DETECÇÃO DE INDÍCIOS FRAUDES CONTÁBEIS POR MEIO DO USO COMBINADO DO POWER BI E DA LEI DE BENFORD

Saulo Martoreli Da Silva De Moraes - Universidade Federal de Santa Catarina - UFSC

Sérgio Murilo Petri - Universidade Federal de Santa Catarina - UFSC

Resumo

A Lei de Benford, ou Lei do Primeiro Dígito, tem sido utilizada como instrumento para a detecção de fraudes contábeis. Auditores internos e externos, controllers e demais responsáveis pela governança das entidades podem se beneficiar deste instrumento estatístico como ponto de partida para a análise de dados inconsistentes. Já o Power BI é uma ferramenta de Business Intelligence que possui a capacidade de analisar grandes volumes de dados, além de agregar diversos benefícios relacionados com a visualização de dados. Dessa forma, este artigo apresenta um estudo de caso em que se desenvolveu um dashboard que demonstra como o uso combinado da Lei de Benford e o Power BI pode trazer benefícios para a detecção de fraudes contábeis. Os resultados demonstram que essa combinação pode ser efetivamente implementada pelos profissionais da área.

Palavras-chave: Fraudes Contábeis; Lei de Benford; Power BI.

Abstract

Benford's Law, or the Law of the First Digit, has been used as a tool for detecting accounting fraud. Internal and external auditors, controllers and other people responsible for the governance of entities can benefit from this statistical tool as a starting point for analyzing inconsistent data. Power BI is a Business Intelligence tool that has the ability to analyze large volumes of data, in addition to adding several benefits related to data visualization. Thus, this article presents a case study in which a dashboard was developed that demonstrates how the combined use of Benford's Law and Power BI can bring benefits to the detection of accounting fraud. The results demonstrate that this combination can be effectively implemented by professionals in the field.

Keywords: Accounting Fraud; Benford's Law; Power BI.

DETECÇÃO DE INDÍCIOS FRAUDES CONTÁBEIS POR MEIO DO USO COMBINADO DO POWER BI E DA LEI DE BENFORD

1 INTRODUÇÃO

A palavra "fraude" tem origem no latim *fraus*, tendo sido usada em um sentido próprio por Tito Lívio em sua "História de Roma", carregando a ideia de se trazer dano a alguém e, usada em um sentido indeterminado por Cícero para significar a ideia de crime ou delito (Hoog; Sá, 2005). Em sentido amplo, o termo "fraude" pode abranger qualquer crime com o objetivo de se obter algum ganho por meio do uso do engano como seu principal *modus operandi* (Wells, 2005). Diferente do erro, que é sempre um ilícito, a fraude é sempre um delito (Hoog; Sá, 2005).

A Association of Certified Fraud Examiners (ACFE, 2023), classifica as fraudes em três categorias: (1) contra indivíduos, ou seja, as fraudes praticadas contra uma pessoa específica, incluindo, por exemplo, o roubo de identidade, golpes de *phishing* e esquemas de taxa antecipada; (2) fraude organizacional interna ou fraude ocupacional, ou seja, aquela que ocorre quando um funcionário, gerente ou executivo de uma organização busca enganar a própria organização à qual pertence; e (3) fraude organizacional externa, ou seja, aquela cometida por agentes externos à organização, como clientes e fornecedores. Dentre estes tipos de fraudes, esta pesquisa explora o tipo de fraude ocupacional (ou fraude organizacional interna), de acordo com a nomenclatura adotada pela ACFE (2023).

Sob a perspectiva contábil e financeira, as fraudes consistem em um problema de amplitude mundial (Bao et al., 2019). Nas últimas décadas, as alegações de fraudes corporativas dominaram as notícias globais (Shahana; Lavanya; Bhat, 2023). Casos como o da Enron, WorldCom, Tyco e Satyam se tornaram clássicos na literatura sobre fraudes contábeis e financeiras. No cenário brasileiro, casos recentes como o das Lojas Americanas (Carvalho; Silva, 2024) e da Via Varejo S.A. (Krauspenhar; Rover, 2020) confirmam a realidade de que nenhuma empresa está imune à fraude e nenhuma empresa pode ter certeza de que não é ou que não será vítima de fraude por parte de seus funcionários, de sua administração ou de terceiros (Krambia-Kapardis; Zopiatis, 2010).

A identificação de fraudes envolve o conhecimento dos sintomas presentes nos dados analisados que apontam para uma possível ocorrência de fraude (Coderre, 2009). Segundo Omidi *et al.* (2019), os procedimentos de auditoria provaram ter muitas deficiências na detecção de relatórios financeiros fraudulentos. Isso ocorre, simplesmente, porque tais procedimentos não foram projetados para isso. Barreto; Graeff (2010) argumentam que a administração da entidade e seus responsáveis pela governança são os principais responsáveis pela prevenção e detecção das fraudes, não sendo, portando, o auditor responsável por isso, já que sua responsabilidade é obter segurança razoável de que as demonstrações contábeis não contêm distorções relevantes causadas por fraudes ou erros. Segundo Omidi *et al.* (2019), em uma organização, o gestor é aquele que é moralmente responsável pela detecção de dados financeiros fraudulentos, mas a maioria das fraudes nas Demonstrações Financeiras são cometidas com o conhecimento ou consentimento da administração. Para Gepp et al. (2018), os auditores poderiam aproveitar técnicas e métodos de *big data* para prever dificuldades financeiras e, combinados com seus julgamentos profissionais, ser mais capazes de avaliar a viabilidade financeira futura de uma empresa.

A tecnologia da informação é uma aliada na aplicação prática das diversas técnicas de detecção de fraudes contábeis e financeiras (Oliveira *et al.*, 2021). *Softwares* especializados de detecção de fraudes possibilitam aos auditores automatizarem diversas tarefas, como a extração e análise de dados, além de poderem executar rotinas específicas de auditoria e análise estatística (Ahmi; Kent, 2012; Wicaksono; Lusianah, 2016; Matherly, 2009). No entanto,

interpretar a saída dessas ferramentas pode exigir habilidade considerável dos auditores, pois as anomalias nos dados podem não ser facilmente aparentes, exceto para o investigador especialista (Dilla; Raschke, 2015). Além disso, estes *softwares* podem apresentar barreiras importantes como os altos custos de implementação, significativa curva de aprendizado e problemas de integração entre o *software* e as fontes externas de informação (Ahmi; Kent, 2012; Wong; Venkatraman, 2015).

Como alternativa a estes softwares de detecção de fraudes, os sistemas de *Business Intelligence* (BI) apresentam características que podem ser muito úteis para a detecção de fraudes contábeis, ainda que muito pouco tenha sido feito para explorar sua eficácia na área de detecção e prevenção de fraudes (Lokanan, 2023). Dentre estas características, está a de fazer uso de várias técnicas de *data mining* para prover *dashboards* para os analistas realizarem avaliações rapidamente (Wong; Venkatraman, 2015). Outra característica importante é que os sistemas de BI garantem a obtenção de informações úteis, corretas e oportunas, geralmente provenientes de fontes de dados diferentes (Aquize; Filho, 2018), além de serem usados para fazer uma previsão para o ambiente dinâmico ou extrair padrões úteis por meio de detecção de valores discrepantes, mineração de processos e *clustering* (Duan; Da Xu, 2012).

Com o avanço dos estudos no campo de detecção de fraudes, diversas técnicas vêm sendo empregadas para dar suporte aos auditores e responsáveis pela governança das entidades. Dentre estas técnicas está a Lei de Benford (*Benford's Law)*, também chamada de Lei do Primeiro Dígito, que se refere à distribuição de frequência dos dígitos em muitas (mas não todas) fontes de dados da vida real (Undavia, 2022). Para detectar comportamento fraudulento em dados contábeis, pode-se comparar a distribuição de dígitos do conjunto de dados com a distribuição teórica da Lei de Benford (Renaldo *et al.,* 2022). Embora diversos trabalhos já tenham sido desenvolvidos no sentido de utilizar a Lei de Benford no contexto da detecção de fraudes contábeis (Undavia, 2022; Renaldo *et al.,* 2022), percebe-se um *gap* na literatura em relação a operacionalização desta técnica por meio do uso do Power BI.

