UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
ESCOLA DE ADMINISTRAÇÃO
DEPARTAMENTO DE CIÊNCIAS ADMINISTRATIVAS

FILIPPO MEZZACASA VILLA

# GESTÃO DE E-COMMERCE NO ATUAL CENÁRIO DIGITAL: prevenção de fraudes com cartões de crédito em vendas on-line de passagens rodoviárias

Porto Alegre
2023

FILIPPO MEZZACASA VILLA

# GESTÃO DE E-COMMERCE NO ATUAL CENÁRIO DIGITAL: prevenção de fraudes com cartões de crédito em vendas on-line de passagens rodoviárias

Trabalho de conclusão do curso de graduação apresentado ao Departamento de Ciências Administrativas da Universidade Federal do Rio Grande do Sul, orientado pelo Professor Doutor Guilherme Kirch.

Porto Alegre
2023

**FOLHA DE APROVAÇÃO**

Conceito Final:

Aprovado em: Porto Alegre, _____ de _____ de 2023.

BANCA EXAMINADORA:

_____

Orientador: Prof. Dr. Guilherme Kirch

Universidade Federal do Rio Grande do Sul - UFRGS

_____

Prof. Dr.

Universidade

_____

Prof. Dr.

Universidade

## RESUMO

O presente estudo aborda a prática de fraude eletrônica com cartão de crédito no site de uma empresa de transporte rodoviário de passageiros, desde a apresentação da forma como ocorrem em seu contexto, dado o crescimento expressivo das transações eletrônicas no mercado de e-commerce em geral e o avanço da prática de fraude, até o entendimento da representatividade das perdas na empresa do estudo tendo como objetivo conhecer a atual ferramenta antifraude da empresa e avaliar as soluções disponíveis no mercado para combate à fraude tomando como parâmetro o desempenho econômico-financeiro do investimento.

As principais análises realizadas estão baseadas em teorias econômicas-financeiras com abordagens que sustentam a análise das alternativas de investimento sugeridos durante o estudo. São avaliadas alternativas que comportam diferentes métodos e tecnologias, cada qual fornecendo uma assertividade e índice de prevenção agregado à solução, respondendo a uma estimativa de retorno do investimento realizado, dada relação de custo-benefício.

Os resultados encontrados de soluções disponíveis no mercado demonstram, em sua totalidade, ampliação da segurança nas transações eletrônicas no site da empresa, acrescentando tecnologia e etapas que contam com a interação e validação de segurança concedida pelo usuário, demonstrando a preocupação com a verificação e uso dos dados financeiros. Por fim, é identificada a alternativa que possui o melhor desempenho econômico-financeiro embasada através dos resultados apresentados.



**Palavras-chave:** fraude eletrônica; cartão de crédito; e-commerce; antifraude; avaliação de investimento

## ABSTRACT

The present study addresses the practice of electronic credit card fraud on the website of a road passenger transport company, from the presentation of how they occur in their context, given the significant growth of electronic transactions in the e-commerce market in general and the advance of the practice of fraud, until the understanding of the representativeness of the losses in the company of the study, having as objective to know the current anti-fraud tool of the company and to evaluate the solutions available in the market to combat the fraud taking as parameter the one that presents the best performance economic-financial.

The main analyzes carried out are based on economic-financial theories with approaches that support the analysis of investment alternatives suggested during the study. Alternatives that include different methods and technologies are evaluated, each one providing an assertiveness and prevention index added to the solution, responding to an estimated return on investment, given the cost-benefit ratio.

The results found from solutions available on the market demonstrate, in their entirety, increased security in electronic transactions on the company's website, adding technology and steps that rely on the interaction and validation of security granted by the user, demonstrating the concern with the verification and use of financial data. Finally, the alternative that has the best economic and financial performance is mentioned based on the financial results presented.



**Keywords:** electronic fraud; credit card; e-commerce; fraud detection; investment evaluation

# LISTA DE ILUSTRAÇÕES

## Figuras



## Gráficos

## LISTA DE TABELAS

## LISTA DE SIGLAS

**API - APPLICATION PROGRAMMING INTERFACE**

**B2C – BUSINESS TO CONSUMER**

**CE – COMÉRCIO ELETRÔNICO**

**EDI - ELETRONIC DATA INTERCHANGE**

**PIN – PERSONAL IDENTIFICATION NUMBER**

**PJ – PESSOA JURÍDICA**

**SMS – SHORT MESSAGE SERVICE**

**TEF - TRANSFERÊNCIA ELETRÔNICA DE FUNDOS**

**TLS - TRANSPORT LAYER SECURITY**

**VPL – VALOR PRESENTE LÍQUIDO**

# SUMÁRIO

## 1. INTRODUÇÃO

O mercado de compra de passagens rodoviárias vem passando por reestruturações de canais na última década devido ao crescimento do e-commerce e a demanda gerada por este possibilitando a pesquisa de diferentes sites que ofertam as passagens rodoviárias facilitando a aquisição do bilhete do serviço sem qualquer deslocamento do usuário. Esse cenário contribui com as negociações e expande as possibilidades de comercializar de maneira prática para um público habituado, hoje, com as aquisições virtuais. “Por meio do comércio eletrônico, os clientes podem projetar, solicitar produtos e serviços e pagar por eles sem precisar sair de casa (..)” (KOTLER, 2006, p. 16).

A demanda do mercado virtual teve avanço no Brasil alinhado com o período de popularização dos smartphones no país conforme demonstram as conclusões de estudo publicado na *Brazilian Journals* (SANTOS, 2018). Nesse caso, para as passagens rodoviárias, extingue a necessidade dos clientes se direcionarem ao ponto de venda mais próximo com dias de antecedência da viagem para garantir a passagem, fazendo com que o cliente compareça à rodoviária apenas para o embarque com o bilhete de passagem eletrônico em mãos, este adquirido através de um e-commerce.

As pesquisas recentes sobre o crescimento constante do e-commerce demonstram a mudança de comportamento do comércio para o meio eletrônico por diversos motivos convenientes para todas as partes. No entanto, essa transição de parte do mercado para o e-commerce devido à crescente demanda pela operação virtual não traz benefícios livres de riscos. Este cenário virtual chama atenção de criminosos para a prática de fraude de cartão de crédito, forma mais utilizada como meio de pagamento em *e-commerce*. Tratando-se de um ambiente onde há maior dificuldade de identificar quem está praticando o crime e a crescente de informações recebidas nos canais eletrônicos, torna-se o cenário propício para atuação de criminosos.

Segundo Ferreira (2021 apud TEIXEIRA, 2020, p. 214):

> A informatização crescente das várias atividades desenvolvidas individual ou coletivamente na sociedade veio colocar novos instrumentos nas mãos dos criminosos, cujo alcance ainda não foi corretamente avaliado, pois surgem a cada dia novas modalidades de lesões aos mais variados bens e interesses que incumbe ao Estado tutelar, propiciando a formação de uma criminalidade específica da informática, cuja tendência é aumentar quantitativamente e, qualitativamente, aperfeiçoar os seus métodos de execução.

Diante disso, o problema da pesquisa está vinculado à fragilidade dos ambientes de *e-commerce* disponibilizados pelos médios e grandes operadores de seus segmentos (vendas de eletrônicos, passagens rodoviárias etc.)

Este estudo trata do impacto de fraudes de cartão de crédito analisando dados fornecidos do e-commerce da empresa de transporte de passageiros em âmbito nacional consolidada com mais de 80 anos de mercado e que há pouco está presente no e-commerce para a venda de passagens na internet, mas que também registrou aumento considerável nas transações em seu e-commerce. Atualmente possui fornecedores da área de tecnologia para combater fraudes, mas ainda assim enfrenta períodos conturbados referente ao assunto, necessitando de maior desenvolvimento em seus métodos de segurança.

A pesquisa será orientada por viés financeiro visando identificar as perdas e seus reflexos advindas das práticas de fraude online de cartão de crédito por uma abordagem quantitativa e qualitativa no sentido de procedimentos, tecnologias e métodos que possam ser pesquisados e abordados para prevenção dessas fraudes.

## 1.1 Problema

Quais são as principais alternativas no mercado para combate à fraude no cartão de crédito em transações online e, entre elas, qual a alternativa mais adequada do ponto de vista econômico-financeiro para a empresa foco do estudo?

## 1.2 Objetivos

### 1.2.1 Objetivo geral

Apresentar as principais alternativas de combate à fraude e avaliar entre elas qual apresenta o melhor desempenho econômico-financeiro para a empresa foco do estudo.

### 1.2.2 Objetivos específicos

- Analisar e apresentar os índices de fraude da empresa nos anos de 2019 a 2022;
- Conhecer as limitações existentes do e-commerce da empresa e do atual prestador de serviço antifraude;
- Apresentar alternativas existentes no mercado para prevenção de fraudes com cartão de crédito;
- Avaliar economicamente as alternativas de prevenção;
- Sugerir a implantação da alternativa mais adequada do ponto de vista econômico-financeiro à empresa foco do estudo;

## 1.3 Justificativa

A definição do setor e tema deste estudo se da em razão do autor atuar profissionalmente na área com ênfase no tema do trabalho com intuito de explorar

assuntos relacionados a atividade e identificar novas possibilidades e propostas para resolução do problema encontrado.

O estudo visa compreender a importância de ações a serem realizadas no ambiente e-commerce da Viação para minimizar ao máximo as perdas com fraude de cartão de crédito colocando prevenção e segurança lado a lado como itens primordiais nessa nova fase a ser consolidada.

Como finalidade, inserir complementos essenciais de validações que ampliem a segurança do e-commerce para aquisições de passagens rodoviárias e reduzir as perdas financeiras com fraude para a empresa foco do estudo.

Outras empresas poderão realizar análises semelhantes baseadas nesta e decidir qual a melhor alternativa para elas. O trabalho também contribuir ao apresentar alternativas para enfretamento do problema que ainda carece de estudos.

# 2. REVISÃO TEÓRICA

## 2.1 Comércio Eletrônico

### 2.1.1 Definição de Comércio Eletrônico

Por comércio eletrônico (CE, e-commerce) entende-se o processo de compra, venda e troca de produtos, serviços e informações por redes de computadores ou pela Internet. Kalakota e Whinston (1997) definem o CE a partir de quatro perspectivas:

- **A perspectiva da comunicação:** o CE é a distribuição de produtos, serviços, informação ou pagamentos por meio de redes de computadores ou outros meios eletrônicos.
- **A perspectiva do processo comercial:** o CE é a aplicação de tecnologia para a automação de transações e do fluxo de trabalho.
- **A perspectiva de serviços:** o CE é uma ferramenta que satisfaz a necessidade de empresas, consumidores e administradores quanto à diminuição de custos e a elevação nos níveis de qualidade e agilidade de atendimento.
- **A perspectiva Online:** o CE é a possibilidade de compra e venda de produtos e informações pela Internet e por outros serviços online.

Adiciono, ainda, mais duas perspectivas à lista:

- **A perspectiva da cooperação:** o CE é um instrumento de mediação inter e intracooperativa dentro de uma organização.
- **A perspectiva comunitária:** o CE é um ponto de encontro para membros da comunidade poderem aprender, realizar negócios e cooperar uns com os outros.

