CENTRO UNIVERSITÁRIO DO ESTADO DO PARÁ - CESUPA
ESCOLA DE NEGÓCIOS, TECNOLOGIA E INOVAÇÃO – ARGO
BACHARELADO EM ENGENHARIA DE COMPUTAÇÃO

LUCAS CARVALHO PEREIRA
YASMIN ADLA DA COSTA BITAR

ESTRATÉGIAS INTELIGENTES DE SEGURANÇA PARA TRANSAÇÃO COM CARTÃO

BELÉM
2018

LUCAS CARVALHO PEREIRA
YASMIN ADLA DA COSTA BITAR

ESTRATÉGIAS INTELIGENTES DE SEGURANÇA PARA TRANSAÇÃO COM CARTÃO

Trabalho de Curso na modalidade Monografia, apresentado como requisito parcial para obtenção do grau em Bacharelado em Engenharia de Computação do Centro Universitário do Estado do Pará – CESUPA, sob orientação da Professora Msc. Polyana Fonseca Nascimento e co-orientação do Esp. Eudes Danilo Mendonça.

BELÉM

2018

Dados Internacionais de Catalogação-na-publicação (CIP)

Biblioteca do Cesupa, Belém - PA

Pereira, Lucas Carvalho.

Estratégias inteligentes de segurança para transação com cartão / Lucas Carvalho Pereira, Yasmin Adla da Costa Bitar; orientação de Polyana Fonseca Nascimento, coorientação de Eudes Danilo Mendonça, 2018.

Trabalho de Conclusão de Curso (Bacharelado em Engenharia de Computação) – Centro Universitário do Pará, Belém, 2018.

1. Criptografia (Computação). 2. Software – Desenvolvimento. 3. Segurança de dados. I. Bitar, Yasmin Adla da Costa. II. Nascimento, Polyana Fonseca (orient.). III. Mendonça, Eudes Danilo (coorient.). IV. Título.

CDD. 23º ed. 005.8

LUCAS CARVALHO PEREIRA
YASMIN ADLA DA COSTA BITAR

ESTRATÉGIAS INTELIGENTES DE SEGURANÇA PARA TRANSAÇÃO COM CARTÃO

Trabalho de Curso apresentado na modalidade monografia, apresentado como requisito parcial para obtenção do grau em Bacharelado em Engenharia de Computação do Centro Universitário do Estado do Pará – CESUPA.

Data da Defesa: 15/06/2018

Banca Examinadora:

_____

Orientadora Prof. Msc. Polyana Fonseca Nascimento - CESUPA

_____

Co-orientador Esp. Eudes Danilo Mendonça – CESUPA

_____

Prof. Dr. Otávio Noura Teixeira – UFPA

BELÉM

2018

Dedicamos esta, bem como todas as nossas demais conquistas, aos nossos amados pais. Agradecemos ao mundo por mudar as coisas, por nunca fazê-las serem da mesma forma, pois assim não teríamos o que pesquisar, o que descobrir e o que fazer, pois através disto conseguimos concluir a nossa monografia.

AGRADECIMENTOS

À minha dupla, Lucas Pereira, pelas horas de dificuldade e de alegria por estar do meu lado nessas horas, com apoio e dedicação a esse trabalho.

Aos meus pais, Katia Costa e Miguel Bitar, pelo amor, incentivo e apoio incondicional.

À minha irmã, Yameh Bitar, pelas revisões e palavras difíceis.

À minha dupla, Yasmin Bitar, que em todo momento tentou ficar firme com o pouco tempo que tivemos para escrever. Por ter aguentado este processo comigo. E por ser a pessoa maravilhosa que é.

Agradeço à minha mãe Maria do Carmo Carvalho, heroína que me deu apoio, incentivo nas horas difíceis, de desânimo e de cansaço. Ao meu pai que, apesar de todas as dificuldades, me fortaleceu e que para mim foi muito importante.

À mulher incrível que está ao meu lado, Jenniffer Assunção, a qual tem me ajudado tanto na elaboração - escrevendo, corrigindo e rindo - quanto na minha vida - incentivando e apoiando nas decisões tomadas.

A esta universidade, seu corpo docente, direção e administração os quais oportunizaram a janela que hoje vislumbramos um horizonte superior, eivado pela acendrada confiança no mérito e ética aqui presentes.

À nossa querida orientadora, Polyana Nascimento, e ao co-orientador, Eudes Danilo, pelo auxílio na elaboração deste trabalho e pelos comentários maravilhosos durante o texto os quais fizeram com que ganhássemos mais ânimo para continuar escrevendo, sem esquecer/deixar de rir dos nossos próprios erros.

Ao professor Otávio Noura, que idealizou este trabalho e, nos momentos em que pôde, nos ajudou a desenvolvê-lo.

Aos funcionários responsáveis pela biblioteca - principalmente, a Raquel - que nos ajudaram a fazer as ‘poucas’ referências bibliográficas e tiveram muita paciência, pois foi o semestre em que mais passamos na biblioteca.

A todos que, direta ou indiretamente, fizeram parte da nossa formação, o nosso muito obrigado.

Se você conhece o inimigo e conhece a si mesmo, não precisa temer o resultado de cem batalhas. Se você se conhece, mas não conhece o inimigo, para cada vitória ganha sofrerá também uma derrota. Se você não conhece nem o inimigo nem a si mesmo, perderá todas as batalhas.

Sun Tzu – A Arte da Guerra

RESUMO

Com o passar dos anos, percebeu-se de forma consistente a evolução da tecnologia na sociedade e nas nossas vidas. Um dos ramos que cresceu com o tempo, foi o comercio com novas formas de pagamentos (cartões de crédito e débito, cheques entre outros). Mas, esse avanço, consequentemente, evidência pontos positivos e negativos. Uns dos pontos negativos que podemos citar é aparição dos *hackers*, que são pessoas que observam brechas em sistemas e tiram aproveito disso por vários motivos, sendo eles realização pessoal ou retorno financeiro. Com uso do cartão cada vez mais presente nos dias atuais, como no *smartphone*, por exemplo, é necessário que a segurança acompanhe a passos largos essa evolução, uma vez que a clonagem e outras formas de ataques também evoluem. Nesse trabalho, busca-se desenvolver uma metodologia de sistema e *hardware,* que visem o aumento da segurança para transações com cartões de crédito e débito e minimiza problemas, como, por exemplo a clonagem. Estudaremos a criptografia e a Inteligência Artificial (Reconhecimento de Padrões) em um protocolo combinado de autenticação para aumento da segurança. A criptografia será utilizada para proteger os dados do cliente no caminho que percorre. E o Reconhecimento de Padrões consiste em um conhecimento utilizado para classificar e reconhecer algumas informações recebidas e enviadas da máquina de cartão de crédito, como por exemplo, impressão digital, íris e voz.

Palavras-chave: Criptografia. Inteligência Artificial. Reconhecimento de Padrões. Cartão de Crédito.

ABSTRACT

As time goes by, we realize that technology's evolution is very consistent in society and our life. One of the branches that has grown in this period was in the commercial area, with new payment options (like credit card, debit card, internet banking, among other choices). However, this progress has positive and negative points. One of the negative points one could mention are hackers: people that observe and use system's weakness for self-benefit. There are many reasons why hackers do it, for instance, for self-realization and financial return. Credit card utilization is getting more frequent each day due to commercial transactions by mobile devices. Information security needs to increase in order to prevent credit card cloning and other forms of cyber-attacks. This study aims to build a methodology using hardware and software. The purpose is to increase security in credit and debit card transactions, minimizing infrastructure related problems, like credit card cloning. Cryptography transactions and artificial intelligence (Pattern Recognitions) applied to authentication multi protocols will be studied. We will also look at improving authentication to increase the security. Cryptography will be used to protect the client's data along the way. Pattern recognition is the knowledge used to classify and recognize in and out information in a credit card machine, like digital impression, iris and voice patterns.

Keywords: Cryptography. Artificial intelligence. Pattern Recognition. Credit card.

