UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE ARTES E COMUNICAÇÃO
DEPARTAMENTO DE CIÊNCIA DA INFORMAÇÃO
CURSO DE GESTÃO DA INFORMAÇÃO

CINTIA VIRGINIA DE LIRA CORDEIRO

ANÁLISE DE SISTEMAS DE INFORMAÇÃO NA PREVENÇÃO DE FRAUDES FINANCEIRAS

Recife

2025

CINTIA VIRGINIA DE LIRA CORDEIRO

ANÁLISE DE SISTEMAS DE INFORMAÇÃO NA PREVENÇÃO DE FRAUDES FINANCEIRAS

Trabalho de Conclusão de Curso apresentado ao Curso de Gestão da Informação da Universidade Federal de Pernambuco, como requisito parcial para obtenção do título de Bacharel em Gestão da Informação.

Orientador: Prof. Dr. Márcio Henrique Wanderley Ferreira

Recife

2025

Ficha de identificação da obra elaborada pelo autor,
através do programa de geração automática do SIB/UFPE

Virginia de Lira Cordeiro, Cintia .
Análise de sistemas de informação na prevenção de fraudes financeiras / Cintia Virginia de Lira Cordeiro. - Recife, 2025.
52, tab.

Orientador(a): Marcio Henrique Wanderley Ferreira
Trabalho de Conclusão de Curso (Graduação) - Universidade Federal de Pernambuco, Centro de Artes e Comunicação, Gestão da Informação - Bacharelado, 2025.
Inclui referências.

1. Fraudes Corporativas. 2. Gestão de Risco. 3. Impactos Tecnológicos. 4. Sistemas de Informação. I. Henrique Wanderley Ferreira, Marcio. (Orientação). II. Título.

020 CDD (22.ed.)

Serviço Público Federal
Universidade Federal de Pernambuco Centro de Artes e Comunicação
Departamento de Ciência da Informação

TRABALHO DE CONCLUSÃO DE CURSO
FOLHA DE APROVAÇÃO

ANÁLISE DE SISTEMAS DE INFORMAÇÃO NA PREVENÇÃO DE FRAUDES FINANCEIRAS

(Título do TCC)

CINTIA VIRGINIA DE LIRA CORDEIRO
(Autor)

Trabalho de Conclusão de Curso submetido à Banca Examinadora, apresentado no Curso de Gestão da Informação, do Departamento de Ciência da Informação, da Universidade Federal de Pernambuco, como requisito parcial para obtenção do título de Bacharel em Gestão da Informação.

TCC aprovado em 04 de Agosto de 2025

Banca Examinadora:

PROF. MÁRCIO HENRIQUE WANDERLEY FERREIRA - Orientador(a)
Universidade Federal de Pernambuco - DCI

PROF. ELANNA BEATRIZ AMERICO FERREIRA – Examinador(a) 1
Universidade Federal de Pernambuco - DCI

PROF. MARCELA LINO DA SILVA - Examinador(a) 2
Universidade Federal de Pernambuco – DCI

Dedico este trabalho a todas as pessoas especiais da minha vida que através de pequenos e grandes gestos, me ajudaram a concluir o meu curso. Desde o fato de me esperarem acordados tarde da noite a conselhos em meu TCC, vocês são pontos fundamentais para essa realização.

AGRADECIMENTOS

Agradeço a todos que contribuíram no decorrer desta jornada, especialmente a Deus, a quem devo minha vida. A minha família que sempre me apoiou nos estudos e nas escolhas tomadas.

“O cipreste inclina-se em fina reverência
e as margaridas estremecem, sobressaltadas.
A grande amendoeira consente que balancem”.

Meireles, 1983, p. 135.

RESUMO

O objetivo deste estudo é investigar a eficácia dos sistemas de informação modernos na detecção precoce e prevenção de fraudes financeiras, comparando-os com sistemas tradicionais. A presente pesquisa adotou uma abordagem qualitativa, de natureza exploratória, com base em revisão de literatura, pesquisa bibliográfica e elementos de observação empírica informal oriunda da vivência profissional. As empresas passam por várias fases em sua trajetória, e para se adequarem às novas tecnologias geralmente seguem um ciclo de adaptação e transformação, envolvendo várias etapas. Essas fases podem variar conforme o setor e a maturidade da empresa. Atualmente com o crescimento imensurável da tecnologia, é possível observar que a forma de estudar e entender os acontecimentos das estruturas organizacionais e das práticas de gestão estão extremamente diferentes. Para isso, foi realizada uma revisão de literatura, para identificar e descrever os principais aspectos tecnológicos e sociais que acabam influenciando na prevenção de fraudes e ataques nas empresas. De modo geral os resultados obtidos através dos estudos bibliográficos apresentaram resultados reveladores que mostram a real importância desse estudo e como a tecnologia e os sistemas de informação irão auxiliar as entidades a prever riscos e se prevenir de golpes financeiros.

Palavras-chave: fraudes corporativas; gestão de risco; impactos tecnológicos; sistemas de informação.

ABSTRACT

The objective of this study is to investigate the effectiveness of modern information systems in the early detection and prevention of financial fraud, comparing them with traditional methods. This research developed a qualitative, exploratory approach, based on a literature review, bibliographic research, and informal empirical observation derived from professional experience. Companies go through various phases in their trajectory, and to adapt to new technologies, they generally follow a cycle of adaptation and transformation, involving several stages. These phases can vary depending on the sector and the company's maturity. Currently, with the immeasurable growth of technology, we can observe that the ways of studying and understanding the events of organizational structures and management practices are extremely different. To this end, a literature review was carried out to identify and describe the main technological and social aspects that ultimately influence the prevention of fraud and attacks in companies. Overall, the results obtained through the bibliographic studies presented revealing findings that demonstrate the true importance of this study and how technology and information systems will help entities anticipate risks and prevent financial scams.

Keywords: corporate fraud; risk management; technological impacts; information systems.

LISTA DE ABREVIATURAS

ERP	*Enterprise Resource Planning*
GDPR	Regulamento Geral sobre a Proteção de Dados
IA	Inteligência Artificial
KPI	Key Performance Indicator ou Indicador-Chave de Desempenho
LGPD	Lei Geral de Proteção de Dados
ML	*Machine Learning*
SI	Sistemas de Informação
SSD	Sistemas de Suporte à Decisão

LISTA DE QUADROS

SUMÁRIO

1 INTRODUÇÃO

No complexo e concorrido panorama de negócios, os diferenciais competitivos são cada vez mais relevantes para que as organizações ganhem destaque no mercado. Nessa busca por sucesso e relevância, as tomadas de decisão devem ser aplicadas com base em todas as informações que podem ser adquiridas por meio da tecnologia de mercado. Estas informações tornam-se então recursos relevantes no processo decisório e como consequência para a evolução das empresas e da economia. Por meio dessa necessidade de busca da informação é que se tornam essenciais os estudos sobre a segurança da informação e sobre como as ferramentas de tecnologia da informação podem promover uma maior eficiência, qualidade e capacidade de resposta a possíveis riscos de fraudes.

A tomada de decisão é a conversão das informações analisadas em ação, e os desafios impostos levam os gestores a buscar informações que espelham fielmente a real situação das organizações, no intuito do processo decisório ser executado de forma mais eficaz, alcançando os resultados pretendidos (Moraes; Costa, 2018). Então, um bom processo de decisão envolve a identificação de um problema específico e a escolha de uma ação para resolvê-lo ou aproveitar uma oportunidade.

Algumas empresas insistem em utilizar sistemas tradicionais que geralmente são mais baseados em processos manuais ou em tecnologias convencionais que não têm a capacidade de processar grandes volumes de dados ou de se adaptar e aprender com novos padrões automaticamente. Além disso, inclui sistemas baseados em processos manuais, como a verificação manual de dados ou o uso de regras fixas para detecção de fraudes. Esses sistemas não integram novas tecnologias de análise, como *Machine Learning* ou algoritmos avançados, para prever ou identificar fraudes de maneira mais eficiente, o que limita sua capacidade de adaptação e resposta rápida a novas ameaças.

As novas ferramentas tecnológicas têm como objetivo auxiliar as organizações a sintetizar informações de forma simples e rápida para tomadas de decisão e prevenção contra possíveis fraudes financeiras. Nesse processo, os dados são processados e transformados e transformados em relatórios significativos, com o objetivo de fornecer informações mais assertivas e que auxiliem no processo decisório.

A tecnologia da informação se tornou componente essencial do estilo competitivo das empresas, e o processo de modernização foi ocorrendo gradativamente, influenciando a maneira como a sociedade é enxergada, além da economia no Brasil e no mundo. A falta de planejamento atrapalha o conhecimento de novas informações e isso torna as empresas menos competitivas.

Com o passar dos anos e o aumento da concorrência foram realizados vários estudos de mercado e os investimentos em tecnologia cresceram cada vez mais, passando a representar um gasto significativo nas organizações.

Portanto, este trabalho parte do seguinte problema de pesquisa: Como a implementação de sistemas de informação avançados e baseados em inteligência artificial pode aprimorar a detecção e prevenção de fraudes financeiras em empresas do ramo de distribuidoras?

O presente trabalho tem como objetivo geral investigar a eficácia dos sistemas de informação modernos na detecção precoce e prevenção de fraudes financeiras, comparando-os com os sistemas tradicionais. Para alcançar esse propósito, busca-se, especificamente: Investigar na literatura científica as características dos sistemas de informação atualmente utilizados na detecção de fraudes financeiras, examinar estudos de caso de instituições que implementaram soluções baseadas em inteligência artificial (IA) para prevenção de fraudes, comparar a eficiência entre sistemas tradicionais e dos sistemas baseados em (IA) em termos de precisão, tempo de resposta e redução de fraudes.

Dessa forma, o planejamento da evolução da tecnologia dentro das organizações vai muito além de simplesmente criar novos sistemas e integrá-los com os existentes. É uma mudança na maneira como a tecnologia é tratada, mudando de um planejamento estilo “apagar incêndio”, onde as necessidades momentâneas são supridas conforme aparecem, para um modelo que contemple o desenvolvimento de todos os sistemas integrados entre si, mas principalmente, integrados com os anseios da instituição.

O mundo vive momentos de transformações muito impactantes e exponenciais e o grande desafio está em trazer novas conquistas e descobertas, pois, a tecnologia irá proporcionar maiores condições para prevenção de possíveis riscos e fraudes. Nessa era de pós-modernidade, será necessário acompanhar cada mudança, absorvendo todos os seus benefícios e melhorias. Por exemplo, toda nossa maneira de viver, fazer comércio, nos relacionar com as pessoas, estão destinados a várias mudanças e teremos que nos esforçar para estarmos aptos para desempenharmos um bom papel e melhorarmos o mercado e seus componentes.

Diante disso, apresenta-se como hipótese que sistemas de informação avançados, especialmente aqueles baseados em inteligência artificial, são significativamente mais eficazes na detecção e prevenção de fraudes financeiras do que os métodos tradicionais utilizados por empresas do setor de distribuição.

Essa pesquisa se justifica, em primeiro lugar, pelo interesse em compreender de forma aprofundada como as tecnologias emergentes, especialmente a inteligência artificial (IA), podem

ser aplicadas de maneira prática e estratégica no fortalecimento da segurança organizacional. Em um cenário corporativo marcado por transformações digitais aceleradas e por ameaças cada vez mais sofisticadas, torna-se indispensável investigar soluções tecnológicas que possam oferecer respostas rápidas e precisas diante de riscos financeiros, como as fraudes. A inteligência artificial, ao possibilitar a análise automatizada de grandes volumes de dados, a detecção de padrões anômalos e a antecipação de comportamentos fraudulentos, representa um diferencial competitivo para as organizações modernas.

Do ponto de vista técnico-científico, esta pesquisa também se justifica pela escassez de estudos aplicados que integrem os campos da inteligência artificial, da gestão da informação e da prevenção de fraudes em setores específicos como o da distribuição. Assim, ao propor uma análise comparativa entre métodos tradicionais e sistemas baseados em IA, este trabalho contribui para a ampliação da literatura existente e para a construção de referenciais teóricos e práticos que possam orientar gestores, auditores e profissionais de tecnologia da informação.

2 FRAUDE FINANCEIRA E INFORMAÇÃO

A fraude financeira é um fenômeno que se manifesta por meio de atos intencionais voltados à manipulação ou ao engano no contexto de transações econômicas e administrativas, ou seja, é uma conduta deliberada, planejada e, muitas vezes, dissimulada, visando obter vantagens indevidas, geralmente por meio da apropriação de recursos, adulteração de registros contábeis ou burla a normas e procedimentos internos. Essa prática, além de lesiva ao patrimônio de empresas e instituições, compromete diretamente os princípios de confiança e transparência que sustentam o ambiente econômico moderno (Martins, 2020).