Alguns definem o termo “comércio” como transações efetuadas entre parceiros de negócios, por essa definição pode se concluir que a expressão “comércio eletrônico” é um tanto restrita. É por isso que muitos preferem o *e-bussines*, uma definição mais ampla de CE que não inclui simplesmente a compra e venda de

produtos e serviços, mas também prestação de serviços a clientes, a cooperação com parceiros comerciais e a realização de negócios eletrônicos dentro de uma organização[1].

### 2.1.2 Breve histórico e crescimento do e-Commerce

As primeiras movimentações do comércio eletrônico ocorreram no início da década de 70, com novidades como a transferência eletrônica de fundos (TEF), na qual se podia transferir o dinheiro eletronicamente. Mas a sua aplicação limitava-se a grandes corporações, instituições financeiras e algumas empresas mais arrojadas. Surgiu então a troca eletrônica de dados (*eletronic data interchange* – EDI), tecnologia que permite a transferência eletrônica de documentos como ordens de compra, faturas e pagamentos eletrônicos entre organizações. Essa nova possibilidade ampliou a participação de empresas financeiras, de manufaturas, de revenda e de prestação de serviços, por exemplo. À medida que a internet se tornou mais comercial e que os usuários passaram a fazer parte da *World Wide Web* no início da década de 90, a expressão *electronic commerce* passou a ser utilizada, e suas aplicações se expandiram rapidamente. Um dos motivos da rápida expansão foi o desenvolvimento de novas redes, protocolos e softwares e especificações. Outro motivo foi o aumento da competitividade e das pressões sobre os negócios[2].

Então, se faz necessário contextualizar o atual cenário do crime virtual também para poder entender o porquê as fraudes com cartão de crédito ganham significativo espaço para discussões e estudos.

Nos últimos anos é evidente a digitalização de processos em todos os âmbitos, o que se começou pensando sobre a economia de papel para com os arquivos digitais e e-mails, serviu e surgiu para muitas outras funções de nosso dia a dia economizando tempo, energia, matérias primas e tornando todos os tipos de relações a cada momento mais próximo daquilo que podemos chamar de instantâneo. Em razão disso,

---

[1] TURBAN, Efraim. **Comércio eletrônico: estratégia e gestão** / Efraim Turban e David King; tradução Arlete Simille Marques. Revisão técnica Belmiro João, Erico Veras Marques. São Paulo: Prentice Hall, 2004. p.03

[2] TURBAN, Efraim, Comércio eletrônico: estratégia e gestão / Efraim Turban e David King; tradução Arlete Simille Marques. Revisão técnica Belmiro João, Erico Veras Marques. São Paulo: Prentice Hall, 2004. p. 07.

passamos a portar cada vez menos itens da forma física em termos de quantidade, porém poucos itens que possuem acesso a todas as informações às quais desejamos em qualquer momento e de praticamente de onde estivermos dentro dos grandes centros urbanos.

Por consequência da evolução da tecnologia estamos menos presentes nas ruas, a circularização de moeda física cai, e o fluxo de informações on-line cresce, dentro disso informações cadastrais de pessoas e seus dados financeiros estão aos montes na internet. O relatório de nº 43 da *Webshoppers*[3] demonstra a estrondosa inserção de novos usuários em *e-commerces* em geral no país (ANEXO B).

O estudo também relata que esse "*boom*" de novos usuários foi contribuído principalmente pela pandemia do coronavírus, que estimulou e antecipou uma tendência que já ocorria de forma gradual, porém tornou-se exponencial nesse período como sendo a única forma viável de manter as relações de compra e venda.

### 2.1.3 Oportunidades e principais ameaças

Em contrapartida a todo crescimento do e-commerce, nunca foram direcionados tantos esforços dos empresários na área de tecnologia da informação para suprir essa nova demanda do público na web. A concorrência torna-se cada vez mais acirrada e faz necessário agir de forma instantânea em resoluções práticas para a experiência do usuário além dos preços praticados. Hoje, pode-se considerar uma não ameaça aos concorrentes, empresas de vendas que não dedicam reais esforços à venda online e, portanto, deixam de ser competitiva no mercado nacional. Entretanto, surge o atual e conhecido grande vilão dos empresários: o *ChargeBack*.

[3] Realizado pela Ebit | Nielsen desde 2001, o Webshoppers é o estudo de maior credibilidade sobre o comércio eletrônico brasileiro e a principal referência para os profissionais do segmento.

O conceito básico de *chargeback*[4] foi brevemente descrito pelo site Curso de E-commerce[5].

Este é o termo que os empresários menos desejam ouvir quando o assunto é o e-commerce da empresa, pois é o tema do momento quando se fala em perdas financeiras.

É notório todo esforço que as instituições financeiras realizam para evitar os transtornos causados pelo crime de fraude de cartão de crédito, mas também são necessárias ações de todos *e-commerces* em revisar, validar e reforçar seus processos na captação e recepção de informações de clientes para que da melhor forma seja possível conciliar o anseio por aumento de receita e a prevenção de perdas por fraude.

### 2..1.4 Pagamento online com cartões de crédito

Alguns anos atrás, a crença geral era de que consumidores ficariam extremamente relutantes em usar seus números de cartão de crédito na Web. Supunha-se que seriam necessárias formas especiais de dinheiro eletrônico para o B2C crescer e se desenvolver. Hoje, o CE está prosperando, e como observamos antes, a maioria das compras na Web são pagas com cartões de crédito e não dinheiro eletrônico[6].

---

[4] *Chargeback* é o cancelamento de uma venda feita com cartão de débito ou crédito, que pode acontecer por dois motivos: um deles é o não reconhecimento da compra por parte do "titular do cartão, e o outro pode se dar pelo fato de a transação não obedecer às regulamentações previstas nos contratos, termos, aditivos e manuais editados pela administradora. Ou seja, o lojista vende e depois descobre que o valor da venda não será creditado porque a compra foi considerada inválida. Os números são desconhecidos, mas o que se sabe é que o volume é assustador, principalmente nas lojas virtuais.

[5] CURSO DE E-COMMERCE. **O Risco do ChargeBack nas vendas por cartão**. Disponível em: <https://www.cursodeecommerce.com.br/chargeback/>. Acesso em 25 de agosto de 2022.

[6] TURBAN, Efraim. **Comércio eletrônico: estratégia e gestão** / Efraim Turban e David King; tradução Arlete Simille Marques. Revisão técnica Belmiro João, Erico Veras Marques. São Paulo: Prentice Hall, 2004. p.334.

### 2.1.5 Segurança para pagamentos eletrônicos (E-PAYMENTS)

Quando usamos o cartão de crédito para fazer uma compra na Internet, como podemos ter a certeza de que alguém não interceptará o número do cartão no seu trajeto pela rede?

Quando contatamos um site de CE com a intenção de fazer uma compra como podemos saber que se trata de um site legítimo? Se uma empresa envia uma fatura para outra empresa pela Internet, como o destinatário pode ter certeza de que a fatura não foi alterada? Esse tipo de pergunta ilustra as questões de confiança (ou “PAIN”) que emergem dos sistemas de pagamento eletrônico (*e-payment*). Com o TSL (Transação eletrônica segura) é possível criptografar números de cartões de crédito enviados do navegador de um consumidor para o site de um comerciante. Primeiro é preciso verificar a validade desse número, depois o banco do consumidor deve autorizar o cartão e por fim a compra precisa ser processada (ANEXO C)[7].

### 2.1.6 Risco nas transações com cartão de crédito

Mesmo que o TLS – *Transport Layer Security* seja utilizado para garantir a segurança da transação entre o navegador e o servidor Web, ainda há riscos quando se fazem pagamentos online com cartão de crédito. Na maior parte das vezes o comerciante arca com a responsabilidade pelos seguintes riscos:

- Cartões roubados: se alguém roubar um cartão de crédito e o verdadeiro proprietário do cartão contestar quaisquer débitos feitos pelo ladrão, o emitente devolverá o dinheiro ao dono do cartão e cobrará o débito do comerciante.
- Repúdio do cliente: um cliente pode autorizar um pagamento e negá-lo. Se a negativa for procedente para o emitente, o comerciante arcará com o prejuízo.
- Roubo de detalhes do cartão armazenados no computador do comerciante: há casos em que hackers invadem eletronicamente o computador de um

[7] Ibid., p. 339.

comerciante onde está armazenado detalhes sobre cartões de créditos. A chave para proteger essas informações é isolar o computador ou arquivos que as armazenam, de modo que não possam ser acessados diretamente pela internet[8].

## 2.2 Fraudes Eletrônicas

De forma ampla, fraudes eletrônicas são crimes virtuais de ato ilegal através de um sistema computacional fazendo uso de transmissão de dados de vítimas de maneira não autorizada para ganho de capital.

Apesar do assunto estar em alta na contenção de perdas nas mais diversas organizações, pouco se encontram estudos relacionados a ações tomadas pelas empresas em seus CE's para contenção e evolução tecnológica para prevenção. De fato, hoje, o ambiente on-line possui um rico e diverso capital, senão o mais valioso, já que possuem além de informações financeiras, dados pessoais que completam o perfil de identidade de uma pessoa existente e financeiramente ativa contendo score bancário vinculado ao seu CPF nas mais diversas plataformas financeiras. Desse modo, é para este ambiente que o crime organizado tem dedicado tempo e espaço conforme trecho do livro Comércio Eletrônico (TURBAN, 2004):

> Anos atrás, perguntaram a Willy Sutton, um assaltante de bancos muito conhecido: 'Por que você rouba bancos?' Sua resposta: 'Porque é onde o dinheiro está''. Hoje, se perguntássemos a um hacker por que ele ataca a internet ou a web, ele talvez desse uma resposta semelhante: 'Porque é onde estão o dinheiro e as informações. O crescimento do CE em si certamente bastou para fazer da internet um sedutor parque de diversões para os fraudadores. (TURBAN, 2004, pg. 316)

Efraim Turban (2004) relata que especialistas em segurança afirmam que os ataques de fraudes na web ocorrem em dois tipos – os não-técnicos e os técnicos. O ataque não-técnico, também conhecido como engenharia social[9], o perpetrador

---

[8] TURBAN, Efraim. **Comércio eletrônico: estratégia e gestão** / Efraim Turban e David King; tradução Arlete Simille Marques. Revisão técnica Belmiro João, Erico Veras Marques. São Paulo: Prentice Hall, 2004. p.341.

[9] **Engenharia Social no contexto de segurança da informação, refere-se à manipulação psicológica de pessoas para a execução de ações ou para a divulgação de informações**

utiliza-se de ardil ou outro tipo de persuasão para enganar obtendo os dados pessoais e financeiros para executar as ações comprometendo a segurança da vítima.

Em contrapartida, o conhecimento de software e de sistemas é peça essencial para o ataque técnico, e é deste tipo de fraude que o trabalho se refere e tem seu foco.

