humans. Actualment, aquest risc té un gran impacte en les organitzacions, va ser des de la seva reglamentació en l'acord de Basilea II quan en el sector financer es van adonar de la seva importància i van desenvolupar mesures i programes de gestió del risc operacional.

Les empreses per a detectar, avaluar i contenir aquest risc utilitzen el Sistema d'Administració de Risc Operacional, un conjunt de polítiques, procediments, estructures organitzacionals i informació, entre altres.

Els principals factors del risc operacional són els següents:

- Processos interns: possibles pèrdues financeres relacionades amb procediments mal dissenyats o inexistents que poden traduir-se en un desenvolupament deficient dels serveis de l'empresa.
- Processos externs: les empreses són susceptibles de ser afectades per esdeveniments externs al control de l'empresa, per què poden alterar el desenvolupament de les seves activitats.
- Recursos humans: les empreses estan condicionades a possibles errors, negligències, fraus o robatoris provocats pels treballadors.
- Tecnologia: aquí entren les possibles pèrdues provocades per bretxes en la seguretat informàtica, errors d'implementació i programació de plataformes tecnològiques, ús de tecnologies incompatibles entre si.

Hi ha diferents enfocaments per a mesurar el risc operacional, segons el Comitè de Basilea són tres:

- L'enfocament d'indicador bàsic (BIA) és molt més simple que les altres tècniques per a mesurar el risc operatiu i és recomanable per a entitats financeres petites amb operacions no molt complexes. Aquest mètode calcula el risc per a tota l'organització i després l'assigna el resultat a les línies operatives. L'indicador es mesura com un percentatge de l'ingrés brut sobre el dels tres anys anteriors.
- Segons l'enfocament estàndard (SA), les activitats dels bancs estan dividides en vuit línies de negoci: finances corporatives, vendes i negociació borsària, banca minorista, banca comercial, pagaments i liquidacions, serveis d'agència, administració d'actius i corretatge minorista. Dintre de cada línia l'ingrés brut serveix com a indicador per a mesurar l'escala de les operacions comercials i per a calcular la possible exposició al risc operacional de cada línia. Per a calcular-la, s'agafa la mitjana dels tres anys de la suma dels càrrecs de capital per cada línia operativa en cada any.
- L'enfocament de mesura avançada (AMA) és el mètode més sofisticat dels tres, amb aquest model els bancs poden crear el seu propi model empíric per a quantificar el capital requerit per al risc operacional. El marc del model AMA ha d'incloure l'ús de quatre elements quantitatius per a la seva elaboració: dades internes de pèrdues, dades externes, anàlisis d'escenaris i entorn empresarial o factors de control intern. Dintre dels models AMA existeixen tres tipus diferents de metodologies: enfocament de mesura interna (IMA), enfocament de distribució de pèrdues agregades (LDA) i quadres de comandament.

Gràcies als plantejaments introduïts pel Comitè de Basilea les entitats poden realitzar una adequada quantificació del risc operacional i això els hi permetrà operar sense exposar-se a perills.

Per a reduir el risc operacional és important identificar els factors interns que poden afectar els processos i avaluar-los correctament per a analitzar el seu impacte en l'entitat i crear un

pla d'operacions en el que es desenvolupi l'estratègia i decisions a prendre per a mitigar el risc.

3.1.5. Risc de país

El risc de país és la probabilitat que es produeixi una pèrdua financera per circumstàncies macroeconòmiques, polítiques o socials en un país determinat. Aquest risc comprèn el risc d'impagament del deute extern sobirà (risc sobirà), i del deute extern privat quan el risc de crèdit es deu a circumstàncies alienes a la situació de solvència o liquiditat del deutor privat. A part també hi ha altres riscos com els de confiscació, expropiació i nacionalització de les inversions estrangeres, incompliment dels contractes, riscos de guerra i violència política.

Un altre concepte dintre del risc país és el del risc polític, aquest seria el derivat d'accions i decisions polítiques concretes.

Alguns exemples d'accions del risc polític podrien ser:

- Promoure lleis i regulacions que afectin el funcionament de les entitats bancàries.
- Es decideix augmentar els impostos a les entitats financeres, això pot reduir els seus beneficis.
- Els polítics decideixen nacionalitzar entitats financeres en situacions de crisis.

Un augment en el risc país es reflecteix directament en l'increment del cost del deute sobirà del país, però a més, també té efectes de difusió negativa, ja que dificulta el finançament de les empreses. Aquest escenari desincentiva l'execució de projectes d'inversió, el qual s'acostuma a traslladar en una reducció del creixement econòmic del país.

Com més arriscat sigui invertir en un país, major seran els interessos que els inversos demanaran per prestar-li diners.

3.1.6. Risc de liquiditat

El risc de liquiditat en l'àmbit de les finances és el risc que un actiu s'hagi de vendre a un preu menor al del mercat a causa de la seva escassa liquiditat. En canvi, en l'àmbit de l'economia, mesura l'habilitat d'algú d'afrontar les seves obligacions a curt termini.

En el món de les finances, quan un actiu és poc líquid significa que no es negocia de manera freqüent, un exemple seria l'habitatge o alguns bons, sobretot els que es van emetre fa molt temps. Quan es necessita vendre de manera urgent un actiu poc líquid, hi podria haver molt pocs compradors interessats, això faria que si aquests pocs compradors no estan

disposats a pagar el preu actual, hauria de disminuir el preu per atraure més compradors i podré vendre l'actiu. Per tant, el risc de liquiditat és més alt en mercats que tenen poca profunditat de mercat i poca liquiditat.

En la renda fixa com pitjor és la qualitat creditícia de l'emissor major és el risc de liquiditat.

A continuació ens centrarem en el risc de liquiditat bancari, en aquest cas es produeix quan una entitat financera no pot atendre les peticions de reemborsament i liquidació dels seus clients. Els bancs agafen els diners que dipositen els clients i una part la guarden com a reserva, això és el que es coneix com el coeficient de caixa, aquest coeficient indica el percentatge dels diners ingressats que s'han de mantenir en reserves líquides, no es pot utilitzar per a inversions ni préstecs. La resta de diners que no han de mantenir en reserva els fan servir per a préstecs i inversions, d'aquí és d'on surten els beneficis del banc. És per aquest motiu que en situacions on es creu que el banc no serà capaç de tornar els dipòsits per una mala gestió de les inversions o un augment de l'impagament dels pagaments dels clients, això provoca que molts clients del banc vulguin retirar els diners, aquesta situació pot empitjorar la situació de liquiditat del banc i generar una crisi financera si no es gestiona adequadament.

La Gestió de Riscos de liquiditat és, per tant, vital per a un banc. Després de la crisi global del 2008, un comitè internacional va establir els acords de Basilea III, que fixen noves formes d'abordar aquest risc. L'objectiu d'aquests acords és millorar la resistència de les entitats financeres davant de pertorbacions de liquiditat.

L'acord de Basilea III crea dos estàndards:

- El primer estàndard és el coeficient de cobertura de liquiditat (LCR). Té l'objectiu d'augmentar les reserves d'actius líquids d'alta qualitat, d'aquesta manera les entitats de crèdit poden suportar situacions d'estrès.
- El segon estàndard és el coeficient de finançament estable net (NSFR). Té un caràcter més estructural i a llarg termini. Amb ell es pretén assegurar un finançament més estable mitjançant passius a mitjà o llarg termini i així afrontar condicions d'estrès més prolongades.

Ambdós estàndards es complementen amb una sèrie d'eines per al seguiment de l'exposició del risc de liquiditat.

Per a la gestió dels riscs estructurals i de la planificació financera en les entitats, s'utilitza els anomenats procediments ALM (*Asset Liabilities Management*). Es tracta d'un conjunt de tècniques per assegurar una correcta presa de decisions d'inversió i finançament. Dintre de l'anàlisi ALM s'inclouen els riscos de tipus d'interès, de liquiditat i de tipus de canvi.

Quant a la rendibilitat, les entitats bancàries compten amb un objectiu de benefici per repartir entre els accionistes. L'activitat lucrativa dels bancs està limitada per la necessitat de liquiditat per fer front a les demandes de diners dels seus dipositats i la solvència. D'aquesta manera, el valor de realització dels seus actius no ha de ser inferior al valor dels seus dipòsits.

3.1.7. Risc legal

El risc legal és la possibilitat d'incórrer en pèrdues a causa de l'incompliment de la legislació que afecta els contractes financers, o la impossibilitat d'exigir el compliment del contracte legalment. Aquest risc també inclou el risc de canvi de regulació per part de les autoritats competents de la normativa, de manera que afecti negativament la posició de l'empresa o entitat financera.

Aquest risc s'ha de tenir en consideració des de tots els departaments de l'empresa perquè afecta diferents entorns. Els principals tipus són:

- Corporatius: són fruit de la naturalesa i estructura legal de l'organització. Són els riscos fiscals, els de responsabilitat civil, absència de documentació, etc.
- Riscos d'actius: tenen a veure amb la protecció del valor dels actius tangibles i intangibles.
- Els riscos legals contractuals: són riscos assumits voluntàriament per la signatura de contractes, errors als contractes, incapacitat de l'empresa de complir el que s'ha pactat, cancel·lació de contractes, etc.
- Els riscos de litigi: estan relacionats amb la resolució de disputes en els tribunals, fruit de demandes, conducta d'empleats, entre altres. Quan hi ha aquest tipus de risc el valor de mercat de les accions d'una empresa cauen a conseqüència de la incertesa del veredicte.
- El risc de regulació: implica la imposició de sancions per infraccions i el canvi de lleis que puguin afectar negativament en l'empresa. Com per exemple, canvis en la regulació del comerç, les regulacions fiscals, entre altres.
- Riscos constitutius: apareixen en el moment de la constitució de la societat. Afecta la denominació de l'empresa i la regulació del tipus d'empresa.
- Els riscos territorials: aquí s'inclourien els tractats, sentències vinculants, normatives de la Unió Europea, normativa internacional, etc.
- Riscos extintius: són riscos legals relacionats amb concursos, fallides o liquidacions.

Les amenaces que resulten de l'incompliment d'obligacions legals i contractuals s'han de tenir en consideració a l'efecte de disposar d'un mapa de riscos complet, així com un sistema de gestió que permeti identificar-los, valorar-los i gestionar-los de manera adequada.

Una correcta gestió dels riscos legals és imprescindible en un sector molt regulat com el financer.

3.2. Tipus de fraus

Ara que ja hem introduït els principals riscos dels bancs ens centrarem en un en específic, que està inclòs en el risc operacional, el frau en targetes de crèdit.

Primer de tot introduirem el concepte de frau, aquest terme es refereix a l'acte intencional que té com a objectiu enganyar a una persona o entitat per a obtenir un benefici o un avantatge indegut. Alguns exemples de possibles fraus dintre del sistema financer són per exemple el blanqueig de diners, manipulació del mercat, el robatori d'identitat, la falsificació de xecs, l'ús de targetes de crèdit robades, entre altres.

Ara ens centrem en el tema principal del treball, el frau en targetes de crèdit. És un tipus de frau financer en el qual s'utilitza de manera il·legal una targeta de crèdit o dèbit per a realitzar transaccions no autoritzades. Aquest frau és una amenaça constant per als usuaris i les entitats financeres, i la seva prevenció és crucial per evitar pèrdues econòmiques i danys en la reputació de les empreses.