Segundo a GTAG (2009, p. 1), fraude financeira nada mais é do que:

> Qualquer ato ilegal caracterizado por engano, ocultação ou violação de confiança. Esses atos não dependem da ameaça de violência ou força física. Fraudes são perpetradas por pessoas e organizações para obter dinheiro, propriedade ou serviços; evitar pagamento ou perda de serviços; ou para garantir vantagem pessoal ou comercial.

No contexto corporativo, as fraudes podem ocorrer de maneira difusa ou sistemática, envolvendo tanto colaboradores internos quanto agentes externos. Embora alguns casos sejam pontuais, outros se revelam como esquemas complexos que operam por longos períodos sem detecção (Nogueira, 2020). Entre os tipos mais comuns de fraude financeira no setor empresarial, destacam-se a falsificação de documentos, pagamentos duplicados, contratação de fornecedores inexistentes, inserção de funcionários fantasmas na folha de pagamento, além do superfaturamento de contratos e o desvio de verbas. Esses crimes, quando não detectados a tempo, geram não apenas prejuízos econômicos, mas também danos reputacionais que podem ser irreparáveis (Souza, 2019).

Um dos aspectos mais relevantes da fraude financeira é a sua estrutura organizada. Diferentemente de erros administrativos, que geralmente decorrem de falhas operacionais ou desconhecimento técnico, a fraude exige planejamento e a intenção consciente de ludibriar o sistema (Martins, 2020). Os agentes envolvidos costumam atuar em silêncio, aproveitando-se de lacunas em processos e da ausência de fiscalização efetiva. Muitos desses esquemas contam com a colaboração ou a omissão de indivíduos em posições estratégicas, o que amplia ainda mais sua gravidade. Nesse sentido, torna-se indispensável a adoção de mecanismos eficazes de controle interno, auditoria contínua, e o uso de tecnologias de monitoramento e rastreamento (Oliveira; Almeida, 2021).

Um conceito amplamente difundido na literatura especializada sobre o tema é o chamado triângulo da fraude, proposto por Donald Cressey e amplamente debatido por

estudiosos contemporâneos. Esse modelo explica que três fatores precisam estar presentes para que a fraude ocorra: a motivação, a oportunidade e a racionalização. A motivação é, muitas vezes, pessoal, como dificuldades financeiras, ambição desmedida ou desejo de status Boldt (2025). A oportunidade está relacionada a falhas nos sistemas de controle ou à confiança excessiva depositada em certos indivíduos. Já a racionalização é o mecanismo psicológico que permite ao fraudador justificar moralmente suas ações, convencendo-se de que o ato é legítimo ou que o dano causado é irrelevante (Nogueira, 2020).

Boldt (2025, p. 8), ao analisar o triângulo da Fraud de Cressey, afirma que:

> O Triângulo da Fraude de Donald Cressey continua sendo uma das principais ferramentas teóricas para explicar os fatores que levam à fraude corporativa, sendo extremamente utilizado, por exemplo, no contexto do compliance. No entanto seu escopo limitado exige complementação e adaptação para lidar com os desafios das fraudes no século XXI, que são mais complexas e sofisticadas. A inclusão de novos elementos, como capacidade, cultura organizacional e fatores externos, é crucial para que o modelo continue sendo útil na detecção e na prevenção de fraudes corporativas.

Com o crescimento das tecnologias digitais e a globalização dos mercados, surgem novas formas de fraude, especialmente no meio digital. Crimes cibernéticos, como o *phishing* (roubo de dados por meio de mensagens falsas), a clonagem de cartões, invasões de sistemas bancários e operações fraudulentas via aplicativos financeiros são alguns dos exemplos mais frequentes (Martins, 2020). Esses delitos, muitas vezes executados com alto grau de sofisticação técnica, desafiam as estruturas tradicionais de segurança da informação. Em resposta, empresas e instituições financeiras têm investido em soluções tecnológicas avançadas, como sistemas baseados em inteligência artificial e machine learning, que permitem analisar grandes volumes de dados e identificar padrões atípicos de comportamento, o que contribui significativamente para a prevenção de fraudes em tempo real (Moraes; Costa, 2018).

Entretanto, a luta contra a fraude financeira não se limita apenas à implantação de ferramentas tecnológicas. É fundamental que as organizações também cultivem uma cultura ética sólida, baseada na integridade, na responsabilidade social e na transparência. Essa cultura deve estar presente em todos os níveis da estrutura corporativa, desde a alta gestão até os setores operacionais (Boldt, 2025). Práticas como programas de compliance, treinamentos regulares, auditorias independentes, códigos de conduta e canais seguros de denúncia ajudam a fortalecer o compromisso institucional com a honestidade e a prevenção de desvios (Ferreira; Tavares, 2021).

Adotar uma postura preventiva é sempre mais eficaz e econômica do que remediar os danos causados por uma fraude consumada. Nesse sentido, a governança corporativa tem uma função importante, garantindo que haja fiscalização adequada, divisão clara de

responsabilidades e mecanismos de accountability. A transparência nos processos, a rastreabilidade das informações e o comprometimento com práticas sustentáveis são fatores que não apenas dificultam a ocorrência de fraudes, como também fortalecem a imagem e a competitividade das organizações no mercado (Ferreira; Tavares, 2021).

Combater a fraude financeira requer uma abordagem multidisciplinar, que envolva tecnologia, gestão eficiente, controle interno rigoroso e, principalmente, um compromisso ético firme com a legalidade e o bem coletivo (Nogueira, 2020).

2.1 A IMPORTÂNCIA DA INFORMAÇÃO NO PROCESSO DECISÓRIO

Em um ambiente empresarial marcado pela competitividade acirrada, pelas constantes transformações tecnológicas e pelas incertezas dos mercados, a informação assume um papel estratégico de valor inestimável. Não se trata apenas de reunir dados ou produzir relatórios: a informação, quando é precisa, contextualizada, confiável e tempestiva, transforma-se em um ativo essencial à sobrevivência e ao crescimento das organizações. Ela orienta o processo decisório, fundamenta estratégias, corrige desvios, antecipa riscos e sustenta a tomada de decisões em todos os níveis hierárquicos. A qualidade das decisões está diretamente condicionada à qualidade da informação disponível (Oliveira, 2019). Nesse sentido, informações imprecisas, incompletas ou desatualizadas podem induzir a erros operacionais e estratégicos, comprometendo seriamente o desempenho organizacional e colocando em risco a sustentabilidade da empresa (Maturo; Carleto, 2020).

De acordo com Maturo e Carleto (2020, p. 659):

> A falta de qualidade da informação em uma organização pode proporcionar impactos sociais e no negócio, devendo ser diagnosticada, e buscar caminhos para solucionar o problema. Informações com múltiplas origens, utilização de julgamentos subjetivos, sistemáticos erros na produção da informação, além do seu armazenamento em grande quantidade são alguns dos fatores que influenciam negativamente a qualidade da informação.

Contudo, a informação não surge de maneira espontânea. Ela é fruto de um processo contínuo de coleta, processamento, análise e interpretação de dados. Cada uma dessas etapas demanda critérios técnicos bem definidos e precisa estar alinhada às necessidades e objetivos da organização. O uso eficaz da informação requer, portanto, não apenas tecnologia adequada, mas também um planejamento consciente e um compromisso ético com a veracidade dos dados. Nesse processo, a intencionalidade ganha destaque: tanto pode ser utilizada de forma benéfica, para otimizar resultados e garantir a transparência, como pode ser distorcida, manipulada ou

ocultada com o objetivo de influenciar decisões de maneira indevida (Maturo; Carleto, 2020). A má utilização da informação, embora menos visível do que outras práticas fraudulentas, é uma das formas mais insidiosas de fraude, pois contamina o processo decisório desde sua origem e compromete toda a cadeia de resultados subsequente (Santos, 2018).

Um dos recursos mais recorrentes na manipulação da informação é a sua ocultação. Informações sensíveis ou comprometedoras podem ser propositalmente omitidas de relatórios, apresentações ou análises, criando uma ilusão de conformidade ou desempenho que não corresponde à realidade. Essa prática, comum em ambientes onde os controles internos são frágeis ou inexistentes, costuma ocorrer por meio de dados apresentados de forma parcial, métricas selecionadas estrategicamente ou interpretações enviesadas dos resultados. Em muitos casos, a ocultação deliberada de informações visa mascarar práticas irregulares ou mesmo sustentar decisões previamente definidas de forma subjetiva. Essa distorção da realidade compromete não apenas a qualidade das decisões, mas também a integridade das estruturas organizacionais, pois mina a confiança entre os agentes envolvidos e cria ambientes propícios ao surgimento de fraudes sistêmicas (Moreira, 2019).

Nesse contexto desafiador, os sistemas de informação (SI) tornam-se essencialmente importante. Mais do que meras ferramentas tecnológicas, eles funcionam como verdadeiras pontes entre os dados brutos e o processo decisório. Sistemas bem estruturados são capazes de reunir grandes volumes de dados, organizá-los, analisá-los e disponibilizá-los em formatos acessíveis por meio de painéis (*dashboards*), relatórios dinâmicos e análises preditivas. Essa infraestrutura oferece aos gestores a possibilidade de compreender, em tempo real, o cenário organizacional em que estão inseridos, identificando riscos, oportunidades e pontos de melhoria. Conforme aponta Maximiano (2020), o processo decisório é composto por diferentes etapas, que vão desde a identificação do problema até a implementação de ações corretivas, e, em todas elas, a presença de informações confiáveis é essencial para que se tomem decisões eficazes e seguras.

Ainda assim, mesmo diante de sistemas tecnológicos avançados, o fator humano continua a exercer influência decisiva sobre a integridade da informação. A confiança depositada em profissionais que ocupam cargos estratégicos pode ser, por vezes, explorada para fins escusos. Manipulações sutis nos registros, interpretações tendenciosas de relatórios ou omissões deliberadas de dados são práticas que, embora difíceis de detectar num primeiro momento, produzem efeitos graves e duradouros (Maximiano, 2020). Essa violação da confiança organizacional compromete a credibilidade das informações e pode resultar em decisões baseadas em premissas falsas, levando a investimentos mal direcionados, perdas

financeiras e problemas de conformidade com legislações e normas regulatórias (Pereira, 2021).

Diante desses riscos, torna-se indispensável repensar o papel da informação como instrumento de governança e de cultura organizacional. A informação, quando utilizada de forma ética e transparente, não apenas fortalece o processo decisório, como também promove um ambiente de confiança, responsabilidade e resiliência institucional. Organizações que cultivam uma cultura voltada para a integridade da informação tendem a tomar decisões mais acertadas, além de responder com maior agilidade às mudanças do mercado e aos desafios imprevistos. Isso passa, necessariamente, por ações educativas e preventivas, como treinamentos periódicos, programas de compliance, canais de denúncia eficazes e a adoção de normas internas claras sobre o uso da informação (Pereira, 2021).

Com o avanço das tecnologias digitais, ferramentas como a inteligência artificial (IA), o aprendizado de máquina (*machine learning*) e os sistemas de análise preditiva vêm ganhando espaço como aliadas no processo decisório. Essas tecnologias são capazes de detectar comportamentos atípicos, prever cenários com base em tendências históricas e identificar, de forma automatizada, pontos de vulnerabilidade nos processos organizacionais. Essa capacidade de antecipação e resposta rápida aos sinais de alerta representa uma grande conquista da era digital, contribuindo não apenas para a prevenção de fraudes, mas também para o aprimoramento da performance organizacional (Lima, 2020).

No entanto, é preciso cautela. A tecnologia, por si só, não é suficiente para garantir decisões éticas e eficazes. É necessário que esses recursos estejam integrados a uma cultura organizacional voltada para a responsabilidade, a transparência e a boa governança. A dependência excessiva de sistemas automatizados, sem a devida supervisão humana, pode gerar uma falsa sensação de segurança e abrir brechas para novas formas de manipulação. O equilíbrio entre tecnologia e ética é, portanto, o caminho mais promissor para construir organizações sólidas, resilientes e confiáveis (Pereira, 2021).