LISTA DE FIGURAS

LISTA DE QUADRO

LISTA DE SIGLAS

3DES	-	*Triple*DES
ABECS	-	Associação Brasileira das Empresas de Cartão de Crédito e Serviços
ABIPAG	-	Associação Brasileira de Instituições de Pagamentos
ACSC	-	*Austrilian Cyber Segurity Centre*
APT	-	*Advanced Persistent Threat*
ATM	-	*Automatic Teller Machine*
AVS	-	*Address Verification Service*
BD	-	Banco de Dados
BIN	-	*Bank Identification Number*
C&C	-	Comando e Controle
CAV	-	*Card Authentication Value* - Valor de Autenticação do Cartão
CID	-	*Card Identification Number* - Número de Identificação de Cartão
CSC	-	*Card Security Code* - Código de Segurança do Cartão
CVC	-	Código de Verificação do Cartão ou *Card Verification Code*
CVV	-	*Card Verification Value* - Valor de Verificação de Cartão
DES	-	*Data Encryption Standard*
DM	-	*Data Mining*
EMV	-	Europay, MasterCard e Visa
FIPS	-	Federal Information Processing Standards - Padrão Federal dos Estados Unidos
FTC	-	*Federal Trade Commission*
HTTP	-	*Hypertext Transfer Protocol*
IA	-	Inteligência Artificial
IBM	-	*International Business Machines*
IEC	-	*International Electrotechnical Commission*
IIN	-	*Issuer Identification Number*
IP	-	*Internet Protocol*
ISO	-	*International Organization for Standardization*

MAC - *Media Access Control*

MD5 - *Message-Digest algorithm* 5

MIT - *Massachusetts Institute of Technology*

ML - *Machine Learning*

NBS - *National Bureau of Standards*

NIST - *National Institute of Standards and Technology*

NSA - *National Security Agency*

P2P - Ponto-a-Ponto

PAN CVC - *Primary Account Number Card Validation Code* - Número de Conta Principal Código de Validação do Cartão

PAN - *Primary Acount Number*

PCI DSS - *Payment Card Industry Data Security Standard*

PDV - Ponto de Venda

PIN - *Personal Identification Number*

POO - *Point of Outdoor*

POS - *Point of Sale*

RC - *Ron's Code* ou *Rivest Cipher*

RFC - *Request of Comments*

RNA - Rede Neural Artificial

RP - Reconhecimento de Padrão

RSA - River, Shmair e Andleman

SHA - *Secure Hash Algorithm*

SI - Sistema da Informação

SSL - *Secure Sockets Layer*

TCP - *Transmission Control Protocol*

TEF - Transferência Eletrônica de Fundos

TLS - *Transport Layer Security*

URL - *Uniform Resource Locator*

VPN - *Virtual Private Network*

SUMÁRIO

1 INTRODUÇÃO

Nesse artigo técnico com a finalidade de trabalho de conclusão do curso, trataremos sobre a segurança nos meios de pagamento eletrônico, mais especificamente dos cartões de crédito/débito, a fim de evitar fraudes. Utilizando conceitos de criptografia, inteligência artificial e algumas possíveis aplicações para as empresas do produto que será objeto de estudo neste presente trabalho teremos a finalidade de garantir a segurança na utilização dos produtos, que abrange os envolvidos nas transações de crédito/débito eletrônicos, incluindo cliente e loja, além dos parceiros da cadeia de transações. Já que o cliente pode ter seus dados fraudados e o estabelecimento perde a credibilidade com o seu consumidor, pelos eventos indevidos. Assim, com o avanço da tecnologia, quando o usuário realizar uma transação, o local ao oferecer seu equipamento, disponibilizará o sistema (*software*/*hardware*) para que o usuário tenha segurança, ocasionando confiabilidade no local.

1.1 JUSTIFICATIVA

Hodiernamente, a segurança é um dos requisitos mais importantes numa transação, seja no que tange aos dados empresariais quanto aos dados pessoais. No decorrer dos anos, também evoluiu a forma de acessar esses dados para finalidades ilegais, umas das formas que podemos exemplificar roubo de dados é a fraude. Devido a isto, nesse trabalho criou-se método de prevenção do mesmo, utilizando-se da Inteligência Artificial (IA) aliado a conceitos de Redes de Computadores como solução.

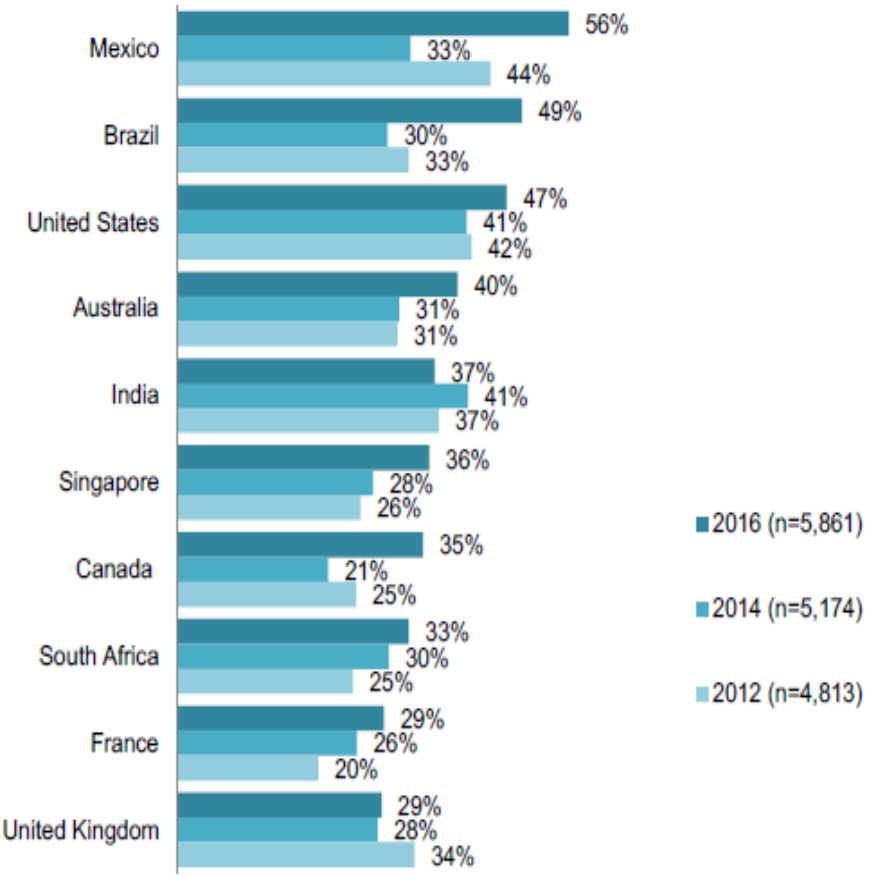
> De todos os titulares de cartão – débito, crédito e pré-pago – 30% já sofreram fraude nessa forma de pagamento nos últimos cincos anos, uma parte significativa de titulares de cartão. Em 2016, 17% dos titulares de débito e de crédito citam ter experimentado fraudes múltiplas vezes nos últimos cincos anos, em comparação com 13% em 2014 (KNIEFF, 2016, p.4, tradução nossa).

No decorrer dos anos, a tecnologia avançou e vieram tanto ponto positivo quanto negativo. Um ramo que evoluiu foi o do comércio, aprova disso é nas diversas formas de pagamentos, por exemplo: dinheiro, cartão de crédito/débito e cheque. Porém existem pessoas que viram como uma oportunidade de ganhar em cima disso de forma ilícita.

> Existem muitas maneiras de fraudar um cartão, incluindo violação de dados, cartões perdidos e/ou roubados quanto por meio da engenharia social, de ataques de *phishing* e também da combinação dessas atividades. Fraude em todo o mundo, variam em muito em diferentes regiões e países (KNIEFF, 2016, p. 7, tradução nossa).

Foram realizados alguns estudos, no período do primeiro trimestre do ano 2014, e a porcentagem a respeito da fraude aumentaram em alguns países, como observa-se na figura 1. As maiores taxas predominam nos países, respectivamente, México (56%, em 2016), Brasil (49%, em 2016) e Estados Unidos (47%, em 2016).