A continuació s'explicaran les diferents formes que utilitzen els delinqüents per a obtenir accés a la informació financera del titular de la targeta per a produir el frau, es parlarà des del robatori fins al *phishing* i el *skimming*, entre altres.

En primer lloc, el robatori de targetes és quan algú roba la targeta d'una altra persona i la utilitza de manera il·legal. En aquest cas el que es recomana fer és anul·lar la targeta el més ràpid possible, contactar amb l'entitat financera per a informar el frau, presentar una denúncia a la policia i notificar qualsevol transacció sospitosa que aparegui.

El *skimming* és la captura i transferència no autoritzada de dades de pagament a una altra font amb la finalitat de cometre frau. Els lladres poden robar les dades directament de la targeta o de la infraestructura de pagaments d'un establiment, ambdues tècniques requereixen un dispositiu físic deshonest.

Un tipus de *skimming* és quan s'aconsegueixen les dades de la targeta directament del dispositiu de pagament del consumidor, es fa utilitzant un lector de targetes petit i portàtil, i acostuma a involucrar personal de l'establiment. És du a terme quan la targeta la té el treballador i el consumidor no l'està veient.

Un altre tipus és quan la captura de les dades succeeix dintre de la infraestructura de pagament del comerciant, tant pot ser que la terminal del punt de venda estigui compromesa o que ho estigui la infraestructura. Els delinqüents insereixen equips electrònics en la

terminal o la infraestructura per a aconseguir les dades dels consumidors. En aquest cas ni el comerciant ni el consumidor en són conscients.

Un altre cas es pot donar a través de tecnologies de xarxes sense fil, com *Bluetooth* i Wi-Fi que permeten transmetre informació entre dispositius. Quan aquestes tecnologies no estan ben xifrades o són xarxes Wi-Fi compartides o sense seguretat, les dades poden ser interceptades.

Per a evitar aquest frau hi ha els sistemes anti-*skimming*. El primer consisteix a xifrar la informació en la banda magnètica de la targeta per a impedir que els delinqüents puguin accedir a la informació. El segon sistema detecta l'existència d'un dispositiu en l'entrada de targetes del caixer automàtic i el bloqueja, per a impedir que l'usuari pugui introduir la seva targeta. Per acabar, hi ha sistemes electrònics que disposen de sensors òptics i infrarojos amb la funció de bloquejar el lector de targetes en cas que es detecti algun dispositiu fraudulent.

Alguns consells per a protegir-te del *skimming* són:

- En un establiment mantenir la targeta a la vista en tot moment per a assegurar-te que només s'utilitza en la màquina de venda.
- No compartir el PIN de la targeta amb ningú.
- Verificar l'extracte de la teva targeta per a identificar possibles transaccions fraudulentes al més aviat possible.

A continuació, es parlarà sobre una altra tècnica utilitzada per a cometre frau amb targetes de crèdit, el *phishing.*

El *phishing* és una de les estafes més antigues i més conegudes. Es podria definir com un frau en les telecomunicacions que utilitza l'enginyeria social per a obtenir dades privades de les víctimes.

L'atac es du a terme a través de mitjans electrònics com poden ser el correu, SMS o una trucada de telèfon. L'atacant es fa passar per una persona o organització de confiança amb l'objectiu d'obtenir informació confidencial com podria ser el número de la targeta de crèdit.

El missatge que s'envia té la finalitat de persuadir a la víctima perquè cliqui en un enllaç, es descarregui un arxiu o enviï informació. Amb les xarxes socials els atacants poden aconseguir informació de la persona per a fer que l'engany estigui personalitzat i així sigui més creïble.

Alguns consells per a protegir-te del *phishing* són:

- Quan rebis correus electrònics, SMS o trucades demanat informació personal sempre has de verificar l'autenticitat del missatge abans de proporcionar la informació.
- Quan entris en un URL assegurat que és autèntic, ja que webs fraudulentes acostumen a tenir URL similars a les de les webs llegítimes.
- Evita obrir enllaços sospitosos que rebis per correu electrònic sense prèviament haver verificat l'autenticitat de l'enllaç.
- No comparteixis informació personal com contrasenyes o el número de targeta.
- Utilitza eines de seguretat com antivirus i *Firewall* per a protegir-te de pàgines web i correus electrònics fraudulents.

L'últim tipus de frau en les targetes de crèdit a veure és el SIM *swapping*, es dona quan algú ha fet un duplicat de la targeta SIM per a poder rebre SMS amb el codi de confirmació que algunes pàgines o bancs envien al mòbil perquè autoritzis una operació per internet.

Els delinqüents poden obtenir el duplicat de la targeta SIM de manera presencial o aconseguir-la per telèfon, depenent de l'operadora mòbil que tinguis, si bé la nostra companyia hauria d'identificar d'alguna manera el titular, mitjançant preguntes personals o ensenyant el DNI, per a assegurar-se que la persona que està demanat la targeta SIM és qui ha de ser, el problema és que a vegades aquesta mesura de seguretat pot ser vulnerada. Una vegada que s'activa la SIM duplicada la que tens es desactiva automàticament, et quedes sense internet i sense poder fer trucades. Si et passa això s'hauria de contactar immediatament amb la teva operadora perquè et confirmi si algú ha fet un duplicat sense el teu permís.

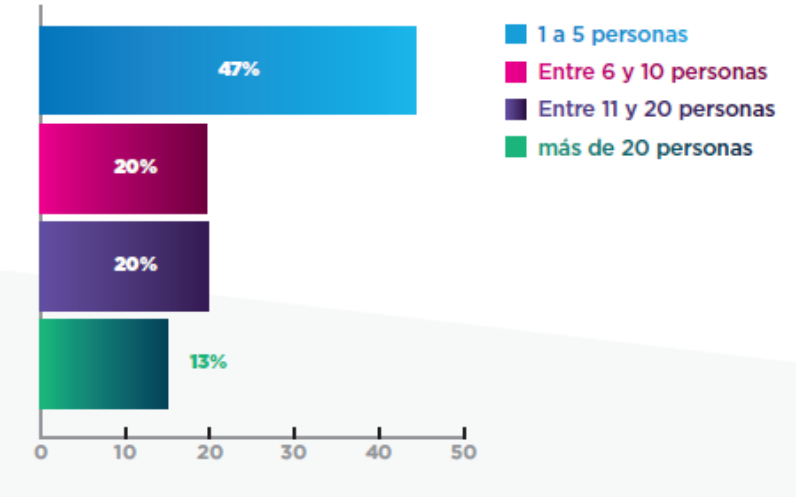
3.3. Estadístiques i dades rellevants sobre el frau en Espanya:

A continuació abordarem un dels temes principals del treball i que és de gran rellevància en l'entorn empresarial, el frau, i en aquest cas enfocat a Espanya. En els darrers anys, hem viscut un augment significatiu de pràctiques fraudulentes que han impactat negativament a les empreses. El desenvolupament tecnològic i els canvis en els hàbits de consum han obert noves oportunitats per als estafadors, plantejant reptes importants per a la protecció i la seguretat de les organitzacions i els clients. A continuació explorarem amb més detall la situació actual del frau a Espanya, analitzant-ne l'impacte, els sectors més afectats i les mesures que s'estan prenent per combatre aquest problema.

Les estadístiques presentades a continuació provenen de l'informe sobre l'estat del frau a Espanya, elaborat per l'Associació Espanyola d'Empreses contra el Frau de l'any 2021-2022. Aquest informe ens ofereix una visió detallada i actualitzada sobre la situació del frau a Espanya, aquesta informació ens serveix per entendre millor i poder afrontar el problema des de l'àmbit empresarial i social.

Pel que fa a la prevenció del frau en les empreses, un 73% dels casos són detectats pels departaments de frau, un 20% dels casos són detectats per les àrees de riscos, mentre que el 7% restant són localitzats pels departaments d'operacions.

Aquestes dades evidencien la importància de preveure el frau dins de les organitzacions, per aquest motiu es creen departaments especialitzats en aquestes àrees clau com el frau i els riscos. Això ens mostra que les empreses estan prenent mesures proactives per combatre i mitigar els riscos associats al frau, d'aquí sorgeix la necessitat de comptar amb estratègies i recursos dedicats a la seva prevenció i detecció.



Gràfic 1. Dotació de recursos per a la gestió d'incidents en matèria delictiva.(AEECF, 2021-2022)

En el gràfic veiem que tot i la necessitat de disposar de mecanismes per a preveure el frau, el nombre de recursos destinats a l'anàlisi i seguiments dels casos de frau en la majoria dels negocis no supera les 5 persones. Només el 13%, principalment del sector de la gran banca i telecomunicacions, disposa d'equips de més de 20 persones per a gestionar incidents relacionats amb el frau.

Més de la meitat de les empreses afirma haver detectat un augment en els intents i casos de frau en comparació els anys anteriors. Això ens mostra com tot i estar creant una estructura cada vegada més consolidada i segura contra les estafes, el frau continua proliferant gràcies a noves metodologies que aconsegueixen vulnerar les mesures antifrau.

No només s'ha observat un augment en els intents i casos de frau, sinó que també les pèrdues s'han fet més grans en la majoria dels negocis. Sobre les quantitats dels fraus, el 74% de les empreses declara una pèrdua mitjana per cada cas de frau inferior als 5.000 €, en canvi, el 7% comunica una pèrdua mitjana per cada cas de més de 50.000 €, aquests casos es produeixen principalment en el sector de les telecomunicacions.

Tot i que la majoria coincideix en el fet que el frau afecta a totes les zones geogràfiques, a l'hora de detectar les regions amb més incidència de frau, destaquen quatre regions: Catalunya, Madrid, València i Andalusia.

Ara parlarem sobre les característiques del perfil de les persones defraudades utilitzant la informació que ens proporcionen les empreses.

Si analitzem per edat, veiem que una àmplia majoria, en concret un 73%, considera que el frau afecta a totes les edats per igual. Tot i això, hi ha una part minoritària que destaca les franges de 25 a 45 anys i dels 45 als 60 anys com les més predisposades a ser estafades.

En l'àmbit laboral podem veure una diferència d'opinions més marcades que en l'edat. El 33% apunta que el frau afecta a totes les situacions laborals, mentre que un altre 33% considera que les persones actives laboralment, tant per compte propi com per compte aliè, són les més perjudicats. De la resta de persones no es compta amb suficient informació

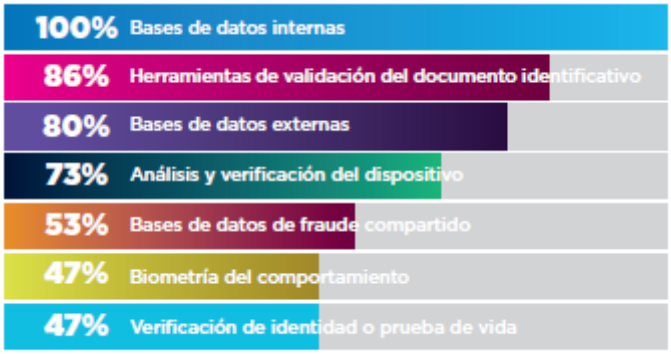
En relació amb el tema dels ingressos, la major part de les entitats manca d'aquesta informació dels seus clients, per tant, només el 20% dels enquestats indica que el frau sol afectar més a persones amb ingressos superiors a la mitjana.

La major part de les empreses, un 67%, assegura que els clients nous, referint-se a persones físiques, són la principal víctima en la majoria dels fraus, en canvi, quan parlem de clients que fa temps que utilitzen els serveis de l'empresa, només un 20% diu que aquests clients són els principals afectats del frau. Quan es tracta de persones jurídiques, només el 13% de les empreses posicionen aquesta figura com a principal afectada de la major part dels fraus.