Dessa forma, pode-se afirmar que a informação representa o alicerce das decisões organizacionais e deve ser tratada como tal. Desde a sua geração até a sua utilização final, ela precisa ser gerida com rigor técnico, responsabilidade ética e vigilância constante. A intencionalidade na produção da informação, os riscos de manipulação e a ocultação de dados são elementos que ameaçam diretamente a qualidade das decisões e, por consequência, a sustentabilidade da organização como um todo. Assim, garantir a integridade da informação e criar estruturas capazes de protegê-la são imperativos para qualquer organização que deseja não apenas sobreviver, mas prosperar em um ambiente cada vez mais exigente, competitivo e interconectado.

2.2 CARACTERÍSTICAS DE FRAUDE FINANCEIRA

A fraude financeira é um fenômeno complexo e multifacetado que afeta de maneira profunda a integridade econômica das organizações. Seus impactos vão além dos prejuízos financeiros diretos, alcançando dimensões intangíveis como o desgaste da imagem institucional, o comprometimento da reputação e a consequente perda da confiança de investidores, clientes, parceiros comerciais e demais *stakeholders*. Em um ambiente empresarial cada vez mais dinâmico e digitalizado, compreender a fraude em sua essência, ou seja, analisando seus aspectos estruturais, psicológicos e operacionais, tornou-se um requisito indispensável para a gestão de riscos e a sustentabilidade das instituições (Medrado, 2016).

Ao contrário de falhas operacionais ou erros não intencionais, a fraude financeira possui características bem definidas que a distinguem de outros tipos de irregularidades. Dentre os elementos mais marcantes, destacam-se três pilares principais: a intencionalidade, a ocultação e a violação de confiança. Esses componentes não apenas revelam a natureza ardilosa do comportamento fraudulento, mas também demonstram seu caráter planejado, persistente e muitas vezes dissimulado, exigindo das organizações uma postura proativa, preventiva e tecnicamente embasada para combatê-la (Santos, 2018).

Para Medrado (2016, p. 31): “As fraudes estão associadas a manipulações contábeis, algo que não ocorre nas decisões estratégicas e contábeis tradicionais. Nas decisões contábeis existem legislações que devem ser seguidas, porém quando os fatos são manipulados é caracterizada a fraude”.

O primeiro aspecto que deve ser ressaltado é a intencionalidade. A fraude financeira não é fruto do acaso. Ela nasce da ação consciente de um ou mais indivíduos que, de maneira deliberada, decidem manipular dados, simular operações, omitir informações ou criar estruturas fictícias com o objetivo de obter vantagem indevida. Trata-se, portanto, de um ato premeditado, muitas vezes sofisticado, que exige conhecimento prévio das fragilidades do sistema de controle da organização. Segundo Santos (2018), a fraude é construída com base no domínio de processos internos, na identificação de brechas operacionais e na convicção de que a ação pode passar despercebida pelos mecanismos formais de auditoria e fiscalização. O autor destaca que a intencionalidade é o que diferencia a fraude de simples falhas administrativas, pois nela há um projeto de engano e apropriação, sustentado pela racionalidade criminosa do agente fraudador (Medrado, 2016).

Além disso, a ocultação é uma característica essencial para o sucesso de qualquer fraude. Segundo Waller Júnior (2003, p. 38), especialista brasileiro em combate à fraude: “a

fraude só é possível quando há um disfarce, uma camuflagem, pois o fraudador precisa simular normalidade para que suas ações passem despercebidas".

Fraudes não resistem à luz da transparência, e por isso dependem de estratégias eficazes de disfarce. A ocultação pode ocorrer de diferentes formas, desde alterações em registros contábeis e fiscais, passando pela criação de documentos falsos, até o uso de empresas de fachada, contas bancárias em nome de terceiros e laranjas. Em muitos casos, os fraudadores exploram lacunas nos sistemas de controle, ausência de auditorias regulares, sobrecarga de processos ou até mesmo confiança excessiva por parte da alta gestão.

Vale salientar que quanto mais elaborada for a estrutura de ocultação, mais difícil será a detecção da fraude e mais tempo ela poderá perdurar, gerando prejuízos acumulados à organização. A sofisticação desses mecanismos revela um grau elevado de planejamento e uma compreensão estratégica do funcionamento interno da empresa (Moreira, 2019).

Nesse sentido, as práticas contábeis fraudulentas também assumem um papel central no processo de ocultação, especialmente quando o objetivo é maquiar a real situação econômica da empresa. Como afirmam Cosenza e Grateron (2003, p. 6), o infrator:

> Apresenta demonstrativos enganosos, que são utilizados com o intuito de elevar ou diminuir o preço das ações de uma empresa, bem como para ocultar certos problemas da empresa, ou seja, para enganar investidores e credores ou, até mesmo, o governo, com fins tributários e fiscais. [...] A política contábil maquiadora está relacionada à redução de picos de receitas ou lucros, no sentido de aumentar o nível de confiança, bem como evitar grandes oscilações que causem prejuízos à política ou imagem social da empresa.

Esse tipo de manipulação revela a intencionalidade por trás da fraude e o grau de cálculo envolvido na escolha dos métodos de disfarce. A contabilidade, que deveria ser um instrumento de transparência e responsabilidade fiscal, torna-se, nesse contexto, uma ferramenta de engano. Os gestores que adotam tais práticas violam não apenas princípios éticos, mas também normativas legais, comprometendo a integridade da organização e dos seus demonstrativos financeiros. Assim, o uso estratégico de técnicas contábeis para ocultar realidades desfavoráveis amplia ainda mais o desafio enfrentado pelas auditorias e pelos sistemas de controle na identificação de fraudes financeiras (Moreira, 2019).

Outro elemento recorrente nas fraudes financeiras é a violação de confiança, talvez o mais doloroso para as instituições. Em geral, os agentes responsáveis por fraudes ocupam cargos de confiança, possuem autonomia para autorizar processos ou têm acesso privilegiado a informações sensíveis. Essa posição lhes confere credibilidade e reduz o nível de vigilância sobre suas ações. A violação da confiança ocorre, portanto, quando um colaborador ou parceiro da organização se aproveita do vínculo estabelecido para agir em benefício próprio, em

detrimento dos valores éticos e dos interesses da instituição. Em muitos casos, a fraude é descoberta com surpresa, pois parte de indivíduos considerados exemplares, com longa trajetória profissional e reputação consolidada. Esse aspecto torna a prevenção ainda mais desafiadora, pois pressupõe um sistema de controle que transcenda a lógica da confiança pessoal, baseando-se em critérios objetivos, monitoramento contínuo e auditoria sistêmica (Pereira, 2021).

Importante destacar que essa quebra de confiança não se limita ao ambiente interno da empresa. Ela pode estender-se a relações comerciais externas, envolvendo fornecedores, clientes ou parceiros estratégicos. Fraudes em contratos de fornecimento, acordos comerciais fraudulentos, superfaturamento de produtos ou serviços e emissão de notas fiscais falsas são exemplos de práticas que, embora externas à estrutura organizacional direta, afetam diretamente sua integridade financeira e reputacional. Em todos esses casos, a confiança, seja contratual, profissional ou institucional, é explorada de forma indevida, e o resultado final é o mesmo: perda de recursos, desgaste de imagem e comprometimento da credibilidade da organização no mercado (Lima, 2020).

A combinação desses três elementos, intencionalidade, ocultação e violação de confiança, compõe o que a literatura especializada denomina tripé da fraude (Lima, 2020). Esse modelo teórico ajuda a entender que a fraude não é um evento isolado, mas sim um processo construído gradualmente, sustentado em estratégias racionais, articulado com conhecimento técnico e motivado por interesses pessoais ou grupais. O tripé da fraude também aponta que não basta combater os sintomas: é preciso atuar nas causas estruturais, culturais e institucionais que possibilitam o surgimento e a manutenção desses comportamentos ilícitos dentro das organizações (Gonçalves; Lima, 2017).

Diante desse panorama, é imprescindível que as organizações adotem políticas de prevenção e dissuasão da fraude, combinando recursos tecnológicos, processos bem definidos e uma cultura organizacional voltada para a ética e a responsabilidade. Sistemas de controle interno robustos, auditorias periódicas, segregação de funções, códigos de conduta atualizados e canais seguros de denúncia são medidas fundamentais nesse sentido. O uso de tecnologias avançadas, como análise preditiva, algoritmos de detecção de anomalias, inteligência artificial e aprendizado de máquina, também pode oferecer suporte valioso na identificação de padrões de comportamento suspeitos e na antecipação de riscos.

Contudo, tão importante quanto a tecnologia é o componente humano. A promoção de uma cultura de integridade, o investimento em treinamentos éticos, a valorização da transparência e a criação de um ambiente em que o erro possa ser identificado e corrigido sem

medo de retaliação são medidas que fortalecem a resiliência organizacional diante do risco de fraudes. Afinal, a fraude é, em última instância, uma escolha e, portanto, deve ser combatida com ações que dificultem sua execução, mas também com uma gestão capaz de formar pessoas e lideranças comprometidas com o bem coletivo.

2.3 DESAFIOS NA DETECÇÃO E PREVENÇÃO DA FRAUDE

A detecção e prevenção de fraudes financeiras constituem tarefas cada vez mais desafiadoras em um cenário corporativo marcado pela digitalização intensiva, pela complexidade dos sistemas e pela sofisticação crescente dos métodos utilizados pelos fraudadores. Ainda que diversas ferramentas tecnológicas tenham sido desenvolvidas com o objetivo de mitigar riscos, é necessário reconhecer que o problema não se limita à tecnologia: fatores humanos, culturais, operacionais e estruturais também contribuem para a manutenção de um ambiente propício à ocorrência de irregularidades. Compreender esses desafios é essencial para construir estratégias robustas de prevenção e resposta (Lima, 2020).

Um dos principais entraves enfrentados pelas organizações refere-se à evolução constante das táticas de fraude. Fraudadores estão em permanente atualização, adaptando suas práticas de acordo com as mudanças nos sistemas de segurança, legislações, normas contábeis e processos corporativos. Esquemas que anteriormente eram facilmente detectáveis passam por reformulações, explorando novas brechas nos sistemas e nas relações humanas. Os fraudadores tendem a agir de forma oportunista e estratégica, antecipando-se às medidas de controle e criando modos criativos de burlar as regras. Isso exige que as empresas adotem posturas dinâmicas, revisem constantemente seus sistemas de compliance e invistam em tecnologias capazes de detectar padrões atípicos em tempo real (Lima, 2020).

Outro obstáculo importante está relacionado à educação e conscientização dos colaboradores. Ainda que sistemas avançados de segurança digital sejam implantados, muitas fraudes se originam da ação ou omissão humana. Funcionários que desconhecem as práticas comuns de fraude, os sinais de alerta ou mesmo os canais adequados para denúncia tornam-se vulneráveis, seja como vítimas, seja como agentes involuntários de irregularidades. De acordo com Silva e Rocha (2019), a capacitação contínua da equipe é uma das ferramentas mais eficazes de prevenção, pois transforma cada colaborador em um agente de vigilância ativa contra comportamentos suspeitos. Promover uma cultura organizacional baseada na ética, na transparência e na responsabilidade é uma estratégia de longo prazo, mas de efeitos comprovadamente positivos (Silva; Rocha, 2019).

Ainda segundo Silva e Rocha (2019, p. 142):

> Ainda que os sistemas de controle internos sejam automatizados e sofisticados, a fragilidade humana continua sendo uma das maiores vulnerabilidades nas organizações. A falta de capacitação, aliada à negligência ou desconhecimento, transforma os colaboradores em potenciais facilitadores de fraudes, mesmo que involuntariamente. Por isso, a formação contínua deve ser entendida como uma estratégia permanente de mitigação de riscos.

Entretanto, muitas empresas enfrentam resistência cultural à mudança, o que dificulta a adoção de novas medidas de prevenção e controle. A introdução de novas tecnologias, processos de auditoria automatizados ou modificações em rotinas tradicionais pode gerar desconforto, medo de exposição e até sabotagem velada por parte de setores que veem essas ações como ameaças ao status quo. Essa resistência costuma ser maior em empresas com estruturas hierárquicas rígidas, pouca comunicação entre os níveis gerenciais e ausência de lideranças comprometidas com a integridade organizacional. Segundo Pereira (2021), superar esse entrave demanda uma abordagem sensível, que combine diálogo, transparência e inclusão dos colaboradores no processo de transformação cultural.

Além disso, a complexidade dos sistemas financeiros atuais representa um desafio técnico relevante. Com a multiplicação de plataformas, aplicativos, transações automatizadas e integração de dados em tempo real, torna-se cada vez mais difícil acompanhar todos os movimentos financeiros com a acurácia necessária para identificar desvios ou inconsistências. Essa complexidade, embora muitas vezes traga ganhos operacionais, cria também um terreno fértil para práticas ilícitas que se camuflam entre milhares de transações legítimas. Ferramentas de inteligência artificial e big data analytics vêm sendo utilizadas para enfrentar esse problema, mas sua eficácia depende da qualidade dos dados inseridos e da capacidade da organização em interpretar os resultados corretamente (Moura; Oliveira, 2020).

