ISCTE IUL
REPOSITÓRIO
INSTITUTO UNIVERSITÁRIO DE LISBOA

Repositório ISCTE-IUL

Deposited in *Repositório ISCTE-IUL*:
2019-03-14

Deposited version:
Post-print

Peer-review status of attached file:
Peer-reviewed

Citation for published item:
Bernardino, D., Pedrosa, I. & Laureano, R. M. S. (2018). Métodos analíticos para auditoria e deteção de anomalias/fraude . In 2018 13th Iberian Conference on Information Systems and Technologies (CISTI). Caceres: IEEE.

Further information on publisher's website:
10.23919/CISTI.2018.8399429

Publisher's copyright statement:
This is the peer reviewed version of the following article: Bernardino, D., Pedrosa, I. & Laureano, R. M. S. (2018). Métodos analíticos para auditoria e deteção de anomalias/fraude . In 2018 13th Iberian Conference on Information Systems and Technologies (CISTI). Caceres: IEEE., which has been published in final form at https://dx.doi.org/10.23919/CISTI.2018.8399429. This article may be used for non-commercial purposes in accordance with the Publisher's Terms and Conditions for self-archiving.

Use policy

Creative Commons CC BY 4.0
The full-text may be used and/or reproduced, and given to third parties in any format or medium, without prior permission or charge, for personal research or study, educational, or not-for-profit purposes provided that:

- a full bibliographic reference is made to the original source
- a link is made to the metadata record in the Repository
- the full-text is not changed in any way

The full-text must not be sold in any format or medium without the formal permission of the copyright holders.

Serviços de Informação e Documentação, Instituto Universitário de Lisboa (ISCTE-IUL)
Av. das Forças Armadas, Edifício II, 1649-026 Lisboa Portugal
Phone: +(351) 217 903 024 | e-mail: administrador.repositorio@iscte-iul.pt
https://repositorio.iscte-iul.pt

Métodos analíticos para auditoria e deteção de anomalias/fraude

Analytical methods for auditing and anomaly/fraud detection

Dília Bernardino
Coimbra Business School – IPC
Quinta Agrícola - Bencanta
Coimbra, Portugal
dilia.bernardino@gmail.com

Isabel Pedrosa
Coimbra Business School – IPC
Quinta Agrícola - Bencanta
Coimbra, Portugal
ipedrosa@iscac.pt

Raul M. S. Laureano
Instituto Universitário de Lisboa
ISCTE- IUL, BRU-IUL, ISTAR-IUL
Lisboa, Portugal
raul.laureano@iscte-iul.pt

Resumo **— A temática da fraude que, nos tempos mais recentes, tem vindo ao de cima, é conhecida como uma infração comum, podendo ser realizada por qualquer pessoa ou resultar de conluio, tendo como fim o decremento patrimonial das organizações. A auditoria externa tem como objetivo principal a obtenção de evidência apropriada e suficiente que forneça uma segurança elevada de que as demonstrações financeiras estão isentas de fraude ou de erros materiais. Já ao nível da auditoria interna, o objetivo passa pela identificação do risco de fraude, através da definição de estratégias com o fim de conceber a capacidade para prevenir e antecipar as necessidades de controlo. Atualmente, as organizações geram e armazenam mais informação do que nunca em formato eletrónico. Assim, as transações que são alvo de planos abusivos são "escondidas" e são de difícil deteção pelos meios tradicionais. Consequentemente, os métodos analíticos tornam-se fundamentais na identificação de potenciais indícios de fraude. Este artigo apresenta diversos métodos analíticos para deteção de anomalias com vista à investigação futura na área de fraude.**

Palavras Chave - Fraude; Auditoria; Análise de Dados; Métodos analíticos; Deteção de Anomalias.

Abstract **—The issue of fraud has recently been more frequent and is a common infraction that can be perpetrated by a single person or arise as a result of collusion, causing asset decrement or theft in organizations. External audits aim to obtain relevant and sufficient evidence that points to high, but not absolute, assurances that the financial statements are free from fraud or material misstatement. On the other hand, the main goal of internal auditing is to identify the risk of fraud by developing strategies that provide the capacity to prevent it and anticipate control needs. Organizations nowadays generate and store more information in electronic format. Because there are large amounts of data, the transactions that are subject of abuse are concealed and harder to detect by traditional means. Thus, analytical methods become increasingly fundamental in identifying and uncovering potential evidence of fraud.**

Keywords - Fraud; Audit; Data Analysis; Analytical Methods; Anomaly Detection.