Figura 1 - Taxa de fraudes em diversos países nos últimos 5 anos

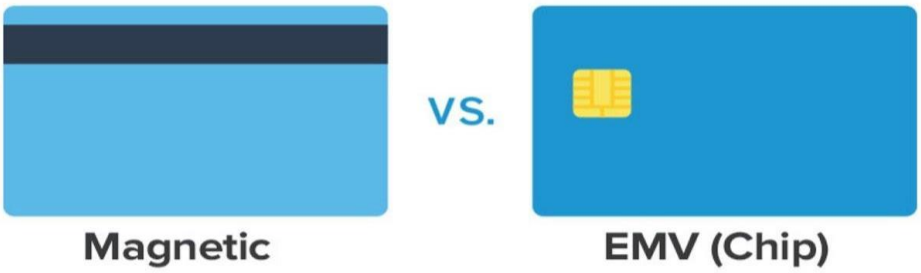


Fonte: Adaptado de Knieff (2016, p. 8)

O México passou pelo processo de implementação do cartão EMV (Europay, MasterCard e Visa), em 2002 (*ACCEO TENDER RETAIL TEAM*, 2017) com desafios tanto na parte do emissor quanto na parte do comerciante. Nos Estados Unidos, tal aumento é explicado por dois fatores: possuir uma grande parcela dos consumidores que utilizam o cartão como método de pagamento e uma adoção lenta do EMV (figura 2) em compras online. Diante de um cenário similar, no Brasil, o *e-commerce* é um dos grandes mercados, porém não possui um eficiente controle para a prevenção de fraudes, somado.

> As taxas de fraudes de cartão de crédito no estudo de 2016 mostram que os consumidores em todo o mundo ainda experimentam fraude de cartão, apesar da implementação de soluções de análise de fraudes e EMV em muitos países. Não há escassez de maneiras pelas quais os criminosos podem tirar proveito dos dados do cartão para cometer fraudes (KNIEFF, 2016, p. 9, tradução nossa).

Figura 2 - A diferença física entre cartão magnético e o EMV

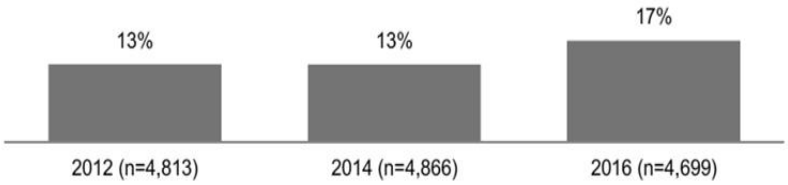


Fonte: Canal no Youtube *Follow The Coin* (2015, online)

Como exposto na figura 3, houve um aumento de clientes que tiveram experiência de fraude tanto com cartão do tipo crédito quanto de débito, nos últimos cinco anos baseado no documento: 2016 *Global Consumer Card Fraud: Where Card Is Coming From* (KNIEFF, 2016). E 17% dos consumidores globais, em 2016, já tiveram mais de uma experiência com fraude, nos últimos cinco anos.

> A riqueza de detalhes de pagamento roubados disponíveis por meio de violações de dados e golpes de *phishing* significa que todos são um alvo e podem ter várias incidências de fraude com cartões diferentes. Como os criminosos tentam maximizar a captura de um único cartão, a fraude também pode ocorrer várias vezes em um único cartão (KNIEFF, 2016, p. 13, tradução nossa).

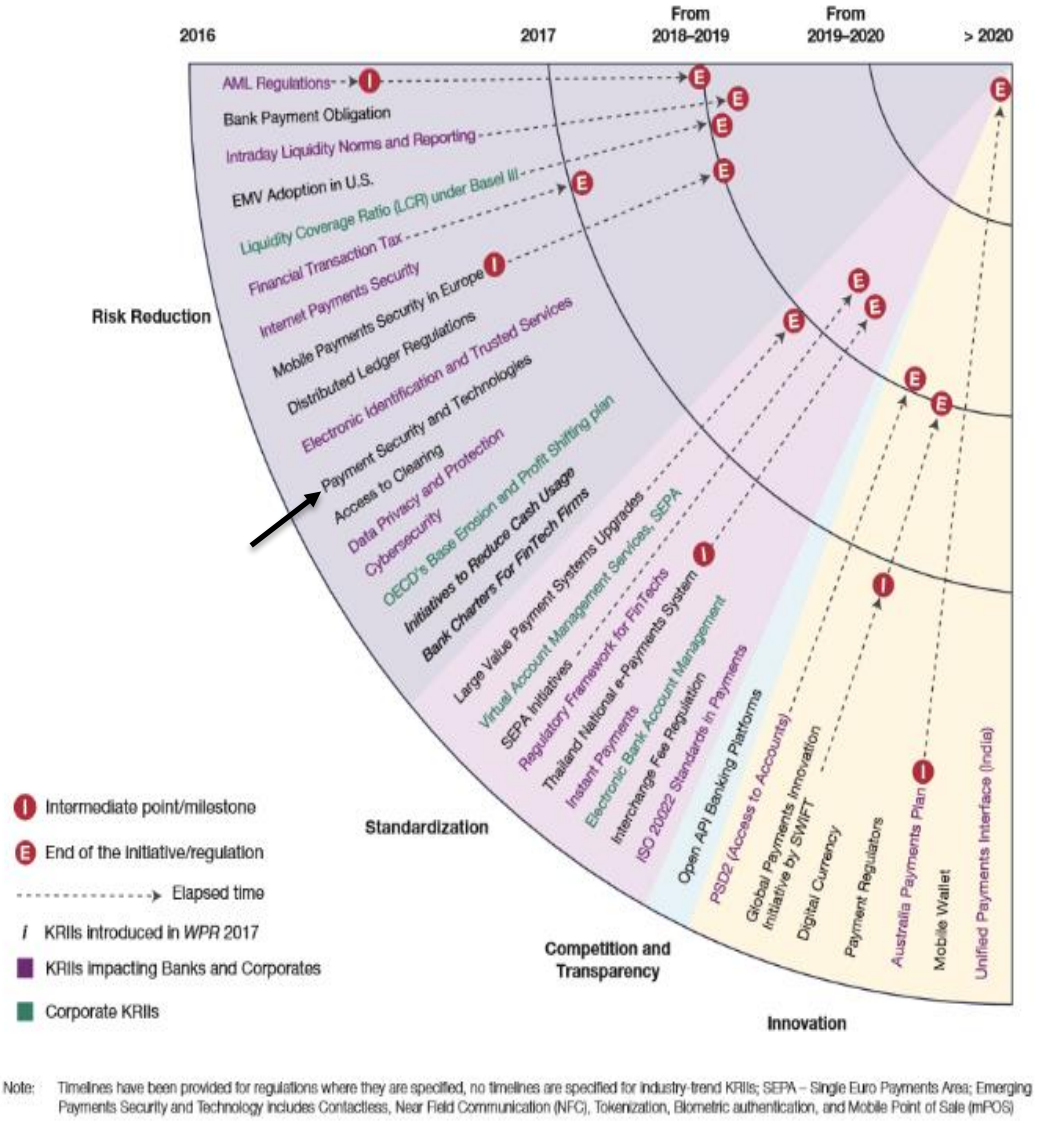
Figura 3 - Índice, em porcentagem, de incidentes de cartão de crédito ou débito, últimos 5 anos



Fonte: Knieff (2016, p.13)

Na figura 4, destaca-se o item *payment security and technologies* (segurança e tecnologias de pagamento), como aponta a seta preta, que não apresenta um ponto intermediário/marco (representado pela letra I) e nem uma a iniciativa/regulamento (representado pela letra E), indicando que, embora seja um problema recorrente na área, não tem havido investimentos em regulamentações ou transformações significativas. Dessa forma, torna-se importante a apresentação de novas propostas, metodologias e/ou protocolos de pagamentos que aumentem a segurança e confiabilidade dos dados, e este é o foco deste trabalho.

Figura 4 - Principais iniciativas regulatórias e setoriais agrupado pelos principais objetivos dos reguladores, 2017



Note: Timelines have been provided for regulations where they are specified, no timelines are specified for industry-trend KRIIs; SEPA – Single Euro Payments Area; Emerging Payments Security and Technology includes Contactless, Near Field Communication (NFC), Tokenization, Biometric authentication, and Mobile Point of Sale (mPOS)

Fonte: *World Payments Report* 2017 (2017, p. 20)

1.2 OBJETIVO GERAL

Desenvolver um método de autenticação do portador do cartão e proteção do processo, juntamente com Inteligência Artificial, com o propósito de aperfeiçoar a compra provida do cartão de crédito/débito, em relação à elaboração de uma metodologia para um *hardware* e *software*.