Por fim, é preciso considerar o desafio dos recursos limitados. Muitas organizações, especialmente de médio e pequeno porte, não dispõem de orçamento suficiente para investir em soluções avançadas de monitoramento, contratar especialistas em auditoria ou desenvolver programas internos de compliance. A ausência de recursos pode levar à priorização de ações imediatistas, em detrimento de estratégias preventivas, deixando a organização vulnerável a fraudes de maior impacto no longo prazo. A prevenção de fraudes não deve ser vista como um custo adicional, mas como um investimento estratégico na sustentabilidade do negócio. Há diversas soluções escaláveis e adaptáveis que permitem às empresas implementar controles eficazes sem comprometer sua viabilidade financeira (Moura; Oliveira, 2020).

A detecção e prevenção de fraudes envolvem um conjunto de desafios interligados,

que vão desde a necessidade de atualização tecnológica até questões culturais e limitações orçamentárias. Para enfrentá-los de forma eficaz, é necessário adotar uma abordagem integrada, que envolva pessoas, processos e tecnologia. Somente com uma cultura de integridade, investimentos contínuos em capacitação e inovação, e comprometimento da alta gestão será possível construir um ambiente organizacional menos propenso à fraude, mais resiliente diante de riscos e alinhado com os princípios de governança e transparência exigidos pelo mercado contemporâneo.

2.4 O PROCESSO DE GESTÃO E A FRAUDE FINANCEIRA

A crescente complexidade dos ambientes organizacionais contemporâneos tem intensificado a centralidade da informação como recurso estratégico. O processo de gestão da informação, entendido como a captação, organização, disseminação e uso adequado da informação no contexto organizacional, desempenha um papel determinante tanto na prevenção quanto na facilitação de fraudes financeiras, dependendo da forma como é conduzido. Nesse sentido, compreender a inter-relação entre a gestão da informação e os mecanismos de fraude é essencial para o fortalecimento da integridade institucional.

A gestão da informação é o conjunto de práticas voltadas à administração eficiente dos ativos informacionais de uma organização, permitindo que decisões mais racionais e fundamentadas sejam tomadas. Entretanto, o mesmo sistema que torna possível a transparência e o controle organizacional pode ser manipulado e utilizado como meio para ocultar condutas fraudulentas, especialmente quando há falhas nos processos de controle e monitoramento da informação (Davenport, 1998).

A fraude financeira, por sua vez, é definida como qualquer ação intencional voltada à obtenção de vantagem ilícita por meio da manipulação de registros contábeis, financeiros ou administrativos. Tais ações se apoiam, muitas vezes, no domínio da informação, seja pela sua ocultação, distorção ou utilização seletiva, o que evidencia uma profunda ligação entre os processos informacionais e o sucesso ou fracasso dos mecanismos antifraude.

A informação organizacional não é apenas um recurso operacional, mas um elemento decisivo para o comportamento organizacional e a estruturação de práticas. Quando a informação é mal gerida, seja por negligência, desconhecimento ou intenção deliberada, abre-se espaço para vulnerabilidades exploráveis por agentes internos e externos. A gestão da informação deve, portanto, incorporar uma dimensão ética e normativa, sob pena de transformar-se em um instrumento que facilita desvios e fraudes (Choo, 2003).

Segundo Bolaño (2000, p. 67), “a assimetria da informação não pode ser entendida apenas como uma falha de mercado, mas como um elemento estrutural do modo capitalista de produção, relacionado à apropriação privada do conhecimento e ao controle dos fluxos informacionais”.

Outro ponto crucial é a busca por informação como um processo que pode tanto proteger quanto comprometer a organização. A maneira como os profissionais buscam, interpretam e utilizam informações determina a qualidade da tomada de decisão. No entanto, quando a busca por informação visa apenas interesses pessoais ou é direcionada a explorar falhas no sistema, torna-se um canal para a prática de fraude. A coleta seletiva de dados, a geração de relatórios falsos ou incompletos e o mascaramento de indicadores de desempenho são práticas recorrentes em esquemas fraudulentos, especialmente aqueles que ocorrem de forma interna (Marchand; Kettinger; Rollins, 2001).

Além disso, a gestão da informação deve estar aliada a sistemas robustos de tecnologia da informação. Os sistemas informacionais devem ser desenhados para garantir a integridade, a rastreabilidade e a verificabilidade das informações. Isso implica na adoção de políticas de segurança, criptografia, trilhas de auditoria e controle de acessos, sem os quais o ambiente informacional torna-se vulnerável às fraudes. A inexistência de camadas protetoras e de fluxos transparentes de dados compromete a confiabilidade do sistema como um todo (Davenport; Prusak, 1998).

Por fim, a relação entre gestão da informação e fraude financeira também se expressa no nível cultural e comportamental das organizações. Ambientes corporativos que não incentivam a cultura da informação e que desvalorizam os registros formais, as evidências documentais e os sistemas de controle interno tendem a ser mais suscetíveis a práticas fraudulentas. Como observam Waller Júnior (2003) e Silva e Moreira (2018), a fraude prospera em ambientes informacionalmente frágeis, onde o conhecimento institucionalizado é precário e a memória organizacional é facilmente manipulável.

Dessa forma, conclui-se que o processo de gestão da informação deve ser compreendido não apenas como um mecanismo de suporte à tomada de decisão, mas como instrumento estruturante da cultura de integridade nas organizações. A forma como a informação é tratada, desde sua coleta até sua disseminação e uso, influencia diretamente a vulnerabilidade ou a resiliência das instituições frente à ameaça das fraudes financeiras. Portanto, uma gestão da informação ética, integrada e tecnicamente sólida é um dos principais antídotos contra práticas fraudulentas no ambiente corporativo.

3 APLICAÇÃO DE SISTEMAS DE INFORMAÇÃO NA PREVENÇÃO DE FRAUDES

A utilização de sistemas de informação (SI) na prevenção de fraudes financeiras constitui uma estratégia essencial para organizações que buscam não apenas proteger seus ativos, mas também promover práticas éticas e sustentáveis. Com o avanço da transformação digital, novas tecnologias vêm sendo integradas aos processos organizacionais, permitindo maior vigilância, agilidade na identificação de riscos e tomada de decisões baseadas em dados confiáveis. Nesse cenário, destaca-se a transição de sistemas tradicionais para ferramentas inteligentes, capazes de processar grandes volumes de dados, identificar padrões de comportamento e detectar anomalias com maior precisão.

3.1 FERRAMENTAS E TECNOLOGIAS UTILIZADAS

A incorporação de tecnologias emergentes nas estratégias de prevenção e combate à fraude tem transformado a forma como as organizações identificam, analisam e respondem a comportamentos suspeitos. Entre essas tecnologias, destacam-se a Inteligência Artificial (IA), o *Machine Learning* (ML), o *Big Data*, a análise preditiva, o Blockchain e os sistemas de criptografia, todos fundamentais para fortalecer a integridade dos sistemas de informação e mitigar riscos operacionais e financeiros (Rezende, 2021).

A Inteligência Artificial e o *Machine Learning* têm sido particularmente eficazes ao permitir que os sistemas computacionais aprendam com dados históricos e identifiquem automaticamente desvios significativos em tempo real. Essas tecnologias possibilitam a construção de modelos preditivos capazes de reconhecer padrões comportamentais atípicos e, com isso, detectar fraudes de maneira mais eficiente, reduzindo falsos positivos e otimizando os recursos humanos e financeiros destinados à auditoria (Rezende, 2021; Costa et al., 2023). Os algoritmos de ML, ao serem alimentados com grandes volumes de dados, tornam-se capazes de classificar transações como suspeitas com base em parâmetros dinâmicos, ajustando-se ao perfil de risco específico da organização. Segundo Rezende (2021, p. 134):

> A inteligência artificial tem se mostrado uma ferramenta poderosa na detecção de fraudes, pois permite que sistemas aprendam com padrões históricos de comportamento e reconheçam, de forma autônoma, desvios estatisticamente relevantes. Isso possibilita uma ação mais rápida e eficaz das equipes de auditoria e compliance, que passam a contar com alertas automatizados e classificações de risco baseadas em análises preditivas, reduzindo consideravelmente a incidência de falsos positivos e aumentando a assertividade das investigações internas.

Essas ferramentas podem ser utilizadas em diferentes fases do processo antifraude,

desde a triagem inicial de transações até a análise de investigações mais aprofundadas. Por exemplo, em bancos e operadoras de cartão de crédito, algoritmos supervisionados são empregados para detectar movimentações atípicas e acionar bloqueios automáticos, evitando a consumação de prejuízos. Em ambientes corporativos, ML também é empregado para cruzar dados de folha de pagamento, reembolsos e contas a pagar, contribuindo para identificar anomalias que indiquem fraudes internas. A aplicação contínua de IA nos setores financeiros tem resultado em um aumento significativo da acurácia na detecção de comportamentos fraudulentos, principalmente quando associada a bases de dados atualizadas e mecanismos de *feedback* humano (Oliveira; Matos, 2022).

O uso de *Big Data* e análise preditiva complementa essas estratégias, ampliando significativamente a capacidade de rastreamento e investigação. A análise preditiva, ao integrar dados em tempo real com algoritmos estatísticos, permite a identificação precoce de padrões que indicam risco iminente. Como afirmam Silva e Moreira (2018), ao processar dados estruturados e não estruturados oriundos de múltiplas fontes, como sistemas de pagamento, redes sociais, sensores IoT e dispositivos móveis, é possível criar modelos de risco muito mais refinados e personalizados.

Com *Big Data*, organizações de diferentes portes podem desenvolver painéis de controle adaptáveis ao seu setor de atuação. Por exemplo, uma empresa do setor varejista pode monitorar mudanças nos ciclos de vendas ou no comportamento de seus clientes e fornecedores, detectando rapidamente ações que desviem do padrão histórico. Além disso, ao integrar fontes externas, como registros públicos, bases de inadimplência e dados fiscais, as análises ganham maior profundidade e assertividade, revelando vulnerabilidades que passariam despercebidas em métodos tradicionais (Fernandes; Nascimento, 2022).

Nesse cenário, uma tecnologia emergente que tem ganhado destaque é o *blockchain*. Caracterizado por sua estrutura descentralizada, criptografada e imutável, o *blockchain* oferece um alto grau de confiabilidade na verificação de transações e registros digitais. Sua aplicação em ambientes corporativos contribui para garantir a autenticidade de contratos, validar cadeias de custódia e monitorar o fluxo de produtos e valores de forma transparente (Moura; Oliveira, 2020). No setor financeiro, o *blockchain* reduz significativamente o risco de adulteração de registros contábeis e de movimentações financeiras ilegítimas, ao criar um histórico permanente e rastreável de todas as operações realizadas.

Além disso, sua utilização tem se expandido para setores como o de saúde, logística e propriedade intelectual. Em cadeias de suprimentos, por exemplo, o blockchain pode ser utilizado para garantir a rastreabilidade de produtos desde a produção até o consumidor final,

coibindo práticas de falsificação e desvios. Já em hospitais e seguradoras, sua aplicação permite validar prontuários médicos e contratos de cobertura, preservando a integridade dos dados sensíveis e assegurando conformidade com legislações como a Lei Geral de Proteção de Dados (LGPD).

Complementarmente, a criptografia continua sendo uma aliada fundamental na proteção de dados sigilosos. Em sistemas de informação, técnicas criptográficas asseguram que as informações transmitidas entre usuários e servidores permaneçam inacessíveis a terceiros não autorizados. A criptografia *end-to-end*, por exemplo, tem sido amplamente utilizada para proteger comunicações empresariais e dados bancários, reduzindo significativamente os riscos de interceptação e vazamento de informações (Pereira; Almeida, 2021). Além disso, tecnologias como autenticação multifator e certificados digitais reforçam ainda mais a camada de segurança dos sistemas corporativos.

Essas ferramentas, quando integradas, promovem uma abordagem sistêmica e inteligente de prevenção à fraude, baseada em dados e com capacidade adaptativa. No entanto, é importante destacar que a tecnologia, por si só, não é suficiente. Sua eficácia está diretamente relacionada ao investimento em capacitação de profissionais, bem como ao fortalecimento da cultura organizacional voltada à ética e à transparência. O sucesso das iniciativas de segurança da informação depende tanto da robustez técnica das soluções quanto do engajamento institucional em criar ambientes seguros e responsáveis (Barros; Souza, 2023).