Sendo assim, esta pesquisa busca dedicar sua atenção à operacionalização da Lei de Benford por meio do Power BI, de forma a ter como produto um *dashboard* que possa trazer *insights* aos auditores, *controllers* e diversos responsáveis pela governança das entidades. Além da Lei de Benford, o *dashboard* será incrementado com outras ferramentas, como *Chi-Square* (X^2) e o *Z Test.*

2 DESENVOLVIMENTO

Esta seção está dividida em três partes. Na primeira parte são apresentados os aspectos relacionados com os conceitos basilares relacionados com as fraudes contábeis e financeiras, bem como, com os fatores motivacionais das fraudes e suas tipificações, além de abordar aspectos relacionados com a prevenção, detecção e a investigação das fraudes. Na segunda parte a Lei de Benford é apresentada em seu aspecto histórico e técnico, demonstrando seu funcionamento teórico. Por fim, a última seção apresenta a metodologia adotada, dando destaque para o instrumento de intervenção utilizado na pesquisa, o Power BI.

2.1 FRAUDES CONTÁBEIS E FINANCEIRAS

A seguir são abordados os aspectos relacionados com a definição e tipificação das fraudes contábeis e financeiras. Além disso, são abordados aspectos relacionados com a prevenção, detecção e investigação das fraudes.

2.1.1 Definição de Fraudes Contábeis e Financeiras

As fraudes contábeis e financeiras têm representado uma preocupação dentro das organizações em vista de seus significativos impactos negativos (Aftabi; Ahmadi; Farzi, 2023; Seify et al., 2022; Tang; Karim, 2019; Costa, 2012). Para Tang e Karim (2019), o tema das fraudes financeiras continua sendo um dos mais discutidos na literatura contábil. Os métodos fraudulentos estão cada vez mais sofisticados, exigindo das organizações níveis de controle cada vez maiores. Um dos fatores que podem tornar a detecção de fraudes contábeis e financeiras mais difícil é que elas são fruto de ações coordenadas, que ocorrem ao longo do tempo (Costa, 2012)

Diversos são os motivos podem levar uma determinada pessoa ou um determinado grupo de pessoas a cometerem uma fraude. O ponto de partida para a teoria das fraudes foi dado pelo sociólogo americano Donald Cressey, que em 1953 apresentou os três elementos do que seria chamado posteriormente de "Triângulo da Fraude" (Wells, 2005; Free, 2015). O Triângulo da Fraude apresenta três elementos que levam um indivíduo a cometer uma fraude: a pressão, a oportunidade e a racionalização. Posteriormente, duas novas teorias buscaram complementar a teoria do Triângulo da Fraude. A primeira delas foi a teoria do "Diamante da Fraude", que acrescentou o elemento "capacidade" ao modelo anterior (Paschoal; Santos; Faroni, 2020). Em um momento posterior, um novo modelo de compreensão da teoria da fraude incluiu o elemento "arrogância", formando, assim, o chamado "Pentágono da Fraude" (Haqq; Budiwitjaksono, 2019).

Nesta seção estes motivos que levam indivíduos ou grupos sociais a cometerem fraudes serão detalhados, buscando demonstrar como a literatura trata os fatores motivacionais das fraudes, bem como suas tipificações e as técnicas de prevenção e detecção delas.

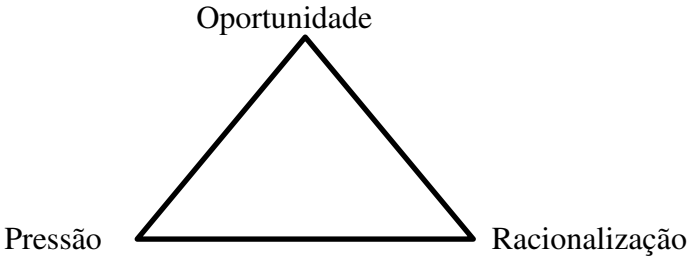
2.1.2 Fatores Motivacionais das Fraudes

Desde 1953 tem-se desenvolvido teorias que buscam compreendem o fenômeno das fraudes, analisando suas causas e motivações. Dentre as teorias de destaque estão as teorias do Triângulo da Fraude, do Diamante da Fraude e do Pentágono da Fraude (Christian; Basri; Arafah, 2019). Em 1953 Donald Cressey, um criminologista, publicou um artigo intitulado "Other People's Money: A Study in the Social Psychology of Embezzlement" ["O dinheiro dos outros: um estudo da psicologia social do desfalque"], onde iniciou o estudo da fraude argumentando que deve haver uma razão por trás de tudo que as pessoas fazem (Cressey, 1953; Abdullahi; Mansor, 2015).

A hipótese criada por Cressey (1953) possibilita a análise do comportamento fraudulento de gestores em corporações por intermédio da análise de três dimensões: pressão, oportunidade e racionalização (Machado; Gartner, 2017). É frequente a atribuição a Cressey o termo "Triângulo da Fraude", no entanto, seus escritos não apresentam este termo, que fora cunhado posteriormente por Joseph Wells (Morales et al., 2014). A partir do trabalho iniciado por Cressey na área da criminologia, Joseph Wells e outros proponentes fizeram traduções significativas no processo, especialmente ao articular uma definição específica de fraude que resultou em uma série de desvios ou vieses do trabalho criminológico original (Morales et al., 2014). Ao longo dos anos, portanto, a hipótese de Cressey tem sido denominada de "Triângulo da Fraude" (Wells, 2005), conforme demonstrado na Figura 1.

Albrecht (2003) faz uma analogia com o "Triângulo do Fogo" para explicar a lógica do "Triângulo da Fraude". Assim como no Triângulo do Fogo é necessário que os três elementos (oxigênio, calor e combustível) estejam presentes para que um incêndio ocorra, no Triângulo da Fraude é preciso que os três elementos (Pressão, Oportunidade e Racionalização) ocorrem simultaneamente para que a fraude seja perpetrada. Wells (2005, p.17) concorda ao afirmar que a o aspecto chave para compreender a "Teoria de Cressey" é lembrar que todos os três elementos devem estar presentes para que a "violação da confiança" ocorra.

Figura 1 – Triângulo da Fraude



Fonte: Adaptado de Wells (2005, p. 13).

Embora a pressão enfrentada pelo perpetrador da fraude possa ser financeira ou não-financeira (Abdullahi; Mansor, 2015), Albrecht (2003) destaca que cerca de 95% dos elementos de pressão das fraudes são financeiros ou relacionados a vícios dos perpetradores das fraudes. Além disso, dentre as principais pressões financeiras relacionadas com o cometimento de fraudes estão a ganância, o desejo de viver além dos próprios meios, contas altas ou dívidas pessoais, indisponibilidade de crédito, perdas financeiras pessoais e necessidades financeiras inesperadas (Albrecht, 2003).

Na visão de Cressey, há dois componentes do elemento "oportunidade": a informação geral, que está relacionada com o conhecimento de que determinada posição de confiança pode ser violada; e a habilidade técnica, ou seja, a detenção das habilidades necessárias para cometer a violação (Wells, 2005). Dito que outra forma, "a oportunidade pressupõe que os fraudadores têm o conhecimento e a chance para cometer a fraude" (Machado; Gartner, 2017, p. 64). É importante destacar que a dimensão da oportunidade está relacionada com a ineficácia dos sistemas de controle ou governança, que permitem que um indivíduo cometa a fraude (Abdullahi; Mansor, 2015). Essas brechas do sistema de controle ou governança podem ocorrer, por exemplo, devido à divisão de trabalho inadequada, controle interno fraco, auditoria irregular e afins (Abdullahi; Mansor, 2015). Albrecht (2003) apresenta uma lista não exaustiva em que destaca como fatores criadores de oportunidades a falta ou evasão de controles que previnam e/ou detectem comportamento fraudulento, incapacidade de julgar a qualidade do desempenho, falha em disciplinar o autor da fraude, falta de acesso à informação, ignorância, apatia e falta de trilhas de auditoria.

Por fim, o último elemento do Triângulo da Fraude consiste na "Racionalização". Wells (2005) explica que na hipótese de Cressey a racionalização não se trata de um elemento que ocorre após a violação, mas antes. Trata-se, portanto, "de uma parte da motivação do crime" (Wells, 2005. p. 17). O conceito de racionalização está relacionado com a ideia que o perpetrador deve formular alguma ideia moralmente aceitável para ele antes de se envolver em comportamento antiético (Abdullahi; Mansor, 2015). Um aspecto interessante é que após a realização do ato criminoso, a racionalização tenderá a ser abandonada (Wells, 2017).