Ainda, em conclusão de seu artigo, Penêdo (2018) define resultados com base no constante empenho e mudanças realizadas pelos criminosos para tentativa de manutenção e ganhos financeiros com fraudes:

> A função do engenheiro social é burlar ferramentas que ameacem a integridade das vítimas, e os hackers o fazem. Poderia, dessa forma, elucidar que a segurança da informação é uma utopia, uma vez que os sistemas burocráticos não conseguem deter a ação dos hackers e engenheiros sociais, nem criar sistemas em que não haja alguma vulnerabilidade que possa ser quebrada. (PENÊDO, 2018)

Quanto à operação, a gestão sobre fraudes eletrônicas tem um extenso campo de atuação que geralmente engloba todos os aspectos de detecção e investigação de qualquer tentativa, com sucesso ou não, de roubo através de enganação ou violação intencional de serviços oferecidos por meio eletrônico (JACOBS, 2002). A gestão do processo de detecção de fraudes depende necessariamente da natureza e ramo do negócio, porém, de maneira geral, existem dois métodos para detecção de fraudes: análise absoluta e análise diferencial. A primeira busca identificar padrões de ataques anteriores para detectar novas ocorrências destes ataques, enquanto a diferencial procura por desvios no padrão de utilização do usuário (MOREAU, 1996). Ambos os métodos de detecção estão suscetíveis a erros. Com relação aos potenciais erros na análise de detecção de fraudes, seja ela diferencial ou absoluta, estes podem ser de dois tipos: falsos positivos e falsos negativos. Um falso positivo ocorre quando um alarme é gerado embora não há um ataque. Em contrapartida, um falso negativo acontece quando um alarme não é gerado apesar do ataque (ARVIDSON, 2003).

BELLA (2008), acrescenta que um processo de detecção de fraudes apresenta muitos desafios, dentre os quais estão o grande número de erros de detecção que podem ser gerados por um sistema de monitoramento de fraudes e o potencial

---

**confidenciais**. Disponível em: https://pt.wikipedia.org/wiki/Engenharia_social. Acesso em 07 de setembro de 2022.

desgaste da privacidade do usuário do serviço. Neste mesmo contexto, Bella (2008) reforça a questão dos falsos negativos quando afirma que, como uma fonte de perda de receitas, falsos negativos são de longe mais ameaçadores para o empresário uma vez que o valor fraudado pode ser muito superior ao trabalho despendido por um analista ao tratar um falso positivo.

As vítimas típicas de fraudes eletrônicas são consumidores, instituições financeiras e prestadoras de serviços de comunicação e empresas que oferecem serviços e venda de bens de consumo via rede internacional de computadores (GHOSH, 2010).

Diante do entendimento da funcionalidade e a persistência nos ganhos advindos de ataques fraudulentos, os estudos mais recentes e ferramentas mais procuradas do mercado tratam como principal método o *Machine Learning*, algoritmo de aprendizado que atua com base na observação do comportamento de cadastros ativos financeiramente no CE a que prestam o serviço. No entanto, a luta e aprendizado da ferramenta contra os fraudadores é diário, e por vezes falho, podendo gerar severos danos ao CE em possíveis brechas existentes na performance de detecção até a identificação humana de desvio de padrões de compra.

Nesta situação, a conclusão sobre o uso de *Machine Learning* e sua importância encontrada no artigo[10], representa lacunas por vezes não preenchidas da forma esperada:

> O *Machine Learning* tem cooperado na detecção de transações de cartão de crédito fraudulento, mas existem caminhos abertos para a evolução e melhoria, buscando cenários que comparem e contemplem diferentes algoritmos, sob abordagens distintas, mas que utilizem um banco de dados similar, destacando, também, quais as variáveis são de maior relevância para o melhor desempenho dos métodos. (LAMARCA, Daniel S. et al, 2019)

Então, torna-se evidente que há espaço para evolução e atuação dos próprios CE's em suas plataformas em paralelo com os serviços já prestados por fornecedores de tecnologias de detecção de fraudes, como é o caso da empresa foco deste estudo, para processos de gestão mais eficientes em relação ao seu e-commerce.

---

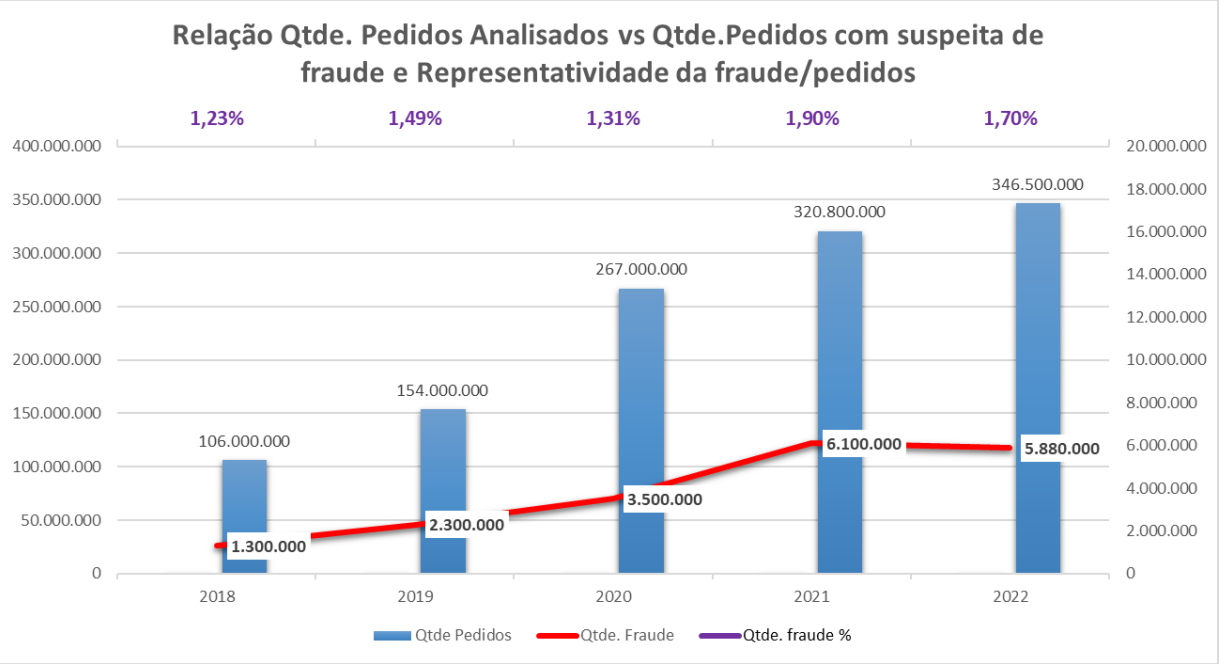
[10] LAMARCA, Daniel S.; SARRIÉS, Gabriel A.; SILVA, Gabriel F.; **Machine learning e fraude de cartão de crédito: uma revisão bibliográfica sistemática**. Revista Intellectus, 2019. Disponível em: < http://www.revistaintellectus.com.br/artigos/77.942.pdf>. Acesso em: 15 de setembro de 2022

A evolução das fraudes eletrônicas no e-commerce é acelerada devido ao avanço da tecnologia, mas um marco do ano de 2020 fomentou, e bastante, o crime cibernético: a pandemia.

Por este período ter direcionado novos usuários e estimular os já habituados a realizar suas relações de compra e venda através da internet, os fraudadores tiveram acesso a uma nova entrada grande de dados na internet e puderam dedicar esforços ao crime para saquear os cartões de crédito através de compras fraudulentas. Diante disso, em consulta aos relatórios de mapa da fraude fornecidos pela *Clear Sale*[11], umas das maiores ferramentas de antifraude de e-commerce e demais mercados, foram capturados e analisados os dados de sua base apresentando as evoluções relacionadas a esses mercados.

Abaixo, Gráfico 1 que se refere somente a vendas de e-commerce com forma de pagamento cartão de crédito no Brasil.

*Gráfico 1 - Evolução de vendas e fraudes no E-commerce brasileiro*




Fonte: Elaborado pelo autor, 2023

[11] Clear Sale. Disponível em: <https://br.clear.sale/mapa-da-fraude>. Acesso em 15 de janeiro de 2023

É possível identificarmos o relevante aumento de pedidos realizados a partir de 2020, assim como a quantidade de tentativas de fraude, o índice de fraude chega a subir 0,4% de representatividade na comparação pré-pandemia (2019) e pós (2021). Portanto, independentemente do tipo de atividade (produto ou serviço), é crucial pensar sobre tecnologias e melhores formas para a prevenção à fraude.

## 2.3 Avaliação Econômica de Alternativas

Partindo de pressupostos básicos para que seja possível analisar as alternativas diante do problema para identificar soluções, se faz necessário refletir sobre possibilidades que atendam da melhor forma a relação custo-benefício de toda operação relacionada à experiência de compra on-line no site da Viação e as questões de disponibilidade de recursos financeiros da empresa. Portanto, essa relação precisa atender aos propósitos apresentados e trazer ganhos ou evitar perdas para a empresa.

Trabalhar as finanças e mitigar alternativas para dar início ao projeto de busca por resoluções através de opções de análises financeiras podem ajudar a buscar respostas fundamentadas para decisões de investimento e avaliação de oportunidades.

Analisando alguns conceitos e dando início ao princípio de que há necessidade de avaliar as oportunidades e investimentos financeiros de projetos elaborados para uma organização, considera-se válido aquele que cria valor para os seus proprietários. No sentido mais geral, apropria-se valor a um investimento que vale mais no mercado do que custa para ser adquirido (ROSS, 2013)

A literatura discorre o assunto entorno do VPL (Valor Presente Líquido), que é o resultado atual de análise do fluxo de caixa do investimento, ou em outras palavras, projetar e simular os acontecimentos futuros com base nos fatos e números já conhecidos que estão relacionados ao âmbito do investimento realizado a fim de estimar, no presente, o resultado futuro do investimento. Em resumo, o VPL pode ser definido como o total de benefícios menos o total de custos para o investimento. O

resultado deve, obrigatoriamente, ser positivo para que seja uma proposta aceitável em termos de viabilidade financeira do projeto de investimento. (BERK, 2009)

Dentro dessas análises, também se faz necessário entender qual o *payback,* que, de modo geral, é o período necessário para recuperar o investimento inicial. Fator importante para comparação com demais alternativas e para validar projetos de investimentos. Em razão disso, se toma como base uma regra para o *payback*, onde somente será um investimento aceitável se o período de retorno for menor que um número pré-determinado de anos. O *payback* é uma das alternativas para auxiliar as análises de resultados do VPL dos fluxos estimados para que seja o mais assertivo possível com a realidade a ser enfrentada. Então, podemos dizer que um investimento que rapidamente se pague e mantenha seus benefícios para além do período de corte provavelmente tem um VPL positivo. (ROSS, 2013)

Nesse sentido, aprofundando as análises sobre determinado investimento, podemos identificar o índice de lucratividade (IL), ou seja, o seu custo-benefício financeiro, o quão vantajoso ou oneroso tornou-se a proposta de investimento analisada e como ela está apresentada em termos de índice frente às demais oportunidades. O IL é mais outra ferramenta suporte para as análises de VPL, o qual deve ser primeiramente identificado e priorizado, já que um projeto de IL maior, não significa possuir um VPL maior também. (ROSS 2013)

Levando em conta os recursos e proporções da empresa desse estudo, faz-se útil a avaliação de projetos com diferentes exigências de recursos, tanto financeiros, como com pessoas e tecnologia. (BERK, 2009) Em resumo, todos levarão a decisões financeiras, mas para fins de entendimento, envolverão decisões de gestão que estão para além do financeiro quando pensado sobre as exigências de recurso para determinado projeto, já que utilizando de recursos de pessoa, por exemplo, estarão vinculadas variáveis não somente financeiras, como motivacionais, psicológicas e outras mais que podem impactar o desempenho e evolução do projeto de tal forma qual foi estimado.