Dessa forma, a aplicação combinada de IA, ML, Big Data, análise preditiva, Blockchain e criptografia representa um avanço significativo na luta contra fraudes corporativas. Tais tecnologias têm proporcionado às organizações não apenas a capacidade de detectar fraudes em tempo real, mas também de antecipar riscos e agir preventivamente, promovendo uma governança mais eficaz e contribuindo para a sustentabilidade dos negócios em um cenário global cada vez mais digital e interconectado.

3.2 MONITORAMENTO E AUDITORIA AUTOMATIZADA

O monitoramento contínuo tem se consolidado como uma das estratégias mais eficazes na identificação precoce de tentativas de fraude, especialmente em ambientes organizacionais que lidam com grandes volumes de dados e transações. Trata-se de um processo baseado em tecnologias avançadas que viabilizam a supervisão em tempo real das operações empresariais, possibilitando respostas rápidas e assertivas diante de anomalias. Os sistemas modernos de detecção de anomalias, por exemplo, utilizam algoritmos de aprendizado de máquina (machine

learning) para comparar dados transacionais com padrões de comportamento historicamente registrados, emitindo alertas sempre que identificam desvios significativos (Carvalho; Andrade, 2019).

A eficiência desses sistemas reside em sua capacidade de aprender continuamente com o comportamento das operações e aprimorar, de forma autônoma, os parâmetros de normalidade. A implementação de um sistema de detecção de anomalias envolve, geralmente, várias etapas estruturadas: a definição inicial dos padrões considerados normais, a coleta e o tratamento de dados em tempo real, a aplicação de métodos estatísticos e computacionais para comparação de dados e, por fim, a geração automatizada de alertas e relatórios. Com isso, torna-se possível o acompanhamento simultâneo de milhares de registros, operações e interações organizacionais, reduzindo significativamente o tempo de resposta das áreas de compliance, auditoria e controle interno (Souza; Campos, 2021).

No que se refere à auditoria automatizada, os Sistemas de Informação (SI) desempenham um papel central ao substituir processos manuais e periódicos por mecanismos automáticos e contínuos de verificação. Tais mecanismos realizam análises de conformidade, detecção de inconsistências e cruzamento de dados com alto nível de precisão. Conforme destacam Gonçalves e Lima (2017), a automação dos processos de auditoria interna não apenas aumenta a abrangência e profundidade das investigações, como também proporciona uma redução substancial de erros humanos, possibilitando que os auditores direcionem seu foco a análises mais estratégicas e interpretativas.

Como ressaltam Silva e Moreira (2018, p. 88), o uso de tecnologia nos controles internos transforma profundamente a capacidade organizacional de detectar e reagir a comportamentos suspeitos:

> A aplicação de tecnologias inteligentes nos controles internos permite que a organização passe de uma postura passiva para uma atitude proativa no enfrentamento de fraudes. Com a automatização dos processos de monitoramento e auditoria, torna-se viável acompanhar em tempo real as operações, identificar comportamentos fora do padrão e reagir com rapidez e precisão, minimizando os impactos das irregularidades e aumentando a confiança nos sistemas de controle.

As ferramentas de auditoria contínua podem ser integradas a sistemas de gestão de riscos, atribuindo escores de risco a cada transação com base em variáveis predefinidas, como valor, frequência, origem, localização e histórico do cliente ou fornecedor. Esse tipo de sistema age como um filtro inteligente que prioriza a revisão de transações potencialmente irregulares, permitindo que os recursos humanos da auditoria sejam utilizados com maior eficiência. Isso representa uma mudança de paradigma na função da auditoria, que deixa de ser meramente

reativa e passa a assumir um papel preventivo e estratégico dentro da organização (Almeida; Ribeiro, 2022).

Além da eficiência operacional, o monitoramento automatizado contribui para o fortalecimento dos controles internos, que se tornam mais estruturados e confiáveis quando integrados a sistemas tecnológicos. A supervisão dos processos operacionais, desde a entrada de dados até a consolidação em relatórios gerenciais, passa a ser contínua, documentada e transparente. A automatização permite, por exemplo, detectar conflitos de interesse por meio da análise de relacionamentos entre colaboradores e fornecedores, ou identificar inconsistências entre lançamentos contábeis e registros bancários. Como ressaltam Silva e Moreira (2018), a tecnologia aplicada aos controles internos amplia significativamente a capacidade das organizações em detectar, prevenir e responder a riscos operacionais e fraudes financeiras.

Entre os mecanismos de controle mais eficazes, destacam-se a segregação de funções, a autenticação multifatorial em transações críticas, a criação de trilhas de auditoria digital e o uso de *dashboards* analíticos em tempo real. Esses recursos proporcionam uma visão holística e integrada do funcionamento organizacional, permitindo que gestores e auditores monitorem indicadores-chave de desempenho (KPIs) e identifiquem variações que possam sinalizar comportamentos inadequados ou riscos emergentes (Freitas; Martins, 2023). A capacidade de visualizar tendências, padrões e anomalias de forma visual e intuitiva reforça o caráter preventivo das práticas de auditoria automatizada.

A adoção de práticas tecnológicas integradas à auditoria e ao monitoramento também contribui para a construção de uma cultura organizacional orientada à ética, transparência e conformidade. Empresas que investem em SI robustos e integrados conseguem não apenas detectar fraudes em curso, mas também dissuadir potenciais infratores ao tornar o ambiente corporativo mais seguro e menos vulnerável a ações ilícitas. Como destacam Costa e Batista (2023), a percepção de vigilância contínua e de resposta rápida atua como fator inibidor de práticas fraudulentas, influenciando positivamente a conduta dos colaboradores.

Em síntese, o monitoramento contínuo, a auditoria automatizada e os controles internos digitais compõem um ecossistema tecnológico e gerencial fundamental para a prevenção de fraudes e a mitigação de riscos organizacionais. Essas ferramentas ampliam a capacidade analítica das organizações, promovem maior transparência nos processos internos e fortalecem a governança corporativa. Ao integrar dados em tempo real, algoritmos de análise avançada e políticas internas bem definidas, as empresas se posicionam de maneira mais segura diante de um cenário corporativo cada vez mais complexo e vulnerável a ameaças financeiras.

3.3 INTEGRAÇÃO DE DADOS E TOMADA DE DECISÃO

A integração de dados entre diferentes setores da organização é um pilar fundamental para a eficácia das estratégias de prevenção e combate à fraude. Em ambientes corporativos cada vez mais complexos e dinâmicos, a unificação de informações oriundas de áreas como finanças, operações, recursos humanos, logística e tecnologia da informação viabiliza análises mais precisas e ações mais coordenadas. Os sistemas de informação (SI) modernos superam as limitações dos sistemas tradicionais, que funcionavam de maneira compartimentalizada, dificultando a comunicação entre departamentos e comprometendo a agilidade na identificação de atividades suspeitas (Moraes; Costa, 2018).

A fragmentação de informações, que por muitos anos foi um dos maiores entraves à gestão eficaz, costumava gerar inconsistência de dados, duplicações e atrasos na resposta a eventos críticos. Departamentos operando de forma isolada frequentemente mantinham bases de dados próprias e incompatíveis, o que impedia uma análise conjunta de variáveis essenciais para a identificação de fraudes. Com o advento das plataformas de gestão integrada, como os sistemas ERP (*Enterprise Resource Planning*), tornou-se possível consolidar em um único ambiente tecnológico informações de múltiplas fontes, promovendo visibilidade total sobre as operações da empresa (Oliveira; Almeira, 2021).

Essa integração possibilita o cruzamento automatizado de dados em tempo real, o que é crucial para o reconhecimento de padrões comportamentais incomuns. Por exemplo, é possível identificar a atuação de um colaborador com acesso simultâneo aos módulos de compras e aprovação de pagamentos, uma falha clássica de segregação de funções que pode indicar fraude interna. A integração de dados operacionais com informações financeiras e de recursos humanos tem sido determinante na detecção de incongruências, especialmente quando essas integrações são sustentadas por políticas de governança e auditoria contínuas (Moraes; Costa, 2018).

Outro diferencial dos sistemas atuais é o suporte à tomada de decisão baseada em dados. Ferramentas como dashboards interativos, painéis analíticos e sistemas de *Business Intelligence* (BI) facilitam a interpretação e o monitoramento de indicadores-chave de desempenho. Esses recursos proporcionam aos gestores uma visão clara e dinâmica do desempenho corporativo, permitindo respostas mais ágeis e fundamentadas. Os Sistemas de Suporte à Decisão (SSD), por sua vez, agregam funcionalidades como modelagem estatística, simulações de cenários e projeções de impacto, tornando-se ferramentas valiosas para a formulação de estratégias preventivas e corretivas (Gonçalves; Lima, 2017).

Essa nova abordagem, como enfatizam Gonçalves e Lima (2017, p. 102), representa uma quebra de paradigma na gestão organizacional:

> A integração de dados e a utilização de sistemas de apoio à decisão representam uma ruptura com o modelo tradicional de gestão fragmentada. Ao reunir informações de múltiplas áreas em uma única plataforma analítica, a organização amplia sua capacidade de identificar riscos, cruzar evidências e agir preventivamente. Essa abordagem permite decisões mais rápidas, embasadas e eficazes, especialmente em ambientes voláteis onde a resposta ao risco precisa ser quase imediata.

Além de organizar e apresentar os dados de forma visualmente acessível, esses sistemas promovem *insights* avançados por meio da mineração de dados (*data mining*). Essa técnica permite detectar padrões ocultos e correlações improváveis, revelando riscos latentes que não seriam identificados em análises convencionais. Em setores altamente expostos a riscos operacionais, como o bancário, o segurador e o varejista, a capacidade de gerar inteligência a partir de grandes volumes de dados é indispensável para responder com agilidade a comportamentos anômalos (Barros; Souza, 2023).

A eficácia da tomada de decisão baseada em dados, no entanto, não depende exclusivamente da tecnologia. É necessário construir uma cultura organizacional orientada à informação, na qual os dados sejam valorizados como ativos estratégicos e utilizados de forma sistemática e ética no processo decisório. Isso implica não apenas em treinamentos técnicos para os gestores e analistas, mas também na definição de políticas de governança de dados, na normatização do uso da informação e na definição de métricas de desempenho que incentivem o uso inteligente e proativo dos sistemas de informação (Moura; Oliveira, 2020).

A mobilidade digital e os sistemas baseados em nuvem também desempenham um papel central nesse processo, pois permitem que os dados sejam acessados e analisados de qualquer lugar e a qualquer momento. Essa flexibilidade amplia a capacidade das empresas de responder rapidamente a eventos suspeitos, especialmente em estruturas organizacionais descentralizadas ou com atuação global. A computação em nuvem ainda oferece escalabilidade, redundância e segurança, características que sustentam a continuidade do negócio e a integridade da informação em ambientes sensíveis (Rezende, 2021).

Dessa forma, os sistemas de informação integrados tornam-se não apenas instrumentos de automação de tarefas operacionais, mas motores de transformação estratégica. A prevenção à fraude, neste contexto, deixa de ser uma ação pontual e reativa para se tornar um processo contínuo, inteligente e orientado por dados. Essa transformação só é possível quando há sinergia entre tecnologia, pessoas e processos, refletindo um modelo de governança moderna voltada à integridade corporativa e à geração de valor sustentável.

Em síntese, a integração de dados e a adoção de sistemas de apoio à decisão possibilitam uma gestão mais transparente, eficiente e resiliente, promovendo a antecipação de riscos, o aprimoramento dos controles internos e o fortalecimento da cultura de prevenção. Tais iniciativas representam um avanço substancial na luta contra fraudes empresariais e posicionam as organizações de maneira mais segura e competitiva diante dos desafios do ambiente corporativo contemporâneo.

4 PROCEDIMENTOS METODOLÓGICOS

A presente pesquisa adotou uma abordagem qualitativa, de natureza exploratória, com base em revisão de literatura, pesquisa bibliográfica e elementos de observação empírica informal oriunda da vivência profissional. Conforme Denzin e Lincoln (2006, p. 17), a pesquisa qualitativa "envolve um conjunto de práticas interpretativas que tornam o mundo visível", sendo adequada para analisar fenômenos complexos relacionados à gestão da informação, uso de tecnologias e prevenção de fraudes corporativas.