I. INTRODUÇÃO

A fraude é um fenómeno sistémico que provoca avultados prejuízos às organizações, sendo de difícil deteção já que, na maioria das vezes, a fraude é cometida pelos próprios funcionários que são conhecedores da organização e do seu modo de funcionamento. A prática da auditoria depara-se com grandes e constantes desafios, que envolvem a análise de um elevado e crescente volume de informação.

Atualmente, as organizações geram e armazenam mais informação em formato eletrónico do que nunca, e, embora sejam realizadas mais análises aos dados disponíveis, a fraude persiste. Como existem avultadas quantidades de dados, as transações que são alvo de planos abusivos são escondidas e são de difícil deteção pelos métodos tradicionais. Assim, cada vez mais os métodos analíticos se tornam fundamentais na identificação de erros/anomalias ou potenciais indícios de fraude por parte dos auditores. Neste contexto o estudo pretende contribuir para responder à questão de investigação: como podem os métodos analíticos serem utilizados para deteção de anomalias e fraude?

Para o efeito identificam-se métodos analíticos que podem ajudar as empresas a obter indícios de fraude, aplicando-os a dados de uma empresa. Para além desta introdução foram definidas mais cinco seções. Na secção II apresenta-se alguns conceitos ligados à fraude e à auditoria. Na secção III ilustra-se como a análise de dados pode ser utilizada para deteção de fraude e na secção IV identificam-se algumas ferramentas informáticas para análise de dados. Por fim, na secção V aplicam-se alguns métodos analíticos para deteção de anomalias e na secção VI apresentam-se as conclusões.

II. A FRAUDE E AUDITORIA

A. *Conceito de fraude*

A fraude pode ser definida como "quaisquer atos ilegais caracterizados pelo engano, encobrimento ou violação da confiança. Tais atos não dependem de ameaça de violência ou de força física. As fraudes são perpetradas por indivíduos e organizações para se apropriarem de dinheiro, bens ou serviços; para evitarem o pagamento ou perda de serviços; ou para obterem vantagens pessoais ou comerciais" [1, p. 37]. Contudo, a fraude é cometida com vista a prejudicar uma pessoa ou uma organização. De modo análogo a ISA 240 - *The Auditor's Responsibilities Relating to Fraud in an Audit of Financial*

Statements [2, p. 3] define fraude como sendo "um ato intencional praticado por um ou mais indivíduos entre a gerência, os encarregados da governação, os empregados ou terceiros, envolvendo o uso propositado de falsidades para obter uma vantagem injusta ou ilegal". A fraude implica, pois, uma má conduta intencional, realizada com o intuito de evitar a sua deteção, e é concebida para enganar outros, resultando, por isso, em perdas para esses e ganhos para o prevaricador [3].

A ACFE (*Association of Certified Fraud Examiners*) considera que o termo fraude abrange muitas formas de má conduta, o uso comum é muito mais amplo e geralmente abrange qualquer tentativa de enganar outra parte para obter um benefício [4]. A fraude cometida contra uma organização pode ser realizada tanto internamente, pelos funcionários, gerentes, diretores ou proprietários, como externamente, por clientes ou fornecedores. Esta situação leva a que a ACFE defina fraude ocupacional como "o uso de uma profissão para enriquecimento pessoal por meio do uso deliberado indevido ou da má aplicação dos recursos ou ativos da organização empregadora" [5, p. 6].

B. Modelo do Triângulo da Fraude

O modelo teórico do triângulo da fraude, desenvolvido por Donald Cressey [6], refere que a prática de um ato de natureza fraudulenta é sempre antecedida de um processo de decisão, por parte do respetivo autor e cujo sentido parece derivar da avaliação que faz sobre determinados aspetos que contextualizam o seu "aqui e agora". Trata-se de uma espécie de equação, cujo resultado depende das três variáveis que a integram, e que são a pressão, a racionalização e a oportunidade (Fig. 1). A pressão/incentivo, própria da vida particular, pode resultar de necessidades urgentes de liquidez financeira (e.g., existência de dívidas, hábitos de jogo ou de consumos aditivos que façam o sujeito sentir-se integrado no grupo social com o qual se revê) [7]. A atitude/racionalização é entendida como a capacidade possuída pelo sujeito para racionalizar os diversos dados que possui sobre a realidade que o rodeia, e cujo somatório entre eventuais perdas e ganhos o levam a decidir ou não pela prática do ato [8]. Quanto à oportunidade para a prática de um ato de natureza fraudulenta, pode dizer-se que a inexistência de um sistema de controlo interno eficaz facilita a realização de atos fraudulentos [9].