Veiem que els resultats no ens permeten detectar un perfil concret de personar defraudada, això és degut al fet que el frau afecta pràcticament a tota la societat.
El canal a través del qual s'estan produint els fraus és en la majoria de les empreses al canal en línia. El segon canal que destaca és el telefònic. Aquests resultats confirmen la tendència creixent en el frau a través de canals en línia a causa dels canvis de consum i l'augment de les transaccions en línia, per això, és important augmentar les mesures de seguretat en entorns digitals.

El principal tipus de frau és el frau d'admissió a punts de venda digitals, amb un 33% del total dels casos. En segon lloc, amb un 27%, hi ha el frau de compte, aquest consisteix en l'inici de transaccions fraudulentes després d'accedir de manera il·lícita al compte d'un client. En tercer i quart lloc, amb un 20% cadascun, hi ha el robatori de dades i el frau d'admissió en punts de venda físics. Si mirem com s'originen aquests fraus, descobrim que en el 40% de les empreses enquestades, la principal causa és la suplantació d'identitat, també cal

destacar que la identitat en línia inventada també ocupa un lloc significatiu. Per al 26% de les empreses el principal origen del frau sorgeix de la manipulació de documents d'identitat.



Gràfic 2.Eines per a lluita contra el frau més aplicades.(AEECF, 2021-2022)

Per a preveure el frau, les solucions tecnològiques continuen sent les protagonistes en les empreses. Aquestes solucions cada vegada es reforcen més per a protegir-se contra l'enginyeria social cada cop més sofisticada i l'aparició de noves tipologies de frau. En el gràfic 2 veiem les iniciatives més utilitzades on, en primer lloc, hi trobem les bases de dades internes, utilitzades en un 100% de les empreses enquestades. En segon lloc, hi trobem les eines de validació de documents identificatius, emprat en el 86% de les empreses. En tercer lloc, hi trobem les bases de dades externes amb un 80% d'ús. A continuació hi trobem altres eines com l'anàlisi i verificació de dispositius amb un 73%, l'ús de bases de dades de frau compartit amb un 53%, biometria del comportament i la verificació d'identitat o prova de vida, amb un 47% cadascuna. Aquí veiem com les empreses adopten diferents eines i tecnologies per reforçar els sistemes de protecció. La valoració mitjana d'aquestes eines per part de les organitzacions és d'un 7,83 sobre 10.

Les eines anteriorment comentades també presenten alguns problemes, on el principal problema és la falta d'automatització, això genera la necessitat de la revisió constant per part d'un gestor. A aquesta primera dificultat l'acompanya els falsos positius, la falta de compartir dades entre entitats, la difícil implementació de les eines i la informació insuficient per a prendre decisions.

Els resultats apunten a l'automatització en la presa de decisions com el principal repte a afrontar per part de les empreses a curt i mitjà termini. Un altre repte és la migració dels clients del canal presencial al canal en línia sense que l'experiència es vegi afectada, s'ha de trobar un equilibri entre seguretat i comoditat del client. Altres objectius a destacar són per exemple, la identificació i prevenció de grups organitzats involucrats en activitats fraudulents i l'accés a noves fonts d'informació per a la detecció del frau. Aquestes estratègies han d'evolucionar ràpidament per a fer fronts als delinqüents, tant a Espanya com en l'àmbit global.

3.4. Models ML

L'aprenentatge automàtic és un camp de la intel·ligència artificial que està dedicat al disseny, anàlisi i el desenvolupament d'algorismes i tècniques que permeten que les màquines evolucionin. És un camp multidisciplinari perquè combina ciències com la computació, les matemàtiques, la lògica i la filosofia per crear programes que puguin generalitzar comportaments a partir del reconeixement de patrons o classificació i de sistemes capaços de resoldre problemes per si mateixos, utilitzant com a paradigma la intel·ligència humana.

Els algoritmes de *Machine Learning* es divideixen en tres categories:

- Models d'aprenentatge supervisat: en aquest tipus de models s'utilitza un conjunt de dades etiquetades per a entrenar el model, aquestes dades inclouen les entrades i les sortides, les entrades són les característiques d'un registre i la sortida és una etiqueta o el valor desitjat.
  L'objectiu és aprendre a predir la sortida per a nous registres donades les característiques d'entrada. Això vol dir que el model ha de ser capaç de generalitzar a partir de les dades d'entrenament i fer prediccions precises sobre dades no vistes prèviament.

- Models d'aprenentatge no supervisat: aquests models s'utilitzen en bases de dades on no es tenen ni etiquetes ni informació de la sortida per a entrenar els models.
  L'objectiu és descobrir patrons, estructures o relacions amagades en les dades, això s'aconsegueix deixant que l'algoritme d'aprenentatge automàtic interpreti grans conjunts de dades i intenti organitzar aquestes dades per a descriure'n l'estructura. A mesura que aquests models avaluen més dades la seva capacitat per prendre decisions millora gradualment.

- Models d'aprenentatge per reforç: aquests models es basen en els processos d'aprenentatge reglamentats, en què es proporcionen algoritmes d'aprenentatge automàtics amb un conjunt d'accions, paràmetres i valors finals.
  En definir les regles, l'algoritme d'aprenentatge automàtic intenta explorar diferents opcions i possibilitats, supervisant i avaluant cada resultat per determinar quin és l'òptim.
  Per tant, aquest sistema ensenya la màquina a través del procés d'assaig i error. Aprèn d'experiències passades i comença a adaptar-ne l'enfocament en resposta a la situació per aconseguir el millor resultat possible.

En el nostre cas d'estudi, la detecció d'anomalies, és un problema on no tenim etiquetes que ens indiquin si les transaccions són anòmales o no, per tant, haurem d'utilitzar models d'aprenentatge no supervisats.

Un dels principals avantatges d'aquest tipus de models és que et permeten descobrir patrons i informació nova i inesperada sobre les dades i aquests coneixements es poden emprar per a prendre decisions, identificar oportunitats o millorar alguns processos.

El principal desavantatge dels models no supervisats és que com que no tenim etiquetes ni informació de la sortida de les dades, pot ser més difícil avaluar i mesurar la qualitat dels resultats. No hi ha cap mesura que ens digui com de bé el model ha après i descobert patrons importants en les dades, això dificulta la comparació entre models.

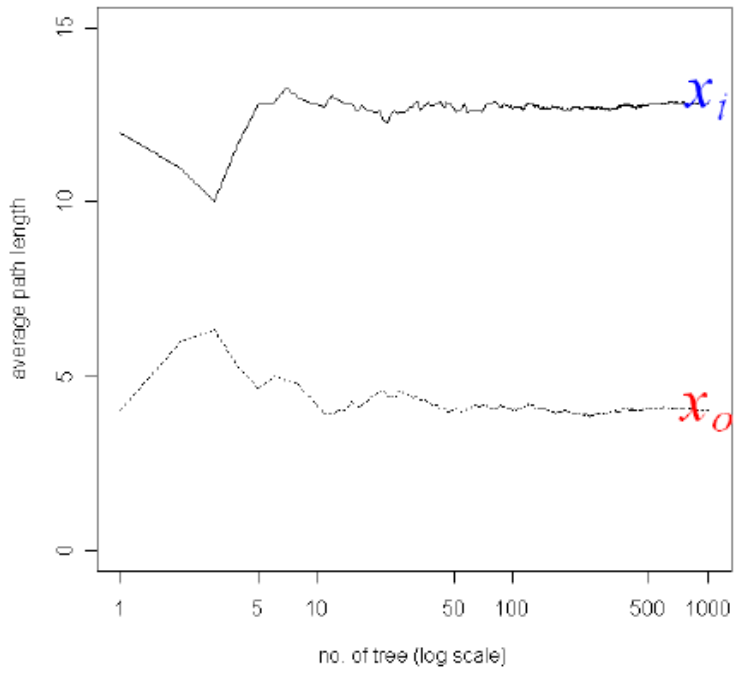
A continuació ens centrarem en el model *Isolation Forest* (*iForest*), una tècnica d'aprenentatge no supervisat que farem servir per a analitzar el nostre cas d'estudi.

3.5. Isolation Forest

La majoria d'enfocaments basats en models per a la detecció d'anomalies construeixen un perfil d'instàncies normals i, a continuació, identifiquen les instàncies que no s'ajusten al perfil normal com a anomalies. Aquest model aïlla explícitament les anomalies en lloc de perfilar els punts normals. Un inconvenient dels models que utilitzen l'enfocament de perfilar punts normals és que el detector d'anomalies està optimitzat per perfilar instàncies normals, però no optimitzat per detectar anomalies, com a conseqüència, pot ser que la detecció d'anomalies no sigui tan bona com s'esperava, causant moltes alarmes falses. Un altre inconvenient és que es limiten a dades de dimensions baixes a causa del seu alt cost computacional.

En un arbre aleatori induït per dades, la partició de les instàncies es repeteix de forma recursiva fins que totes les instàncies s'aïllen. Aquesta partició aleatòria produeix camins notablement més curts per a anomalies, ja que menys instàncies d'anomalies donen lloc a un nombre menor de particions. Un altre motiu pel qual els camins són més curts quan representen possibles anomalies, és pel fet que les instàncies amb valors d'atributs distingibles tenen més probabilitats de separar-se en les primeres particions.

Per a veure de manera gràfica el que acabo d'explicar comentaré el següent gràfic:



Gràfic 3. Longitud mitjana dels camins. (Fei Tony Liu i Kai Ming Ting, 2008)

En aquest cas està representat en l'eix d'abscisses el nombre d'arbres creats i en l'eix d'ordenades el nombre mitjà de la longitud del camí fins a arribar als punts x_o i x_i, on x_o és una anomalia i x_i és un punt normal. El que veiem en el gràfic és que utilitzant 1000 arbres la longitud mitjana del camí de x_o i x_i convergeixen aproximadament a 4 i 13 respectivament. Això ens mostra que les anomalies tenen recorreguts més curts que instàncies normals.

Per explicar els fonaments matemàtics del model primer introduirem dos conceptes importants.

Arbre d'aïllament, en anglès *isolation tree*, sigui T un node d'un arbre d'aïllament. T és un node extern sense fill, o un node intern amb una prova i exactament dos nodes fills (T_l,T_r). Una prova consisteix en un atribut *q* i un valor dividit *p* de manera que la prova $q < p$ divideix els punts de dades en T_l i T_r.

La longitud del camí *h(x)*, en anglès *path length*, d'un punt x es mesura pel nombre d'arestes que x travessa en arbre d'aïllament (*isolation tree*) des del node arrel fins que el recorregut s'acaba en un node extern.

Com a mètode de detecció d'anomalies requereix una puntuació d'anomalia. La dificultat per obtenir aquesta puntuació a partir de *h(x)* és que mentre la màxima alçada possible de l'arbre d'aïllament creix en l'ordre de *n*, l'alçada mitjana creix en l'ordre de log(n). La

normalització de *h(x)* per qualsevol dels termes anteriors no està limitada o no es pot comparar directament.