Numa tentativa de desenvolver o entendimento acerca dos fatores que influenciam o cometimento de fraudes, surgiu a teoria do Diamante da Fraude, que incluiu o elemento "capacidade" à teria anterior do Triângulo da Fraude (Nurkhin et al., 2018; Haqq; Budiwitjaksono; 2019). Esta teoria foi proposta por Wolfe; Hermanson (2004), que acreditavam que o triângulo da fraude poderia ser aprimorado para melhorar tanto a prevenção quanto a detecção de fraudes, considerando um quarto elemento, a capacidade. Para os autores, muitas fraudes, especialmente algumas multibilionárias, não teriam ocorrido sem a presença da pessoa certa com os recursos certos. A oportunidade, segundo eles, abre a porta para a fraude, e o incentivo e a racionalização podem atrair a pessoa para ela. No entanto, eles apontam que a pessoa deve ter a capacidade de reconhecer a porta aberta como uma oportunidade e aproveitá-

la caminhando por ela, não apenas uma vez, mas repetidas vezes. Assim, a questão crítica consiste em identificar quem poderia transformar uma oportunidade de fraude em realidade.

Posteriormente, a Teoria do Pentágono da Fraude trouxe uma nova dimensão à teoria do Diamante da Fraude. Esta teoria adicionou a dimensão "arrogância" às quatro dimensões anteriores (Apriliana; Agustina, 2017). A arrogância, no âmbito corporativo representa a natureza gananciosa e a superioridade de si mesmo sobre as políticas corporativas (Mangala; Kumari, 2015). Quraini; Rimawati (2018) explicam que um alto grau de arrogância e superioridade pode levar à fraude porque o CEO sente que qualquer controle interno não se aplica a ele.

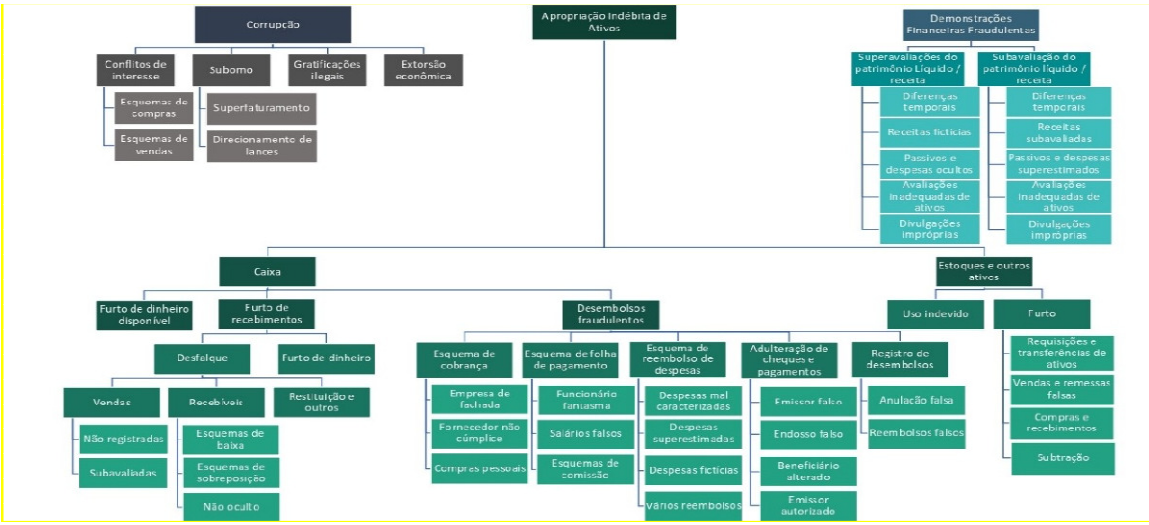
Dessa forma, tem-se um desenho dos fatores motivacionais das fraudes. O desafio dos controles internos está em buscar limitar as possibilidades que possam criar motivações para o cometimento de ilícitos que possam prejudicar a organização.

Se houver uma força do conselho de administração para atingir um determinado montante de ganhos, e os rendimentos auferidos estiverem ligados aos bónus da administração, foram criados estímulos motivacionais suficientes para relatórios financeiros fraudulentos (Lokanan; Sharma, 2022).

2.1.3 Características e Tipos de Fraudes

A ACFE (2023) classifica as fraudes em duas categorias básicas: fraudes cometidas contra indivíduos e fraudes cometidas contra organizações, sendo que esta última é subdivida em duas partes; as fraudes organizacionais externas e as internas (também conhecidas como "fraudes ocupacionais").

Figura 2 – Árvore das Fraudes Ocupacionais e Abusos



Fonte: Said (2020, p. 61).

As fraudes ocupacionais (ou internas), objeto desta pesquisa, contêm uma grande variedade de esquemas específicos, com suas caraterísticas próprias. Esse tipo de fraude resulta da má conduta de funcionários, gerentes ou executivos (Albrecht, 2003).

Em 1996 a Association of Certified Fraud Examiners (ACFE) criou a chamada "Árvore da Fraude", que busca, desde então, classificar os tipos de Fraudes Ocupacionais. A ACFE define três ramos principais na Árvore da Fraude: (i) apropriação indébita de ativos; (ii) corrupção e (iii) relatórios (Demonstrações Financeiras) fraudulentos (Mackevičius; Kazlauskienė, 2009; Said, 2020). A Figura 2 – Árvore das Fraudes Ocupacionais e Abusos, apresenta a estrutura proposta pela ACFE (2023).

2.1.4 Prevenção, Detecção e Investigação de Fraudes

Albrecht (2003) estabelece uma distinção entre a prevenção, a detecção e a investigação de fraudes. Segundo ele, a prevenção das fraudes representa a forma que possui o maior custo-benefício quando se tem por objetivo reduzir as perdas com fraudes. Além disso, pensando na criação de um ambiente favorável, ele explica que a prevenção de fraudes pode ser obtida: (1) criando uma cultura de integridade e honestidade; e, (2) avaliando o risco de fraude e desenvolvendo respostas concretas para minimizar o risco e eliminar oportunidades. Mangala; Kumari (2015) adicionam que a busca pela prevenção da fraude começa com o conhecimento do que é realmente a fraude, suas consequências, formas de cometê-la e como preveni-la. Essas informações, quando obtidas, devem ser colocadas no sistema de controle para implementar medidas de prevenção e o monitoramento deve ser feito para evitar a reincidência de fraudes. A prevenção de fraudes, portanto, descreve medidas para impedir, primeiramente, que a fraude ocorra, enquanto a detecção envolve a identificação da fraude o mais rápido possível, uma vez que ela tenha sido perpetrada (Bolton; Hand, 2002).

Quanto à detecção de fraudes, Bolton; Hand (2002) explicam que esta é uma estratégia *post hoc*, sendo aplicada depois que a prevenção falhou. Como a maioria das fraudes aumenta drasticamente com o tempo, é muito importante que as fraudes, quando ocorrerem, sejam detectadas com antecedência (Albrecht, 2003). Nesta direção, os métodos de detecção ajudam a detectar fraudes e denunciá-las à autoridade apropriada (Mangala; Kumari, 2015). Oliveira et al. (2021, p. 160) analisaram o uso de tecnologias para detecção de Fraudes na Pandemia da Covid-19 e citam que "Na era digital novas técnicas de detecção de fraudes, foram transformadas, em decorrência do 'DigitalEra Governance', concebida por frameworks como Big Data, Internet das coisas (IoT) e inteligência artificial.". Dado o aumento considerável no volume de dados gerados pelas organizações, o uso destas tecnologias, portanto, pode ser um grande aliado na identificação de anomalias durante o processo de detecção de fraudes.

Já a etapa de investigação tem como propósito encontrar a verdade a partir de sintomas identificados, para verificar se eles representam uma fraude ou um erro não intencional, sempre mantendo o cuidado para que ela seja conduzida de maneira apropriada, sem causar danos à reputação de pessoas inocentes ou deixando de identificar os reais culpados (Albrecht, 2003). Trata-se, portanto, de uma etapa posterior, que se baseia em evidências identificadas na fase de detecção.

2.2 LEI DE BENFORD

Esta seção está dividida em duas partes. Na primeira são apresentados os aspectos teóricos relacionados com a Lei de Benford, dando destaque para a distribuição da ocorrência do primeiro dígito. Na segunda parte são apresentados estudos anteriores que aplicaram a Lei de Benford no contexto da detecção de fraudes contábeis e financeiras.

2.2.1 Lei de Benford - Definições

A Lei de Benford é um fenômeno numérico no qual conjuntos de dados que contam ou medem algum evento seguem uma determinada distribuição. Também conhecida como lei do primeiro dígito, esta lei revela um padrão surpreendente na distribuição dos dígitos em diversos conjuntos de dados. Essa lei afirma que, em muitos conjuntos de dados gerados por processos naturais e sociais, a probabilidade de um dígito ser o primeiro (da esquerda para a direita) segue uma distribuição logarítmica. (Geyer; Williamson, 2004, p. 229).