Figura 1. Triângulo da fraude de Cressey [7, p. 316]

No entanto, Hencsey considera que nenhum modelo é capaz de descrever sozinho a complexidade da motivação para a realização de crimes empresariais e que não é pela subjetividade da racionalização que este argumento se torna verdadeiro [8]. Kassem e Higson [10], críticos do triângulo da fraude e citando a obra de Dorminey, Fleming, Kranacher, & Riley [11], argumentam que esta teoria sozinha não pode explicar os desvios empresariais, uma vez que a racionalização e a pressão não podem ser observados. A fraude pode ocorrer quando a intuição dos indivíduos lhes diz que é aceitável cometer fraude por causa de uma racionalização [12].

C. A Auditoria Interna e a Fraude

"A auditoria interna é uma atividade independente de garantia e de consultoria, destinada a acrescentar valor e a melhorar as operações de uma organização. Ajudar a organização a alcançar os seus objetivos, através de uma abordagem sistemática e disciplinada, na avaliação e melhoria da eficácia dos processos de gestão de risco, de controlo e de governação" [1, p. 10].

A função dos auditores internos relativamente à fraude foi contemplada no IPPF – *International Professional Practices Framework do IIA* (*The Institute of Internal Auditors*). As normas mais relevantes sobre a responsabilidade da auditoria interna no que cinge ao risco de fraude são as seguintes: a) Proficiência (1210.A2): os auditores internos devem ter conhecimento suficiente para avaliar o risco de fraude e o modo como este é gerido na organização, mas não é esperado que os auditores internos tenham o mesmo conhecimento de uma pessoa cuja primeira responsabilidade seja a de detetar e investigar fraude; b) Gestão de Risco (2120.A2): a atividade de auditoria interna deve avaliar a potencial ocorrência de fraude e a forma como a organização faz a gestão do risco de fraude; e c) Objetivos do Trabalho de Auditoria (2210.A2): os auditores internos devem considerar a probabilidade de erros significativos, fraude, não conformidades e outras exposições ao desenvolver os objetivos do seu trabalho.

Deste modo, há necessidade de verificação e revisão periódicas do controlo interno, para reduzir o risco de ocorrência de erros ou para que as tentativas de fraude não fiquem encobertas por muito tempo. É responsabilidade da auditoria interna testar o controlo interno e assimilar os possíveis erros e deficiências que possam acontecer e definir soluções. Os auditores internos podem apoiar diretamente o órgão de gestão na implementação de sistemas mais adequados, podendo monitorizar de forma continuada e sistemática o sistema de controlo interno, através da identificação e investigação dos sinais de alerta suscetíveis de serem indiciadores de fraude [13].

D. A Auditoria Externa e a Fraude

O trabalho da auditoria externa incide, por regra ou fundamentalmente, sobre as áreas contabilística e financeira, sendo este tipo de trabalho muitas vezes designado por auditoria financeira [14]. Por outro lado, o auditor é responsável por obter uma segurança razoável de que as demonstrações financeiras, consideradas como um todo, estão isentas de distorções materiais causadas por fraude ou erro [15][2].

A responsabilidade pela prevenção e deteção de fraude cabe à gestão, mas a pressão exercida sobre os auditores para partilhar os resultados das suas análises de dados com a gestão só se tornará mais forte, dando origem a dilemas éticos. Os auditores consideram a ISA 240 sobre fraude e ISA 520 sobre procedimentos analíticos como áreas problemáticas. Todavia, a ISA 240 identifica explicitamente os procedimentos analíticos como um método para avaliar o risco de fraude [2]. No entanto, os auditores consideram que os procedimentos estão

desatualizados, e não são amplamente utilizados no contexto da fraude, embora possam ser usados para mostrar certos erros.

III. A Fraude e Análise de Dados

A. Análise de Dados

A análise de dados pode ser definida como a aplicação de sistemas informáticos na análise de grandes conjuntos de dados, para apoiar na tomada de decisão. Os dados são avaliados, selecionados, tratados, visualizados e, analisados, sendo, no final, interpretados os resultados [16]. A análise de dados fornece informação sobre o conjunto de dados, identifica as relações e estruturas de dados subjacentes, suposições e hipóteses de teste, reconhece variáveis de relacionamentos causais e deteta anomalias [17]. Pode ser aplicada na deteção de fraude e os algoritmos de identificação de exceções são muitas vezes baseados em esquemas de deteção de anomalias [18].

B. Ferramentas de Análise de Dados, Auditoria e Anomalias

A análise de dados envolve extração, usando campos dentro da estrutura básica dos dados. Quanto melhor for a qualidade dos dados, mais informação se obterá da sua visualização e melhor se procederá a análises corretas. Atualmente, existem muitas empresas dedicadas a obter dados e a colocá-los no formato certo, mas nesse ponto não existe evidência para apoiar uma opinião, pelo que o valor da auditoria vem da análise dos dados [19].