É provável que quando começamos a pensar em alternativas e possibilidades, surjam mais projetos aparentemente viáveis e atraentes em termos de ideias para mudança e investimento. No entanto, pela primeira ideia de VPL, todo e qualquer projeto com VPL positivo é um projeto de investimento aceitável, porém dentre as

análises e oportunidades surgidas, pode-se ter alguns projetos de investimento interessantes contendo o VPL positivo. E aí? Qual devemos priorizar?

A segunda premissa do VPL para mais de um projeto com índice positivo é de que devemos priorizar projetos de investimento com VPL e retorno maior possível (BERK,2009), ou seja, aquele que resultará em maior valor de resultado quando subtraído os custos do total de benefícios de um dado projeto de investimento.

Reforçando a premissa de priorização do projeto com maior VPL e enfrentando opiniões e tomadas de decisão de gestão da empresa, a obra também nos traz a independência de preferências, ou seja, a escolha de projeto não será baseada em preferências da gestão, pessoais ou outras quaisquer que não sejam baseadas em resultado financeiro, o maior VPL apresentado dentre as alternativas como bem coloca o autor.

> Independentemente de nossas preferências por dinheiro hoje versus dinheiro no futuro, devemos sempre maximizar o VPL primeiro. Podemos, então, contrair ou conceder um empréstimo para variar os fluxos de caixa ao longo do tempo, e encontrar nosso padrão preferido de fluxos de caixa. (BERK, 2009, pg. 93)

Também relacionado às análises e projetos de investimento, o conceito de externalidade de projeto é um ponto de atenção, já que trata de efeitos indiretos do projeto que podem aumentar ou diminuir lucros de outras atividades da empresa (BERK, 2009) e, portanto, devem ser levados em consideração para que não diminua ou inverta os benefícios do projeto de investimento.

Considerando decisões financeiras, trataremos de fluxo de caixa, um específico que contém um princípio geral, que é o fluxo de caixa relevante para um projeto, isto é, qualquer variação nos fluxos de caixa futuros da empresa que ocorre por consequência da decisão de investir em tal projeto, sendo definidos com base nas variações ou incrementos nos fluxos da empresa, são chamados de fluxos de caixa incrementais do projeto (ROSS, 2013)

Sabendo que fluxo de caixa incremental de um projeto inclui todas as alterações que ocorrem nos fluxos futuros da empresa, então é comum que surjam os efeitos colaterais (bons e ruins) no decorrer do tempo. Estão, os fluxos, à mercê de novas tecnologias, mudanças nos hábitos a que os fluxos de caixa da operação estão

atrelados, gerar os tais efeitos colaterais, e quando negativos podem ser chamados de erosão. (ROSS, 2013)

Para além da decisão de um projeto de investimento, existe a alternativa de nenhuma escolha, e assumir o que conhecemos por custo de oportunidade para quaisquer das escolhas, inclusive a não escolha, que também passa a ser uma. Uma alternativa pode estar atrelada a decisões de gestão sem investimento financeiro imediato, ou seja, aparentemente sem um custo financeiro imediato e/ou pré-determinado no momento da decisão. Mencionar custo, normalmente traz o pensamento de quanto teremos de desembolsar para tal, mas o custo de oportunidade é diferente, ele trata de desistir de um benefício. (ROSS, 2013) Toda decisão envolve um custo de oportunidade, diariamente realizamos escolhas, bem baseadas ou não, em custos financeiros. Neste estudo poderemos compreender melhor as consequências dos custos de decisão, que estão diretamente vinculados ao custo de oportunidade, que nada mais é realizar a escolha do projeto onde seu custo financeiro será aproveitado da melhor forma. (BERK, 2009)

## 3. PROCEDIMENTOS METODOLÓGICOS

A pesquisa se caracteriza como um estudo de caso, possui uma abordagem qualitativa e descritiva. O caráter qualitativo se dá por apresentarmos um estudo de caso que gera um prejuízo financeiro decorrente da fragilidade do site de vendas, que possibilita a aplicação de fraudes nas compras das passagens rodoviárias (GODOY, 1995).

Para atingir os objetivos propostos, serão necessárias as seguintes informações tomando como base temporal período de 12 meses contemplando períodos sazonais existentes na Viação:

- As fragilidades e critérios inicialmente básicos de segurança que atualmente a plataforma web da Viação, respectivamente, possuem e carecem.
- Os atuais métodos tecnológicos disponíveis para prevenção a fraudes eletrônicas com cartão de crédito e quais os direcionamentos e vantagens cada um apresenta.
- Perdas financeiras existentes na empresa decorrentes de fraudes eletrônicas com cartão de crédito.
- Comparativo de índices, perdas, representatividades e impactos das fraudes.

Identificadas as informações necessárias, as coletas se darão da seguinte forma, sequencialmente:

- Acesso e pesquisa interna, em conjunto com a área de tecnologia da informação da Viação.
- Pesquisa de mercado voltado aos métodos de prevenção no segmento de serviços e, se possível, transporte de passageiros.

- Exportação de relatórios de controles internos contendo as informações completas de quantidades, valores e índices da operação de fraudes comparando resultados do setor anteriormente já realizados.

As informações coletadas serão organizadas por critério de relevância e importância de correção dentro da operação, partindo do mais urgente.

Em continuidade à sequência apresentada nas informações necessárias, a análise dessas se dará por:

- Identificação, levantamento e comparação através de estudos e resultados relevantes do mercado de e-commerce para suas plataformas.
- Análise das perdas frente aos resultados apresentados de receita e os motivos existentes para as perdas por fraudes.
- Análise dos índices apresentados pela Viação e suas relevâncias.
- Analisar quais os métodos viáveis e que fazem mais sentido para a operação da Viação visando a performance de experiência entre usuário e plataforma web.

O método de pesquisa utilizado neste trabalho será quantitativo, em virtude da maneira que será abordado o problema. Uma vez que tem como principal característica a utilização da quantificação, seja nas modalidades de coleta de informações ou no tratamento delas. Realizado através de técnicas estatísticas.[12]

O emprego da quantificação tanto nas modalidades de coleta de informação, quanto no tratamento dessas através de técnicas estatísticas desde as mais simples como percentual, média, desvio padrão, às mais complexas, como coeficiente de correlação, análise de regressão etc. se necessário.[13]

---

[12] MATIAS, José Pereira. **Manual de metodologia da pesquisa científica**. 3 ed. São Paulo: Atlas, 2012. p.84.

[13] BOAVENTURA, Edivaldo M. **Metodologia da pesquisa: monografia, dissertação, tese.** 1 ed. – 4 reimp. São Paulo: Atlas, 2009.

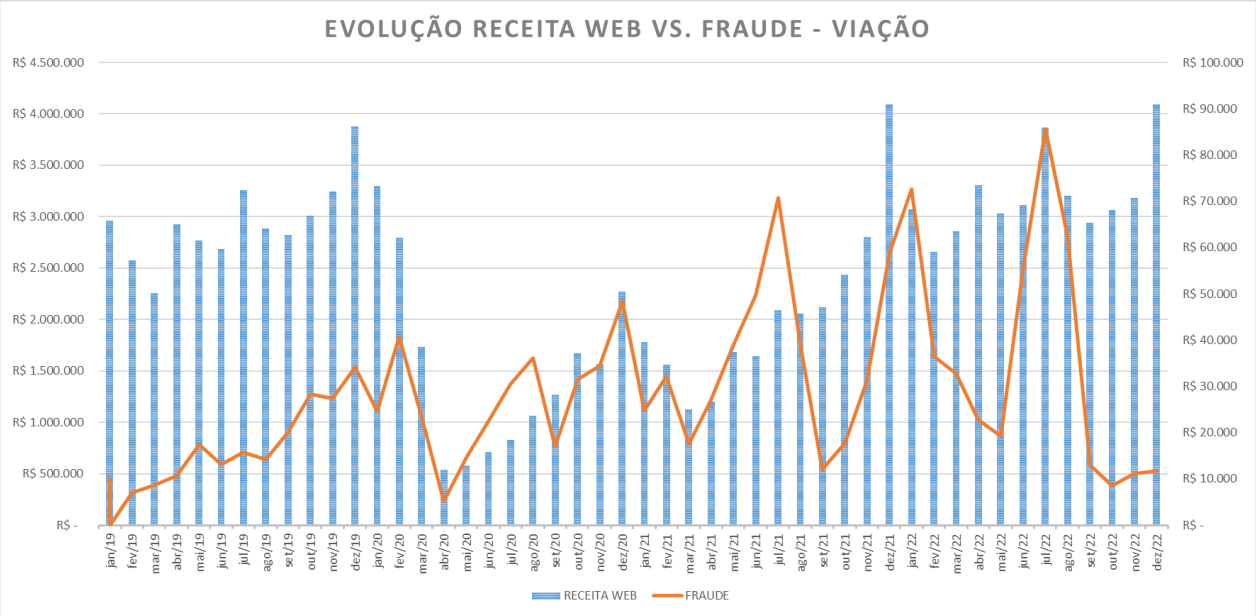
As alternativas de controles de fraudes eletrônicas serão levantadas e analisadas através de pesquisa de mercado junto a empresas que propõe soluções para o problema enfrentado na empresa estudada. As informações necessárias para que seja possível avaliar as alternativas encontradas são o custo da solução para a empresa deste estudo e o índice de efetividade no combate à fraude proposto por cada solução.

## 4. ESTUDO DE CASO

Para que seja possível compreender o atual cenário da Viação e quais as necessidades frente ao problema a empresa requer, inicia-se pelos registros disponíveis do problema na empresa e posteriormente se identifica as estimativas da permanência e qual a tendência do comportamento do problema sem quaisquer alterações e melhorias aplicadas.

Nos registros da Viação, constam históricos de operações realizadas via web a partir do ano de 2010, porém sem controle administrativo pela empresa, constam dados consistentes dos valores fraudados a partir de 2019, ano em que as análises de perdas com fraudes ganham maior importância, com os devidos levantamentos conforme gráfico 2.

*Gráfico 2 - Evolução de vendas e Fraudes da Viação*




Fonte: Elaborado pelo autor, 2023

São visíveis os picos de fraude que ocorrem no site da empresa e que a Viação arca com a perda financeira. Nos 3 últimos, (jun21-ago21), (dez/21-jan/22) e (jul/22-ago/22) foram devidamente mapeadas e compreendidas as falhas existentes que permitiram os ataques.

No primeiro desses ataques, (jun/21-ago/21), foi identificada falha do fornecedor antifraude Konduto, que habilitou regras na plataforma do antifraude para estimular as vendas da Viação no período de retomada pós-pandemia, criando medidas que violavam regras internas de negócio da Viação.