Esta lei foi concebida pelo astrônomo e matemático Simon Newcomb, em 1881. Seus estudos demonstraram que a ocorrência de um número natural, de modo espontâneo ou

aleatório, não se dava na proporção esperada de 1/9, mas segundo uma distribuição logarítmica (Orth; Michaelsen; Lerner, 2020). No entanto, foi somente em 1938 que Frank Benford, um físico do Schenectady, Nova York, General Electric Research Laboratories, notou, quase por acidente, que havia um padrão natural na frequência do aparecimento de números de baixa ordem em conjuntos legítimos de dados. Posteriormente, depois de quase 50 anos, Mark Nigrini descobriu que a lei de Benford poderia ser uma valiosa ferramenta de auditoria (Nigrini; 2001).

Segundo Nickell; Schwebke; Goldwater (2023) a Lei de Benford é uma observação sobre a distribuição de frequência dos dígitos iniciais em muitos conjuntos de dados numéricos da vida real. A lei afirma que, em muitas coleções de números que ocorrem naturalmente, o dígito significativo inicial provavelmente será pequeno. Por exemplo, em conjuntos de dados que obedecem à lei, o número 1 aparece como o dígito mais significativo cerca de 30% do tempo, enquanto 9 aparece como o dígito mais significativo <5% do tempo (vide Tabela 1).

Nguyen; Duong; Nguyen (2021) explicam que a Lei de Benford se refere à probabilidade distribucional dos dígitos de números em um conjunto de dados. A lei indica que cada dígito aparecerá com uma certa frequência no conjunto de dados. Desvios das frequências esperadas são indicações da existência de vieses, por exemplo, erros não intencionais ou alterações deliberadas, em conjuntos de dados.

Boritz; Covvey (2006) explicam que a Lei de Benford requer que: (1) As entradas em um conjunto de dados devem registrar valores de fenômenos semelhantes. Ou seja, os dados registrados não podem incluir entradas de dois fenômenos diferentes, como registros populacionais de censo e medições dentárias; (2) Não deve haver valores mínimos ou máximos incorporados no conjunto de dados. Sendo assim, os registros para os fenômenos devem ser completos, sem valor inicial artificial ou valor de corte final; (3) o conjunto de dados não deve ser composto de números atribuídos, como números de telefone; e (4) o conjunto de dados deve ter mais entradas de valores pequenos do que entradas de valores grandes.

A lei de Benford prevê, portanto, a frequência esperada do aparecimento dos dígitos em qualquer matriz estatística ou geométrica (Nigrini, 2001). A Tabela 1- Frequências de dígitos para números de Benford apresenta a distribuição dos primeiros dígitos.

Tabela 1- Frequências de dígitos para números de Benford

Dígito	Primeiro Dígito	Segundo Dígito	Terceiro Dígito	Quarto Dígito
0	–	11,968%	10,178%	10,018%
1	30,103%	11,389%	10,138%	10,014%
2	17,609%	10,882%	10,097%	10,010%
3	12,494%	10,433%	10,057%	10,006%
4	9,691%	10,031%	10,018%	10,002%
5	7,918%	9,668%	9,979%	9,998%
6	6,695%	9,337%	9,940%	9,994%
7	5,799%	9,035%	9,902%	9,990%
8	5,115%	8,757%	9,864%	9,986%
9	4,576%	8,500%	9,827%	9,982%
Total	100%	100%	100%	100%

Fonte: Adaptado de Busta; Weinberg (1998, p. 359).

Como pode ser observado na Tabela 1, a probabilidade de ocorrência, por exemplo, do dígito 1 na primeira posição (ou primeiro dígito) é de 30,103%, enquanto a probabilidade de ocorrência do dígito 9 na primeira posição é de apenas 4,576%

2.2.2 Lei de Benford – Estudos Anteriores

Diversos estudos anteriores buscaram demonstrar a efetividade da aplicação da Lei de Benford no empreendimento de detecção de fraudes contábeis e financeiras. Mark Nigrini foi um dos pioneiros na aplicação da Lei de Benford na auditoria (Nigrini, 2001).

Nickell; Schwebke; Goldwater (2023) realizaram uma pesquisa para avaliar o uso do *software* Power BI para detectar irregularidades contábeis utilizando a técnica Benford's Law. O estudo de caso elaborado pelos autores apresenta o uso da análise de dados na contabilidade para fins de identificação de irregularidades em um grande conjunto de dados de *invoices* usando o Microsoft Power BI. A pesquisa demonstrou ser possível a combinação desta técnica com o Power BI, apresentando um roteiro detalhado de como a análise dos dados por meio da Lei de Benford usando o Power BI.

Aybars; Ataunal (2016) testaram a conformidade dos números relatados pelas empresas listadas na bolsa de valores da Turquia, a Borsa Istanbul (BIST), com a Lei de Benford, por meio de dados entre 2005 e 2015 cobrindo 148 empresas. Para isso, os autores aplicaram uma metodologia que avaliou os dois primeiros dígitos à luz da Lei de Benford, combinando esta análise com o teste qui-quadrado (χ^2) e o teste Z. Eles identificaram que os números relatados de ativos circulantes e vendas líquidas pareciam estar quase em perfeita conformidade com a Lei de Benford. No entanto, o estudo detectou vários pontos de desvio nos dados de ativos totais e números de lucro líquido da Lei de Benford. Segundo eles, na aplicação da Lei de Benford, a não conformidade deve ser avaliada com discrição. Os desvios são apenas um sinal para analisar os dados mais profundamente e não devem ser vistos como uma prova sólida de fraude ou manipulação.

Undavia (2022) realizou um estudo de caso, onde procurou aplicar a Lei de Benford para detectar fraude contábil no banco *Punjab & Sind.* O autor analisou as demonstrações financeiras do banco no período de 2011 a 2021. Para isso, ele utilizou ferramentas estatísticas como o Teste Qui-Quadrado e o Teste Z para analisar a Demonstração de Resultados, o Balanço Patrimonial e a Demonstração do Fluxo de Caixa. Os resultados obtidos sinalizaram desvios importantes em relação à distribuição de frequência esperada pela Lei de Benford, especialmente para os dígitos 3 e 8, sugerindo possíveis manipulações financeiras.

Gonçalves *et al.* (2023) realizaram um estudo que objetivou identificar se o modelo proposto por Newcomb Benford pode ser utilizado como *red flag* na avaliação dos pagamentos realizados pela administração pública federal do Brasil. Para isso, os autores coletaram as ordens de pagamentos emitidas pela administração pública federal brasileira de janeiro a dezembro de 2020, dados estes que foram obtidos por meio do Portal de Transparência. Após a aplicação do Teste Z e o Teste Qui-Quadrado em comparação com a distribuição padrão da Lei de Benford, os autores identificaram, entre os órgãos analisados, maior discrepância nos dados dos Ministérios da Ciência e Tecnologia (dígitos 1 a 9, com preponderância nos dígitos 3 a 7), Educação (dígitos 1 a 9, com preponderância para os dígitos 4, 5 e 9), Desenvolvimento Regional (dígitos 1, 2 e 3), Justiça (dígitos 5 e 6) e da Saúde (dígitos 4, 5 e 9).

Dessa forma, como pôde ser demonstrado anteriormente, a Lei de Benford pode ser uma ferramenta útil para identificar potenciais transações fraudulentas num grande conjunto de dados, destacando as transações que podem exigir uma investigação mais aprofundada (Nickell et al., 2023, p. 2). Segundo Dsouza (2020), esta técnica pode ser aplicada de forma prática no campo dos negócios, além de poder apoiar as áreas de exame de fraude, análise de dados ou auditoria.

2.3 METODOLOGIA

Esta seção apresenta a metodologia utilizada na execução da pesquisa. Para melhor compreensão, a seção está dividida em duas partes, sendo a primeira relacionada com o

enquadramento metodológico, segundo a classificação trazida pela literatura. Na segunda parte são apresentados os instrumentos ou procedimentos propriamente ditos que serão adotados para a consecução dos objetivos da pesquisa.