A auditoria contínua é o uso de análise de dados em tempo real, permitindo que a gestão e a auditoria identifiquem e relatem mais rapidamente a atividade fraudulenta. O acompanhamento contínuo das transações, sujeitas a certos sinais de alerta (*red flags*), pode promover uma análise mais rápida das transações de alto risco [20].

Normalmente, as transações fraudulentas em registos eletrónicos são poucas em relação à grande quantidade de registos disponível. Transações fraudulentas ou com anomalias não são a norma. Outras anomalias, como nos registos contabilísticos, são devidas a procedimentos inadequados ou a outras deficiências do controlo interno. Compreender o negócio, as suas práticas e procedimentos ajudam a explicar a maioria das anomalias [17].

C. Análise de Dados e Fraude

A proatividade com a qual alguns esquemas de fraude originam transações identificáveis, amplia a efetiva capacidade de uma organização projetar e implementar análises de dados. A análise de dados pode ser usada para assegurar a eficácia no controlo preventivo de fraude [20]. Os responsáveis pelo controlo interno têm de analisar todas as transações que ocorrem, o que exige o uso de ferramentas de análise de dados.

De um modo geral, as organizações necessitam de implementar processos de contínua monitorização, a fim de identificar anomalias nos fluxos de dados ou padrões comportamentais potencialmente fraudulentos [21]. A título de exemplo, os criadores dos cartões de crédito conceberam controlos e análise de dados para tentar minimizar o risco de esquemas fraudulentos [22]. Para se aplicar e interpretar os resultados, usando métodos estatísticos tradicionais ou avançados, o auditor ou o investigador têm de dispor de um bom conhecimento sobre o ambiente do negócio, bem como estar familiarizado com o *software* utilizado para a análise [23].

IV. *Software* de Análise de Dados para Auditoria

A. Técnicas de Auditoria Assistidas Por Computador – CAAT

Nos últimos anos, foi desenvolvido muito *software* de análise de dados para auxiliar o trabalho dos investigadores e auditores na deteção de fraudes e anomalias. Estes programas informáticos são denominados por CAAT (Técnicas de Auditoria Assistidas por Computador).

Os objetivos da utilização de CAAT em análise e extração de dados são vários. Destacam-se: i) aceder e analisar informação de distintas proveniências; ii) garantir integridade dos dados originais; iii) utilizar técnicas de amostragem; iv) registar o histórico dos procedimentos e das análises efetuadas; e v) automatizar análises [24].

Esta utilização de CAAT traz algumas vantagens, tais como, processamento mais rápido de dados, maleabilidade e facilidade de utilização, dispensa de conhecimentos relativos a SQL (*Structured Query Language*), melhor eficiência e *performance* das auditorias, e fornecimento de dados que aumentam a credibilidade da auditoria [24].

B. Programas Disponíveis para Análise de Dados

Dada a amplitude de usos que pode ser dada à análise de dados, não é possível enumerar todos os programas informáticos disponíveis. Assim, enumeram-se os que são mais amplamente usados:

- ACL (*Audit Command Language*): é uma ferramenta de auditoria que tem disponível um módulo de deteção de fraude;
- Caseware IDEA: centra-se primordialmente na auditoria, apresentando nas versões mais recentes um crescente número de técnicas de deteção de anomalias/fraude [25].
- ActiveData: trata-se de um *plug-in* para o Microsoft Office que fornece procedimentos aperfeiçoados de análise de dados. É uma alternativa menos dispendiosa do que o ACL e IDEA e que, acima de tudo, pretende capitalizar os conhecimentos de Excel dos auditores / investigadores;
- TeamMate Analytics: suplemento para Excel, que inclui ferramentas de descoberta interativa para detetar anomalias e características incomuns nos dados a investigar;
- Picalo: é um *software open source* que incorpora pequenos *plug-ins* para detetar indicadores de fraude, sendo semelhante ao IDEA e ACL.

Existem ainda outros programas que, embora não sejam ferramentas específicas para análise de dados em auditoria, podem possibilitar realizar análises úteis. Destacam-se o SAS e o SPSS, que são programas de análise estatística e de *data mining* com módulos de fraude disponíveis, e as linguagens de programação tradicionais, como Java, Perl, Python, R, Ruby e Visual Basic [25].

Os resultados do *Survey Report on Data Analysis Audit Software*, publicado em 2012, evidenciam que dos auditores que têm *software* de análise de dados, 64% utiliza o ACL, 16% o IDEA e 47% o Microsoft Access [26]. O mesmo estudo, replicado em 2015, revela que 60% das empresas possuem uma solução para análise de dados e, que dessas, 39% possui ACL,

18% IDEA, 36% Access e 70% Excel [27]. Em Portugal, um estudo realizado junto dos Revisores Oficiais de Contas (ROC) apresenta um cenário um pouco distinto. Estes profissionais utilizam o Excel (100%), o IDEA (30%), o ACL (12%) e, apenas, 7% indica utilizar ferramentas de *Data Mining* [24].