A pesquisa exploratória permitiu desenvolver uma compreensão inicial sobre os aspectos teóricos e práticos do tema, bem como formular hipóteses interpretativas para sustentar o desenvolvimento da análise. Segundo Cervo e Silva (2006, p. 61), a pesquisa exploratória é utilizada "especialmente quando o tema é pouco explorado ou quando se quer desenvolver novas abordagens sobre ele", o que se aplica ao estudo da integração tecnológica em sistemas antifraude no contexto contemporâneo. Para dar suporte à fundamentação teórica, recorreu-se à revisão de literatura, que teve como finalidade tanto a construção de uma contextualização conceitual quanto a análise das possibilidades interpretativas fornecidas pelas obras consultadas. De acordo com Mazzotti (2014, p. 6), "a revisão de literatura ou revisão bibliográfica tem como objetivo construir uma base de conhecimento a partir da produção científica já existente sobre determinado tema".

A pesquisa bibliográfica foi construída com base em publicações científicas que abordam temas como assimetria de informação, economia de rede, capitalismo de vigilância, sistemas de informação, fraudes corporativas, ferramentas de Inteligência Artificial e tecnologias da informação aplicadas à gestão de risco. Foram consultadas diversas fontes, incluindo livros, artigos científicos, dissertações, periódicos acadêmicos e documentos eletrônicos, disponíveis em bases como Brapci, Google Scholar, Web of Science, Scopus, BDTD e OasisBR. Esses materiais forneceram os fundamentos teóricos necessários para compreender a influência das tecnologias na prevenção e no combate às fraudes.

Complementarmente, a pesquisa contou com uma dimensão empírica indireta, fundamentada na experiência adquirida ao longo da graduação e na atuação profissional em grandes empresas do setor de tecnologia. Essa vivência prática permitiu observar a aplicação de sistemas de informação e a valorização dos dados como ativos estratégicos, enriquecendo a interpretação das fontes bibliográficas com elementos observacionais oriundos do cotidiano organizacional.

A abordagem qualitativa norteou a análise das informações, uma vez que o estudo não

se propôs à quantificação de dados, mas sim à compreensão e interpretação crítica do fenômeno investigado. Como afirma Flick (2009, p. 15), a pesquisa qualitativa "é centrada no entendimento dos significados e não na quantificação dos dados, sendo útil para explorar processos sociais e tecnológicos". A análise das fontes foi realizada a partir de fichamentos temáticos e sínteses interpretativas que permitiram o cruzamento de dados e a elaboração de inferências coerentes com os objetivos da pesquisa.

Foram adotados critérios de inclusão para garantir a pertinência dos materiais analisados. Os trabalhos selecionados apresentavam, em seus títulos, resumos ou palavras-chave, temas relacionados à avaliação de desempenho, sistemas de informação, gestão de risco, fraudes corporativas e impactos tecnológicos. Também foram incluídas produções teóricas voltadas às transformações socioeconômicas que influenciam o mercado global e estudos experimentais que validam abordagens tecnológicas aplicadas à prevenção de fraudes. Por outro lado, foram excluídos os trabalhos que apresentavam fontes não confiáveis, artigos incompletos ou infundados, bem como estudos sem descrição metodológica adequada.

Essa organização metodológica foi fundamental para conferir transparência, coerência e legitimidade científica à investigação. Como destacam Lakatos e Marconi (2003, p. 186), "a clareza na exposição dos procedimentos metodológicos é fundamental para garantir a legitimidade da pesquisa científica". Assim, a integração entre teoria, prática e metodologia permitiu construir um estudo consistente, voltado à compreensão crítica das tecnologias da informação como instrumentos de prevenção de fraudes em ambientes corporativos.

Com a finalidade de alcançar os objetivos específicos, algumas peculiaridades foram executadas. Em primeiro lugar, para avaliar os tipos e as características dos sistemas de informação atualmente utilizados na detecção de fraudes financeiras, a pesquisa buscou uma revisão bibliográfica especializada, a partir de livros, artigos científicos, relatórios técnicos e bases de dados acadêmicas, que enfatizassem as tecnologias mais frequentemente utilizadas no combate a fraudes no setor financeiro.

Essa etapa permitiu o levantamento de exemplos como sistemas de auditoria contínua e softwares de monitoramento com módulos antifraude. A seguir, os sistemas identificados foram classificados conforme sua natureza funcional, sendo agrupados segundo critérios como o tipo de abordagem (preventiva, reativa ou híbrida), a origem dos dados utilizados (transacionais, comportamentais ou biométricos) e os métodos empregados para detecção (como regras de negócios, análise estatística ou algoritmos de *machine learning*). Finalmente, realiza-se uma caracterização técnica e funcional dos sistemas, na qual se descrevem suas principais funcionalidades, as arquiteturas adotadas, a compatibilidade com outros sistemas

corporativos e a forma como se integram aos processos organizacionais das instituições financeiras.

Com o objetivo de examinar estudos de caso de instituições que implementaram soluções baseadas em inteligência artificial (IA) para prevenção de fraudes, são selecionadas instituições representativas do setor, que tenham adotado estratégias tecnológicas inovadoras com uso de IA. Essa seleção se baseia na análise de publicações científicas, relatórios corporativos e documentos oriundos de bases de dados de boas práticas. A etapa seguinte consiste na coleta de dados sobre os casos, reunindo informações específicas sobre o tipo de inteligência artificial adotada, as ferramentas e plataformas utilizadas, o escopo da aplicação (se em toda a organização ou apenas em áreas específicas) e o volume de dados tratados. Esses dados foram analisados a partir de seu impacto prático, levando em consideração indicadores como a redução de perdas financeiras, a melhoria na taxa de detecção de fraudes e o desempenho de tempo de resposta.

Para comparar a eficiência dos sistemas tradicionais com os sistemas baseados em IA, a pesquisa definiu, inicialmente, um conjunto de métricas comparativas, como a taxa de falsos positivos e negativos, o tempo médio de resposta frente a uma ameaça e a eficácia na redução de fraudes consumadas. Em seguida, realizou-se uma coleta de dados secundários, valendo-se de estudos de *benchmarking*, relatórios de auditorias e dados divulgados por entidades especializadas. Esses dados foram submetidos a uma análise comparativa, que envolveu abordagens qualitativas (ex: entrevistas e análises documentais) e quantitativas (quando houve dados estatísticos disponíveis), com o objetivo de verificar o desempenho relativo das soluções tradicionais, geralmente baseadas em regras fixas e estatísticas descritivas, frente às tecnologias mais recentes que empregam aprendizado de máquina e redes neurais profundas. Ao final, elaborou-se uma síntese crítica dos resultados, destacando os pontos fortes, limitações e os contextos mais apropriados para cada tipo de solução antifraude.

Por fim, para investigar os desafios e limitações enfrentados pelas entidades na implementação de tecnologias avançadas para prevenção de fraudes, o estudo promoveu um levantamento teórico e prático sobre os principais obstáculos relatados na literatura. Entre os aspectos identificados estão os altos custos de aquisição e manutenção de sistemas, a escassez de profissionais capacitados para operar soluções baseadas em IA, barreiras culturais dentro das instituições e questões éticas e legais envolvendo o uso de dados sensíveis. Essa análise é complementada por um mapeamento das dificuldades observadas nos estudos de caso já analisados, permitindo compreender os entraves enfrentados em contextos reais de aplicação. Realizaram-se entrevistas com especialistas da área ou gestores envolvidos na implementação

de tais tecnologias, a fim de aprofundar o entendimento das barreiras enfrentadas. Por fim, os desafios foram organizados e classificados em categorias temáticas, como tecnológicos, humanos, organizacionais e regulatórios, e são propostas estratégias de mitigação com base nas melhores práticas descritas na literatura científica e técnica da área.

Quadro 1. Alinhamento entre objetivos e etapas da pesquisa

Objetivo Específico	Etapas da Pesquisa Associadas
Investigar na literatura científica as características dos sistemas de informação utilizados na detecção de fraudes financeiras	- Revisão bibliográfica especializada - Classificação dos sistemas - Caracterização técnica e funcional
Examinar estudos de caso de instituições que implementaram soluções baseadas em inteligência artificial (IA) para prevenção de fraudes	- Seleção de estudos de caso - Coleta de dados - Análise do impacto
Comparar a eficiência entre sistemas tradicionais e dos sistemas baseados em (IA) em termos de precisão, tempo de resposta e redução de fraudes	- Definição de métricas comparativas - Coleta de dados secundários - Análise comparativa - Síntese dos resultados

Fonte: Elaborada pela autora (2025)

A estrutura metodológica foi elaborada para assegurar que cada objetivo específico fosse examinado de forma adequada, com técnicas que correspondessem à natureza do problema e aos dados disponíveis. O fluxo de etapas criado garante a consistência lógica entre o problema de pesquisa, os métodos utilizados e os resultados esperados. As análises foram desenvolvidas com base em dados secundários extraídos de publicações especializadas, documentos institucionais e estudos de caso disponíveis na literatura, o que permitiu uma abordagem comparativa mais ampla. Desta forma, essas etapas contribuem para alcançar o objetivo geral da pesquisa: investigar a eficácia dos sistemas de informação modernos na detecção precoce e prevenção de fraudes financeiras, comparando-os com os sistemas tradicionais, a partir de uma análise crítica e comparativa.

5 ANÁLISE E DISCUSSÃO DOS DADOS

A análise revelou padrões recorrentes que evidenciam a eficácia da aplicação integrada de tecnologias como Inteligência Artificial (IA), Machine Learning (ML), Big Data, blockchain e análise preditiva. Notou-se que instituições que utilizam IA e ML apresentaram redução significativa nas taxas de falsos positivos, conforme relatado por Rezende (2021) e Costa e Batista (2023). Em determinados cenários, sistemas baseados em ML alcançaram grande margem de precisão na classificação de transações suspeitas, aumentando a eficácia das auditorias internas e diminuindo o tempo de resposta a fraudes. A eficiência na filtragem de transações também repercute diretamente nos custos operacionais e na satisfação dos clientes, uma vez que reduz o número de bloqueios indevidos e melhora a experiência de uso.

Adicionalmente, estudos de campo demonstraram que o uso da IA permite um monitoramento contínuo e em tempo real, possibilitando que desvios sejam identificados instantaneamente. Isso é especialmente relevante em ambientes de alta transacionalidade, como os mercados financeiros e varejistas. A IA consegue aprender padrões de comportamento com base em históricos de dados, ajustando os modelos preditivos de forma dinâmica, o que amplia sua acurácia ao longo do tempo e reduz significativamente as perdas financeiras associadas a fraudes.

A aplicação de Big Data mostrou-se eficaz na ampliação do escopo de análise, possibilitando o cruzamento de dados de diversas fontes internas e externas. Com isso, empresas conseguem detectar padrões atípicos com maior antecedência, como indicam Fernandes e Nascimento (2022). O Big Data permite que sistemas de fraude operem com grandes volumes de informação não estruturada, como dados de redes sociais, histórico de navegação e interações com canais digitais, agregando mais profundidade à análise preditiva. Os estudos demonstraram que, após a adoção dessas tecnologias, muitas empresas conseguem reduzir ocorrências de fraudes internas ligadas a processos de reembolso e contas a pagar.

Outro ponto relevante nos dados analisados é a integração dos sistemas de Big Data com modelos estatísticos avançados, o que proporciona análises em tempo quase real. A capacidade de rastrear anomalias antes que estas causem danos sistêmicos proporciona uma vantagem competitiva significativa. Empresas que adotaram esse tipo de abordagem relataram não apenas redução nas perdas, mas também uma melhora na imagem institucional e na confiança de investidores e clientes.

Em relação ao uso do blockchain, evidências empíricas apontam ganhos substanciais em transparência e confiabilidade de registros, especialmente em ambientes de cadeia de

suprimentos e contratos digitais. Moura e Oliveira (2020) destacam que o blockchain contribui para a rastreabilidade de operações e a prevenção de manipulações contábeis. Sua estrutura descentralizada impede alterações não autorizadas e facilita auditorias, conferindo mais segurança às transações comerciais. O registro imutável das operações permite que inconsistências sejam detectadas com mais facilidade, o que aumenta o grau de confiança no sistema.

A aplicabilidade do blockchain também foi verificada em sistemas de autenticação de identidade digital, diminuindo fraudes associadas ao roubo de identidade. Organizações que incorporaram esse recurso conseguiram eliminar redundâncias nos processos de verificação, reduzir o tempo de onboarding de clientes e melhorar a conformidade com exigências regulatórias como o LGPD e o GDPR.