1.3 OBJETIVO ESPECÍFICO

a. Estudar métodos de reconhecimentos de padrões e autenticações nos dias atuais;
b. Compreender tendências de segurança;
c. Analisar documentos de riscos globais de segurança;
d. Analisar o funcionamento da máquina de cartão de crédito e débito;

e. Entender como a inteligência artificial pode ajudar na criptografia de dados utilizando o Reconhecimento de Padrões;
f. Propor uma metodologia mais adequada para aumentar a segurança;
g. Propor um *hardware* que faça as combinações citadas anteriormente.

1.4 METODOLOGIA

Esse trabalho é desenvolvido a partir do estudo do problema decorrente do uso de cartão de crédito, a fraude, não por falta de conhecimento técnico, mas devido ao avanço da tecnologia e conhecimento dos criminosos. Partindo do princípio que é necessário proporcionar maior segurança aos usuários, assim com uma base de conhecimento sobre rede de computadores, inteligência artificial e até mesmo sobre cartão de crédito, busca-se reduzir esse evento.

No que diz respeito a rede de computadores, a pesquisa está em alguns temas relacionados a criptografia, por exemplo, os tipos de chaves de criptografia, pois será utilizado para manter seguro os dados que passam pelo processo do cartão de crédito e ter sigilo dos dados. O autor utilizado Willian Stallings, responsável por alguns livros como “Criptografia e segurança de redes: princípios e práticas” (2008, 4° Edição) e também a obra atualizada para a 6° versão (2015).

E inteligência artificial, dissertando sobre seus conceitos e alguns métodos como redes neurais tratado no livro “Redes neurais: princípios e práticas” de Simon Haykin, para então falar sobre o reconhecimento de padrões, como uma maneira mais eficaz de autenticar utilizando as características biométricas do ser humano para uma maior segurança.

Para auxílio no conhecimento de cartões de forma geral, com base em um levantamento de documentos de segurança, como por exemplo, *The Global Risks Report* 2018 e 2016 *Global Consumer Card Fraud: Where Card Is Coming From*. E foi estudado em algumas informações adquiridas pela Associação Brasileira das Empresas de Cartão de Crédito e Serviços (ABECS) e Associação Brasileira de Instituições de Pagamentos (ABIPAG).

Partindo do pressuposto que há algo implementado e dos conhecimentos adquiridos para a melhoria de todo o processo desde o ato de inserir o cartão na máquina até a aprovação da transação, assim fazemos a verificação de cada etapa e analisando cada vulnerabilidade. A problemática escolhida então será estudada com assuntos já mencionados, para que a partir dessas informações, uma nova sugestão seja criada, tendo em base o que já está em funcionamento no mercado.

1.5 ORGANIZAÇÃO DO TRABALHO

O capitulo 1 é apresenta o contexto, objetivos, motivação e a justificativa para este documento. Perpassando para o capítulo 2 que trata de segurança nos dias atuais, visando a atuais formas de ataques como, *cyberattack* e *data fraud and theft*, pois apresenta um aumento com o avanço da tecnologia. No Capítulo 3 é apresentado brevemente a definição do mesmo e é explanado criptografia simétrica e assimétrica. E com a evolução da criptografia é apresentado aplicações nos dias atuais que utilizam com conceitos dos protocolos SSL e TLS.

Apresenta-se a definição de Inteligência Artificial, no capitulo 4, assim como alguns métodos como o *data mining*, *machine learning*, redes neurais e logica nebulosa. Continuando esta linha, o capítulo 5 inicia com a definição de Reconhecimento de Padrão e como ela é realizada, logo a seguir específica o reconhecimento biométrico (impressão digital, íris e voz), tal qual o porquê usa-la ou não. O capítulo 6 trata do funcionamento da máquina do cartão, bem como seus agentes, tipos de cartão, tipos de máquina mais utilizadas. Também é apresentado sua regulamentação utilizando o padrão PCI DSS. Assim como são expostos o mercado brasileiro nessa modalidade de pagamento e as fraudes no país.

Capítulo 7 complementa o estudo, e demonstra as tendências dos maiores Bancos do mundo em relação ao reconhecimento biométrico. Para o capítulo 8 é demonstrado uma nova metodologia para a realização da autenticação do usuário e segurança da transação. Para finalizar o capítulo 9, com base no referencial teórico, conseguiu-se almejar um novo método de autenticação como proposto.

2 SEGURANÇA

2.1 SEGURANÇA NO DECORRER DOS ANOS

No decorrer dos anos, observou-se que cada vez mais precisa-se de segurança no ambiente virtual, independe da atividade realizada do usuário. Algumas medidas são sugeridas como, por exemplo: manter o antivírus atualizado, tomar cuidado com anexos com fontes desconhecidas em e-mails, baixar arquivos em URL's (*Uniform Resource Locator*) desconhecidas, entre outras. Além de medidas de segurança que devemos tomar, as vulnerabilidades de sistemas também são uma porta de entrada para cibercriminosos e *hackers*.

> Todo software pode ter falhas e defeitos e um cibercriminoso só precisa encontrar uma nova vulnerabilidade não revelada (*zero-day*) ou usar uma das muitas vulnerabilidades já divulgadas para criar um *exploit*[1]preparado para comprometer uma máquina ou dispositivo. Isso aconteceu com as principais ameaças em 2017, incluindo *WannaCry, Petya*/*Not-Petya* e a violação da *Equifax* (COSTA, 2018, online).

Entretanto, algumas áreas são importantes proteger devido sua responsabilidade que emprega para sociedade, como um Banco ou um hospital. Nelas, há dados de extremo valor devido possuir informações de clientes ou pacientes, segundo o exemplo citado. Mas existem ferramentas para proteger esses dados e informações e o conjunto delas ajuda a proteger os usuários.

A importância de proteger a parte da infraestrutura da rede também é imprescindível, segundo William Stallings. O começo, meio e fim do caminho percorrido pela informação é vulnerável a riscos.

> O relatório *Security in the internet architecture* (RFC 1636) estabelecia o consenso geral de que a Internet precisa de mais e melhor segurança, e identificava as principais áreas para mecanismos de segurança. Entre estas estavam a necessidade de proteger a infraestrutura da rede contra monitoração e o controle não autorizados do tráfego da rede, e a necessidade de proteger o tráfego de usuário final para usuário final usando mecanismos de autenticação e de criptografia (STALLINGS,2008, p.4).

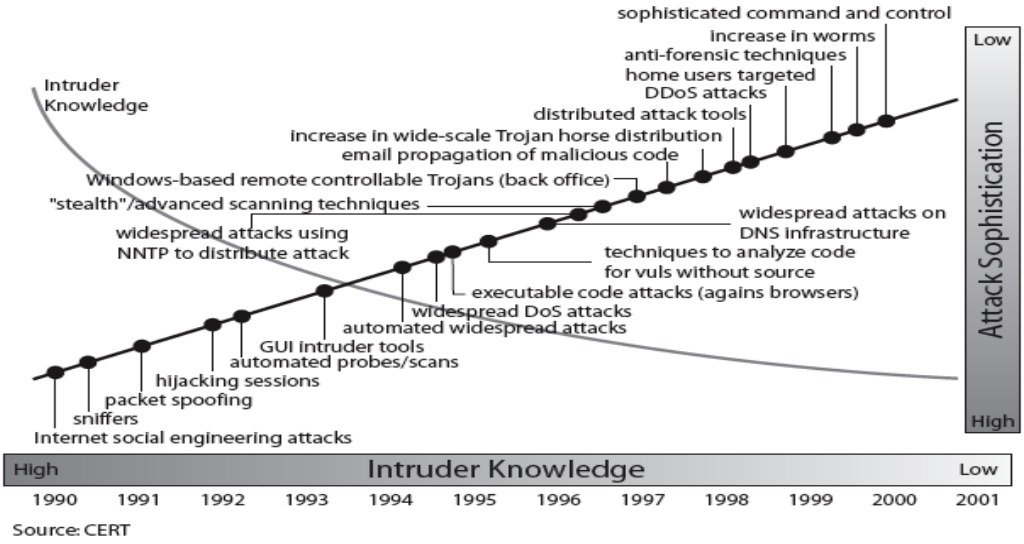
Podemos ver na figura 5 um avanço dos ataques, na Internet, com o decorrer dos anos. Observa-se que os ataques aumentaram, mas o conhecimento exigido diminui devido encontramos todo tipo de conteúdo na *common web*[2]. Com o passar dos anos, a Internet tornou-se mais conectada, assim os danos causam maior impacto.