A causa de la seva similitud, agafem l'anàlisi de BST (Binary Search Tree) per a estimar la longitud mitjana del camí d'un arbre d'aïllament. Donat un conjunt de dades de *n* instàncies, ens dona la longitud mitjana del camí com:

$$c(n) = 2H(n-1) - (\frac{2(n-1)}{n})$$

On *H(i)* és el nombre harmònic i es pot estimar com ln(i) + 0.5772156649 (constant d'Euler). Com *c(n)* és la mitjana de *h(x)* donat n, s'utilitza per normalitzar *h(x)*. La puntuació d'anomalia *s* d'una instància *x* es defineix com:

$$s(x,n) = 2^{-\frac{E(h(x))}{c(n)}}$$

On *E(h(x))* és la mitjana d'*h(x)* d'una col·lecció d'arbres d'aïllament.

D'aquesta equació podem treure les relacions amb possibles valors d'*E(h(x))*:

- Quan *E(h(x))* sigui igual a *c(n)*, *s* en valdrà 0,5.
- Quan *E(h(x))* sigui igual a 0, *s* en valdrà 1.
- Quan *E(h(x))* sigui igual a *n*-1, *s* en valdrà 0.

A partir d'aquí podem treure les següents valoracions:

- Si les instàncies tornen una *s* propera a 1, aleshores definitivament són anomalies.
- Si les instàncies tenen valors *s* molt més *petits* que 0,5, llavors amb bastant seguretat podem considerar-les com instàncies normals.
- Si totes les instàncies retornen una *s* ≈ 0,5, aleshores la mostra sencera no té cap anomalia.

Com a conjunt d'arbres d'aïllament, *iForest* identifica anomalies com a punts amb camins més curts i té múltiples arbres que ajuden a orientar diferents anomalies. El fet que *iForest* no necessiti aïllar totes les instàncies normals fa que funcioni bé amb models parcials, sense aïllar tots els punts normals i creant models amb una mida de mostra petita.

Al contrari que altres mètodes on una mida de mostreig gran és més desitjable, el mètode d'aïllament funciona millor quan la mida del mostreig es manté petita. Una mida de mostreig gran redueix la capacitat d'*iForest* d'aïllar anomalies, ja que els casos normals poden

interferir amb el procés d'aïllament i, per tant, redueix la seva capacitat d'aïllar clarament les anomalies. Així, el submostreig proporciona un entorn favorable perquè *iForest* funcioni bé.

iForest té una complexitat temporal lineal amb una constant baixa i un requisit de memòria baix, ideal per a conjunts de dades de gran volum. A més, *iForest* convergeix ràpidament amb una petita mida de conjunt, això li permet detectar anomalies amb una alta eficiència.

Per a problemes de grans dimensions que contenen un gran nombre d'atributs irrellevants, *iForest* pot aconseguir un alt rendiment amb un selector d'atributs addicional. També s'ha vist que *iForest* funciona bé fins i tot quan no hi ha anomalies.

En conclusió, *iForest* és un detector d'anomalies precís i eficient, especialment per a grans bases de dades, aquesta última característica és important per a aplicacions de la vida real com és el cas que estudiarem en aquest treball, la detecció del frau en targetes de crèdit.

4. CAS PRÀCTIC

Després de comentar els principals riscos financers i introduir els models d'aprenentatge automàtic, és moment d'endinsar-nos en un cas real on posarem en pràctica els coneixements teòrics adquirits.

Primer, recapitularem els objectius d'aquest cas pràctic, el nostre objectiu és analitzar els registres de transaccions d'un banc i estudiar el nombre de transaccions realitzades en diferents intervals de temps. A partir d'aquests valors agrupats crearem una sèrie temporal que ens permetrà aplicar l'algorisme *Isolation Forest* per a detectar possibles anomalies.

És important destacar que aquest cas d'estudi és no supervisat, per tant, no comptem amb etiquetes o categories predefinides per identificar les anomalies en les transaccions. Per això, utilitzarem un algorisme de detecció d'anomalies no supervisat.

Esperem que l'algorisme ens identifiqui instants on el nombre de transaccions d'un establiment es desviïn significativament dels seus patrons normals. Aquestes anomalies podrien indicar possibles activitats fraudulentes o irregularitat a les operacions del banc. L'objectiu final és implementar aquest algorisme en temps real en el banc per a poder detectar el més ràpid possible les anomalies i poder prendre mesures per a parar el frau.

Al llarg d'aquesta secció es detallarà el procés de creació de la sèrie temporal a partir dels registres de transaccions, així com la implementació de l'*Isolation Forest*.

En últim lloc, cal especificar que aquesta part pràctica del treball va sorgir com a resposta a un problema concret que tenia una entitat financera, i que es va considerar com un cas que es podia abordar dintre d'un treball final de grau.

4.1. Base de dades:

És difícil trobar bases de dades públiques relacionades amb el risc financer o registres de transaccions perquè inclouen informació confidencial dels clients i estan protegides per lleis de privacitat i seguretat.

En aquest cas vaig aconseguir una base de dades d'un petit banc sobre les transaccions dels seus clients, amb prèvia autorització i consentiment, del període compres entre el 23 de desembre del 2022 i el 23 d'abril de 2023, un total de 4 mesos.

Per a obtenir aquestes dades s'ha firmat un contracte de confidencialitat pel qual no es mencionarà el nom del banc i s'anonimitzaran les dades perquè no apareguin noms que puguin identificar el banc amb el qual s'està treballant.

Les dades dels registres de les transaccions estaven recopilats en fitxers de text, on cada arxiu corresponia a les transaccions d'un dia.

Dins de cada fitxer, cada línia feia referència a la informació d'una transacció específica. El format de cada línia estava dissenyat de manera que una part de la cadena de text corresponia a un objecte JSON. Aquest objecte JSON incloïa la informació rellevant on trobem les següents variables que ens seran útils pel treball:

Variable	Descripció
timestamp	Indica la data i hora exacta de la transacció
operationId	Identifica de manera única cada transacció
merchantType	Indica el sector al qual pertany l'establiment
merchantName	Representa el nom de l'establiment on es realitza la transacció
purchaseAmonut	Indica el valor de la compra realitzada

Taula 1. Definició variables.

Aquesta informació es va passar del format JSON a un format estructurat on cada variable era una columna, així era més fàcil manipular i analitzar les dades.

4.2. Anàlisi descriptiu

Sempre que treballem amb una base de dades és necessari dur a terme una anàlisi detallada de les variables presents. Aquest estudi ens permet tenir una visió general de la base de dades, però el seu principal objectiu és identificar la presència de patrons de comportament o anomalies. Si detectem errors en aquesta part del projecte encara som a temps de corregir les dades per a solucionar els problemes. Per això és important estudiar les dades amb les quals treballarem.

En la primera fase de l'anàlisi descriptiva és essencial revisar si existeixen dades faltant o també conegudes com a *missings*, és a dir, observacions que manquen d'informació en una o més variables. Detectar i treballar de manera adequada els missings és fonamental per a garantir la qualitat, funcionament i fiabilitat de les modelitzacions posteriors. En el nostre cas hem vist que la base de dades utilitzada no presenta cap valor faltant, això garanteix una base sòlida a l'hora d'elaborar l'anàlisi i la presa de decisions basades en les dades.

La primera variable és 'operationId', aquesta variable és un índex únic per a cada registre, és un codi que serveix per a identificar cada transacció, ens serà útil quan vulguem comptar el nombre d'operacions que s'han dut a terme en un període concret de temps.

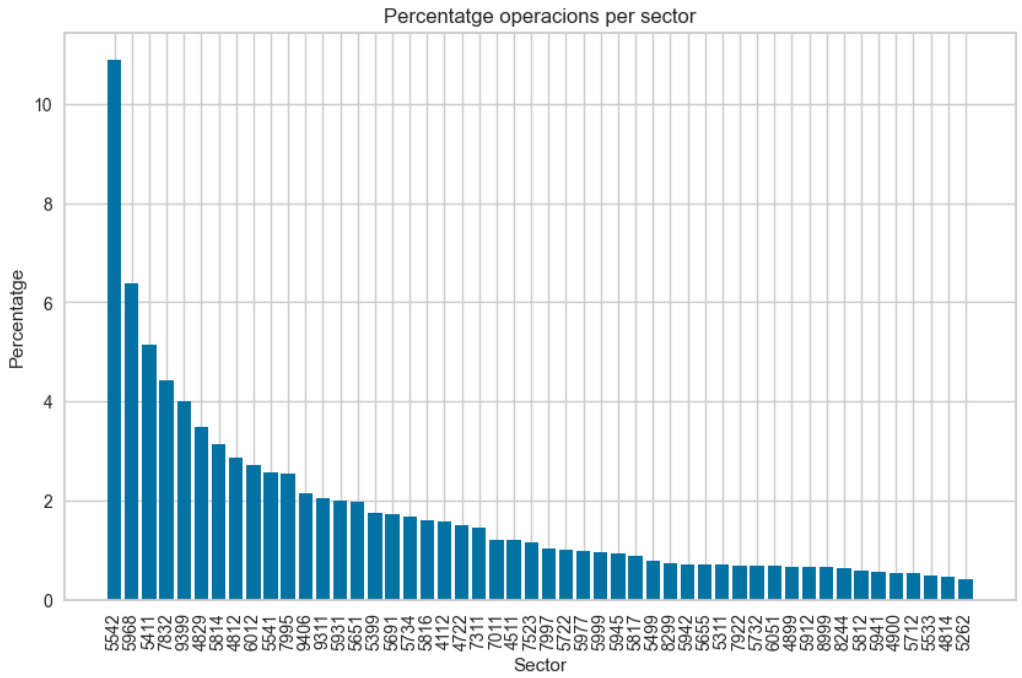
La variable 'timestamp' captura la informació temporal de cada transacció. Aquesta variable representa les dates amb una resolució de nanosegons i la referència a la zona horària és UTC (*Universal Time Coordinated*). Que la zona horària sigui UTC ens assegura que les dades es mantenen consistents i es poden interpretar correctament en diferents contextos i ubicacions geogràfiques. L'ús de la variable en l'anàlisi de dades permet fer un seguiment precís de quan es va dur a terme la transacció.

4.2.1. Variables categòriques

Les variables categòriques són un tipus de variable que representa diferents categories o grups, poden prendre un nombre finit de valors. Les categories poden ser qualitatives o nominals, quan no tenen un ordre, o poden ser ordinals, en aquest cas existeix un ordre específic entre les categories. En la nostra base de dades només tenim dues variables categòriques però en crearem dues més a partir de la variable 'timestamp'.

La variable 'merchatType' és una variable categòrica que representa el codi del sector al qual pertany l'establiment on s'ha realitzat la transacció. Ens proporciona informació sobre la naturalesa del negoci o l'activitat comercial associada a cada transacció.

Tenim un total de 294 tipus de sectors, si ens centrem en els 50 amb més operacions, podem veure que recullen el 88,93% de les operacions.