V. Métodos Analíticos na Deteção de Anomalias

Para aplicar métodos estatísticos, tradicionais ou avançados, e interpretar efetivamente os seus resultados, o auditor ou o investigador têm que ter um bom conhecimento sobre o ambiente do negócio e têm que estar familiarizados com o *software* utilizado para a análise [23]. Os métodos analíticos tradicionais de análise de dados incluem: extrações; estatísticas; ordenações; duplicações; amostras; resumos; estratificações; junções; e comparações. Para realizar análises mais simples pode usar-se o Microsoft Excel ou Access [23].

Vários investigadores sugeriram o uso da análise de dígitos como ferramenta para os auditores detetarem dados suspeitos [28][29]. A taxa de ocorrência real ou padrão de dígitos dentro dos dados é comparada à taxa de ocorrência ou padrão de dígitos hipotéticos para determinar se os dados podem conter dados suspeitos. Embora as técnicas não identifiquem quais pontos de dados são suspeitos, as técnicas podem alertar o auditor sobre a possível presença de dados suspeitos [30]. Assim, enumeraram--se alguns dos testes que se podem utilizar para análise de dados a nível de ferramentas informáticas para auditoria.

A. *Lei de Benford*

A Lei de Benford afirma que os dígitos e as sequências de dígitos num conjunto de dados seguem um padrão previsível, pelo que permite realizar análises de dígitos em dados numéricos. Esta análise ajuda a identificar anomalias, como a manipulação sistemática de dados, fraude potencial e outras irregularidades. Adicionalmente, esta técnica identifica duplicações incomuns ou excessivas de dígitos.

Conforme observado na Fig. 2, os números cujo primeiro dígito mais significativo é 1 devem ocorrer em 30 por cento dos casos, enquanto os números que começam com o dígito 9 só ocorrem com uma frequência de 4,6 por cento.

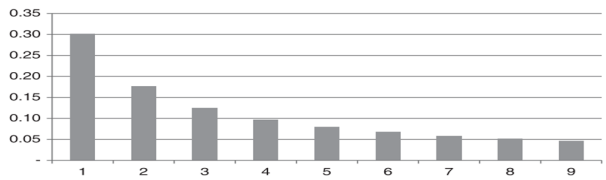

Figura 2. Lei de Benford distribuição de frequência do primeiro dígito [31, p. 50]

Existem algumas condições para que a Lei de Benford constitua um conjunto válido de frequências de dígitos esperados: i) a lista de números deve descrever fenómenos de dimensões semelhantes; ii) os números não devem ter máximos ou mínimos internos; iii) não devem ser atribuídos números usados para descrever elementos de um conjunto de dados (e.g., número segurança social ou número de conta corrente) [32].

A Lei de Benford faz parte de muitos planos de auditoria e é frequentemente utilizada pelos auditores. No entanto, nem sempre é bem interpretada. De facto, os resultados da aplicação da Lei de Benford devem ser o ponto de partida para o auditor [17], ou seja, ser uma ferramenta útil para auxiliar na identificação de alguns itens para novos testes [33] e identificar situações de fraude [22].

B. *Number Duplication Test ou Teste da Duplicação dos Números*

O *Number Duplication Test* (NDT) é um teste que pode ser usado para proporcionar mais informação decorrente da aplicação da Lei de Benford. Permite extrair números específicos que instigaram os picos no teste de primeira ordem e no teste da soma. Os picos no teste de primeira ordem são causados por números que ocorrem com maior frequência do que o esperado, enquanto os picos no teste da soma geralmente devem-se a elevadas quantidades dos mesmos números que se repetem com mais frequência do que o normal [17].

O resultado do NDT é uma tabela em formato de relatório que exibe: a classificação, o valor que foi duplicado, e a contagem para cada montante. O relatório mostra quais os números que ocorreram com maior frequência e com que frequência ocorreram. A tabela seria ordenada por contagem decrescente, de modo que a quantidade que ocorreu mais frequentemente apareça primeiro [29]. Este teste pode detetar possíveis ineficiências de processamento, ou seja, quando uma pequena transação foi processada mais que uma vez [17].

C. *Z-Score*

O *Z-score* é uma medida estatística de um número em relação à média do grupo de números. Refere-se a pontos ao longo da curva normal padronizada, sendo que o ponto central da curva tem um valor Z de zero. Um valor de Z à direita revela que está acima da média e à esquerda revela que está abaixo da média. A distância à média é medida pelo desvio padrão, que na distribuição normal padrão tem valor unitário. Assim, se o valor Z for de dois, significa que o número se afasta da média, para cima, em dois desvio-padrão.