---

[1] ***Exploit***: "É um aparelho ou método do qual um agressor se aproveita da vulnerabilidade para atingir qualquer tipo de sistema de *hardware* ou *software*" (KASPERSKY *LAB DAILY*, 2013, online).

[2] ***Commom Web:*** "É composta por sites como Google, Facebook, Twitter, Yahoo!" (SITE *GEEK STORM*, 2015, online), YouTube. É de fácil acesso com navegadores como *FireFox* ou *Google Chorme*, por exemplo.

Figura 5 - Tendências nos ataques e conhecimentos do intruso



Fonte: Stallings (2008, p. 5)

2.2 ATUAIS FORMAS DE ATAQUE NA INTERNET

Existem diversas formas de ataque na Internet nos dias atuais, que variam entre o alvo principal e a maneira de ataque, como exemplo, o *cyberattack* e *data fraud and theft*. Os alvos podem ser dados, pessoas, organizações entre outros e maneiras podem ser através de e-mail ou vulnerabilidades em sistemas, por exemplo.

2.2.1 *Cyberattack*

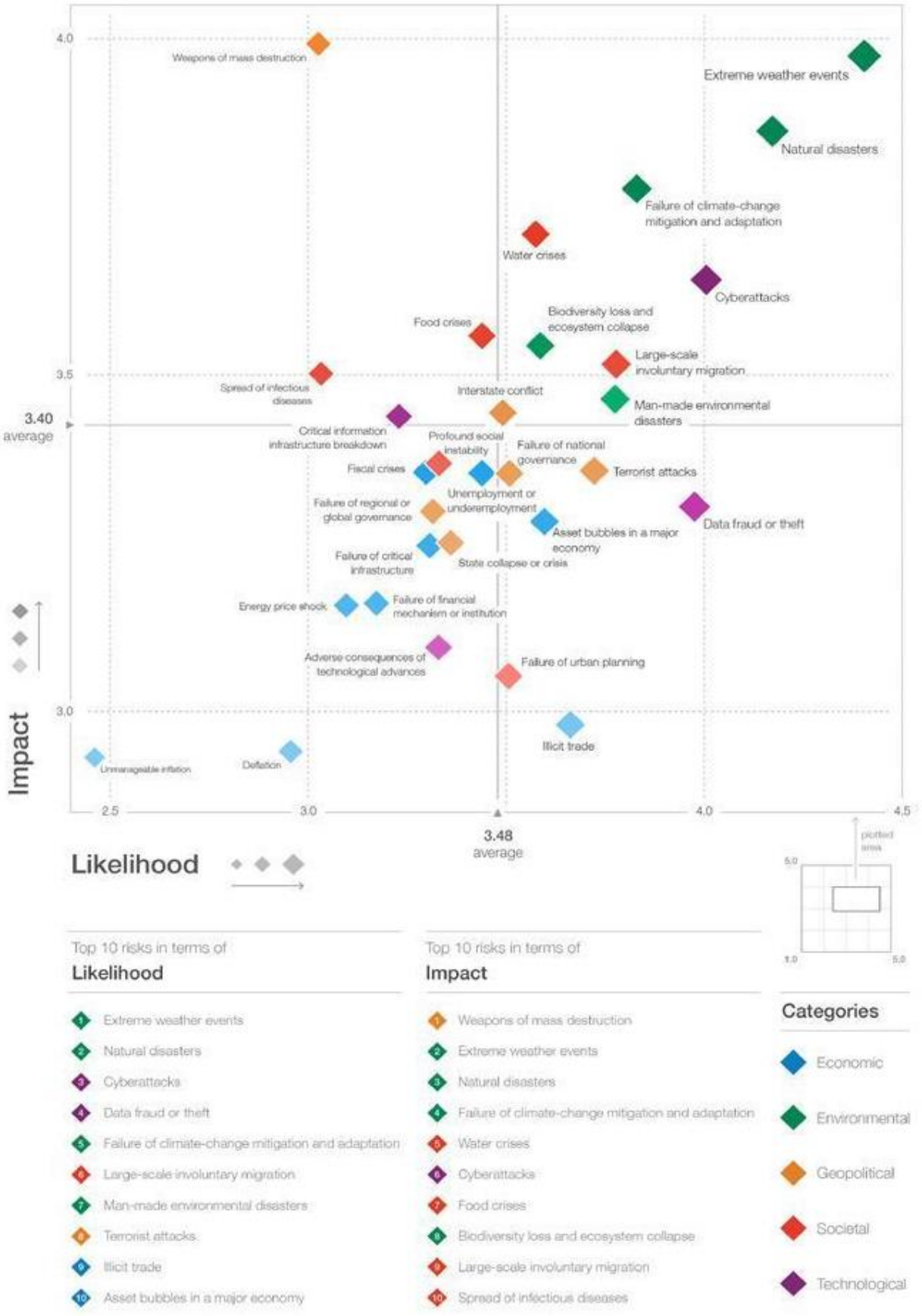
A definição de *cyberattack*, segundo o Governo da Austrália, no documento ACSC (*Austrilian Cyber Segurity Centre*) *Threat Report 2017*:

> Um ato deliberado através do ciberespaço para manipular, interromper, negar, degradar ou destruir computadores ou redes, ou a informação presente neles, com o efeito de comprometer seriamente a segurança nacional, estabilidade ou prosperidade (ACSC, 2017, p. 28, tradução nossa).

A pesquisa mostra alguns estudos em forma de gráfico: impacto *vs* probabilidade, como na figura 6, mostrando que *cyberattack* (em roxo) é um dos eventos que causa maior impacto com alta probabilidade de ocorrência, perdendo apenas para desastres naturais e eventos climáticos (em verde).

> Ataques contra empresas quase que dobraram em cinco anos, e incidentes que antes seriam considerados excepcionais estão se tornando cada vez mais comuns. O impacto financeiro de falhas na cibersegurança está crescendo e alguns dos maiores custos de 2017 estão relacionados com ataques pedindo resgate, que representaram 64% de todos os e-mails mal-intencionados. Exemplos notáveis incluem o ataque *WannaCry* – que afetou 300 mil computadores em 150 países – e *NotPetya*, que causou perdas trimestrais de US$ 300 milhões para uma série de empresas afetadas (*WORLD ECONOMIC FORUM*, 2018, p. 2).

Figura 6 - *The Global Risks Landscape 2018*



Fonte: Martin (2018, online)

Existem alguns tipos comuns e bem-sucedidos de *cyberattacks*, segundo Grimes (2017), como: *malware*[3] de engenharia social, ataque de *phishing* para senhas, *softwares* com vulnerabilidades, ameaças de mídia social e ameaça persistente avançada (APT - *Advanced Persistent Threat*).

Grimes (2017) afirma que o *malware* de engenharia social é uma forma de ataque ao usuário que induz a executar um programa com algum vírus em um site que visita frequentemente, são liderados pelo uso do método de *ransomware*[4] de criptografia de dados. "É uma forma muito usada por cibercriminosos para descobrir informações pessoais de usuários – como senhas ou dados bancários – sem precisar explorar falhas de segurança de sistemas" (KURTS, 2016, online).

"Ataque de *phishing* é uma forma de ataque via e-mail, páginas web ou mensagem de texto", utilizado para obter senhas e dados pessoais, segundo Infosec *Institute* (2016, online). Cerca de 60% a 70% dos e-mails são *spam*[5], e dentro dessa porcentagem são ataques de *phishing*, afirma Grimes (2017).

Software com vulnerabilidades "é similar ao *malware* e *phishing* de engenharia social" (GRIMES, 2017, online, tradução nossa), são comuns em programas de extensão de navegadores, como Adobe Reader. As ameaças de mídia social são uma forma de buscar vulnerabilidades em redes sociais, como Facebook e Linkedln, onde informações pessoais estão expostas ao público de forma geral. Em alguns casos os *hackers* corporativos começam por essa forma de ataque, procurando por brechas em perfis específicos de pessoas que trabalham em uma empresa, onde possam ter acesso a essas informações e fazer um ataque direcionado.

APT é um ataque que utiliza Cavalo de Tróia[6] ou *phishing* por meio de engenharia social. Um método que pode ser praticado por *hackers* é um *spear phishing*, "uma forma direcionada de *phishing* na qual e-mails fraudulentos são direcionados a organizações específicas em um esforço para obter informações confidenciais" (Trend Micro, 2015, online).