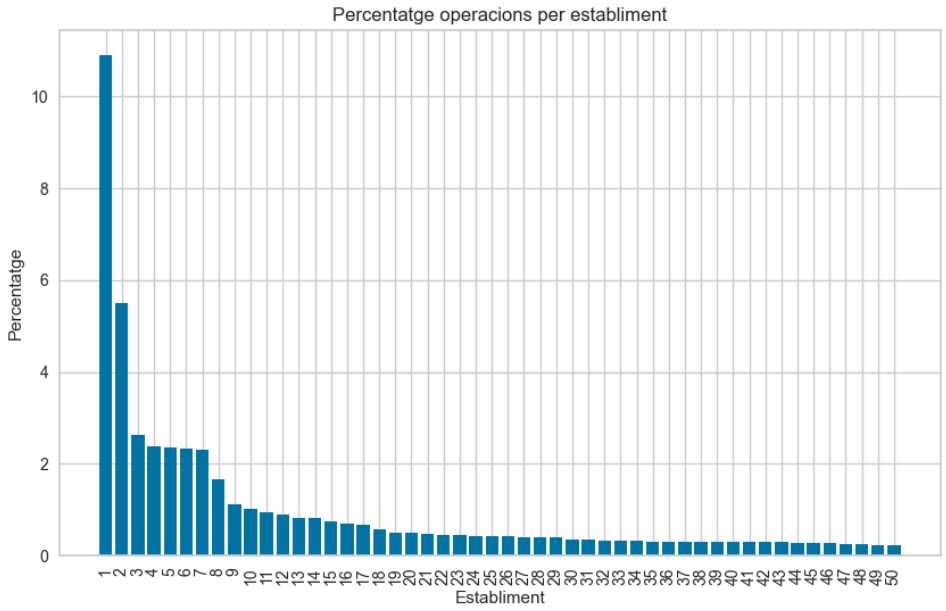


Gràfic 4. Percentatge d'operacions per sector.

Això ens permet veure com el consum està centrat en pocs sectors.

La variable 'merchantName' és una variable categòrica que ens mostra el nom de l'establiment on s'ha dut a terme la compra. L'anàlisi de la variable 'merchantName' pot proporcionar informació rellevant, com ara la diversitat d'establiments involucrats en les transaccions, la popularitat de certs comerços, o fins i tot la segmentació dels comerços en diferents categories o sectors.

En la nostra base tenim un total de 14.911 establiments diferents on s'ha realitzat un total de 185.133 transaccions. Si ens fixem només en els 50 establiments amb més operacions, podem veure que recullen el 49,47% de les operacions.



Gràfic 5. Percentatge d'operacions per establiment.

En aquest cas en lloc del nom dels establiments es mostra un número per motius de confidencialitat com s'ha especificat en la presentació de la base de dades.

La tercera variable categòrica és el dia de la setmana, aquesta variable no està en la base de dades, però la creem a partir de la variable 'timestamp', ja que ens pot ser útil quan mirem les variables numèriques.

L'última variable categòrica és l'hora del dia, a l'igual que el dia de la setmana aquesta variable la creem a partir de 'timestamp' i l'utilitzarem després junt amb les variables numèriques.

4.2.2. Variables numèriques

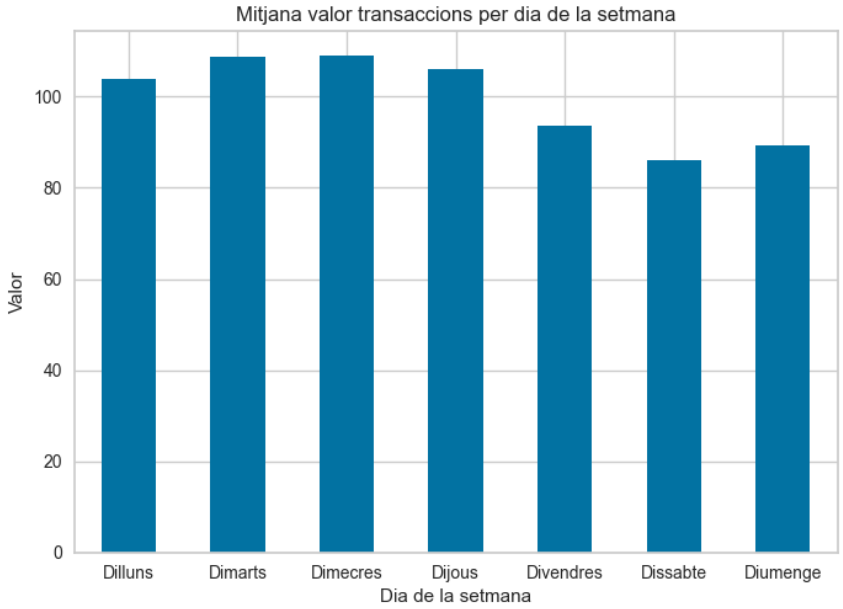
Són aquelles variables que es representen amb números. Poden ser de dos tipus: variables contínues o discretes. Les continues són les que poden prendre qualsevol valor en un rang, es caracteritzen per tenir infinites possibilitats de valors en un interval. Les discretes són aquelles que només poden prendre valors enters. En la nostra base de dades només tenim una variable numèrica.

En últim lloc, tenim 'purchaseAmount' que és una variable numèrica continua, aquesta representa el valor de la compra realitzada en cada transacció. Al ser una variable numèrica podem calcular els següents estadístics descriptius:

Mitjana	106,01€
Desviació típica	517,46€
Mínim	0,01€
Percentil 25	11,44€
Mediana	37€
Percentil 75	87,82€
Màxim	170.629,26€

Taula 2. Anàlisi descriptiu variable ‘purchaseAmount’.

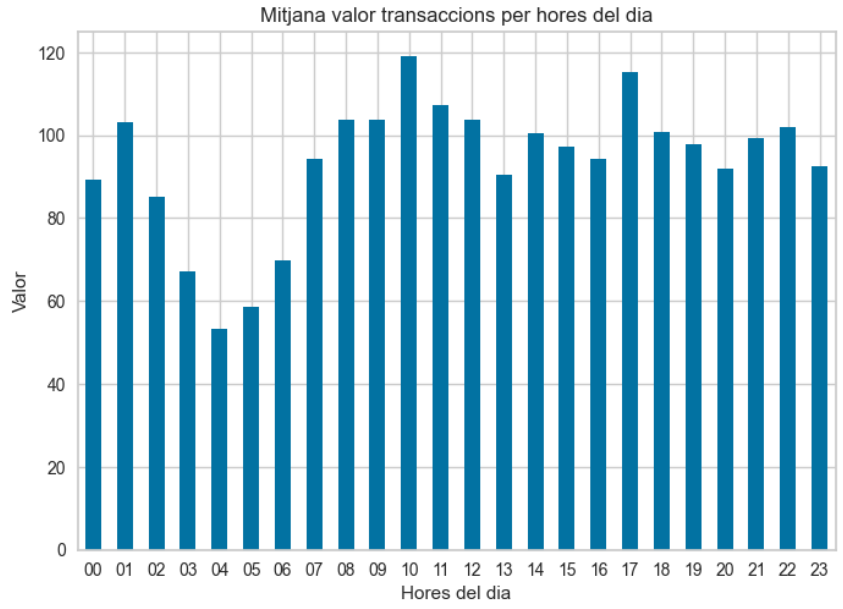
També podem utilitzar aquesta variable numèrica per a analitzar per dia de la setmana, agrupem les dades segons el dia corresponent i mirem el valor mitjà de les transaccions per cada dia. Això ens permetrà identificar possibles patrons del valor mitjà de les transaccions al llarg de la setmana.



Gràfic 6. Valor mitjà transaccions per dia de la setmana.

Aquí podem veure com el valor mitjà de les compres és lleugerament inferior durant els caps de setmana.

També podem veure com evoluciona aquest cost mitjà durant les hores del dia.

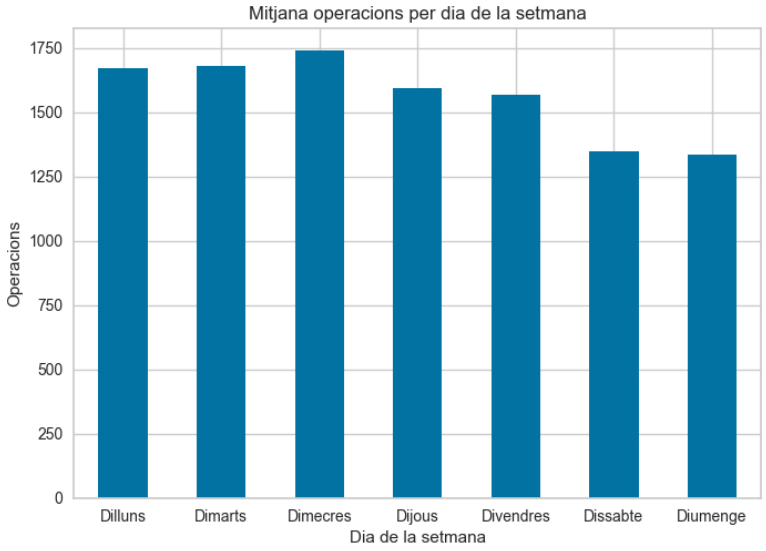


Gràfic 7. Valor mitjà transaccions per hores del dia.

En aquest cas sí que podem veure un patró més clar, hi ha pics on el valor mitjà de les transaccions és més gran, com són les 10 del matí i les 5 de la tarda, en canvi, en hores nocturnes veiem uns valors clarament inferiors a la resta del dia.

Utilitzant la variable que indica el moment de la transacció i 'operationId', l'índex únic per a cada transacció, podem analitzar el nombre de transaccions per dia de la setmana i per les hores del dia.

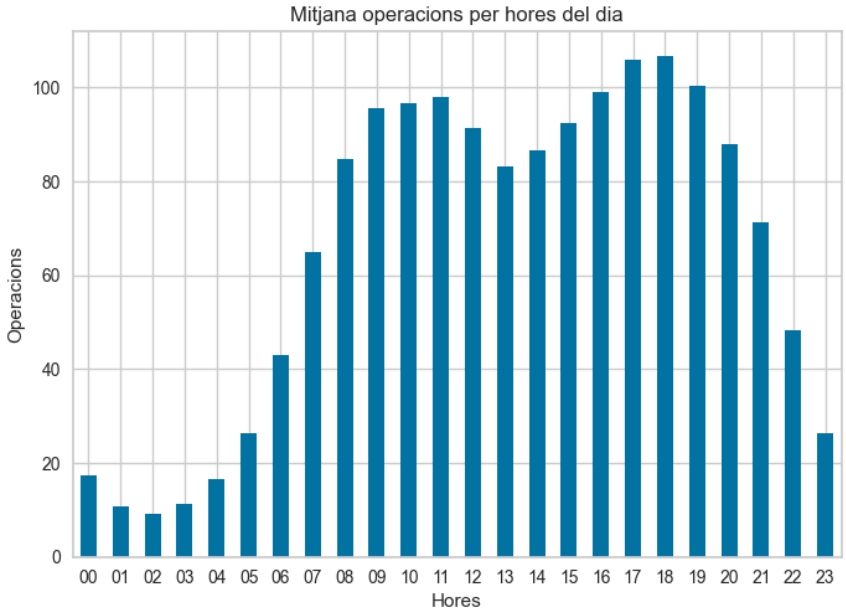
Primer agruparem les dades per dia de la setmana i mirarem la mitjana de transaccions que es realitzen cada dia, això ens permetrà veure possibles variacions al llarg de la setmana.



Gràfic 8. Nombre mitjà de transaccions per dia de la setmana.

Veiem que durant els caps de setmana el nombre de transaccions que es duen a terme són inferiors en comparació amb la resta de dies.

També podem veure com evoluciona el nombre de transaccions durant les hores del dia.



Gràfic 9. Nombre mitjà de transaccions per hores del dia.

Podem observar com durant les hores diürnes, des del matí fins a la tarda, es registra un major nombre de transaccions en comparació amb les hores nocturnes. Això es pot entendre, ja que durant les hores diürnes, les persones en general estan més actives fent compres i transaccions, en canvi, durant les hores nocturnes, l'activitat comercial i el nombre de transaccions disminueix.