2.3.1 Enquadramento Metodológico

Quanto aos objetivos, a presente pesquisa pode ser classificada como descritiva e exploratória; descritiva por apresentar uma revisão da literatura a respeito dos dois eixos da pesquisa, ou seja, as fraudes contábeis e financeiras, bem como os softwares de Business Intelligence; e exploratória por buscar alcançar uma maior familiaridade com as técnicas de detecção de fraudes contábeis e financeiras, o que pode ser obtido através de levantamento bibliográfico, entrevistas com profissionais da área e análise de exemplos que possam trazer mais compreensão do tema (Gil, 2002)

Quanto à sua natureza, a pesquisa se configura como aplicada, na medida em que tem por objetivo produzir conhecimento para aplicação prática e dirigida, com a finalidade de resolver problemas específicos (Gerhardt, 2009).

Quanto à forma de abordagem do problema, a pesquisa se enquadra como quantitativa, cuja característica é empregar "instrumentos estatísticos, tanto na coleta quanto no tratamento dos dados." (Raupp; Beuren, 2006, p. 92). Para Silva et al. (2014), esse tipo de pesquisa se aplica a situações em que se tenha um problema de pesquisa muito bem definido, haja informação e teoria a respeito do objeto de conhecimento. Ainda segundo eles, os dados da abordagem quantitativa devem possuir natureza numérica, com grandezas monetárias, físicas, de escalas de atitude ou de notas de especialistas.

2.3.2 Procedimentos Metodológicos

Embora haja uma pluralidade de definições em relação ao termo "Business Intelligence" (Khallaf, 2021), algumas definições gerais podem ser identificadas na literatura, que aproximam o termo a um ponto de vista de processo de negócio que faz uso de dados para a tomada de decisão. Para De Leon et al. (2012) o termo Business Intelligence é definido como o uso intencional de dados para tomar decisões, criar valor e promover os objetivos estratégicos de uma organização, suas unidades e seus funcionários. Para Correia; Água (2021), três aspectos são essenciais para a definição do BI: (i) realizar o recolhimento e armazenamento de dados; (ii) realizar a análise dos dados e informação, e posterior utilização; e (iii) apoiar a tomada de decisão. Tavera Romero et al. (2021) definem Business Intelligence como um processo de tomada de decisão suportado pela integração e análise dos recursos de dados de uma organização. Antonelli (2010) define Business Intelligence como sendo um conjunto de conceitos e metodologias que, fazendo uso de dados extraídos de uma organização, apoia a tomada de decisão. Negash (2004) explica que os sistemas de Business Intelligence combinam dados operacionais com ferramentas analíticas para apresentar informações complexas e competitivas para planejadores e tomadores de decisão. Ainda segundo ele, Business Intelligence é usado para entender os recursos disponíveis na empresa; o estado da arte, tendências e direções futuras nos mercados, tecnologias e ambiente regulatório no qual a empresa compete; e as ações dos concorrentes e as implicações dessas ações.

O BI tem sido aplicado, principalmente, para tomar decisões ou para fornecer informações para a tomada de decisões em diversos domínios, como, cursos superiores, ensino à distância, elaboração de estratégias, finanças, dentre outros (Aruldoss et al., 2014).

Uma forma objetiva de se implementar os conceitos e metodologias de *Business Intelligence* está relacionada com o uso de *softwares* especializados. Atualmente, o mercado

oferece diversas alternativas para todos os tipos de organizações e projetos. Estes *softwares* são capazes de extrair informações de diversas bases de dados, transformando uma massa de dados em informações inteligíveis para a tomada de decisões. Dentre estes *softwares* pode-se citar líderes de mercado como Power BI, Qlik Sense, Tableau, dentre outros.

Esta pesquisa fará uso do Power BI como instrumento de intervenção, já que a ferramenta permite a criação e o compartilhamento de *dashboards* com facilidade (Michalczyk, 2020), permite que os auditores analisem enormes conjuntos de dados muito rapidamente (Nickell; Schwebke; Goldwater, 2023), é fácil de usar, acessível para implantação na infraestrutura de nuvem (Sriram et al., 2022), sendo uma das ferramentas líderes na visualização de dados (Lousa; Pedrosa; Bernardino, 2019), além de permitir que os auditores detectem possíveis fraudes em menos tempo e com mais precisão do que os auditores que usam métodos tradicionais (Sabry, 2023), e ser a ferramenta de BI que o pesquisador possui mais familiaridade.

2.3.3 Conjunto de Dados

O conjunto de dados utilizado no estudo de caso foi composto de dados antigos de uma empresa brasileira, contendo lançamentos de contas a pagar entre 2012 e 2016. Foram considerados 5 tipos de dados: código do lançamento, data de emissão, código do credor, código da conta contábil e valor do lançamento.

O conjunto de dados foi armazenado em uma planilha Excel em formato xls, contendo 6.946 linhas de registros de lançamentos.

2.3.4 Construção do Dashboard

O dashboard foi construído utilizando a Versão: 2.136.1202.0 64-bit (setembro de 2024) do Power BI. Inicialmente, o conjunto de dados foi importando para o Power BI utilizando o tipo de fonte “Pasta de Trabalho do Excel”.

Figura 3 –Distribuições de Ocorrências pela Lei de Benford

	A	B	C	D	E
1	Digit	1st Place	2nd Place	3rd Place	4th Place
2	0		0,11968	0,10178	0,10018
3	1	0,30103	0,11389	0,10138	0,10014
4	2	0,17609	0,10882	0,10097	0,1001

Fonte: Autores

Além do conjunto de dados de lançamentos financeiros de contas a pagar, foi criado uma planilha Excel com as probabilidades de ocorrência de cada dígito, conforme a Lei de Benford (vide Figura 3 –Distribuições de Ocorrências pela Lei de Benford).

2.3.5 Técnica de Análise dos Dados

A primeira etapa do processo de análise dos dados consistiu em identificar, no conjunto de dados, a distribuição de ocorrências do primeiro e do segundo dígitos de cada lançamento. Essa informação foi registrada em uma medida chamada “Registros Observados”. Em seguida, tendo-se a quantidade de ocorrência de cada dígito, foi realizado o cálculo do percentual de ocorrência equivalente em relação ao total de lançamentos contidos no conjunto de dados. Com isso, foi possível obter o percentual da “Frequência Observada”.

Na sequência, os valores contidos na Figura 3 foram armazenados na medida “%

Frequência Benford" e serviram de base para calcular os valores da medida "Registros Esperados". Com isso, foi possível calcular a diferença (Dif) entre a quantidade de registros observados no conjunto de dados e a quantidade de registros esperados pela Lei de Benford.

Em seguida, seguindo a metodologia adotada por Undavia (2014), foi realizado o cálculo do Valor Absoluto (ABS) da variação percentual entre os percentuais de distribuição observados e esperados do conjunto de dados.

Finalizada a etapa de compilação dos dados do conjunto de dados e a sua comparação com os valores esperados pela Lei de Benford, partiu-se para a etapa do Teste de Hipóteses. Seguindo a proposição de Nigrini (2012), esta pesquisa fez uso dos testes estatísticos Teste Z e Teste Qui-Quadrado (X^2).

O teste qui-quadrado foi usado para medir a adequação à Lei de Benford, assim como o fizeram Nigrini; Miller (2007), Undavia (2014) e Gonçalves *et al.* (2023). Segundo Barbetta (2001) o X^2 é uma espécie de medida de distância entre as frequências observadas e as frequências esperadas, supondo-se que as variáveis são independentes. Segundo Gonçalves *et al.* (2023, p. 35), o Teste X^2 é utilizado para comparar um conjunto de resultados reais com um conjunto de resultados esperados, num "contexto global". Dessa forma, considerando que na análise do primeiro dígito são considerados os dígitos 1 a 9, e $\alpha = 0,05$, obtém-se o grau de liberdade (gl) igual a 8, o que, por meio da Tabela de Distribuição do Qui-Quadrado, chega-se ao valor de referência do Qui-Quadrado (VRX^2) de 15,51. Já na análise do segundo dígito, considerando que são considerados 10 dígitos diferentes (0 a 9), o grau de liberdade é 9, que combinado com $\alpha = 0,05$ resulta em um valor de referência do Qui-Quadrado (VRX^2) 16,92, conforme a Tabela de Distribuição do Qui-Quadrado.