Afirma Kaspersky Lab (2017) que a diferença entre *phishing* e *spear phishing* é a maneira como o alvo é atingido. No *spear phishing*, o *hacker* tem um alvo específico, fazendo

---

[3] ***Malware:*** "Trata-se de um *software* destinado a se infiltrar em um computador alheio de forma ilícita, com o intuito de causar algum dano ou roubo de informações (confidenciais ou não) " (Site UOL Segurança Digital, 2013, online).

[4] ***Ransomware***: "É um tipo de *malware* que sequestra o computador da vítima e cobra um valor em dinheiro pelo resgate, geralmente usando a moeda virtual *bitcoin* " (CARDOSO, 2016, online).

[5] ***Spam*:** "É uma mensagem eletrônica não-solicitada enviada em massa. [...]consiste numa mensagem de correio eletrônico com fins publicitários " (POZZEBOM, 2014, online).

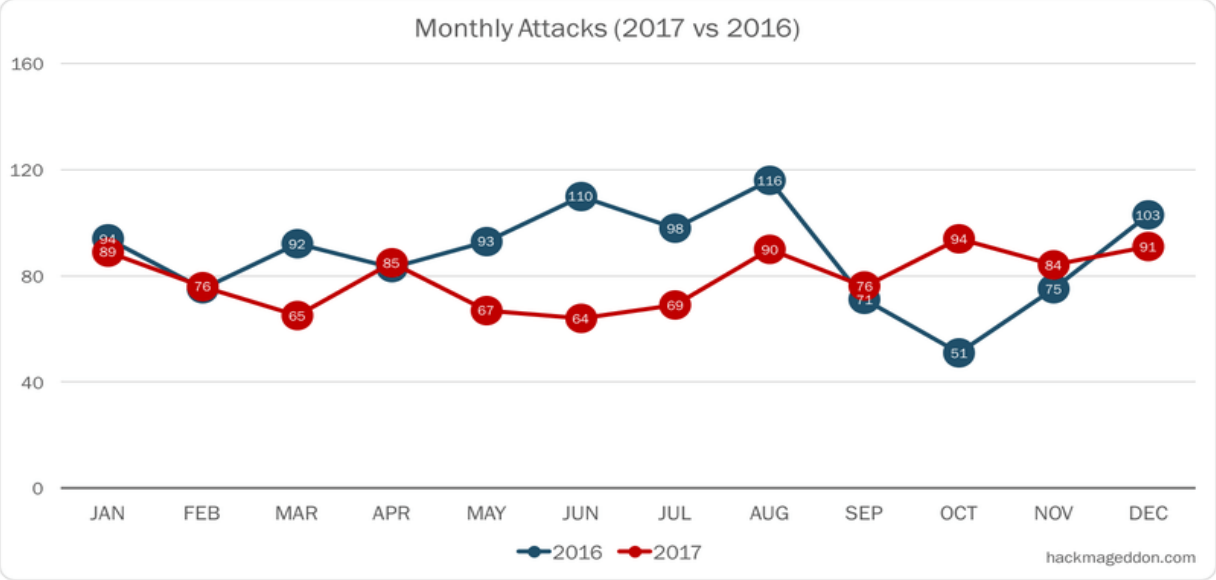
[6] **Cavalo de Tróia**: "É um programa que se oculta dentro de outro, legítimo, com a finalidade de abrir uma porta para que o *hacker* mal-intencionado tenha acesso ao computador infectado " (DUARTE, 2014, online).

coleta e estudo detalhado a respeito da vítima o que torna o ataque mais perigoso. São desenvolvidos e-mails mais atrativos, tornando a autenticidade confusa e o ataque mais eficiente. Geralmente, os ataques agem em torno de pessoas que um nível de acesso a informações que possuem valor, seja estratégico ou financeiro, ou ao setor responsável pela contabilidade de uma empresa, porém não exclui outros setores de uma instituição do grupo de risco.

Na figura 7, de acordo com Passeri (2018), houveram variações de ataques no decorrer dos anos de 2016 e 2017. O ano 2017, os números de ataques foram menores do que em 2016, porém houveram ataques em grande escala que marcaram o ano 2017, como *WannaCry* e *NotPetya*.

> O *Petya* em si é cerca de um ano mais antigo do que o *WannaCry*. A primeira versão do *Petya* foi disseminada no início de 2016 e sua função criptográfica logo foi quebrada. O mesmo aconteceu com a segunda versão do vírus. Foi só na terceira versão que a praga enfim conseguiu usar uma criptografia robusta. O *WannaCry* só surgiu neste ano de 2017, e não há até o momento registro de qualquer fraqueza em sua criptografia (RORH, 2017, online).

Figura 7 - Ataques mensais durante os anos de 2016 e 2017



Fonte: Passari (2018, online)

Cossetti (2017) afirma que o *WannaCry* (ou *WannaCrypt*) é *malware* que criptografa arquivos e exige pagamento de *bitcoin*[7] para decriptar. Esse *malware* possui uma característica de *worm*.

> A diferença entre os ataques anteriores do *WannaCry* e o mais recente é a existência de um componente do tipo *worm* que infecta outros computadores explorando uma vulnerabilidade de execução crítica de código remoto na implementação do protocolo *Server Message Block* 1.0 (SMBv1) do Windows (COMPUTERWORLD, 2017, online).

[7] ***Bitcoin***: "É basicamente um arquivo digital que existe online e funciona como uma moeda alternativa" (BBC BRASIL, 2017, online). Em outras palavras, é uma moeda virtual.

O *NotPetya* é uma variação do *ransomware Petya* porém com um ponto divergente. A Redação do Olhar Digital (2018) afirma que mediante a um "sequestro" e criptografia dos dados, é exigido pagamento para liberar ao usuário seus dados. Porém, a diferença entre os mesmos é a chave de decriptografia, o *NotPetya* não oferece nenhuma chave, o que provoca a perda total dos computadores infectados.

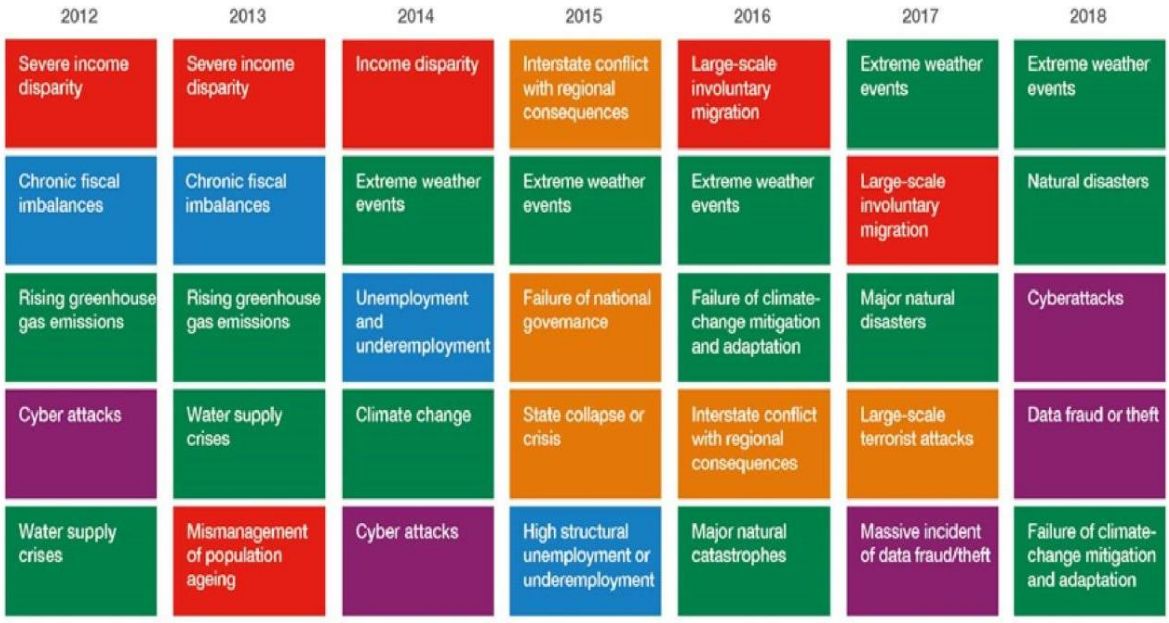
2.2.2 *Data fraud and theft*

Data theft pode ser definido como, "a cópia ou remoção não autorizada de uma informação confidencial para uma empresa" (MILLER, 2008, online). Não se restringe apenas a empresas, mas também clientes de uma determinada loja ou alguma propriedade intelectual, por exemplo.