O *Z-score* é calculado pela diferença entre o número ($\boldsymbol{X}$) e a média da população ($\boldsymbol{\mu}$), e dividindo a diferença obtida pelo desvio padrão populacional ($\boldsymbol{\sigma}$):

$$Z = \frac{(X - \mu)}{\sigma} \qquad (1)$$

Com o *Z-score*, a área sob a curva normal pode ser determinada pelo cálculo do computador ou observando as tabelas conforme exemplificado na Tabela 1. Uma pontuação Z de 1,50 indica que 43,32% por cento da área sob a curva normal está localizada entre a média e o valor Z. Quanto maior o valor absoluto do *Z-Score*, mais o número se afasta da média (da norma), podendo o auditor querer examinar transações que são *outliers* (valores extremos), isto é, que se afastam da média em, por exemplo, mais do que três desvios-padrão [17].

Tabela 1. Tabela Parcial de Z-Score [17, p. 82]

Z	Area between Mean and Z
0.30	.1179
0.50	.1915
0.80	.2881
1.00	.3413
1.50	.4332
1.80	.4649
1.96	.4750
2.58	.4951
3.90	.4999

D. Relative Size Factor Test (RSF)

O *Relative Size Factor Test (*RSF) identifica subconjuntos, em que o maior valor está fora de linha com os outros montantes para esse subconjunto [29]. Trata-se de um teste relevante para detetar erros. Ao existirem diferenças, estas podem ficar a dever-se ao facto de o maior registo pertencer a outro subconjunto, ou de pertencer ao subconjunto em análise, mas o valor numérico estar registado incorretamente. O teste RSF identifica subconjuntos onde a maior quantidade é significativamente maior do que os outros itens no subconjunto.

$$RSF = \frac{MAIOR\ REGISTO\ NUM\ SUBCONJUNTO}{SEGUNDO\ MAIOR\ REGISTO\ NUM\ SUBCONJUNTO} \quad (2)$$

A desvantagem deste teste é que é bastante difícil de programar, porque um subconjunto com apenas um registo não pode ter um RSF, uma vez que não há um segundo número maior. As etapas na execução deste teste são: i) excluir os números pequenos e irrelevantes; e ii) excluir todos os subconjuntos com apenas um registo. É pois necessário identificar o maior e o segundo maior número para cada subconjunto e estabelecer uma regra que se aplique se o maior e o segundo maior número forem ambos iguais [29].

Com este teste, os *outliers* podem não ser os maiores montantes em todo o conjunto de dados. Os *outliers* são apenas os valores elevados no subconjunto em análise. Grandes diferenças podem ser atribuídas a erros, tais como, o registo pertencer a outro subconjunto ou as quantidades estarem incorretamente atribuídas (e.g., ponto decimal deslocado). No entanto, podem ser uma indicação de atividade fraudulenta (e.g., fraude ocupacional de contas a pagar, faturas falsas, ou vendas de produtos para empresas relacionadas - preços de transferência *offshore*) [17].

E. Same-Same-Same Test (SSS)

O objetivo do *Same-Same-Same Test* (SSS) é identificar duplicações anormais como indicadores potenciais de erros ou fraude [17] e testar os controlos [29]. O objetivo é identificar duplicações exatas e podem-se usar vários campos para determinar se os registos são duplicados [29]. Exemplos de aplicação: os inventários terem o mesmo número de produto e a mesma quantidade disponível; num cartão bancário poder haver casos em que para o mesmo cartão, são apresentados os mesmos valores cobrados na mesma data (compra dividida para manter o limite abaixo do valor de controlo), reembolsos a funcionários; reembolsos a clientes.

Na Fig. 3 é apresentado o resultado de um teste em que se identifica os mesmos cartões, as mesmas datas, o mesmo fornecedor, e as mesmas quantidades. O campo mais à direita é a contagem e a maioria dos casos foi para duas compras idênticas. Resumindo, o teste SSS permite identificar registos que contêm campos com dados que são duplicações exatas de outros registos e duplicações anormais que sejam indicadores de potenciais erros ou fraude.