Sendo assim, as hipóteses testadas para o X^2 foram:

H_0 – Não existe diferença superior ao valor de referência do Qui-Quadrado (VRX^2) entre a Frequência Percentual Observada e a Frequência Percentual Esperada;

H_1 –Existe diferença superior ao valor de referência do Qui-Quadrado (VRX^2) entre a Frequência Percentual Observada e a Frequência Percentual Esperada;

Já o Teste Z foi utilizado para testar a distribuição real de um dígito em relação a distribuição esperada do respectivo dígito na Lei de Benford, buscando identificar se havia diferença significativa entre ambos, do ponto de vista estatístico (Gonçalves *et al.,* 2023). Assim como o fizeram Undavia (2014) e Gonçalves *et al.* (2023), o nível de significância adotado foi $\alpha = 0,05$, resultando em um Valor de Referência do Teste Z (VRZ) de 1,96.

Sendo assim, as hipóteses testadas para o Teste Z foram:

H_0 – Não existe diferença superior ao Valor de Referência do Teste Z (VRZ) entre a Frequência Percentual Observada e a Frequência Percentual Esperada;

H_1 –Existe diferença superior ao Valor de Referência do Teste Z (VRZ) entre a Frequência Percentual Observada e a Frequência Percentual Esperada;

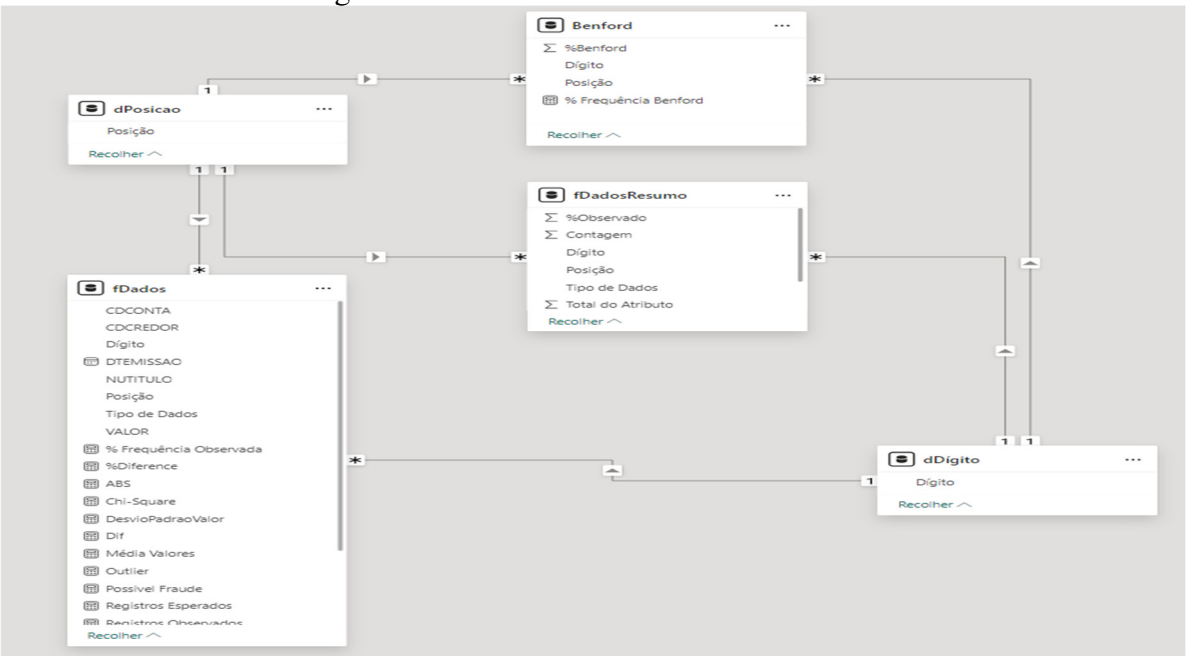
Dessa forma, foram considerados como possíveis fraudes os registros dos dígitos que atenderam tanto a H_1 do Teste Qui-Quadrado (X^2) quanto do Teste Z.

2.4 RESULTADOS

Em relação ao modelo conceitual do *dashboard*, a Figura 4 – Modelo Conceitual do *dashboard* apresenta a relação entre as 5 tabelas do mencionadas na Tabela 2. Como pode ser observado, o modelo conceitual utilizou o relacionamento 1:* (um para muitos) na ligação entre

as tabelas dimensão e as tabelas fato. O ponto de destaque está na necessidade de criação da tabela fDadosResumo, para poder obter-se o valor global do Qui-Quadrado.

Figura 4 – Modelo Conceitual do *dashboard*

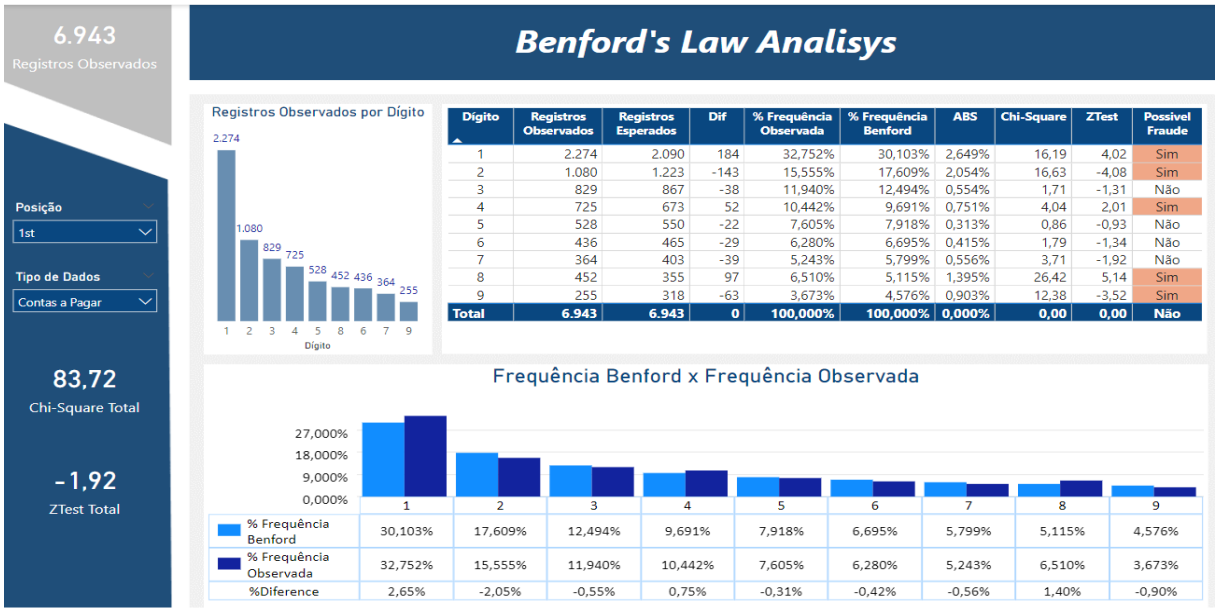


Fonte: Autores

Em relação à parte funcional, propriamente dita, o *dashboard* foi estruturado em duas partes. Na primeira, demonstrada na Figura 5 – *Benford's Law Analisys (Parte I)* são apresentados dois filtros que possibilitam ao usuário selecionar o tipo de análise que deseja fazer (Contas a Pagar, Contas a Receber, Estoques etc.). O filtro "Posição" permite ao usuário selecionar qual dígito deseja analisar. No exemplo descrito na Figura 5, a análise está considerando a posição do primeiro dígito.