4.3. Tractament dades

La primera idea consistia a contar el nombre de transaccions en intervals d'una hora per a crear una sèrie temporal per a cada establiment. Posteriorment, aplicaríem l'algorisme *iForest* per detectar anomalies en aquestes sèries temporals i enregistraríem els moments on es produïssin les anomalies junt amb el nom de l'establiment. Finalment, quan ho traslladéssim a la realitat, la idea era que cada hora es calculés el nombre de transaccions que havia rebut cada establiment i afegir aquest valor a la sèrie corresponent. Després aplicaríem l'algorisme a cada establiment i faríem que ens arribes una notificació per correu de les anomalies que detectéssim en l'última hora, aquest procés es repetiria cada hora. Però quan vam començar a treballar amb aquesta idea ens vam trobar amb els següents inconvenients:

- Aquest plantejament podia suposar que quan un establiment havia tingut molt poques transaccions, la sèrie de dades tindria molts valors a 0, ja que durant la gran majoria d'intervals d'1 hora no hi hauria transaccions. Això es podia traslladar al fet que quan comences a tenir algunes transaccions, aquestes les detectes com a anomalies sense ser un nombre de transaccions sospitós. Un exemple, seria el d'un establiment on en els últims 4 mesos només ha tingut 3 transaccions repartides en

diferents hores, quasi ve tots els valors serien 0, excepte 3 valors que serien 1. Si quan posem el model a funcionar en temps real rebéssim en una mateixa hora 3 compres en aquest establiment, és probable que ens saltes l'alerta, ja que seria un valor anòmal per les dades que tenim.

- L'altre problema, és que el nombre d'establiments diferents que teníem era molt gran, més de 10.000. Aleshores haver d'executar l'algoritme *iForest* per a cada un era una feina que tardava molt de temps, arribant a estar més d'1 hora per a processar-los tots. Això feia que fos impossible poder-lo executar en temps real cada hora.
- El fet d'executar-lo cada hora era una cosa que havíem decidit arbitràriament perquè veiem que de la manera que ho estàvem fent tardava molt a executar-se. Havíem de buscar una manera on poguéssim executar el procés en un període més curt de temps, com per exemple, cada 5 o 10 minuts, així podríem detectar els possibles fraus quan començaven i actuar amb més rapidesa.

Després d'haver vist que era inviable fer-ho d'aquesta manera vam decidir plantejar-ho de nou, a continuació exposarem aquest nou plantejament.

En aquest nou enfocament comencem seleccionant les dues primeres setmanes que tenim dades, del 23 de desembre del 2022 fins el 5 de gener del 2023. D'aquest període calculem la mitjana de transaccions que té cada establiment en mig dia, 12 hores. Un cop obtinguda aquesta mitjana, ens enfocarem en les 12 hores posteriors a aquest període de dues setmanes, on enregistrarem les transaccions realitzades en cada establiment durant aquest lapse de temps.

A continuació explicaré punt per punt com es construeix el valor per a ordenar els establiments de més a menys risc en cada iteració:

- Per a cada establiment, utilitzarem el valor obtingut de contar les transaccions durant el període de 12 hores i l'hi restarem la mitjana de les dues últimes setmanes.
- Ens fixarem només en els valors on la diferència sigui positiva, ja que en el cas on la diferència fos negativa, ens indicaria que les transaccions són inferiors a la mitjana de les últimes 2 setmanes i quedaria descartat com un frau a causa d'un gran nombre de transaccions.
- Dels casos on la diferència és positiva, calculem la diferència de logaritmes per no quedar-nos amb la diferència absoluta, sinó que ens fixem en la diferència proporcional entre els valors, el resultat d'aquest càlcul és el valor que usarem per ordenar els establiments i posteriorment, analitzar-ho per a veure si en aquell lapse de temps hi ha una anomalia o no.
- Ordenarem els resultats de major a menor, això ens permetrà ordenar els comerços en funció del seu possible risc.

Ara anem a veure un cas per a entendre-ho millor. Imaginem que un establiment durant les dues primeres setmanes té una mitjana de 40 transaccions cada 12 hores, i en les 12 hores posteriors té un total de 50 transaccions. Primer miraríem que la resta d'aquests valors fos superior a 0, en aquest cas ho és. Aleshores el valor que miraríem per després poder ordenar els comerços seria el següent:

$$valor = \ln(50) - \ln(40) = \ln\left(\frac{50}{40}\right) = \ln(1{,}25) = 0{,}22314$$

En cada una de les iteracions guardem el valor més gran, junt amb el nom de l'establiment. Farem el mateix per al segon valor més gran, però en aquest cas ho guardarem en una altra base de dades, això ens permetrà més endavant poder arribar a detectar si ens ataquen a dos establiments diferents al mateix temps.

Aquest càlcul l'anem executant cada 10 minuts, el que resulta d'aquí són dues bases de dades, un que correspon al valor més gran en cada iteració i un altre que correspon al segon valor més gran, tots dos tenen la mateixa estructura, on cada registre hi ha el moment de temps on s'ha executat la iteració, el nom de l'establiment, el nombre de transaccions en el període de 12 hores i el valor de la diferència de logaritmes.

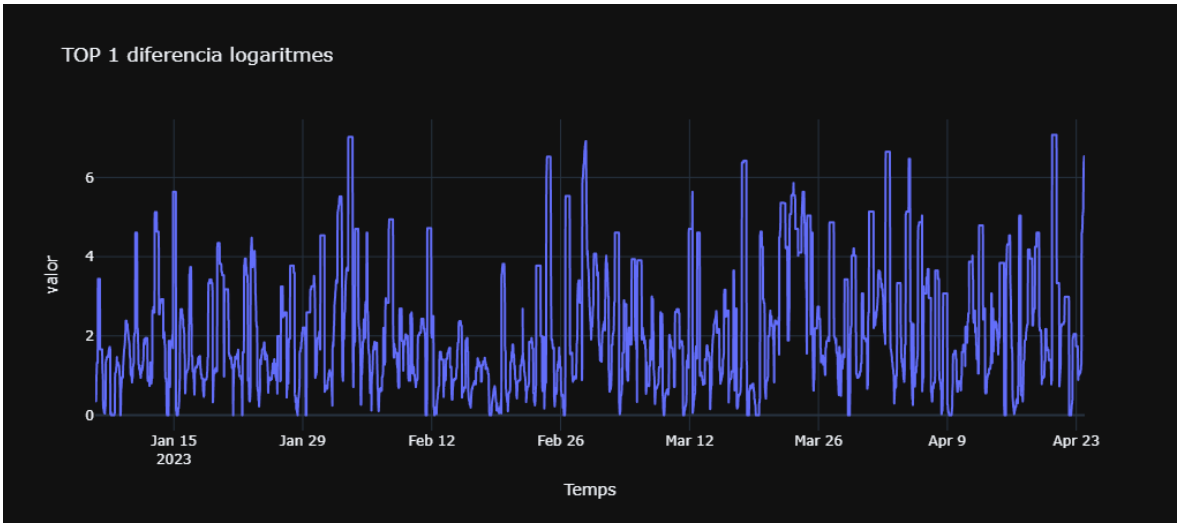
Amb aquest plantejament aconseguim un valor que posteriorment ens servirà per detectar les anomalies, ja que els atacs de moltes operacions que rep el banc no és una cosa molt comuna, per tant, esperem que els valors de la diferència de logaritmes dels casos on hi ha els atacs difereixi bastant dels valors on no hi ha frau, i així poder localitzar els atacs. La base de dades que guarda el segon establiment amb un valor més gran de la diferència de logaritmes ens serveix perquè si detectem un atac en l'altra base de dades poder mirar en aquell moment si s'està atacant un segon comerç al mateix temps.

Aquest plantejament té alguns inconvenients:

- Només podem detectar un màxim de 2 atacs en un mateix moment, això és un problema, ja que si ataquen més de 2 comerços al mateix temps, no podrem veure la totalitat d'establiments atacs.
- El valor de la diferència de logaritmes pot ser molt gran en casos on la mitjana de transaccions de les 2 setmanes sigui molt baixa o quasi ve nul·la i les transaccions en les següents 12 hores siguin no molt grans. Un exemple seria si la mitjana de les 2 setmanes és de 0,5 transaccions i les transaccions en les 12 hores següents fos de 8. En aquest cas el valor seria igual a $\ln\left(\frac{8}{0.5}\right) = 2{,}77258$ i podria sortir que fos una anomalia, però no seria un atac de moltes transaccions perquè 8 són poques. Per a solucionar aquest petit problema vam establir un nombre mínim de transaccions i en cas de no superar-les en el període de 12 hores, no tenim en compte l'establiment a l'hora de calcular la diferència de logaritmes. Això ho fem perquè casos com el que

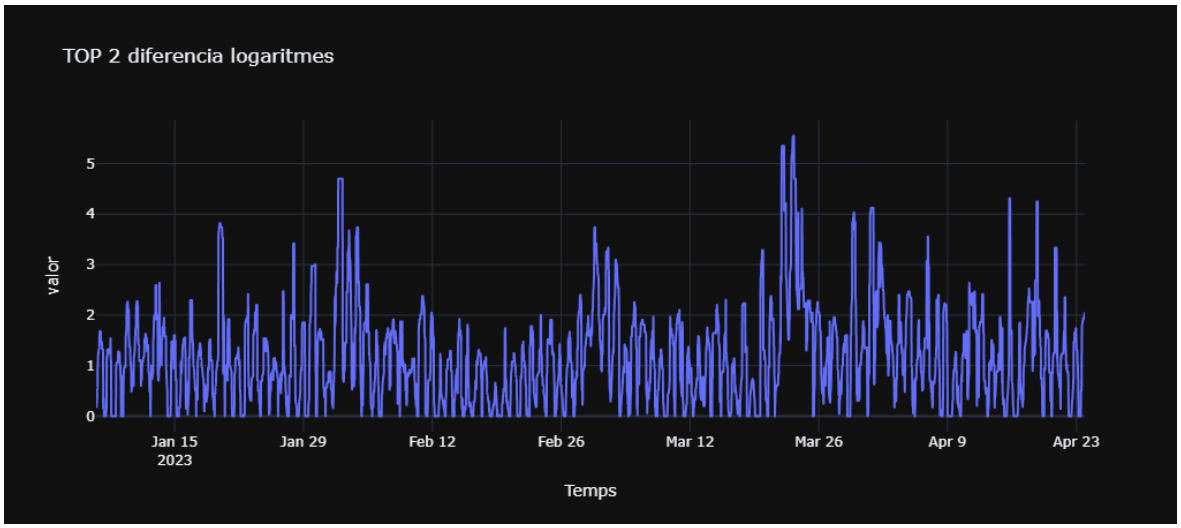
acabo de mostrar no ens surtin com a anomalies, ja que tot i ser una anomalia no és l'atac d'un gran nombre de transaccions que estem buscant.

A continuació podem veure com queda la sèrie dels valors per a la diferència de logaritmes més grans.



Gràfic 10. Valors dels establiments amb diferència de logaritmes més grans.

A continuació tenim la sèrie pel segon valor més gran en cada lapse de temps.



Gràfic 11. Valors dels segons establiments amb diferència de logaritmes més grans.

Ara que ja hem vist les sèries de valors procedirem a la part del model.