Existem outras modalidades que afetam não apenas, mas com o foco principal na pessoa física e seus dados eletrônicos. Um dos exemplos que afeta pessoa física é o roubo de identidade, onde os maiores alvos são dados pessoais. "Tornou-se um grande negócio para os criminosos: 15,4 milhões de americanos foram vítimas de roubo de identidade em 2016" (TATHAM, 2018, online). Nos últimos 17 anos, o roubo de identidade é uma das importantes queixas por consumidores com a *Federal Trade Commission* (FTC).

No ano 2018, *cyberattack* e *data fraud and theft* (em roxo) aparecerem 3° e 4° lugar no ano de 2018, respectivamente, como podemos ver na imagem a seguir, figura 8. Em primeiro lugar (verde) encontram-se eventos climático extremos e em segundo (também em verde), desastres naturais.

Figura 8 - *Top 5 Global Risks in Terms of Likelihood*



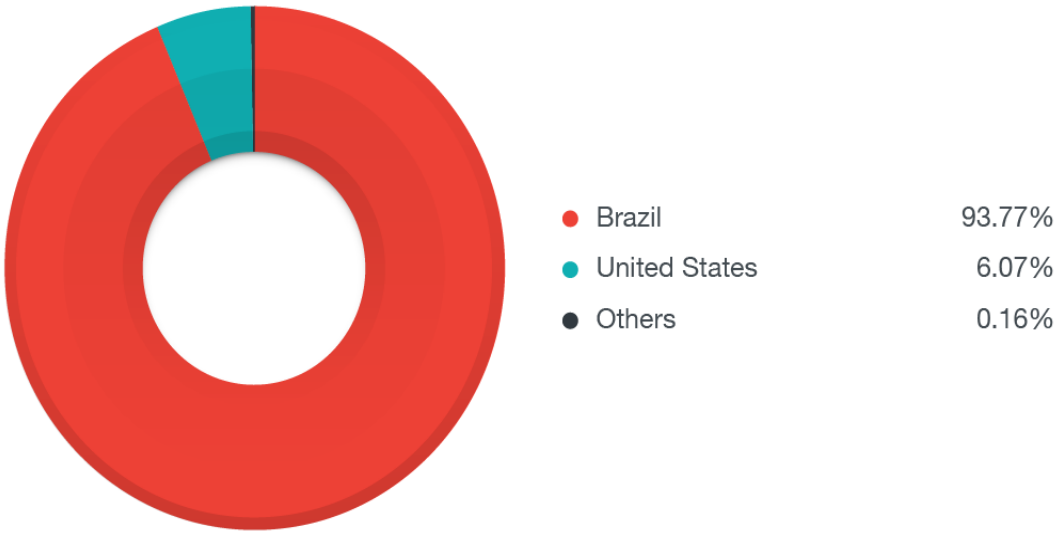
Fonte: *Global Risks Report 2018* (2018, p. 6)

Existem diversos tipos de roubo de identidade e fraude como, por exemplo: roubo de biometria, fraude de empréstimos automáticos, fraude de cartão de crédito e débito, entre outros (TATHAM, 2018).

Um estudo de caso de fraude de cartão de crédito e débito que ocorreu em abril de 2015 no Brasil, a respeito de *data fraud and theft* foi analisado pela empresa de segurança Trend Micro (2016) a respeito de um *malware* de Ponto de Venda (PDV), chamado FighterPOS. O fato ocasionou em vinte e dois mil números de cartão de crédito e tinha a característica de propagação entre terminais, o que afetou mais de 100 terminais do tipo POS (*Point of Sale* - ponto de venda) no Brasil e entre países.

Segundo o blog da Trend Micro (2016), TrendMicro *Smart Protection Network*[8] reuniu os dados e demonstraram que mais de 90% das tentativas de conexão dos servidores C&C[9]do *FighterPOS*, estão localizadas em terras brasileiras e 6% são dos sistemas infectados nos Estados Unidos, como mostra na figura 9.

Figura 9 - Servidores C&C do *malware* FighterPOS



Fonte: Blog Trend Micro (2016, online)

Devido aos exemplos de ataques mencionados nesse capítulo são necessárias medidas de segurança para evitar ou diminuir o índice de prejuízo de perda de dados, por exemplo. Com a

[8] **Trend Micro *Smart Protection Network***: "É a inteligência global de ameaças que rapidamente e coleta e identifica com precisão novas ameaças, oferecendo proteção instantânea aos dados onde quer que eles residam " (Trend Micro, 2013, p. 1, tradução nossa).

[9] **C&C**: Comando e Controle. "São computadores sob controle de um *hacker* ou um grupo de *hackers* que pode enviar comandos aos *bots* na *botnet* e também recebe informações que os *bots* coletam. Por sua vez, *botnet* é uma rede de dispositivos conectados à Internet, chamados de *bots*, que estão infectados com *software* malicioso" (BÄR, 2017, online).

utilização da criptografia como um auxílio para proteger os dados ou até mesmo para o envio de uma mensagem sigilosa.

É notório, nesse sentido, realizar um foco maior nas ferramentas que objetivam maior segurança ao usuário final por exemplo, mas no caso dessa monografia é ao portador do cartão e no processo de transação à medida que com o aumento de *cyberattack* e de outras ameaças há uma diminuição da fidelidade do cliente, o que impulsiona maiores investimentos das empresas nesses setores de segurança. Assim, conclui-se que com auxílio da criptografia é atingido a meta desejada da segurança.

3 CRIPTOGRAFIA

A criptografia é uma ferramenta utilizada para segurança, seja para envio de uma mensagem seja para guardar um dado. Zochio (2016) afirma que surgiu para fins militares durante a Segunda Guerra Mundial (1939-1945) para enviar mensagens e comandos para tropas em combate, visando sigilo - pois caso fosse interceptado por adversários seria usado para antecipar os planos dos oponentes. Assim, a criptografia, inicialmente, foi se aprimorando para influenciar nos resultados de batalhas.

O site TechTerms define criptografia como,

> Criptografia é uma ciência que protege a informação, transformando em um formato seguro [...], é usado há séculos para impedir que mensagens manuscritas sejam lidas por destinatários indesejados. Hoje, a criptografia é usada para proteger dados digitais (*TECHTERMS*, 2015, online).

A criptografia possui princípios básicos que são definidos para que seja definida como a mesma e que ao mesmo tempo precisam ser oferecidos a quem utiliza, Alecrim (2012). Princípios esse que são: confidencialidade, autenticação, integridade da informação e não repudiabilidade (em outras palavras, o receptor não pode negar o envio da informação). Tento isso em vista, a aplicabilidade foi aumentando com o decorrer dos anos e podemos observar em redes sociais e aplicativos de conversa como, Telegram e Signal.