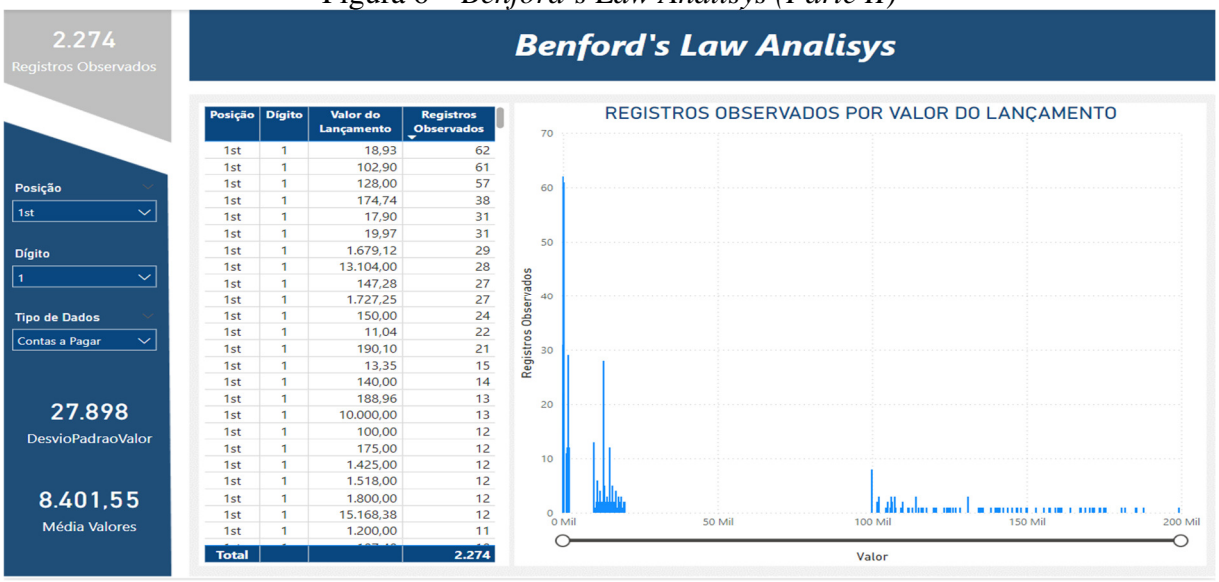
Como pode ser observado na Figura 5, a análise do conjunto de dados para o primeiro dígito apresentou um valor de 83,72 para o Chi-Quadrado (X^2). Considerando que este valor é superior ao Valor de Referência do Qui-Quadrado (VRX^2), a H_0 deve ser rejeitada, indicando que a possibilidade de manipulação dos dados não pode ser rejeitada. Além disso, como pode ser observado na Figura 5, o Teste Z resultou em 5 dígitos que apresentaram o valor do Teste Z superior ao Valor de Referência do Teste Z (VRZ). Sendo assim, a H_0 deve ser rejeitada, indicando que os lançamentos que começam com os dígitos 1, 2, 4, 8 e 9 merecem uma análise complementar, pois, podem ter sido manipulados.

Figura 5 – *Benford's Law Analisys (Parte I)*



Fonte: Autores

Figura 6 – *Benford's Law Analisys (Parte II)*



Fonte: Autores

Os dígitos identificamos como possuidores de lançamentos com possibilidade de manipulação foram carregados automaticamente para a segunda parte do *dashboard*, como pode ser observado na Figura 6 - *Benford's Law Analisys (Parte II)*. Os registros observados para cada dígito analisado foram classificados em ordem decrescente, de forma que foi possível identificar os valores que ocorreram com maior frequência no conjunto de dados. Além disso, por meio do gráfico de distribuição dos valores é possível identificar valores que destoam da distribuição normal dos valores.

Considerações Finais

Como pôde ser observado, o *dashboard* demonstrou-se funcional, ao contabilizar o total de Registros Observados (6.943), bem como, identificar de forma automatizada os registros que podem ser considerados com possibilidade de terem sido manipulados. Embora a análise do conjunto de dados à luz da Lei de Benford possa ser feita por meio do Microsoft Excel, isso

pode se demonstrar complexo de ser elaborado, além de poder apresentar problemas de desempenho quando se tenta analisar um conjunto de dados com muitos registros.

No estudo de caso foram usados somente registros de Contas a Pagar. No entanto, o modelo se mostra perfeitamente viável para analisar outros conjuntos de dados, como de Contas a Receber, Movimentação de Estoques, Movimentações de Contas Correntes, dentre outros.

Dentre as principais dificuldades encontradas na construção do *dashboard* está a criação dos relacionamentos entre as tabelas que continham a distribuição segundo a Lei de Benford e a tabela que continha o conjunto de dados. Isto foi superado por meio da criação das tabelas auxiliares contendo a relação de dígitos (0 a 9) e a posição de cada número (1 a 4). Além disso, foi necessária a criação de uma tabela-resumo (fDadosResumo) para ser possível calcular os valores do Chi-Quadrado e do Teste Z de forma geral, e não somente por dígito. É possível que em novas pesquisas, outras soluções possam ser encontradas para estas situações.

A pesquisa não teve como finalidade apresentar um modelo exaustivo, mas demonstrar que a análise por meio da Lei de Benford pode ser operacionalizada com eficiência por meio do uso do Microsoft Power BI. Como limitações da pesquisa, pode-se mencionar o uso de dados de somente uma empresa, durante um período específico (2012 a 2016). Além disso, foram utilizados somente dados relativos a contas a pagar desta empresa.

Embora o uso do Microsoft Power BI tenha se mostrado aderente à operacionalização da Lei de Benford para a detecção de possíveis fraudes, nem todos os recursos do *software* foram utilizados. Pode-se citar como exemplo, a não simulação com fontes de dados distintas do Microsoft Excel, como SQL Server, PDF, XML, JSON, Web, dentre outras.

Recomenda-se para próximas pesquisas a construção de novos *dashboards* semelhantes em outros *softwares*, como Tableau e QlikSense, além de buscar-se avançar na construção deste *dashboard* com a implementação de técnicas supervisionadas de *machine learning,* por exemplo.

REFERÊNCIAS

ABDULLAHI, Rabiu; MANSOR, Noorhayati. Fraud triangle theory and fraud diamond theory. Understanding the convergent and divergent for future research. **International Journal of Academic Research in Accounting, Finance and Management Science**, v. 1, n. 4, p. 38-45, 2015.

ACFE, ASSOCIATION OF CERTIFIED FRAUD EXAMINERS. **What Is Fraud?** Disponível em: https://www.acfe.com/fraud-resources/fraud-101-what-is-fraud. Acesso em: 17 out. 2023.

AFTABI, Seyyede Zahra; AHMADI, Ali; FARZI, Saeed. **Fraud detection in financial statements using data mining and GAN models.** Expert Systems with Applications, v. 227, p. 120144, 2023.

AHMI, Aidi; KENT, Simon. The utilisation of generalized audit software (GAS) by external auditors. **Managerial Auditing Journal**, v. 28, n. 2, p. 88-113, 2012.

ALBRECHT, W. Steve et al. **Fraud examination.** Thompson South-Western, 2003.

ANTONELLI, Ricardo Adriano. Conhecendo o business intelligence (BI). **CAP Accounting and Management-B4**, v. 3, n. 3, p. 79-85, 2010.

APRILIANA, Siska; AGUSTINA, Linda. The analysis of fraudulent financial reporting determinant through fraud pentagon approach. **Jurnal Dinamika Akuntansi**, v. 9, n. 2, p. 154-165, 2017.

AQUIZE, Vanessa Adriana Gironda; DOS SANTOS FILHO, Mailson Melo. Business Intelligence for the detection of anomalies in records of fueling. **Revista de Engenharia e Pesquisa Aplicada**, v. 3, n. 3, 2018.

ARULDOSS, Martin; TRAVIS, Miranda Lakshmi; VENKATESAN, V. Prasanna. A survey on recent research in business intelligence. **Journal of Enterprise Information Management**, 2014.

BAO, Yang et al. Detecting accounting fraud in publicly traded US firms using a machine learning approach. **Journal of Accounting Research**, v. 58, n. 1, p. 199-235, 2020.

CARVALHO, Ricardo Pereira; SILVA, Adolfo Henrique Coutinho e. A Irrelevância dos Indicadores Econômico-Financeiros como Red Flags para Detecção de Fraudes em Demonstrações Financeiras: O Caso Americanas SA. **Pensar Contábil**, 2024.