4.4. Construcció del model Isolation Forest

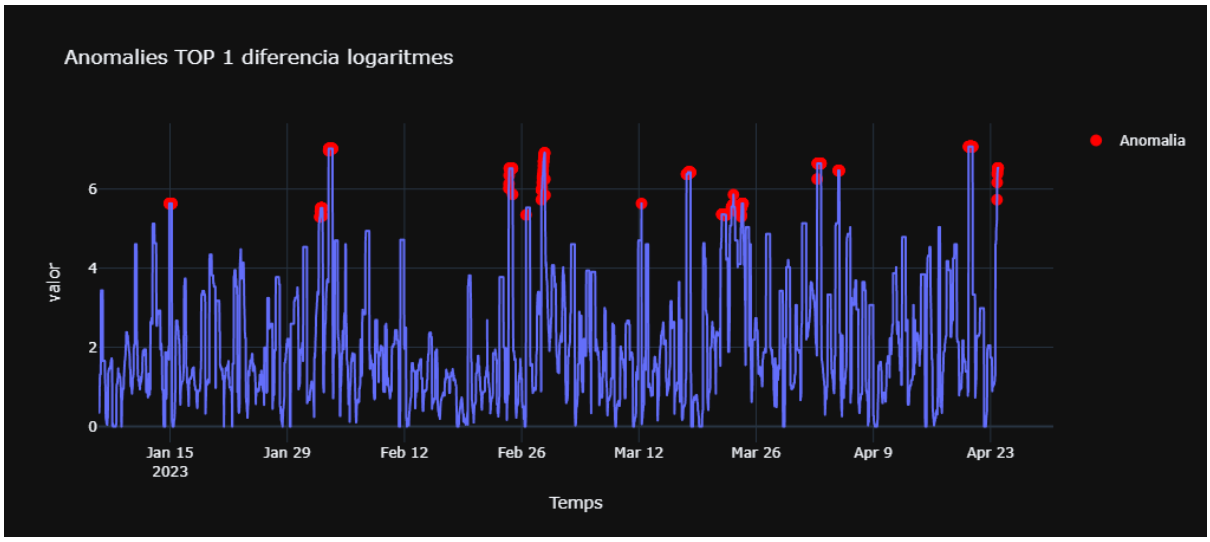
Prèviament, ja hem vist els fonaments del model en detall, però per a recordar la idea general del model, comentar que l'algoritme Isolation Forest és una tècnica de detecció d'anomalies que es basa en la idea que les anomalies són punts atípics que s'aïllen fàcilment en un conjunt de dades.

En aplicar l'algorisme a les dades de la diferència de logaritmes, busquem identificar les possibles anomalies en funció del comportament inusual en relació amb la resta de dades. L'algorisme construeix un conjunt d'arbres de decisió que divideixen repetidament les dades en subconjunts, cosa que permet identificar els punts que es troben en regions menys poblades, és a dir, les anomalies.

En utilitzar l'algoritme obtenim una puntuació d'anormalitat per a cada punt en funció de quant aïllat està del conjunt de dades. Els punts amb puntuacions més altes s'assignen a valors atípics.

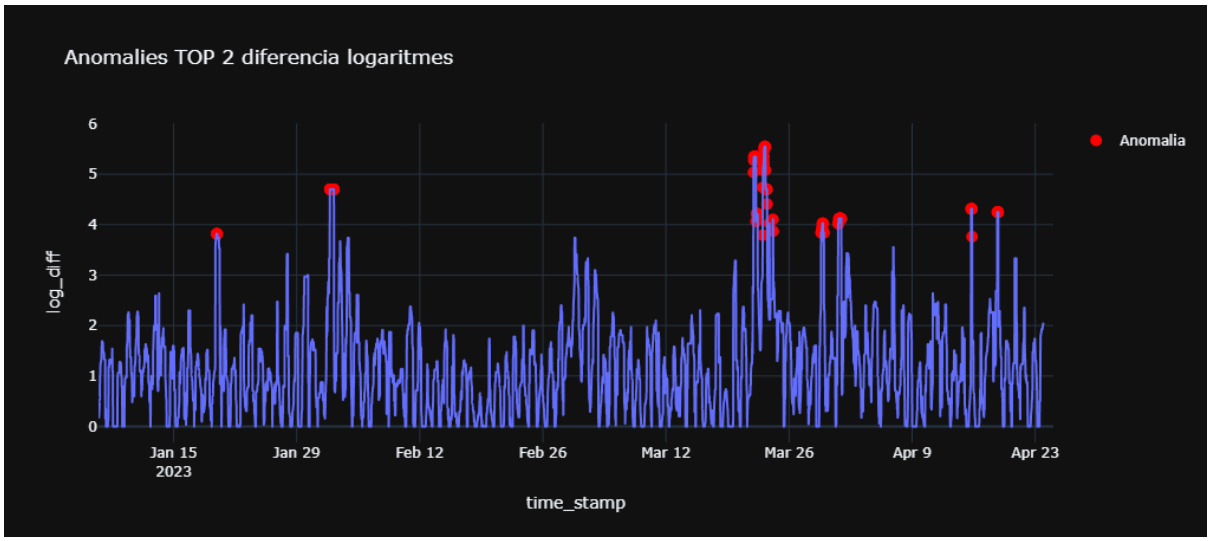
En aquest cas, al ser sense supervisió li hem d'introduir un valor que és la proporció d'anomalies que hi ha en la nostra base de dades, però com que és sense supervisió aquest valor serà el percentatge de valors amb una puntuació d'anormalitat més gran. Nosaltres hem treballat amb un 5%, això vol dir que el que ens ha agafat com a valors atípics són el 5% dels registres amb la puntuació d'anomalia més gran.

A continuació, en un gràfic representarem els valors de les observacions i ressaltarem les anomalies que ha detectat el model. Aquests valors anòmals estan marcats mitjançant punts de color vermell.



Gràfic 12. Anomalies valors dels establiments amb diferència de logaritmes més grans.

Quan en un lloc veiem que hi ha molts punts vermells consecutius, en la majoria dels casos és degut a com està construïda la sèrie, on comparem les ultimes 12 hores amb les 2 setmanes anteriors i això fem que s'executi cada 10 minuts, aleshores quan hi ha un atac on hi ha moltes transaccions, a mesura que aquestes arriben i les comptabilitzem en les últimes 12 hores el valor que calculem va variant, i com que és un valor gran si no arriba cap valor més gran, aquest establiment continuarà apareixent fins que el final de l'atac quedi fora de les 12 últimes hores.

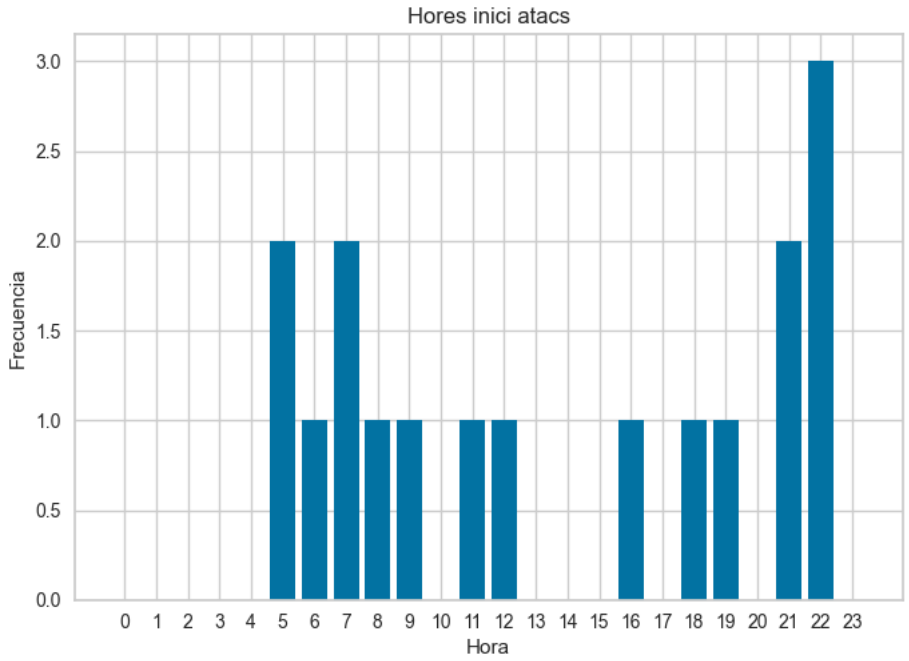


Gràfic 13. Anomalies valors dels segons establiments amb diferència de logaritmes més grans.

Mirant els dos gràfics podem observar com en certs punts, com per exemple, els situats durant el 2 de febrer i el 23 de març, es pot observar anomalies en ambdós gràfics, això és perquè probablement en aquests dies els atacs es cometien a més d'un establiment al mateix temps.

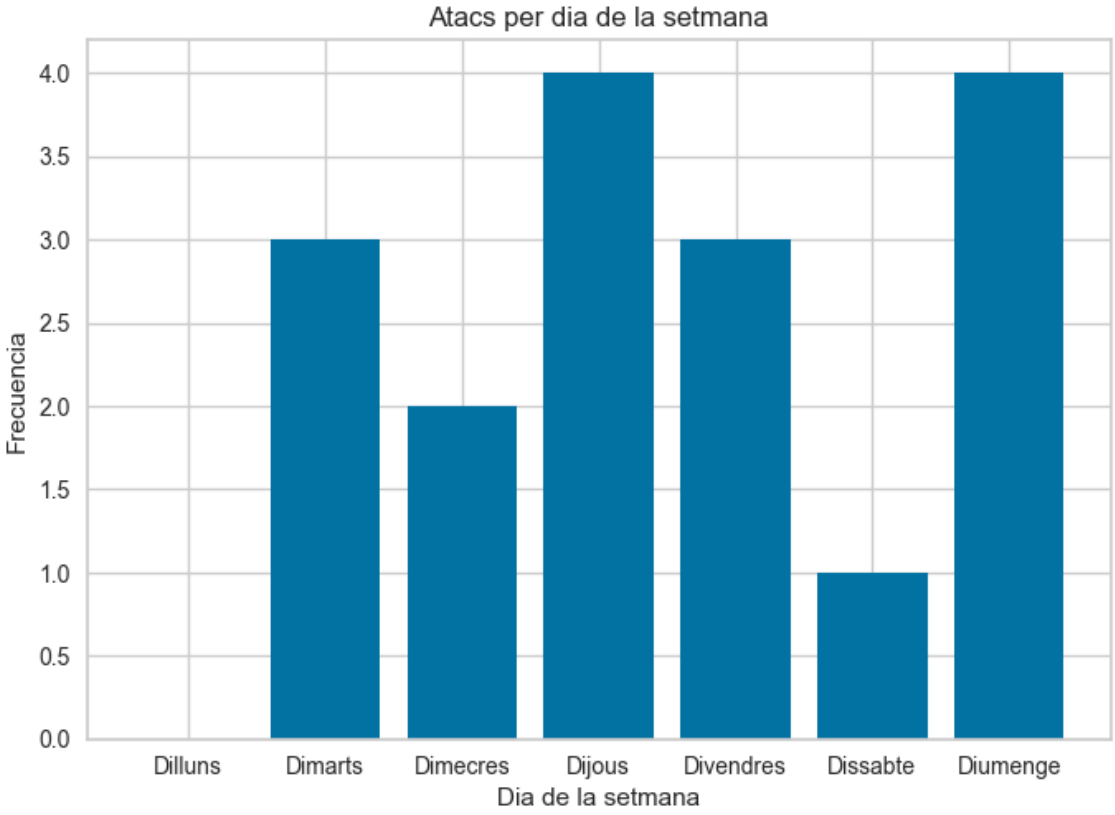
4.5. Anàlisis d'anomalies detectades

En total hem detectat 17 establiments diferents que han sigut atacats. A continuació intentarem mirar amb gràfics si hi ha algun patró en les hores del dia on comença l'atac o en els dies de la setmana en què es du a terme.