A auditoria automatizada e o monitoramento em tempo real também se mostraram centrais na gestão de riscos. Estudos de Souza e Campos (2021) evidenciam que sistemas de detecção de anomalias reduziram em até 60% o tempo de resposta às irregularidades, enquanto empresas que implementaram dashboards analíticos relataram maior capacidade de antecipação de riscos e de alocação inteligente de recursos de compliance. A auditoria contínua, baseada em dados transacionais, permite uma avaliação permanente das operações, eliminando lacunas entre as auditorias periódicas tradicionais.

O uso de *dashboards* inteligentes para visualização de indicadores de risco também foi destacado como uma ferramenta de apoio estratégico para a alta gestão. Tais *dashboards* são capazes de gerar alertas personalizados, priorizar investigações e apresentar relatórios em formatos intuitivos, o que facilita a tomada de decisões rápidas e fundamentadas.

Por fim, a integração de dados intersetoriais, conforme analisado por Moraes e Costa (2018) e Gonçalves e Lima (2017), revelou ser fator determinante para o sucesso das iniciativas antifraude. Empresas com sistemas integrados tendem a ter maior agilidade na tomada de decisão e redução na fragmentação da informação, criando um ambiente corporativo mais responsivo e resiliente. A interoperabilidade entre departamentos como compliance, auditoria, jurídico e financeiro é essencial para garantir que as medidas de prevenção sejam eficazes e sustentáveis a longo prazo.

A análise dos dados evidencia que a combinação sinérgica entre tecnologias de ponta e uma abordagem organizacional integrada constitui o alicerce da luta contra as fraudes financeiras. Os resultados observados demonstram que os SI, quando bem implementados, não apenas reduzem os riscos como promovem um novo patamar de excelência na governança corporativa.

A análise dos dados corrobora a literatura revisada, confirmando que a adoção de Sistemas de Informação não apenas fortalece os controles internos como também transforma a cultura organizacional em direção à transparência, à ética e à prevenção. A transição de sistemas tradicionais para soluções inteligentes reflete uma mudança de paradigma que alinha tecnologia à estratégia empresarial.

Essa nova centralidade dos SI é resultado da sua capacidade de antecipação. Sistemas que antes apenas relatavam dados passados agora preveem comportamentos futuros, baseando-se em padrões estatísticos, históricos e contextuais. Isso transforma o papel da gestão de risco de uma abordagem reativa para uma postura preditiva e proativa. Além disso, essa proatividade contribui para o fortalecimento da reputação institucional, reduzindo passivos financeiros e jurídicos decorrentes de fraudes não detectadas a tempo.

A discussão também evidencia que o sucesso dessas iniciativas está condicionado à capacidade de integração entre tecnologias, dados e cultura organizacional. Como apontado por Barros e Souza (2023), tecnologia sem governança ou capacitação humana reduz seu potencial. A implementação eficaz dos SI requer não apenas infraestrutura tecnológica, mas também liderança institucional comprometida, treinamento continuado e cultura voltada à ética. A governança de dados se torna, portanto, peça-chave para garantir que os sistemas operem com segurança, precisão e em conformidade com os princípios legais e morais.

A cultura organizacional assume um papel protagonista na efetividade dos SI antifraude. Organizações que cultivam valores éticos e promovem a transparência tendem a obter melhores resultados com a adoção de novas tecnologias. O envolvimento ativo da alta gestão é crucial, pois permite alinhar os objetivos estratégicos aos esforços de prevenção, garantindo a alocação de recursos e o engajamento das equipes.

Além disso, destaca-se o papel da auditoria automatizada, que transforma a função tradicional da auditoria de reativa para preventiva, conforme argumentam Almeida e Ribeiro (2022). Essa mudança fortalece o papel estratégico dos auditores e amplia a abrangência do controle organizacional. Os auditores passam a atuar como analistas de risco, interpretando dados em tempo real e propondo intervenções imediatas. A integração da auditoria contínua aos fluxos operacionais também reduz os custos associados a fraudes e amplia a efetividade das medidas de compliance.

Outro ponto relevante discutido é a eficiência proporcionada pela automação na conformidade regulatória. Sistemas de informação modernos são capazes de mapear exigências legais, monitorar o cumprimento de normas e gerar relatórios automatizados para órgãos de fiscalização. Isso não apenas reduz o risco de penalidades, mas também libera recursos

humanos para atividades mais estratégicas.

A discussão também permite refletir sobre os desafios enfrentados na implementação dos SI antifraude. Entre eles, destacam-se a resistência à mudança, a escassez de profissionais capacitados e os altos custos iniciais de implantação. Superar esses obstáculos exige uma estratégia clara de transformação digital, comunicação eficaz com os colaboradores e investimento em capacitação contínua. A adoção de tecnologias emergentes também deve ser acompanhada de políticas robustas de proteção de dados e segurança da informação, conforme previsto na legislação brasileira.

Assim, os dados confirmam a premissa teórica de que os Sistemas de Informação, quando bem integrados e apoiados por uma cultura de governança, representam um dos pilares mais eficazes para a prevenção de fraudes financeiras no ambiente corporativo contemporâneo. A convergência entre tecnologia, gestão e cultura ética se mostra como a base sólida para uma atuação empresarial segura, eficiente e sustentável em um cenário cada vez mais digital e vulnerável a ameaças.

Quadro 2. Comparativo dos Sistemas IA vs Sistemas Tradicionais

SISTEMAS	CATEGORIA	NÍVEL DE PRECISÃO	TEMPO DE RESPOSTA	ÍNDICE DE REDUÇÃO DE FRAUDES
Baseado em IA (Inteligência Artificial e Machine Learning)	Baseado em IA	Muito alta (precisão aprimorada com IA e aprendizado de máquina, identificando transações suspeitas com grande precisão)	Muito baixo (monitoramento contínuo em tempo real, ajustando os modelos conforme novos dados, resultando em respostas quase instantâneas)	Muito significativo (redução de fraudes em tempo real devido à análise preditiva e capacidade de aprender padrões de comportamento, reduzindo falsos positivos e aumentando a detecção de fraudes em tempo real)
Sistema "simples" (Tradicional)	Sistema "simples"	Média (baseado em regras fixas e modelos estáticos, o que resulta em uma	Alto (depende de processos manuais e auditorias periódicas, o que leva a	Baixo (o sistema tem maior risco de fraudar transações devido à

		capacidade limitada de identificar novas formas de fraude)	tempos de resposta mais longos, afetando a agilidade na detecção)	dependência de regras predefinidas e monitoramento reativo, o que aumenta a chance de falhas no reconhecimento de atividades suspeitas)
Baseado em IA (Big Data e Blockchain)	Baseado em IA	Muito alta (uso de Big Data para cruzamento de dados internos e externos, com IA ajustando continuamente os modelos para melhorar a precisão, e blockchain proporcionando uma rastreabilidade imutável das transações)	Extremamente baixo (tempo de resposta quase imediato devido ao processamento paralelo de grandes volumes de dados e à utilização de blockchain para registros imutáveis)	Altíssimo (Big Data e blockchain permitem uma rastreabilidade total, reduzindo fraudes internas e externas, especialmente em sistemas financeiros e de cadeia de suprimentos, além de fornecer segurança adicional em transações digitais)

Fonte: Elaborada pela autora (Dados da pesquisa 2025)

A análise dos dados reforça que a implementação de IA e aprendizado de máquina nos sistemas de informação aumenta consideravelmente a precisão, pois esses sistemas aprendem com os dados, adaptando-se a novos padrões e reduzindo os falsos positivos, o que resulta em uma maior detecção precisa de fraudes. Em contraposição, os sistemas tradicionais, embasados em regras rígidas, são mais restritos e podem cometer erros na detecção de transações fraudulentas, especialmente em virtude de novas práticas fraudulentas que surgiram.

No que diz respeito ao tempo de resposta, sistemas baseados em Inteligência Artificial têm uma resposta rápida e quase em tempo real e podem detectar rapidamente desvios e eventos problemáticos em transações, enquanto sistemas antigos, que dependem de intervenções humanas e auditorias periódicas, possuem tempos de resposta mais prolongados e, assim, se tornam ineficazes para a agilidade na tomada de decisão em situações indesejadas.

Além disso, sistemas modernos, utilizando IA, aprendizado de máquina e Big Data, permitem um monitoramento contínuo que ajuda a detectar fraudes antes que ocorram, reduzindo assim perdas financeiras e impactos negativos para as empresas. Já os sistemas tradicionais, ao dependerem de análise manual e carecerem de modelos preditivos, são mais suscetíveis a fraudes não identificadas até que seja tarde demais.

Em síntese, os modernos, com IA, aprendizado de máquina, Big Data e blockchain, superam os tradicionais, gerando maior precisão, respostas mais rápidas e maior eficiência na detecção, e prevenção de fraudes financeiras. Os tradicionais , baseados em regras fixas e auditorias manuais, mostram limitações que podem interferir na agilidade e na eficácia na detecção e prevenção das fraudes.

6 CONSIDERAÇÕES FINAIS

A presente pesquisa teve como objetivo central investigar a eficácia dos sistemas de informação modernos na detecção precoce e prevenção de fraudes financeiras, comparando-os com os sistemas tradicionais. Para tanto, adotou-se uma abordagem qualitativa e exploratória, sustentada em revisão bibliográfica criteriosa e enriquecida com observações empíricas. O conjunto de dados teóricos e práticos permitiu compreender de maneira aprofundada os mecanismos, desafios e potencialidades associados ao uso das tecnologias da informação no combate a práticas fraudulentas no ambiente corporativo contemporâneo.

Ao longo do trabalho, ficou evidente que a fraude financeira é um fenômeno complexo, multicausal e em constante transformação. As práticas fraudulentas, embora historicamente associadas a condutas individuais e pontuais, passaram a assumir contornos estruturais, explorando vulnerabilidades sistêmicas, falhas nos controles internos e assimetrias informacionais que permeiam as organizações. Esse cenário exige das instituições uma postura proativa, integrativa e tecnologicamente embasada na gestão dos riscos financeiros e na proteção de seus ativos.

A pesquisa demonstrou que os sistemas de informação desempenham papel decisivo nesse processo. Mais do que meras ferramentas de suporte operacional, os SI modernos configuram-se como instrumentos estratégicos capazes de transformar a maneira como as organizações captam, processam, analisam e utilizam a informação para detectar irregularidades e evitar prejuízos. O cruzamento automatizado de dados, a geração de alertas em tempo real e a integração de fontes internas e externas proporcionam uma nova abordagem à gestão de riscos: mais ágil, precisa, preventiva e adaptativa.

A análise revelou, por meio de múltiplas fontes, que tecnologias como a inteligência artificial e o aprendizado de máquina são capazes de identificar padrões de comportamento fraudulentos com alta acurácia, superando com frequência os modelos tradicionais baseados em regras fixas. A capacidade dessas tecnologias de aprender com grandes volumes de dados e ajustar dinamicamente seus parâmetros de classificação representa um avanço notável, pois amplia significativamente a efetividade dos mecanismos de controle. Além disso, sua aplicação em ambientes de alta transacionalidade, como o setor financeiro, mostrou-se promissora na redução de falsos positivos e no aumento da confiabilidade das investigações internas.

O uso de big data, por sua vez, reforça a profundidade e a abrangência das análises, permitindo a integração de múltiplas fontes de dados para formar um panorama mais completo das operações corporativas. Ao processar informações oriundas de sistemas internos, mídias

sociais, sensores IoT e canais digitais, as organizações conseguem visualizar interações e movimentos que antes passavam despercebidos. Essa capacidade de rastreamento antecipado proporciona vantagem competitiva, pois permite que a organização antecipe riscos, reforce controles e preserve sua reputação no mercado.

O blockchain, tecnologia emergente analisada ao longo da pesquisa, destacou-se por seu potencial de garantir a imutabilidade, a rastreabilidade e a descentralização dos registros digitais. Sua aplicação em contratos inteligentes, autenticação de identidade e rastreamento de cadeias produtivas tem se consolidado como um mecanismo eficaz de transparência e verificação de autenticidade. A pesquisa revelou que a incorporação do blockchain aos processos organizacionais contribui para a mitigação de fraudes contábeis e operacionais, além de reduzir significativamente as possibilidades de adulteração de dados.

Ainda no campo das ferramentas tecnológicas, a auditoria automatizada e os sistemas de monitoramento contínuo demonstraram ser alternativas robustas aos modelos tradicionais de controle, que operavam de forma periódica e reativa. A automatização da auditoria possibilita o acompanhamento constante das operações, reduz o tempo de resposta às irregularidades, aumenta a abrangência das análises e libera os profissionais de auditoria para atividades mais estratégicas. Nesse contexto, dashboards analíticos, algoritmos de detecção de anomalias e trilhas de auditoria digitais configuram um novo ecossistema de prevenção à fraude, mais responsivo, inteligente e alinhado com os princípios da governança corporativa contemporânea.