CHRISTIAN, N.; BASRI, Y. Z.; ARAFAH, W. Analysis of fraud triangle, fraud diamond and fraud pentagon theory to detecting corporate fraud in Indonesia. **The International Journal of Business Management and Technology**, v. 3, n. 4, p. 73-78, 2019.
CODERRE, D.. **Fraud analysis techniques using ACL**. John Wiley & Sons, 2009.
COSTA, A. P. P.; WOOD JR, T.. Fraudes corporativas. **Revista de Administração de Empresas**, v. 52, p. 464-472, 2012.
CRESSEY, D. R. **Other people's money; a study of the social psychology of embezzlement.** 1953.
DE LEON, L.; RAFFERTY, P. D.; HERSCHEL, R.. **Replacing the annual budget with business intelligence driver-based forecasts**. 2012.
DILLA,W. N.; RASCHKE, R. L. Data visualization for fraud detection: Practice implications and a call for future research. **International Journal of Accounting Information Systems**, v. 16, p. 1-22, 2015.
DSOUZA, S. **Big Data, Benford's Law and Financial Analytics**. 2020.
DUAN, L.; DA XU, L.. Business intelligence for enterprise systems: a survey. **IEEE Transactions on Industrial Informatics**, v. 8, n. 3, p. 679-687, 2012.
FREE, C.. Looking through the fraud triangle: A review and call for new directions. **Meditari Accountancy Research**, v. 23, n. 2, p. 175-196, 2015.
GEPP, A. et al. Big data techniques in auditing research and practice: Current trends and future opportunities. **Journal of Accounting Literature**, v. 40, n. 1, p. 102-115, 2018.
GERHARDT, Tatiana Engel; SILVEIRA, Denise Tolfo. **Métodos de pesquisa**. Plageder, 2009.
GEYER, Christina Lynn; WILLIAMSON, Patricia Pepple. Detecting fraud in data sets using Benford's law. **Communications in Statistics-Simulation and Computation**, v. 33, n. 1, p. 229-246, 2004.
GIL, Antônio Carlos. **Como elaborar projetos de pesquisa**. 4ª ed, São Paulo: Atlas, 2002.
HAQQ, A. P. N. A.; BUDIWITJAKSONO, G. S.. Fraud pentagon for detecting financial statement fraud. **Journal of Economics, Business, and Accountancy Ventura**, v. 22, n. 3, p. 319-332, 2019.
HOOG, W.; SÁ, A. L. **Corrupção, fraude e contabilidade**. Curitiba: Ed. Juruá, 2005.
KHALLAF, A. et al. L'impact des systèmes de Business Intelligence sur la gestion budgétaire. **Information Systems Management and Innovation**, v. 5, n. 2, p. 41-54, 2021.
KRAMBIA-KAPARDIS, M.; ZOPIATIS, A.. Investigating incidents of fraud in small economies: the case for Cyprus. **Journal of Financial Crime**, v. 17, n. 2, p. 195-209, 2010.
KRAUSPENHAR, J. H.; ROVER, S.. A relevância da fraude contábil ocorrida na Via Varejo SA: um estudo de eventos. **Revista Brasileira de Administração Científica**, v. 11, n. 3, p. 242-257, 2020.
LOKANAN, M. E. Financial fraud detection: the use of visualization techniques in credit card fraud and money laundering domains. **Journal of Money Laundering Control**, v. 26, n. 3, p. 436-444, 2023.
LOKANAN, M. E.; SHARMA, Kush. Fraud prediction using machine learning: The case of investment advisors in Canada. **Machine Learning with Applications**, v. 8, p. 100269, 2022.
LOUSA, A.; PEDROSA, I; BERNARDINO, J.. Evaluation and analysis of business intelligence data visualization tools. In: 2019 14th Iberian Conference on Information Systems and Technologies (CISTI). **IEEE**, 2019. p. 1-6.
MACHADO, M. R. R.; GARTNER, I. R.. A hipótese de Cressey (1953) e a investigação da ocorrência de fraudes corporativas: uma análise empírica em instituições bancárias brasileiras. **Revista Contabilidade & Finanças**, v. 29, p. 60-81, 2017.
MACKEVIČIUS, Jonas; KAZLAUSKIENĖ, Laimutė. The fraud tree and its investigation in audit. **Ekonomika**, v. 85, p. 90-101, 2009.
MANGALA, D.; KUMARI, P.. Corporate fraud prevention and detection: Revisiting the literature. **Journal of Commerce & Accounting Research**, v. 4, n. 1, p. 35-45, 2015.
MATHERLY, M.; WATSON, M.W.; IVANCEVICH, S.. Implementing generalized audit software in the classroom. **AIS Educator Journal**, v. 4, n. 1, p. 27-57, 2009.
MICHALCZYK, S. et al. **A state-of-the-art overview and future research avenues of self-service business intelligence and analytics**. 2020.
NEGASH, S. **Business Intelligence**. Communications of the Association for Information Systems. v. 177, n. 195, p. 177, 2004.
NICKELL, E.B.; SCHWEBKE, J.; GOLDWATER, P.. An introductory audit data analytics case study: Using Microsoft Power BI and Benford's Law to detect accounting irregularities. **Journal of Accounting Education**, v. 64, p. 100855, 2023.
NURKHIN, A.; KARDOYO; MUHSIN. What determinants of academic fraud behavior? from fraud

triangle to fraud pentagon perspective. **KnE Social Sciences**, p. 154–167-154–167, 2018.
OLIVEIRA, E.F. et al. O uso de tecnologias para detecção de fraudes na pandemia da covid-19. **Revista de Contabilidade e Controladoria**, v. 13, n. 1, 2021.
OMIDI, Mahdi et al. The efficacy of predictive methods in financial statement fraud. **Discrete Dynamics in Nature and Society**, v. 2019, 2019.
ORTH, C.O.; MICHAELSEN , A.T.; LERNER, A.F.. Lei de newcomb benford e auditoria contábil: uma revisão sistemática de literature. **Revista Gestão e Conhecimento**. Mai/ago, 2020.
PASCHOAL, A. L P.; DE ARAÚJO SANTOS, N.; FARONI, W.. Diamante da fraude: evidências empíricas nos relatórios de demandas externas do Ministério da Transparência e Controladoria Geral da União (CGU) dos municípios brasileiros. **REVISTA AMBIENTE CONTÁBIL-Universidade Federal do Rio Grande do Norte-ISSN 2176-9036**, v. 12, n. 2, p. 136-156, 2020.
QURAINI, Fidyah; RIMAWATI, Yuni. Determinan fraudulent financial reporting using fraud pentagon analysis. **Journal of Auditing, Finance, and Forensic Accounting**, v. 6, n. 2, p. 105-114, 2018.
RAUPP, F. M.; BEUREN, I. M.. **Metodologia da pesquisa aplicável às ciências**. Como elaborar trabalhos monográficos em contabilidade: teoria e prática. São Paulo: Atlas, p. 76-97, 2006.
RENALDO, N. et al. Forensic accounting: the use of Benford's law to evaluate indications of fraud. **Redeca, Revista Eletrônica do Departamento de Ciências Contábeis & Departamento de Atuária e Métodos Quantitativos**, v. 9, p. e57343-e57343, 2022.
SABRY, S. H. A.. The Impact of Using Business Intelligence on Potential Fraud Detection: An Experimental Study. مجلة بحوث محاسبية, v. 10, n. 4, p. 196-233, 2023.
SAID, R. M. (2020). **Um estudo das principais fraudes em instituições financeiras no Brasil: Reflexões sobre lições aprendidas.** Tese de Doutorado, Faculdade de Economia, Administração e Contabilidade, Universidade de São Paulo, São Paulo, 2020.
SEIFY, M. et al. Fraud Detection in Supply Chain with Machine Learning. **IFAC-PapersOnLine**, v. 55, n. 10, p. 406-411, 2022.
SHAHANA, T.; LAVANYA, Vilvanathan; BHAT, Aamir Rashid. State of the art in financial statement fraud detection: A systematic review. **Technological Forecasting and Social Change**, v. 192, p. 122527, 2023.
SILVA, D.; LOPES, E.L.; BRAGA JUNIOR, S.S.**. Pesquisa quantitativa: elementos, paradigmas e definições. Revista de Gestão e Secretariado (Management and Administrative Professional Review)**, v. 5, n. 1, p. 01-18, 2014.
SRIRAM, T. V. S. et al. Exploratory Of Data Visualization With Tools. **Journal of Pharmaceutical Negative Results**, p. 5115-5121, 2022.
TANG, J.; KARIM, K. E. Financial fraud detection and big data analytics–implications on auditors' use of fraud brainstorming session. **Managerial Auditing Journal**, v. 34, n. 3, p. 324-337, 2019.
TAVERA ROMERO, C. A. *et al.* Business intelligence: business evolution after industry 4.0. **Sustainability**, v. 13, n. 18, p. 10026, 2021.
UNDAVIA, M. B. **APPLICATION OF BENFORD'S LAW TO DETECT ACCOUNTING FRAUD IN PUNJAB & SIND BANK**. Journal of Emerging Technologies and Innovative Research (JETIR), v. 9, n. 11, p. e402-e410, nov. 2022. Disponível em: https://www.jetir.org/papers/JETIRM006007.pdf. Acesso em: 14 dez. 2023.
WELLS, J. T. CFE, CPA, **Principles of Fraud Examination**. 2005.
WICAKSONO, A; LUSIANAH, L.. Impact analysis of generalized audit software (GAS) utilization to auditor performances. **Binus Business Review**, v. 7, n. 2, p. 131-136, 2016.
WOLFE, D. T.; HERMANSON, D. R. **The fraud diamond: Considering the four elements of fraud.** 2004.
WONG, S.; VENKATRAMAN, S.. Financial accounting fraud detection using business intelligence. **Asian Economic and Financial Review**, v. 5, n. 11, p. 1187, 2015.