Para o segundo, falha interna da Viação, na área de T.I., em atualizações do layout e outros parâmetros do site, que interromperam as comunicações devidas com o fornecedor antifraude Konduto e tornaram vulnerável todas as transações ocorridas no período compreendido (dez/21-jan/22)

O terceiro e mais atual ataque de fraude ocorrido, não se trata exatamente de erros contendo, através de mapeamento, culpados de ambas as partes da relação (Viação – Konduto), mas sim o vazamento massivo de dados ocorridos externamente ao site da Viação, mas que esse se tornou canal de uso desses dados para a prática de fraude e que o antifraude da Konduto também não foi capaz de conter.

Este terceiro caso, pelo histórico, é o que representa a atual vulnerabilidade e descontrole por parte da Viação, que é foco do estudo de caso a fim de identificar alternativas que garantam mais segurança para a Viação nas transações on-line com os solicitantes e quais as melhorias propostas para suportar um novo ataque desse tipo, sem deixar que toda a responsabilidade de análise e identificação de usuários para potenciais fraudadores esteja somente sob responsabilidade do fornecedor contratado Konduto.

Então pelo Gráfico 2 é possível verificar que há períodos mais estáveis, quando comparados aos picos, porém quando os ataques ocorrem, descompensam as estabilidades existentes nos demais períodos, tornando uma média total de fraude elevada. Para esse exemplo, levando em consideração o ano de 2022, a média de fraude ficou em R$ 36 mil mensais, gerando um percentual médio de 1,12%, índice acima do aceitável pelas grandes bandeiras de cartões[14].

A evolução mencionada durante o trabalho no mercado de e-commerce em geral também é identificado na Viação, quando comparamos dois períodos pré e pós pandemia, 2019 e 2022, respectivamente, o ano de 2019 foi faturado no site o

[14] CARNEIRO, Eduardo.; **Saiba os limites de chargebacks e fraudes que as bandeiras de cartão aceitam** Disponível em: <https://blog.konduto.com/pt/2019/09/limites-chargebacks-fraudes-bandeiras-cartoes/> Acesso em 01 de fevereiro de 2023.

equivalente à 91,7% do faturamento de 2022, mas a proximidade não ocorre para o total fraudado nesses anos, 2019 registrou apenas 47,9% do total fraudado em 2022, ou seja, o comparativo de faturamento entre 2019 e 2022 no site permaneceu próximo (91,7% x 100%), mas o total de fraude existente nos anos analisados mais que dobrou de 2019 para 2022. Tudo isso mantendo os mesmos fornecedores de site e antifraude, com modelos de trabalho e análises semelhantes, mas em evolução durante estes anos. Isso significa que houve uma “especialização” dos fraudadores para identificar as fragilidades e maior atuação nesse tipo de crime.

Com o entendimento desse comparativo e com o devido acesso às informações de fraudes ocorridas dentro da Viação dos últimos 4 anos, elabora-se uma estimativa de valores fraudados para o ano vigente 2023.

*Tabela 1 – Evolução anual comparativa de fraudes online com cartão de crédito*

| Crescimento Fraude (R$) | **Média** |
|---|---|
| 2019 ⇨ 2020 | **92,84%** |
| 2020 ⇨ 2021 | **62,29%** |
| 2021 ⇨ 2022 | **10,87%** |
| 2019 ⇨ 2022 | **194,42%** |

Fonte: elaborado pelo autor.

Com base nos dados da tabela 1 comparativa de evolução financeira das perdas decorrentes de fraude com cartão de crédito no site da Viação, pode-se concluir algumas características que auxiliam para uma utilização mais adequada para criação de estimativa de perdas com fraude para 2023. Os dados apresentam que um novo cenário de fraude, conforme mencionado anteriormente neste trabalho, surgiu para a Viação no período em que se inicia a pandemia COVID-19 a partir do ano de 2020. Portanto, identificam-se algumas premissas para a utilização dos valores que são:

- Os valores de 2019 estão muito aquém dos valores apresentados nos anos seguintes, que representam o novo cenário de fraudes.
- O ano de 2020 apresentou um período considerável de paralisação da operação e, também, de prejuízos à empresa quanto às análises, pessoas, financeiro e descontroles advindos da abrupta mudança nos fluxos de caixa

resultantes de paralisações. Portanto, é um ano de criação e evolução do cenário crítico de fraudes.

- Os anos de 2021 e 2022 são representados pelo retorno da operação e a consolidação de novos números relacionados à fraude, ou seja, o novo cenário de emergência do crime está consolidado em termos de números, tanto que o seu crescimento de um período ao outro é de aproximadamente 10%.

Portanto, seguindo as premissas detalhadas, utilizam-se os anos de 2021 e 2022 para identificar a média de valor de fraudes a que a Viação está exposta para o ano de 2023 considerando o novo cenário enfrentado.

*Tabela 2 – Média estimada com perdas de fraude em 2023*

| | |
|---|---|
| Média Mensal Estimada de Fraudes 2023 | R$ 35.457,76 |

Fonte: o próprio autor

Levando em consideração o valor estimado, chega-se à conclusão de que, não havendo intervenções, o valor de fraude para 2023 será semelhante ao encontrado em 2022, em seu maior valor até o momento no histórico de transações on-line da Viação e podendo sofrer aumentos caso haja descobertas de novas oportunidades quanto ao comportamento de prevenção do atual antifraude, único responsável pela segurança das transações do site da Viação que atua através de *machine learning* para, com referência na sua base de dados advindas do mercado, analisar e compor informações suspeitas da conjuntura de dados de um determinado cadastro que realiza tentativa de compras. Essa tática se baseia em probabilidades de o pedido do cadastro ser uma possível fraude, porém como deve ser tratado em alternativas para contenção, há exigências de outros métodos que não dependam apenas dos fornecidos pelo antifraude, já que ele cobre a parcela que lhe é fornecida: os dados já existentes e aceitos no site da Viação, e em muitos casos, pode ser falho havendo vazamento externos de dados que podem chegar como ataque até o ambiente da Viação para a análise da Konduto.

Assim, dando sequência ao estudo do caso, apresentam-se alternativas a serem analisadas para implementação e ampliação de segurança das transações on-line da Viação.

## 4.1 Sugestões de implantações para prevenção de fraudes na compra online com cartão de crédito

A primeira solução para prevenção, denominada de **Solução KDT**, foi pensada logo retirando uma forte parcela identificada de tentativas de ataque com dados frágeis para composição de cadastro, ou seja, cadastros que são criados sem a devida validação entre Nome, CPF e data de nascimento, dados que estão devidamente atrelados em consultas na Receita Federal e demais canais com considerável criticidade para liberação de produtos e/ou crédito.

Para este caso, foi analisada a possibilidade com a contratação de serviço do antifraude já utilizado, produto que agregaria ao pacote já existente para a integração do site via API/WebService.

Neste método, a implementação é prática e deve apenas ser solicitada ao fornecedor as devidas configurações. No entanto, em todas as tentativas de compra serão cobradas consultas, além das já existentes. O valor apurado é de R$ 0,35 a mais por pedido. Em 2022, a quantidade média mensal de pedidos **aprovados** no site, são 16.363 pedidos, então para cada tentativa de compra via site independente do status final, considerando a consulta do cadastro pelo fornecedor, o custo mensal desse serviço seria de R$ 5.727,05.

Essa alternativa propõe a consulta dos dados cadastrais Nome, data de nascimento, CPF, endereço etc. comparando com a extensa base de dados da Konduto.

Em questão de benefícios, traz uma considerável probabilidade de identificar as informações cadastrais na base de dados e retornar com a recomendação informando o resultado de análise, sendo um cadastro real, a aprovação ocorre automática, e em casos de “dúvidas” no processo de inteligência artificial, a transação fica pendente para aprovação manual da própria empresa (casos isolados, índice de até 4% apenas).

No entanto, para esta alternativa apresentada, não há cobertura para casos de vazamento de dados e demais ataques existentes, por isso o valor razoável de incremento do serviço, pois não abrange um leque maior de possibilidades de invasão, porém, com base na análise das fraudes ocorridas na Viação, é possível identificar que aproximadamente 35% das fraudes são advindas de cadastros com informações comprometidas e que não possuem o menor vínculo. Portanto, essa alternativa tem a expectativa de redução de 35% do valor médio previsto de fraudes em 2023.

A segunda alternativa de solução orçada, denominada **Solução PIN**, é um desenvolvimento interno e em conjunto com o fornecedor do site Rodosoft que é a autenticação e validação do número de celular fornecido. A alternativa consiste basicamente em, no momento do cadastro, a plataforma solicitar o melhor número de celular que o proprietário do cadastro possua e realizar as validações das seguintes formas por etapa:

- Se cadastro novo: Site verifica se o número preenchido já não está sendo utilizado em outro cadastro. Caso não esteja, dispara SMS com código PIN para o devido vínculo do número fornecido ao cadastro novo. Nos casos em que o número de celular já tenha sido vinculado a outro cadastro anteriormente, o site nega a validação do cadastro e impede compras.
- Para os cadastros já criados: O método de validação é extremamente útil para verificação em duas etapas na modalidade atualmente existente de compra Rápida, que não exige o login do cadastro para realização de compra de passagem em cadastros de CPF já existente na plataforma. Assim, além das informações de pagamento e de comprador, o número de telefone deve ser inserido tal qual cadastrado para validação em duas etapas, através de código enviado via SMS.

Custo prévio: R$ 20.000 – Desenvolvimento e manutenções *Rodosoft* contando com suporte e apoio de analistas internos da Viação (custo de analistas já integrado à atual folha de pagamento), mais o custo do canal de SMS, que fica R$ 0,02 por SMS disparada contando com suporte de manutenção e observação de serviço, também fornecidos pela Rodosoft.

A alternativa apresentada insere mais uma etapa de verificação dificultando a ação dos fraudadores, visto que há necessidade de possuir, além de e-mail, muitos números de telefone disponíveis para a realização de cada cadastro, sem afetar os bons clientes. O envio de códigos PIN via SMS se destaca pois não requer nenhum

hardware especial (como seria o caso de uma impressão digital, por exemplo) e não é fácil de ser descoberto, pois o número é gerado aleatoriamente no momento do envio do SMS, além do fato de o celular estar sempre próximo às pessoas. Outro benefício é a impossibilidade de compra no site utilizando o CPF de um cadastro já existente sem a verificação em duas etapas via SMS do número registrado no cadastro do proprietário.

Nas estimativas de eficácia, são consideradas que 48% das fraudes ainda não podem ser barradas pela autenticação de dois fatores[15], o que representa então que 52% das tentativas seriam impedidas pela solução, também desestimulando mais tentativas diante de maior negativa para estas, ou seja, tornando mais difícil e desgastando o processo do fraudador.

Uma terceira alternativa, denominada **Solução Único**, traz uma rápida conferência e usabilidade para os usuários, que em sua maioria, já estão habituados e simpatizam com essa forma de identificação facial[16], que é o envio de documento com foto e uma gravação/foto selfie para validação cadastral.