qrySameSameSame

CardNumber	Date	MerchantName	Amount	PurchaseCount
5142189945	12/28/2010	GE REUTER-STOKES, INC	$24,845.00	2
5142189945	9/18/2010	DELL MARKETING L.P.	$23,130.00	2
5142121593	12/22/2010	DELL MARKETING L.P.	$6,296.00	2
5142288601	9/11/2010	CHEM-TECH CONSULTING GR	$3,144.00	2
5142189945	5/10/2010	LYNDE-ORDWAY CO, INC.	$3,115.00	2
5142117663	8/18/2010	INORGANIC VENTURES INC	$2,542.68	2
5142123687	10/13/2010	RETAIL DEBIT ADJUSTMENT	$2,500.00	2
5142131721	5/11/2010	FBM COMPUTER & OFFICE SU	$2,500.00	2
5142149042	3/13/2010	CROWN PLAZA HOTEL	$2,500.00	4
5142153646	3/22/2010	INFORMATION MAPPING	$2,500.00	4
5142251068	4/11/2010	COLE INDUSTRIAL INC	$2,500.00	2
5142251068	4/24/2010	COLE INDUSTRIAL INC	$2,500.00	2

Figura 3. Exemplo de compras semelhantes na mesma data com o mesmo cartão

F. Same-Same-Different Test

O *Same-Same-Different Test* (SSD) é usado para identificar registos duplicados semelhantes nos campos selecionados pelo auditor [17]. É preponderante para detetar erros e fraude, sendo um aliado nos projetos de análise forense. Recentemente numa investigação de compra de cartões de uma empresa de serviços públicos, este teste evidenciou vários casos em que dois funcionários dividiam a mesma compra usando cartões diferentes[29]. O teste é executado de modo a que o campo que difere seja um campo do subconjunto detetando as transações que estão ligadas a dois subconjuntos diferentes. O pressuposto é que uma das transações é um erro e não deve ter sido vinculada ao segundo (subconjunto diferente), ou seja, cada caso corresponde a duas linhas na tabela de resultados [17].

G. Even Amount/Números Redondos

Números pares ou arredondados normalmente não ocorrem com uma elevada taxa de frequência. Por conseguinte, os números que são arredondados para dezenas, centenas ou milhares podem ser considerados anomalias, devendo ser-lhe ser dada atenção especial. Relativamente a faturas a pagamento, geralmente dá-se mais destaque às que têm valores mais altos, mas as de valores baixos, também são suscetíveis a fraude. A título de exemplo, quando se fixam tetos máximos para a realização de determinadas despesas (almoços, jantares, alojamento), para garantir que não há abuso, deve-se verificar tanto os valores como as quantidades [17]. Este teste permite identificar, por exemplo, os fornecedores que têm uma elevada percentagem de faturas com montantes arredondados. Há situações que não são anomalias, como, por exemplo trabalhos de consultoria ou rendas [17].

VI. CONCLUSÕES

Pretendeu-se com este trabalho fazer um breve enquadramento da fraude. Este trabalho debruçou-se sobre métodos analíticos para deteção de irregularidades e fraude, já que estas são preocupações da profissão de auditor.

Ilustrou-se a análise de dígitos através da Lei de Benford e, também, outros testes, nomeadamente, os testes da duplicação de números, *Relative size factor*, *Same-same-same*, *same-same-different* e *Z-score.* Estes podem ser utilizados para análise de dados a nível de ferramentas de auditoria e podem ser executados através do *software* de análise de dados. Todos eles visam ajudar os auditores a detetarem dados suspeitos. Embora as técnicas não identifiquem os pontos de dados que são suspeitos, as técnicas podem alertar o auditor sobre a possível presença de dados suspeitos.

Os testes propostos podem ser aplicados em empresas de qualquer dimensão para detetar anomalias e fornecer evidência para investigação futura na área de fraude. Assim, propõe-se, como trabalho futuro, a aplicação destes testes sobre os dados das vendas disponíveis no ficheiro SAFT-PT, nomeadamente, para detetar a correção dos valores por tipo de documento, apurar desvios quanto a descontos efetuados, e analisar ofertas sistemáticas de produtos aos mesmos clientes. Este conjunto de análises, caso identifique anomalias, pode permitir proceder a recomendações ao nível dos procedimentos de controlo interno das organizações.

AGRADECIMENTO

À FCT-Fundação para a Ciência e Tecnologia, pelo apoio no âmbito do projeto estratégico UID/GES/00315/2013