A integração de dados intersetoriais, viabilizada pelos sistemas ERP e pelas plataformas de Business Intelligence, foi outro ponto destacado pela análise. A capacidade de cruzar informações de setores como compras, financeiro, RH, logística e jurídico, em tempo real, permite identificar falhas estruturais de segregação de funções, detectar transações atípicas e promover ações corretivas imediatas. Essa integração rompe com o modelo departamentalizado e fragmentado, conferindo maior fluidez à comunicação organizacional e promovendo um ambiente mais seguro e transparente.

A pesquisa também apontou os principais desafios enfrentados pelas organizações na implementação dessas tecnologias. Entre eles, destacam-se os altos custos iniciais de aquisição e manutenção, a escassez de mão de obra especializada, as barreiras culturais à inovação e as preocupações éticas e legais quanto ao uso de dados sensíveis. A superação desses obstáculos demanda não apenas investimentos financeiros, mas também a promoção de uma cultura organizacional orientada à ética, à transparência e ao uso responsável da tecnologia. É necessário criar um ambiente institucional que valorize a integridade da informação e a formação contínua de seus colaboradores, pois, como demonstrado, a fraude não é apenas um

problema técnico, mas também cultural e comportamental.

Nesse aspecto, o trabalho evidenciou que o fator humano continua sendo um ponto sensível na luta contra fraudes. Mesmo diante de sistemas sofisticados e automatizados, a confiança indevida, a falta de capacitação e a cultura permissiva podem comprometer a eficácia dos controles e abrir brechas para irregularidades. Por isso, os investimentos em tecnologia devem ser acompanhados de ações formativas, treinamentos éticos, canais de denúncia seguros e políticas internas claras sobre a manipulação e o uso da informação. A construção de uma cultura organizacional pautada na integridade é, portanto, condição indispensável para o sucesso de qualquer sistema antifraude.

Do ponto de vista metodológico, a adoção de uma abordagem qualitativa permitiu compreender em profundidade os aspectos subjetivos e institucionais que envolvem a prevenção de fraudes. A utilização da revisão bibliográfica sistemática, aliada à análise crítica de estudos de caso e à experiência prática da autora, possibilitou a construção de uma narrativa analítica coerente, sensível às particularidades do tema e capaz de oferecer contribuições teóricas e aplicadas. A opção por não quantificar os dados reforça o caráter interpretativo da pesquisa, que privilegia o entendimento dos processos sociais e organizacionais em detrimento de generalizações estatísticas.

Do ponto de vista prático, os resultados obtidos oferecem subsídios relevantes para gestores, auditores, profissionais da área de tecnologia e estudiosos interessados na temática. A pesquisa sugere que a prevenção de fraudes deve ser tratada como uma dimensão estratégica da gestão organizacional, exigindo políticas estruturadas, investimentos contínuos e acompanhamento sistemático. Mais do que um problema a ser resolvido pontualmente, a fraude representa um risco sistêmico que precisa ser enfrentado de forma integrada, envolvendo tecnologia, processos e pessoas.

Além disso, destaca-se que a prevenção à fraude não deve ser encarada como um custo adicional, mas como um investimento estratégico na perenidade da organização. Empresas que adotam sistemas eficazes de controle interno, auditoria automatizada e governança de dados não apenas reduzem perdas financeiras, mas também fortalecem sua reputação no mercado, atraem investidores e consolidam relações de confiança com clientes e parceiros. Em um mundo cada vez mais interconectado e sensível à integridade corporativa, esses diferenciais são cruciais para a sustentabilidade dos negócios.

Diante de todas essas observações, pode-se afirmar que a hipótese central da pesquisa, a de que sistemas de informação modernos, especialmente os baseados em inteligência artificial, são mais eficazes na detecção e prevenção de fraudes financeiras do que os métodos

tradicionais, foi confirmada. Os dados teóricos e empíricos reunidos ao longo do trabalho demonstraram que as tecnologias emergentes oferecem não apenas maior precisão e agilidade, mas também permitem a antecipação de riscos e a construção de uma cultura organizacional mais robusta e comprometida com a legalidade.

Como sugestões para trabalhos futuros, recomenda-se aprofundar as análises empíricas, por meio de estudos de campo, entrevistas com especialistas e análise de dados quantitativos relacionados à implementação de SI antifraude em diferentes setores da economia. Também seria interessante explorar mais detalhadamente as implicações éticas e jurídicas da adoção de tecnologias de vigilância algorítmica no ambiente corporativo, especialmente em contextos regulatórios como a LGPD (Lei Geral de Proteção de Dados) e o GDPR europeu.

Por fim, conclui-se que o enfrentamento das fraudes financeiras no ambiente corporativo do século XXI requer uma abordagem multidisciplinar, inovadora e eticamente comprometida. Os sistemas de informação, nesse contexto, representam não apenas ferramentas operacionais, mas verdadeiros aliados estratégicos na construção de organizações mais transparentes, resilientes e sustentáveis. Ao conjugar tecnologia de ponta com uma cultura organizacional voltada à integridade, as empresas estarão mais preparadas para enfrentar os desafios do futuro e garantir a confiança necessária à sua atuação no mercado.

REFERÊNCIAS

ALMEIDA, J. P.; RIBEIRO, V. L. Auditoria contínua baseada em dados: uma abordagem estratégica para prevenção de fraudes. **Revista Brasileira de Contabilidade**, v. 35, n. 140, p. 78-95, 2022.

BARROS, M. L.; SOUZA, V. R. Cultura organizacional e segurança da informação: desafios contemporâneos. **Revista de Administração Contemporânea**, v. 27, n. 1, p. 215-233, 2023.

BOLDT, R. Uma análise crítica do triângulo da fraude de Donald Cressey: limitações e aplicações no contexto dos crimes corporativos. **Boletim Ibccrim**. ano 33, n. 388, mar. 2025.

BOLAÑO, C. R. S. **Indústria cultural, informação e capitalismo**. São Paulo: Hucitec, 2000.

CARVALHO, M. P.; ANDRADE, T. C. **Tecnologia da informação e auditoria contínua**: um estudo em empresas brasileiras. Belo Horizonte: D'Plácido, 2019.

CERVO, A. L.; SILVA, A. B. **Metodologia científica**. 6. ed. São Paulo: Pearson Prentice Hall, 2006.

CHOO, C. W. **A organização do conhecimento: como as organizações usam a informação para criar significado, construir conhecimento e tomar decisões**. São Paulo: SENAC, 2003.

COSENZA, J. P.; GRATERON, L.S. **Contabilidade criativa**: uma perspectiva de abordagem. São Paulo: Atlas, 2003.

COSTA, R. F.; BATISTA, M. A. Governança de dados e ética empresarial: o papel da auditoria digital. **Revista de Governança Corporativa**, v. 10, n. 2, p. 33-49, 2023.

DAVENPORT, T. H. **Missão crítica**: obtendo vantagem competitiva com os ativos de informação. São Paulo: Makron Books, 1998.

DAVENPORT, T. H.; PRUSAK, L. **Conhecimento empresarial**: como as organizações gerenciam seu capital intelectual. Rio de Janeiro: Campus, 1998.

DENZIN, N. K.; LINCOLN, Y. S. **O planejamento da pesquisa qualitativa**: teorias e abordagens. 2. ed. Porto Alegre: Artmed, 2006.

FERNANDES, P. R.; NASCIMENTO, D. F. Big data e tomada de decisão nas organizações: uma abordagem preditiva. **Revista Gestão e Desenvolvimento**, v. 19, n. 1, p. 88-104, 2022.

FERREIRA, T. M.; TAVARES, D. L. **Gestão da integridade e cultura organizacional**: fundamentos para a prevenção à fraude. São Paulo: Atlas, 2021.

FLICK, U. **Introdução à pesquisa qualitativa**. 3. ed. Porto Alegre: Artmed, 2009.

FREITAS, T. M.; MARTINS, C. E. Controles internos digitais e a resiliência organizacional: uma análise prática. **Revista de Administração e Inovação**, v. 19, n. 1, p. 122-139, 2023.

GONÇALVES, M. F.; LIMA, R. N. **Sistemas de informação gerencial e tomada de decisão estratégica**. São Paulo: Atlas, 2017.

GTAG. **Prevenção e detecção de fraudes em um mundo automatizado**. Global Technology Audit Guide. 2009.

LAKATOS, E. M.; MARCONI, M. A. **Fundamentos de metodologia científica**. 5. ed. São Paulo: Atlas, 2003.

LIMA, R. A. **Fraudes Corporativas**: detecção, prevenção e investigação. São Paulo: Atlas, 2020.

MARCHAND, D. A.; KETTINGER, W.J.; ROLLINS, Jack D. **Gestão da informação**: estratégia, valor e desempenho. São Paulo: Atlas, 2001.

MARTINS, C. S. **Fraudes corporativas**: práticas, consequências e estratégias de prevenção. Rio de Janeiro: Elsevier, 2020.

MATURO, G. R.; CARLETO, N. O impacto da qualidade da informação no processo decisório em uma empresa metalúrgica: um estudo de caso utilizando o fluxograma e o diagrama de Pareto. **Interface Tecnológica**. v. 12, n. 2, 2020.

MAXIMIANO, A. C. A. **Administração**: teoria e prática no contexto brasileiro. 9. ed. São Paulo: Atlas, 2020.

MAZZOTTI, A. J. A. O método nas ciências naturais e nas ciências sociais. In: VOSGERAU, Dilmeire Sant'Anna. **Educação**: pesquisa e conhecimento. Curitiba: Ibpex, 2014.

MEDRADO, F. C. **Indicadores economico-financeiros como red flags de riscos de fraudes ou manipulação contábil**. Dissertação de Mestrado em Ciências Contábeis. Brasília, Universidade de Brasília, 2016.

MEIRELES, C. **Flor de poemas**. 8. ed. Rio de Janeiro: Nova Fronteira, 1983.

MORAES, J. L.; COSTA, H. F. **Tecnologia e prevenção de fraudes financeiras**: uma abordagem aplicada à era digital. Curitiba: Appris, 2018.

MOREIRA, C. H. **Segurança da informação e gestão de riscos empresariais**. 2. ed. Rio de Janeiro: FGV Editora, 2019.

MOURA, F. A.; OLIVEIRA, C. R. **Blockchain e criptografia no combate à fraude**: desafios e possibilidades para o setor financeiro. Rio de Janeiro: Elsevier, 2020.

NOGUEIRA, R. A. **Fraude e governança corporativa**: uma análise do triângulo da fraude nas organizações brasileiras. Belo Horizonte: D'Plácido, 2020.

OLIVEIRA, D. P. R. **Sistemas, Organização e Métodos**. 29. ed. São Paulo: Atlas, 2019.

OLIVEIRA, R. P.; MATOS, S. M. Machine Learning aplicado à segurança bancária: estudo de casos. **Revista de Sistemas de Informação**, v. 14, n. 2, p. 125-140, 2022.

OLIVEIRA, R. D.; ALMEIDA, M. H. **Controles internos e o combate à fraude nas empresas brasileiras**. São Paulo: Saraiva Educação, 2021.

PEREIRA, A. P. B. **Ética e confiança nas organizações**: uma abordagem estratégica. Curitiba:

Appris, 2021.

REZENDE, D. A. **Planejamento de sistemas de informação e informática**: guia prático para planejar a TI com foco nos negócios. 5. ed. São Paulo: Atlas, 2021.

SANTOS, R. J. **Controles internos e prevenção à fraude**: fundamentos e práticas. Belo Horizonte: Fórum, 2018.

SARACEVIC, T. Information science. **Journal of the American Society for Information Science**, v. 50, n. 12, p. 1051-1063, 1999.

SILVA, J. L.; ROCHA, A. R. **Gestão de riscos corporativos**: teoria e prática na prevenção de fraudes. São Paulo: Atlas, 2019.

SILVA, J. A.; MOREIRA, R. S. **Fraude corporativa e segurança da informação**: uma abordagem integrada. Florianópolis: EdUFSC, 2018.

SOUZA, K. L.; CAMPOS, L. M. Machine learning e detecção de fraudes: uma revisão de aplicações em auditoria. **Revista Sistemas & Computação**, v. 31, n. 2, p. 91-106, 2021.

SOUZA, M. V. **Fraudes financeiras**: desafios para a auditoria e a contabilidade. Porto Alegre: Bookman, 2019.

WALLER, G. J. **Fraudes corporativas**: prevenção, detecção e investigação. São Paulo: Atlas, 2003.