Desse modo, o usuário ao realizar o cadastro no e-commerce da Viação deve enviar foto do seu documento frente e verso e uma foto/gravação da face no modo selfie para análise. Posterior ao procedimento realizado pelo usuário, o fornecedor Único[17] fará todo o processo de validação e identificação deste. Importante ressaltar que essa tecnologia de identificação e validação cadastral faz parte das mais atuais disponíveis no mercado e com maior índice de assertividade divulgado em todas as campanhas envolvendo as ferramentas que utilizam do método.

O índice de assertividade que a Único fornece contra fraudes são de incríveis 99%.

Desse modo, foi realizada cotação para o perfil da empresa do estudo a fim de identificar os custos desta operação atuando com a Único.

---

[15] CARNEIRO, Eduardo.; **Autenticação de dois fatores previne, mas não basta contra invasão de contas** Disponível em: < https://blog.konduto.com/pt/2020/10/autenticacao-de-dois-fatores-invasao-de-contas/> Acesso em 19 de fevereiro de 2023.

[16] Redação; **Brasileiro gosta de usar biometria digital, aponta pesquisa** Disponível em: < https://www.mobiletime.com.br/noticias/13/06/2019/brasileiro-gosta-de-usar-biometria-digital-aponta-pesquisa/> Acesso em 20 de fevereiro de 2023.

[17] A IDTech brasileira a frente da transformação da sociedade por meio da identidade digital. Disponível em: < https://unico.io/quem-somos/> Acesso em 20 de fevereiro de 2023.

Os custos a serem investidos para a ferramenta, com base no perfil transacional em termos de quantidade da empresa do estudo, estão no seguinte patamar: R$ 0,89 por transação efetuada, ou seja, descartam-se tentativas que não foram bem-sucedidas, considerando para fins de custos apenas as transações aprovadas pela instituição financeira do cliente. A solução também não pratica custos adicionais de integração, porém como exige mudanças existentes no site da Viação, o desenvolvimento orçado para as mudanças a serem realizadas no site ficam em torno de R$ 8 mil junto à Rodosoft.

Para fins de esclarecimento de uma prática adotada por muitos e-commerces sobre informações diretas de forma de pagamento, infelizmente as instituições financeiras não realizam confirmações de informações que possam ser enviadas juntamente aos dados do cartão, como o CPF do titular, conforme publicado[18] como curiosidades do cartão de crédito no site da Konduto.

## 4.2 Análise financeira de viabilidade das sugestões de implantações para prevenção de fraudes

Dadas as alternativas apresentadas para contribuir com a prevenção e aumentar o nível de segurança das transações online da Viação, para tomada de decisão, é necessária a análise financeira e de proposta de desempenho de cada solução, avaliando os custos e benefícios quando comparados com a previsão de despesa com fraudes apresentadas para o ano de 2023.

Dessa forma, analisando a **Solução KDT**, esta possui um perfil incremental aos serviços já existentes, inclusive utilizando do mesmo fornecedor atuante, acrescentando aos atuais custos (R$ 3 mil mensais) a faixa média de R$ 5,8 mil mensais. Entretanto, com base na análise realizada dos pedidos fraudulentos existentes da Viação, identificou-se um percentual aproximado de 35% diretamente relacionados com a proposta apresentada pela Solução KDT. Então, com o investimento mensal do custo da solução e considerando o ganho estimado em prevenção de aproximadamente 35% do valor despendido com fraudes estimado,

[18] CANABARRO, Tom.; **5 coisas que você não sabia sobre cartão de crédito**. Disponível em: < https://blog.konduto.com/pt/2014/09/5-coisas-que-voce-nao-sabia-sobre-cartao-de-credito/> Acesso em 15 de Janeiro de 2023.

ainda haveria um ganho de R$ 6,6 mil por mês. Considerando esta proposta, o resultado da solução para o ano de 2023, seria um total de R$ 79 mil de ganhos através da prevenção.

*Tabela 3 – Finanças da Solução KDT*

| Solução KDT | |
|---|---|
| *Custo Mensal Existente Fornecedor* | *R$ 3.000,00* |
| Perda mensal com fraudes estimada para 2023 | **R$ 35.457,76** |
| % aproximado de impacto da Solução no combate a fraude sobre a perda estimada para 2023: **35%** | **R$ 12.410,22** |
| Valor resultante dos 65% de fraude estimada não evitada pela Solução | R$ 23.047,54 |
| Custo Mensal Incremento Solução KDT | R$ 5.800,00 |
| Despesas Fraudes + Custo Solução | **R$ 28.847,54** |
| | |
| **Resultado (Perda Estimada - Total Despesas c/ Solução** | |
| Ganho Mensal | **R$ 6.610,22** |
| Ganho Anual | **R$ 79.322,59** |

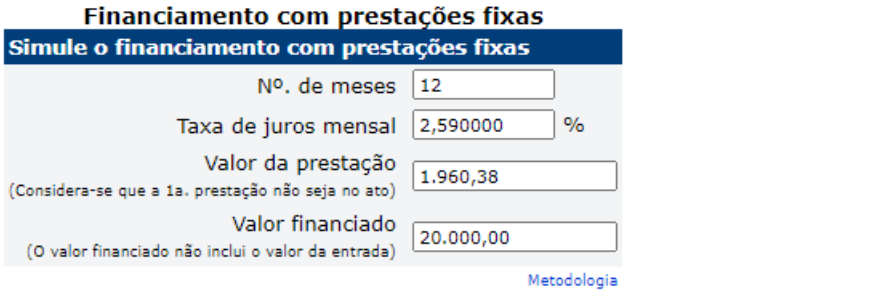
Fonte: elaborado pelo autor.

Importante ressaltar que o custo de R$ 3 mil já existente do atual fornecedor antifraude não está considerado nos cálculos, pois ele não afeta a decisão dessa alternativa, pois já é um custo existente e não deixará de ocorrer caso essa seja a opção definida para prevenção.

Avaliando as demais propostas, para a **Solução PIN**, ainda que não seja o mais atual processo tecnológico de verificações do mercado, mas que ainda é uma ferramenta que traz certa eficácia e propõe resultados diante da inexistência de ferramentas de autenticação de dois fatores, o resultado que pode ser encontrado, conforme as estimativas de ganhos da solução através da prevenção, é de 52% do valor estimado da despesa com fraudes, ou seja, sobre o valor de fraudes, a solução evita um total de aproximadamente R$ 18,4 mil mensais. Considerando os custos de implementação e manutenção da solução, para que seja possível a análise com as demais propostas, foi dissolvido o custo de implementação de R$ 20 mil em 12 parcelas iguais para fins comparativos dentro de um ano. Em razão dessa tomada de

capital no valor de R$ 20 mil a ser liquidado em 12 parcelas fixas, deve-se considerar os juros da operação de antecipação do fluxo de caixa criado desta tomada de capital (ROSS, 2013), considerando a taxa de juros do banco usual da empresa, Banco do Brasil, no percentual de 2,59% a.m. para Capital de Giro PJ com prazo de até 365 dias[19], calculados em ferramenta disponível do Banco Central do Brasil[20], totalizando a parcela de R$ 1.960,38 mensais.

*Figura 1 - Financiamento com prestações fixas (Solução PIN)*




Fonte: Calculadora do cidadão. Banco Central do Brasil.

Em conjunto, um custo de manutenção das SMS's de R$ 0,02 por SMS enviada e o total de pedidos realizados da média de 2022, sabendo que haveria mais SMS's por retentativas e demais processos da compra online, considera-se como custo o cálculo da média mensal de pedido acrescido de 50% dessa quantidade para as questões mencionadas, ficando um total médio de R$ 489 mensais de custo de parte da solução.

[19] Taxas de Juros Banco Central do Brasil. Disponível em: < https://www.bcb.gov.br/estatisticas/txjuros>. Acesso em 12 de março de 2023.
[20] Calculadora do Cidadão. Disponível em: < https://www3.bcb.gov.br/CALCIDADAO/publico/exibirFormFinanciamentoPrestacoesFixas.do?method=exibirFormFinanciamentoPrestacoesFixas>. Acesso em 12 de março de 2023.

*Tabela 4 - Finanças da Solução PIN*

| Solução PIN | | |
|---|---|---|
| *Custo Mensal Existente Fornecedor* | *R$* | *3.000,00* |
| Perda mensal com fraudes estimada para 2023 | **R$** | **35.457,76** |
| % aproximado de impacto da Solução no combate a fraude sobre a perda estimada para 2023: **52%** | **R$** | **18.438,04** |
| Valor resultante dos 48% de fraude estimada não evitada pela Solução | R$ | 17.019,72 |
| **Total Custo Mensal Incremento Solução PIN** | **R$** | **2.449,38** |
| Custo Mensal (12 meses) Desenvolvimento Rodosoft | | 1960,38 |
| Custo Mensal SMS (Qtde Pedidos x R$ 0,02) | | 489,00 |
| Despesas Fraudes + Custo Solução | **R$** | **19.469,10** |
| **Resultado (Perda Estimada - Total Despesas c/ Solução** | | |
| Ganho Mensal | **R$** | **15.988,66** |
| Ganho Anual | **R$** | **191.863,86** |

Fonte: elaborado pelo autor.

Considerando então o resultado da proposta da **Solução PIN**, levantando despesas ainda existentes com o que a solução não consegue cobrir de prevenção, mais os custos da própria solução e os seus resultados de perdas evitadas, sugere-se um ganho mensal de aproximadamente R$ 16 mil e, para o ano, um total aproximado de R$ 192 mil de ganhos através da prevenção.

Assim como na solução KDT apresentada anteriormente, para esta alternativa também segue o custo de R$ 3 mil com o antifraude já existente, e por esse motivo não foi considerado nos cálculos, já que independe da tomada de decisão diante da alternativa.

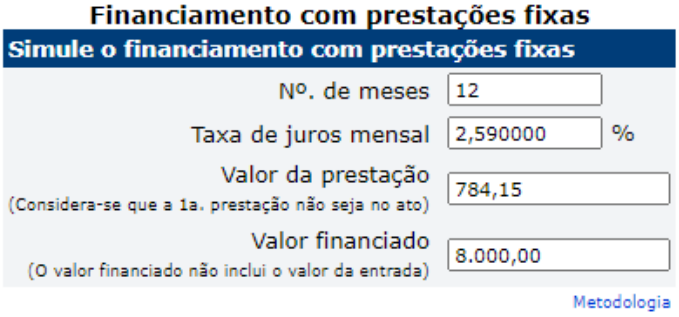
Por fim, a análise da alternativa com maior conceito tecnológico, atual e com os índices de estimativa de prevenção mais agressivos e resolutivos do mercado, a Solução Único. O nome da ferramenta retrata uma possibilidade: contar apenas com ela, a única ferramenta necessária para a solução com fraudes eletrônicas.

A proposta traz um conceito bastante atual e de relevante permanência no mercado, dadas as atualizações de identificações em smartphones e acessos a locais restritos exigindo o reconhecimento facial. Então é de conhecimento que a tecnologia agrada os usuários no atual momento.

Com a estimativa de resolução de 99% dos casos, o custo com fraudes eletrônicas da Viação praticamente se extinguiria, então podemos considerar que as perdas com fraudes se tornariam eventos bastante específicos e de pouca probabilidade.