REFERÊNCIAS BIBLIOGRÁFICAS

[1] IPAI, "Enquadramento Internacional de Práticas Profissionais de Auditoria Interna," 2009.
[2] IFAC, "ISA 240 - As Responsabilidades do Auditor Relativas a Fraude numa Auditoria de Demonstrações Financeiras," pp. 1–26, 2012.
[3] O. C. Bunget, L. Grigoroi, and A. C. Dumitrescu, "Detecting and Reporting the Frauds and Errors By the Auditor.," *Megatrend Rev.*, vol. 6, no. 1, pp. 279–291, 2009.
[4] Association of Certified Fraud Examiners, "Report To The Nations 2012, Global Fraud Study," 2012.
[5] ACFE - Association of Certified Fraud Examiners, "Report To The Nations 2016, Global Fraud Study," 2016.
[6] D. R. Cressey, "Other People's Money," Montclair: Patterson Smith, Ed. 1953.
[7] A. A. Arens, R. J. Elder, and M. S. Beasley, *Auditoría : un enfoque integral*, 11ª Edición. 2007.
[8] A. C. Hencsey, "A definição, o processo de racionalização no triângulo da fraude e a complexidade de sua construção psicológica," 53/2016, 2016.
[9] F. Dal-Ri Murcia, J. A. Borba, and E. Schiehll, "Relevância dos Red Flags na Avaliação do Risco de Fraudes nas Demonstrações Contábeis: a Percepção de Auditores Independentes Brasileiros," *Rev. Universo Contábil*, pp. 25–44, 2008.
[10] R. Kassem and A. Higson, "The New Fraud Triangle Model," *J. Emerg. Trends Econ. Manag. Sci.*, vol. 3, no. No. 3, p. 191–195 MAZAR, 2012.
[11] J. Dorminey, S. Fleming, M. Kranacher, and R. Riley, "The evolution of fraud theory," *American Accounting Association Annual Meeting*, Denver, pp. 1–58, 2011.
[12] P. R. Murphy and M. T. Dacin, "Psychological Pathways to Fraud : Understanding and Preventing Fraud in Organizations," vol. 99, pp. 601–618, 2011.
[13] Z. Rezaee, *Financial Statement Fraud Prevention and Detection*. New York, 2002.
[14] M. Marques, *Auditoria e Gestão*, 1ª EDIÇÃO. 1997.
[15] C. B. Costa, *Auditoria Financeira-Teoria & Prática*, 9ª. Letras e Conceitos, Lda., 2010.
[16] T. A. Runkler, *Data Analytics - Models and Algorithms for Intelligent Data Analysis*. Germany, 2012.
[17] S. Gee, *Fraud and Fraud Detection A Data Analytics Approach*. 2015.
[18] Deloitte, "Adding insight to audit - Transforming Internal Audit through data analytics," *Detroit, MI : Deloitte Touche Tohmatsu LTD*, 2012. [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/audit/us-aers-adding-insight-pov-mobile-061913.pdf. [Accessed: 20-Jul-2017].
[19] ICAEW, *Data analytics for auditors*. 2016.
[20] T. Bishop *et al.*, "Managing the Business Risk of Fraud : A Practical Guide," pp. 1–80, 2007.
[21] A. Banarescu, "Detecting and Preventing Fraud with Data Analytics," vol. 32, no. 15, pp. 1827–1836, 2015.
[22] M. F. Hess and J. H. Cottrell, "Fraud risk management: A small business perspective," *Business Horizons*, vol. 59, no. 1, Elsevier Inc., pp. 13–18, 2016.
[23] S. Gee, *Bringing Sophistication to Data Analytics*. 2012.
[24] I. Pedrosa, "THESIS: Computer-assisted audit tools and techniques use: determinants for individual acceptance," ISCTE - Instituto Universitário de Lisboa, 2015.
[25] W. S. Albrecht, C. O. Albrecht, C. C. Albrecht, and M. F. Zimbelman, *Fraud Examination*, 5ª. 2016.
[26] J. Kaplan, "2012 Survey Report on Data Analysis Audit Software," *AuditNet*, 2012.
[27] J. Kaplan, "Turning Analytics From 'Nice to Have' 'Must Have,'" *Audinet*, 2016. .
[28] W. A. Wallace, "Assessing the quality of data used for benchmarking and decision making," *Journal of Government Financial Management 51*, pp. 16–22, 2002.
[29] M. J. Nigrini, "Forensic Analytics Methods and Techniques for Forensic Accounting Investigations," Wiley, Ed. 2011.
[30] R. Lowe, "Benford"s law and fraud detection," *Chart. Accountants J. New Zeal.*, pp. 32–36, 2000.
[31] B. Baesens, V. Van Vlasselaer, and W. Verbeke, "Fraud Analytics Using Descriptive, predictive, and social Network Techniques - A Guide to Data Science for Fraud Detection," Hoboken, New Jersey.: John Wiley & Sons, Inc., 2015.
[32] M. J. Nigrini and L. I. Mittermaier, "The Use of Benford's Law as an Aid in Analytical Procedures," *A J. Pract. Theory*, vol. 16, no. 2, pp. 1–8, 1997.
[33] C. Durtschi, W. Hillison, and C. Pacini, "The Effective Use of Benford ' s Law to Assist in Detecting Fraud in Accounting," *J. Forensic Account.*, no. January, pp. 17–34, 2004.