Gràfic 14. Gràfic de freqüències de les hores d'inici de possibles atacs.

Veiem que una gran part dels atacs comencen en hores nocturnes, entre les 9 del vespre i les 7 del matí.



Gràfic 15. Gràfic de freqüències dels dies de la setmana dels possibles atacs.

En aquest cas veiem que no hi ha un patró clar de comportament en aquest aspecte.

4.6. Implementació tractament de dades i algoritme en temps real

En aquest apartat ens centrarem a aplicar en el banc el que hem vist prèviament, i explicaré punt per punt com ho hem fet.

- El primer pas és fer que l'script funcioni connectant-se a Elasticsearch per a poder agafar les dades d'allà. Les dades que tenim aquí van des del setembre del 2022 fins a l'actualitat. Anteriorment, no hem treballat amb aquestes dades perquè al servidor d'Elasticsearch només si podien connectar els que tenien permisos i aquests eren treballadors del banc, i el fet que m'haguessis donat els permisos hauria sigut difícil i hagués portat temps.

- En segon lloc, agafarem les dades i farem el que hem vist a l'apartat 4.3, el tractament de les dades, on el que obtindrem serà el valor més gran i el segon valor més gran de la diferència de logaritmes, això ho tindrem per intervals de 10 minuts de tot l'històric de dades. Així tindrem les sèries de dades creades.

- Ara que ja tenim les dades de l'històric fins al moment actual, programarem que cada 10 minuts que passin en temps real es calculi el nombre de transaccions de cada establiment en les últimes 12 hores i el nombre de transaccions mitjà per cada 12 hores de les 2 setmanes anteriors a les 12 hores. A partir d'aquests valors calcularem la diferència de logaritmes entre el valor de les 2 setmanes i el de les 12 hores, el valor més gran i el segon més gran l'afegirem a la sèrie de dades que hem creat en el punt anterior.

- Ara tenim una sèrie de dades que s'actualitzarà en temps real, en concret cada 10 minuts. El que farem és que quan ja s'hagi executat el càlcul anterior aplicarem l'algoritme *iForest* sobre les dades.

- En últim lloc, comprovarem si l'algoritme ha detectat l'última dada com una anomalia o no, en cas afirmatiu, s'enviarà automàticament una notificació per correu amb la informació sobre el moment de temps, el nom de l'establiment, el nombre de transaccions en el període de 12 hores i el valor de la diferència de logaritmes.

Així obtenim un sistema que cada 10 minuts ens avaluarà en temps real si algun establiment és atacat. Per a fer que els càlculs fossin més ràpids hem utilitzat *Dask*, una biblioteca de Python que permet dividir els processos en parts més petites i executar-les en paral·lel.

4.7. Limitacions

Una de les principals limitacions amb la que ens hem trobat és la falta d'una variable que indiques si una transacció es tractava d'un frau o no. Haver tingut aquesta informació ens hauria permès poder utilitzar models supervisats i haver avaluat el seu funcionament amb mètriques com la precisió, la sensibilitat, l'AUC o altres tècniques com la *cross-validation*. Si haguéssim tingut les transaccions etiquetades, hauríem pogut detectar si una transacció era fraudulenta o no, i amb el que hem fet només podem detectar si un establiment és atacat o no. Per a superar aquesta limitació el que vam fer va ser explorar tècniques d'aprenentatge no supervisat per no haver de dependre de dades etiquetades.

Cal comentar que després d'haver parlat aquest tema amb el banc es va decidir que per a poder millorar la seguretat, a partir d'ara es treballaria amb el departament de ciberseguretat perquè qualsevol frau que es detectés tant amb el model que hem creat i que posteriorment és vàlida com a frau, o fraus que ens comuniquin des del departament de ciberseguretat, es deixarà constància en un camp de la transacció. Quan tinguem bastants registres de transaccions i en aquestes estiguin etiquetats els fraus podrem treballar amb models supervisats i també valorar si les alertes que s'obtenen del model no supervisat són o no certes.

Una altra limitació és que només podem detectar quan un establiment li cometen moltes transaccions fraudulentes, en altres casos on el frau s'enfoqués a fer moltes compres amb una targeta en diferents establiments, nosaltres no el detectaríem per com hem plantejat la solució a un problema concret. En les dades que se'ns van proporcionar la informació sobre la targeta estava encriptada.

4.8. Futures millores

A continuació, explicarem futures millores que treballarem fora del treball de final de grau. En aquest cas consistirà en buscar una estructura de dades adequada per a poder desenvolupar un model que ens permeti detectar anomalies utilitzant múltiples variables, tant numèriques com categòriques. Aleshores, a part de poder treballar amb el nombre de transaccions que ha rebut l'establiment en un període també podríem tenir en compte l'import total, l'hora del dia, si es tracta d'un cap de setmana o d'un dia festiu, entre altres variables. Serà una millora important, ja que ens permetrà obtenir una visió més completa i detallada.

5. CONCLUSIONS

Ara que ja hem arribat al final del treball, és important fer una mirada als objectius que ens vam marcar al principi. El propòsit principal era crear un model que fos capaç de detectar anomalies en el nombre de transaccions que rep un establiment en un període concret. L'altre tema rellevant era investigar i entendre els atacs que podia tenir l'entitat financera i crear un mètode que fos útil en el seu dia a dia.

De tot el procés, la part de les dades és la més important i a la que s'ha dedicat més temps, per a assegurar-nos que els resultats són correctes. Ens hem d'assegurar que quan fèiem les proves és llegíssim correctament tots els arxius, i posteriorment, quan creem el model pel banc assegurar-nos que la connexió amb l'Elasticsearch funciona correctament. És rellevant que quan tenim les dades carregades, analitzar que totes les variables tinguin la informació que s'espera i que no hi hagi valors erronis. La part on construïm el model depèn principalment de com hàgim tractat les dades que hi introduirem. Així, és crucial tenir tant coneixements tècnics per a poder treballar correctament les dades, com coneixements del sector per a entendre de què tracten i si hi ha algun valor incorrecte.

El model que hem desenvolupat és una solució eficient i ràpida per al problema que plantejava el banc. De la manera que l'hem dissenyat, hem aconseguit que s'executi en temps real cada 10 minuts i que doni la resposta sobre si l'últim valor de la sèrie de dades és una anomalia o no en menys de 30 segons. Amb aquest monitoratge en temps real obtenim que el banc pugui prendre decisions de manera immediata, ja que amb la informació que reben de l'anomalia poden ubicar l'atac amb facilitat. En conclusió, el model contribueix a millorar la seguretat de l'entitat i a protegir els clients.

Tot i això, és important destacar que encara hi ha àrees de millora, com treballar amb models de múltiples variables per a incorporar més informació, o identificar les transaccions fraudulentes i etiquetar-les per a poder investigar mètodes supervisats amb models com *XGBoost*, *Random Forest* o SVM entre altres.

Amb aquest treball hem demostrat que tot i trobar-nos amb una situació on no tinguem dades etiquetades podem trobar altres models que són senzills, però a la vegada útils i fàcils d'aplicar. A part, hem vist que tenim la capacitat de poder-los crear des de dintre del banc, sense haver de contractar un servei extern, el qual acabaria fent un model similar, però no podríem veure el funcionament intern del model i suposaria un cost econòmic més gran. Un exemple d'aquest servei extern és l'eina de pagament que té Elasticsearch, el qual utilitza l'algoritme *Random Cut Forest* per a detectar anomalies en temps real.

6. BIBLIOGRAFIA

Ali, M. (2021). Towards Data Science. Obtingut de https://towardsdatascience.com/introduction-to-anomaly-detection-in-python-with-pycaret-2fecd7144f87

Antonio Ludeña, J. (2021). Economipedia. Obtingut de https://economipedia.com/definiciones/riesgo-financiero.html

Ayudaley (sense data). Ayudaley. Obtingut de https://ayudaleyprotecciondatos.es/2020/06/10/skimming/#Codificacion_de_bandas_magneticas

Bankinter (sense data). Bankinter. Obtingut de https://roboadvisor.bankinter.com/magazine/noticia/inversion-que-es-riesgo-tipo-cambio

CESCE (2021). CESCE. Obtingut de https://www.cesce.es/es/w/asesores-de-pymes/que-es-el-riesgo-operacional

CESCE (sense data). CESCE. Obtingut de https://www.cesce.es/es/seguros-de-credito/riesgo-de-credito

Hernández, J. (2022). Asociación Española de Empresas Contra el Fraude. Informe sobre el estado del fraude en España 2021-2022.

INESDI Business Techschool (2022). INESDI Business Techschool. Obtingut de https://www.inesdi.com/blog/que-es-aprendizaje-no-supervisado/

Iranzo, S. (2008). BDE. Introducción al riesgo-país. Obtingut de https://www.bde.es/f/webbde/SES/Secciones/Publicaciones/PublicacionesSeriadas/DocumentosOcasionales/08/Fic/do0802.pdf

Jorge Pedros, S. (sense data). Economipedia. Obtingut de https://economipedia.com/definiciones/riesgo-tipo-interes.html

Kanuparthy, P. (2019). OpenSearch. Obtingut de https://opensearch.org/blog/real-time-anomaly-detection-in-open-distro-for-elasticsearch/

Kirui, C. (2022). Section. Obtingut de https://www.section.io/engineering-education/anomaly-detection-model-on-time-series-data-using-isolation-forest/#prerequisites

Lim, Y. (2022). Mèdium. Obtingut de https://medium.com/mlearning-ai/unsupervised-outlier-detection-with-isolation-forest-eab398c593b2

Liu, F. T., & Ting, K. M. & Zhou, Z. -H, “Isolation Forest,” 2008 Eighth IEEE International Conference on Data Mining, 2008, pp. 413–422, doi: 10.1109/ICDM.2008.17. Obtingut de https://cs.nju.edu.cn/zhouzh/zhouzh.files/publication/icdm08b.pdf?q=isolation-forest

McDonald, A. (2022). Towards Data Science. Obtingut de https://towardsdatascience.com/isolation-forest-auto-anomaly-detection-with-python-e7a8559d4562

Pablo Calle, J. (2022). Pirani. Obtingut de https://www.piranirisk.com/es/blog/3-enfoques-para-medir-el-riesgo-operacional

Pelgrim, R. (2023). Towards Data Science. Obtingut de https://towardsdatascience.com/sliding-windows-in-pandas-40b79edefa34

ProjectPro (2023). ProjectPro. Obtingut de https://www.projectpro.io/article/anomaly-detection-using-machine-learning-in-python-with-example/555#mcetoc_1fqgmt45ri

Riveros, A. (2018). EALDE Business School. Obtingut de https://www.ealde.es/gestion-de-riesgos-financieros-clasificacion/

Riveros, A. (2021). EALDE Business School. Obtingut de https://www.ealde.es/riesgo-legal-gestion-empresarial/

Sevilla Arias, A., & Pedrosa, S. J. (2020)). Economipedia. Obtingut de https://economipedia.com/definiciones/riesgo-de-liquidez.html