Diante dos custos apresentados pela Solução Único, considerando em média 15000 transações financeiras mensais concluídas com sucesso no site da empresa, e a dissolução dos R$ 8 mil de adaptações do site ao período de um ano para fins comparativos com as demais propostas de solução, admitindo os mesmos critérios para a tomada de capital, apresentada na solução anterior, a uma taxa de juros de 2,59% a.m., determina-se a parcela de R$ 784,15 de custos fixos mensais durante 12 meses para as melhorias necessárias no site da empresa a fim de implantar a solução.

*Figura 2 - Financiamento com prestações fixas (Solução Único)*




O total desse financiamento de 12,00 parcelas de 784,15 reais é 9.409,80 reais, sendo 1.409,80 de juros.

Fonte: Calculadora do cidadão. Banco Central do Brasil.

Dessa forma, há um custo médio total mensal aproximado de R$ 14 mil, que, em comparação com a média estimada de perdas com fraudes mensais de 2023 no valor de R$ 35,5 mil, sugere um retorno mensal com perdas evitadas de fraudes no montante aproximado de R$ 21 mil, ou ainda, R$ 251,6 mil no total do primeiro ano de implementação.

*Tabela 5 - Finanças da Solução Único*

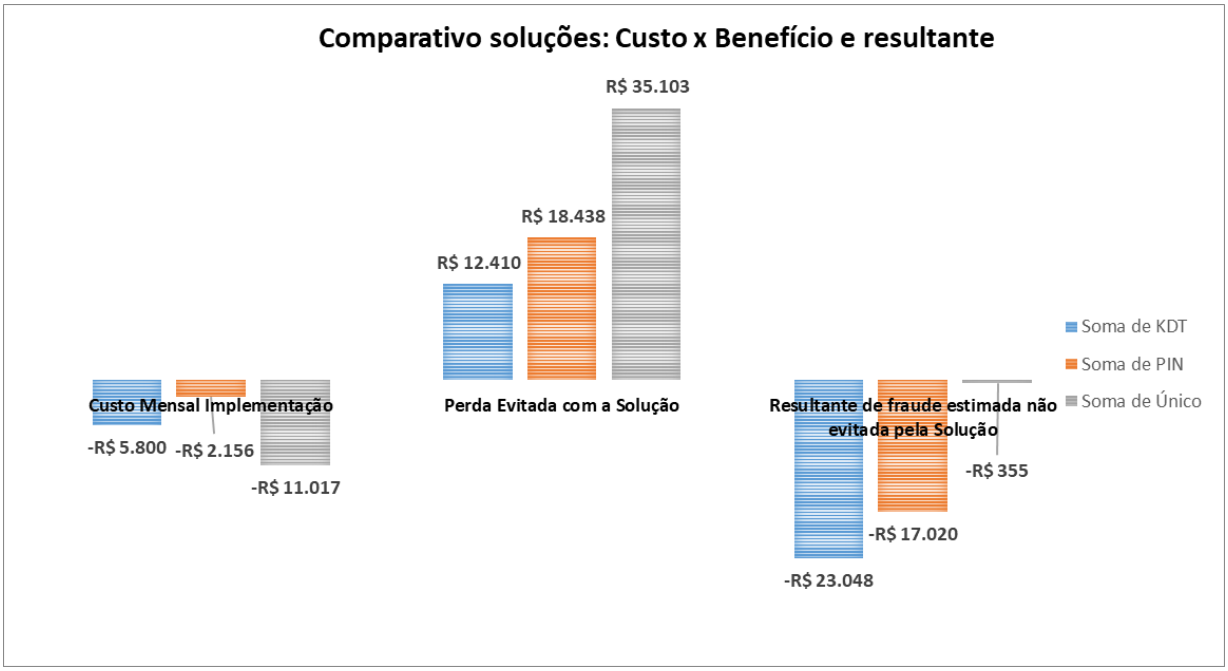
| Solução Único | | |
|---|---|---|
| *Custo Mensal Existente Fornecedor* | *R$* | *3.000,00* |
| Perda mensal com fraudes estimada para 2023 | R$ | 35.457,76 |
| % aproximado de impacto da Solução no combate a fraude sobre a perda estimada para 2023: **99%** | R$ | 35.103,18 |
| Valor resultante dos 1% de fraude estimada não evitada pela Solução | R$ | 354,58 |
| **Total Custo Mensal Incremento Solução Único** | R$ | 14.134,15 |
| Custo Mensal (12 meses) Desenvolvimento Rodosoft | | 784,15 |
| Custo Mensal ID Transações sucedidas (Qtde Pedidos x R$ 0,89) | | 13350,00 |
| Despesas Fraudes + Custo Solução | R$ | 11.488,73 |
| **Resultado (Perda Estimada - Total Despesas c/ Solução** | | |
| Ganho Mensal | R$ | 23.969,03 |
| Ganho Anual | R$ | 287.628,39 |

Fonte: elaborado pelo autor.

Para esta alternativa foi considerada a economia com o custo de R$ 3 mil do antifraude existente da Konduto, já que a proposta da Único substituiria os serviços fornecidos pelo atual antifraude.

Portanto, diante das teorias de investimentos apresentadas no capítulo anterior, considerando o principal direcionador que é o VPL, a Solução Único traz o melhor investimento financeiro considerando qualquer prazo de análise obtendo o maior retorno financeiro diante das opções de soluções apresentadas conforme pode ser observado no Gráfico 3.

*Gráfico 3 - Análise de Custo-Benefício entre Soluções*




Fonte: elaborado pelo autor.

Analisando o Gráfico 3, é possível identificar que a Solução Único exige o maior investimento (custo), mas em contrapartida propõe o maior retorno (Perda Evitada), considerada uma proporção de custo-benefício, ficando mais evidente a performance com maior retorno do investimento para a Solução Único, tornando-a a melhor alternativa de investimento para prevenção de fraudes com cartão de crédito no site da empresa.

Em complemento, a ferramenta pode elevar o nível de satisfação em segurança do cliente, também agregar tecnologia à plataforma deste segmento, dando sequência na busca de valor agregado por tecnológica na Viação representando o segmento de transporte rodoviário tendo, do ponto de vista tecnológico, a solução que está mais avançada e mais longe de ser tornar obsoleta quando comparada às demais alternativas.

## CONCLUSÃO

Diante do problema de fraudes com cartão de crédito no e-commerce encontrado na empresa foco do estudo, o objetivo do trabalho foi identificar alternativas de soluções que pudessem conter o avanço das fraudes e realizar prevenções com as perdas sob análise econômico-financeira.

O problema é resolvido através da implementação da Solução Único que apresentou a melhor e atual tecnologia agregada à solução e, mais importante, o melhor índice de prevenção gerando o maior retorno financeiro dado o investimento realizado.

Dentre as principais conclusões encontradas, destacam-se a necessidade de analisar e avaliar também maiores investimentos em termos de custos para se obter maiores retornos desses, e a importância de processos atualizados de tecnologia para o combate à fraude de cartão de crédito em compras on-line.

Dessa forma, os objetivos específicos propostos para identificar a solução do problema foram devidamente cumpridos analisando os índices de fraudes encontrados na empresa, conhecendo as limitações existentes na plataforma e-commerce e do atual fornecedor antifraude, buscando alternativas existentes no mercado para prevenção com fraudes de cartão de crédito, avaliando-as economicamente e sugerindo a implementação da solução mais adequada do ponto de vista econômico-financeiro à empresa foco do estudo.

**REFERÊNCIAS**

ARVIDSON, M.; CARLBARK, M.; **Intrusion detection systems - technologies, weaknesses and trends. Department of Electrical Engineering**, Linko ping University, 2003.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 6023: **Informação e documentação**: **Referências.** Rio de Janeiro. 2018. Disponível em: <www.abntcatalogo.com.br>. Acesso em 11 de outubro de 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 10520: 2002: **Informação e documentação: Citações em documentos: Apresentação.** Rio de Janeiro: ABNT, 2002. Disponível em: <www.abntcatalogo.com.br>. Acesso em 11 de janeiro de 2023.

BASTOS, Brena R.; GABRIEL, Julia B.; SANTOS, Daiane Rodrigues; **Vendas no varejo eletrônico (via internet) no Brasil antes e depois da popularização dos smartphones**. Curitiba: Brazilian Journals, 2018. Disponível em: <https://brazilianjournals.com/ojs/index.php/BASR/article/view/543>. Acesso 25 de julho de 2022.

BELLA, M. A.; ELOFF, J.H.P.; OLIVER, M.S.; **A fraud management system architecture for next-generation networks. Forensic science international**. v. 185, n. 1-3, p. 51-58, 2008.

BERK, J.; DEMARZO, P; **Finanças Empresariais**. Disponível em: <https://app.minhabiblioteca.com.br/reader/books/9788577804214>. Acesso em 04 de fevereiro de 2023.

BILLAS, Richard A. **Teoria Microeconômica**. Rio de Janeiro. Forense Universitária. 1973.

BOAVENTURA, Edivaldo M. **Metodologia da pesquisa: monografia, dissertação, tese.** 1 ed. – 4 reimp. São Paulo: Atlas, 2009.

BRAGA, Roberto. **Fundamentos e técnicas de administração financeira**. São Paulo: Atlas, 1989.

CALCULADORA DO CIDADÃO. **Simulador de financiamento com prestações fixas.** Disponível em: < https://www3.bcb.gov.br/CALCIDADAO/publico/exibirFormFinanciamentoPrestacoesFixas.do?method=exibirFormFinanciamentoPrestacoesFixas>. Acesso em 11 de março de 2023.

CANABARRO, Tom.; **5 coisas que você não sabia sobre cartão de crédito**. Disponível em: <https://blog.konduto.com/pt/2014/09/5-coisas-que-voce-nao-sabia-sobre-cartao-de-credito/> Acesso em 15 de Janeiro de 2023.

CURSO DE E-COMMERCE. **O Risco do ChargeBack nas vendas por cartão**. Disponível em: <https://www.cursodeecommerce.com.br/chargeback/>. Acesso em 25 de agosto de 2022.

**ENTENDENDO A ENGENHARIA SOCIAL**. In: WIKIPÉDIA: a enciclopédia livre. Wikimedia, 2022. Disponível em: <https://pt.wikipedia.org/wiki/Engenharia_social>. Acesso em 07 de setembro de 2022.

GHOSH, M. **Telecoms Fraud. Computer fraud and security** v. 2010 n. 7 p. 14-17. 2010.

GODOY, A. S. **Pesquisa qualitativa: tipos fundamentais**. Revista de Administração de empresas, v.35, n.3.

JACOBS, R. **Telecommunications Fraud, Dimension Data White Paper**. Dimension Data, 2005. Disponível em: < https://www.scss.tcd.ie/~htewari/bib_files/didata03.pdf>. Acesso em 29 de agosto de 2022.

KALAKOTA, Ravi. **E-business: estratégias para alcançar o sucesso no mundo digital.** Ravi Kalakota e Marcia Robinson; trad. Carlos Alberto Picanço de Carvalho. – 2 ed. Porto Alegre: Bookman, 2002.

KOTLER, Philip. 12ª edição. **Administração de Marketing.** São Paulo: Prentice Hall, 2006.

LAMARCA, Daniel S.; SARRIÉS, Gabriel A.; SILVA, Gabriel F.; **Machine learning e fraude de cartão de crédito: uma revisão bibliográfica sistemática.** Revista Intellectus, 2019. Disponível em: < http://www.revistaintellectus.com.br/artigos/77.942.pdf>. Acesso em: 15 de setembro de 2022.

MATIAS, José Pereira. **Manual de metodologia da pesquisa científica**. 3 ed. São Paulo: Atlas, 2012.

MILLER, Roger Leroy. Microeconomia: teoria, questões e aplicações. Rio de Janeiro. McGraw-Hill do Brasil, 1981.

MOREAU, Y.; PRENEEL, B.; BURGE, P.; SHAWE-TAYLOR, J.; STOERMANN, C.; COOKE, C. **Novel techniques for fraud detection in mobile telecommunication networks**. ACTS (Advanced Communications Technologies and Services). 1996.

OLIVEIRA, Silvio Luiz de. **Tratado de metodologia científica: projetos de pesquisa, TGI, TCC, Monografias, Dissertações e Teses**. São Paulo: Pioneira Thomson Learning, 2001.

PENÊDO, Joana. **A fraude no campo da informação: Engenharia Social, Big Data e a manipulação do usuário na rede**. Disponível em: <https://periodicos.ufmg.br/index.php/revistarbu/article/view/3110/pdf>. Universidade Federal de Minas Gerais - Periódicos, 2018. Acesso em 01 de setembro de 2022.

ROSS, Stephen A. et al. **Fundamentos de Administração Financeira**. 9. Ed. Porto Alegre: AMGH, 2013.

SMITH, Rob. **O mais completo guia sobre e-commerce**. Rob Smith, Mark Speaker, Mark Thompson; tradução Bazán. Tecnologia e Lingüística. São Paulo: Futura, 2000.

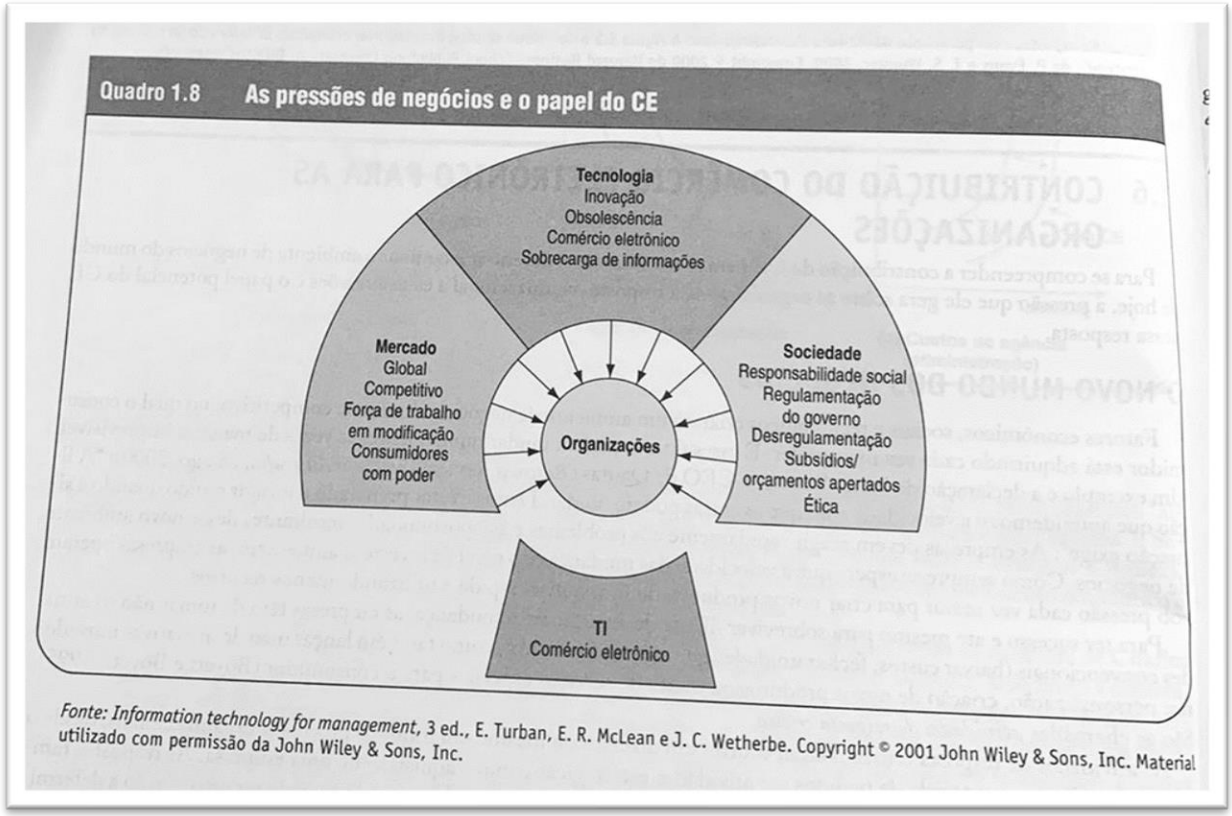
Taxas de Juros Banco Central do Brasil. Disponível em: < https://www.bcb.gov.br/estatisticas/txjuros>. Acesso em 12 de março de 2023.

TEIXEIRA, T. **Direito Digital e Processo Eletrônico**. São Paulo: Saraiva, 2020. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786555591484/>. Acesso em: 05 de julho de 2022.

TURBAN, Efraim. **Comércio eletrônico: estratégia e gestão**. Efraim Turban e David King; tradução Arlete Simille Marques. Revisão técnica Belmiro João, Erico Veras Marques. São Paulo: Prentice Hall, 2004.

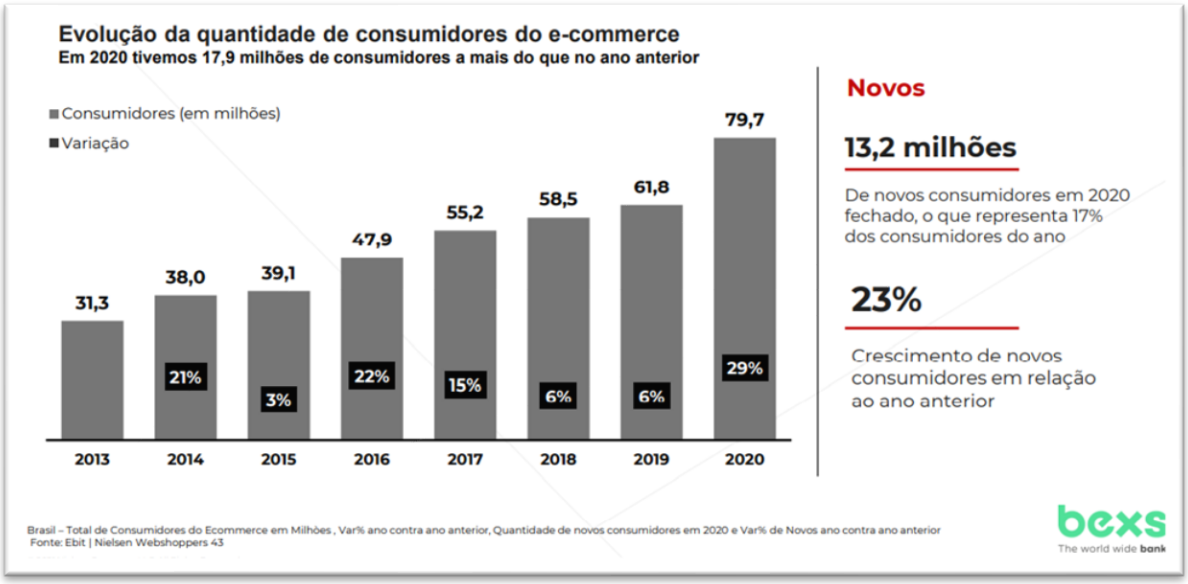
# ANEXOS

## ANEXO A - RELACIONAMENTO ENTRE PRESSÕES DE NEGÓCIOS

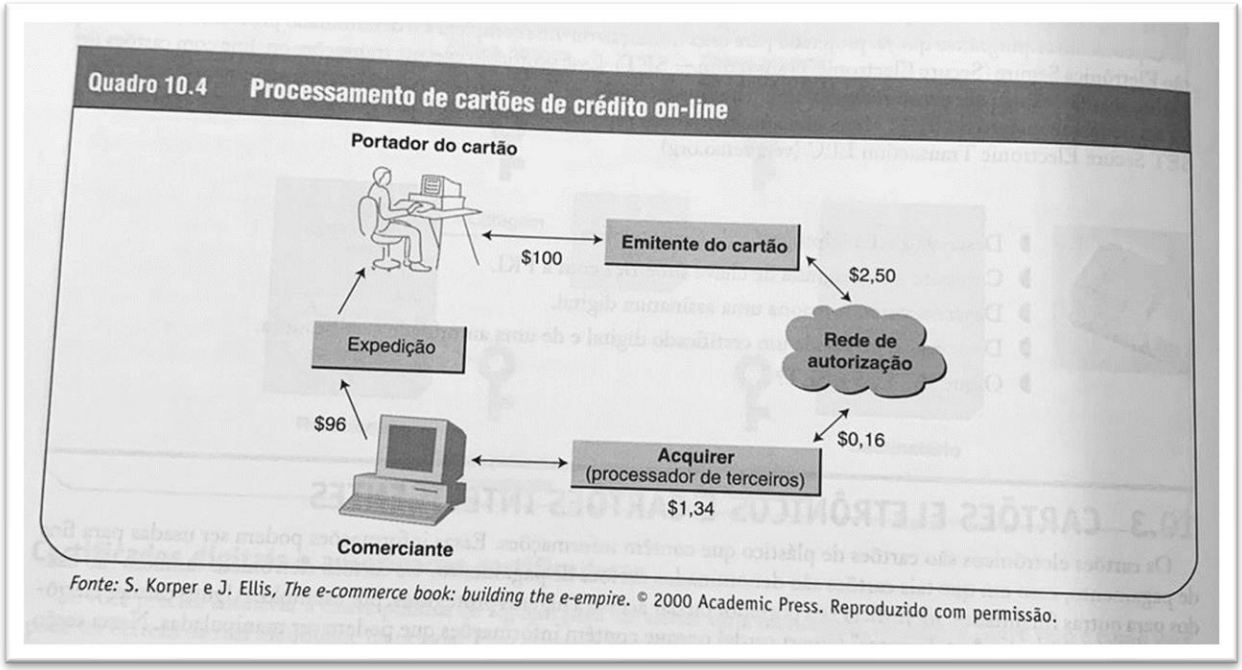



*Fonte: Information technology for management*, 3 ed., E. Turban, E. R. McLean e J. C. Wetherbe. Copyright © 2001 John Wiley & Sons, Inc. Material utilizado com permissão da John Wiley & Sons, Inc.

## ANEXO B – GRÁFICO NOVOS USUÁRIOS EM E-COMMERCES NO PAÍS



# ANEXO C – FLUXO DO PROCESSAMENTO DE CARTÕES DE CRÉDITO




*Fonte:* S. Korper e J. Ellis, *The e-commerce book: building the e-empire.* © 2000 Academic Press. Reproduzido com permissão.