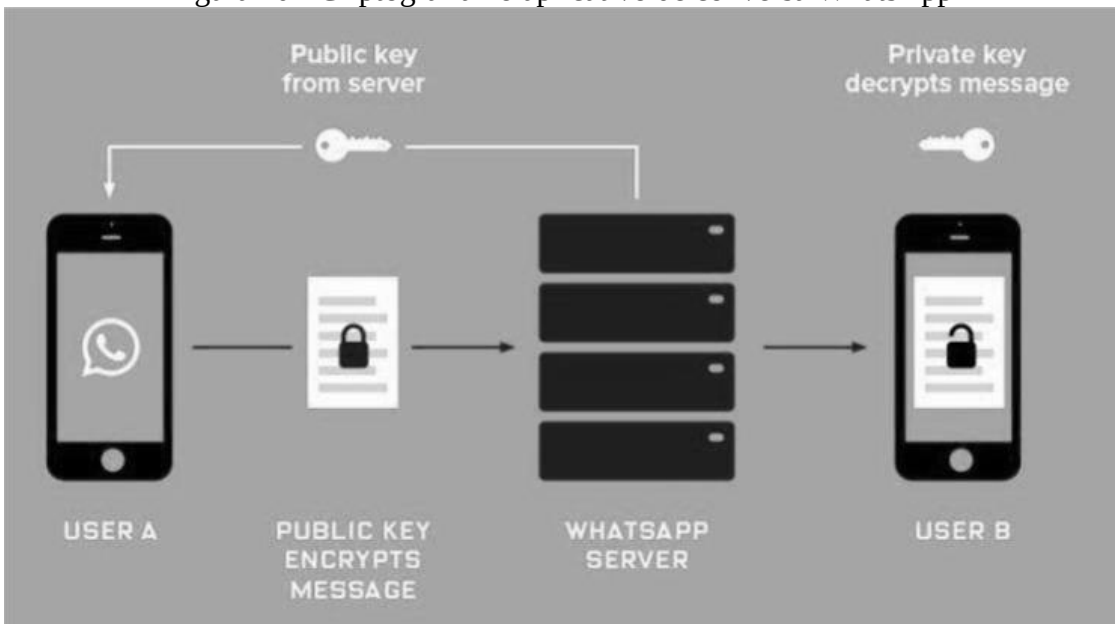
No aplicativo de conversa WhatsApp utiliza dessa ferramenta também (figura 10). Segundo o próprio suporte do aplicativo de mensagens, o uso da criptografia visa e disponibiliza automaticamente a segurança e sigilo dos vídeos, fotos, mensagem de voz, chamadas e mensagem de texto trocadas entre usuários.

> A criptografia de ponta-a-ponta do WhatsApp está disponível quando você e as pessoas com as quais você conversa estão na versão mais recente do nosso aplicativo. Muitos aplicativos criptografam mensagens entre você e eles próprios, já a criptografia de ponta-a-ponta[10] do WhatsApp assegura que somente você e a pessoa com a qual você está se comunicando podem ler o que é enviado e ninguém mais, nem mesmo o WhatsApp (SUPORTE WHATSAPP, [201-?], online).

Na figura 10, observa-se a troca de mensagens entre o usuário A e B. O usuário A é o emissor da mensagem, que utilizando de uma chave pública que é trocada com o servidor do aplicativo e outra chave também publica, é para criptografar a mensagem. Assim, o usuário B que é o receptor da mensagem, decriptografar a mensagem enviada com uma chave privada correspondente a chave pública do servidor.

[10] **Criptografia ponto-a-ponto**: "Apenas os usuários envolvidos na conversa terão acesso às mensagens, já que para decriptografá-las é necessário possuir uma chave particular, que somente eles possuirão" (HIGA, 2015, online).

Figura 10 - Criptografia no aplicativo de conversa WhatsApp



Fonte: Zurianrrain (2016, online)

Devido a essa importância da segurança da informação e dos dados, a criptografia pode ser utilizada para atividades, visando a confidencialidade e integridade do processo e dados. Rover (2012, online) afirma criptografia é utilizada para:

- Sigilo: somente os usuários autorizados têm acesso à informação;
- Integridade da informação: garantia oferecida ao usuário de que a informação correta, original, não foi alterada, nem intencionalmente, nem acidentalmente;
- Autenticação do usuário: é o processo que permite ao sistema verificar se a pessoa com quem está se comunicando é de fato a pessoa que alega ser;
- Autenticação de remetente: é o processo que permite a um usuário certificar-se de que a mensagem recebida foi de fato enviada pelo remetente, podendo-se inclusive provar perante um juiz, que o remetente enviou aquela mensagem;
- Autenticação do destinatário: consiste em se ter uma prova de que a mensagem enviada foi como tal, recebida pelo destinatário;
- Autenticação de atualidade: consiste em provar que a mensagem é atual, não se tratando de mensagens antigas reenviadas.

3.1 CRIPTOGRAFIA BASEADA EM CHAVES

Quando enviamos uma mensagem utilizando criptografia, ela está em um formato seguro, conforme mencionado no início deste capítulo, e nesse formato é gerado a partir de um código chamado chave criptográfica. A definição de chave criptográfica é como “um valor secreto que modifica um algoritmo de encriptação” (ROMAGNOLO, 2007, online).

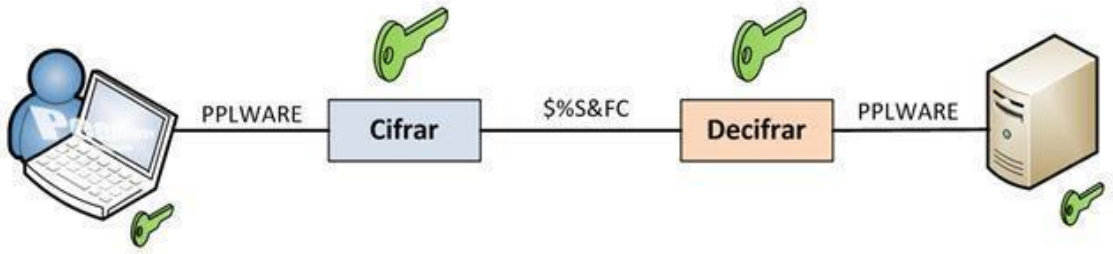
Existem dois personagens principais no cenário que será explanado, sendo eles o emissor e o receptor. O receptor faz o papel de quem recebe a mensagem enviada pelo emissor, que por sua vez é o responsável por iniciar o processo e é quem emite a mensagem.

Existem dois tipos de chaves: pública e privada. A chave pública, é utilizada apenas uma chave para criptografar e decriptografar. Já a chave privada, possui chaves diferentes tanto para criptografar e quanto para decriptografar. Somente o receptor e o emissor o acesso a essa chave, por segurança, que pode ser simétrica ou assimétrica. Caso uma terceira pessoa queira usar uma chave diferente para fazer esse acesso a mensagem não iria conseguir, por exemplo, pois não possui acesso a chave. Seria como tentar entrar em uma casa X com a chave de outra casa Y, por exemplo

3.1.1 Criptografia simétrica

"A criptografia simétrica é também conhecida por criptografia de chave secreta" (PINTO, 2010, online). Na qual é utilizada uma única chave para acessar a mensagem compartilhada entre emissor e receptor e assim, uma chave será usada pelo emissor para criptografar[11] a mensagem e a mesma será utilizada pelo receptor para decriptografar[12] (figura 11).

Figura 11 - Arquitetura da criptografia de chave secreta (simétrica)



Fonte: Pinto (2015, online)

As vantagens da criptografia simétrica, segundo Amaro (2007) são: velocidade, chaves relativamente pequenas e simples e atingir os objetivos de confidencialidade e privacidade. Desvantagens podem ser listadas como: compartilhamento de chaves, não permite autenticação do remetente e não permite o não-repúdio do remetente. Um exemplo de algoritmo de criptografia de chave secreta detalhados brevemente, no tópico a seguir.

[11] **Criptografar**: "Transformação reversível dos dados por forma a torná-los inteligíveis " (PINTO, 2010, online).

[12] **Decriptografar**: "Operação inversa da encriptação " (PINTO, 2010, online).

3.1.1.1 RC (Ron's Code ou Rivest Cipher)

Foi criado por Ron Rivest, na empresa RSA *Data Security.* Amaro (2007) afirma que o algoritmo RC possui chaves no intervalo que variam entre 8 a 1024 *bits*. Possui algumas variações que podemos citar como exemplo: RC2, RC4, RC5 e RC6. Cada variação possui um tamanho para a chave possuindo maior complexidade devido ao tamanho. Uma aplicação nos presentes dias é em e-mails.

No quadro 1 são apresentadas algumas breves diferenças entre as variações do a partir do algoritmo RC.

Quadro 1 - Comparação dos algoritmos que variam do RC

Algoritmos	**RC2**	**RC4**	**RC5**	**RC6**
Criado por	Ron Riverst em 1994	Ron Rivest (RSA *Security*) em 1994	Ron Riverst em 1994	Yiqnn Lisa Yin em 1998
Tamanho (bloco)	64 bits	2.064 bits (efetivos 1.684)	32, 64 ou 128 bits	128 bits
Tamanho (chave)	8 a 1.024 bits em 8 etapas de 8 bits. Por padrão 64 bits	40 a 2.048 bits	0 a 2040 bits (Sugestão 128 bits)	128, 192 ou 256 bits
Eficácia	Eficiente em *software*	Eficiente em *software* e *hardware*	Lenta	Lenta

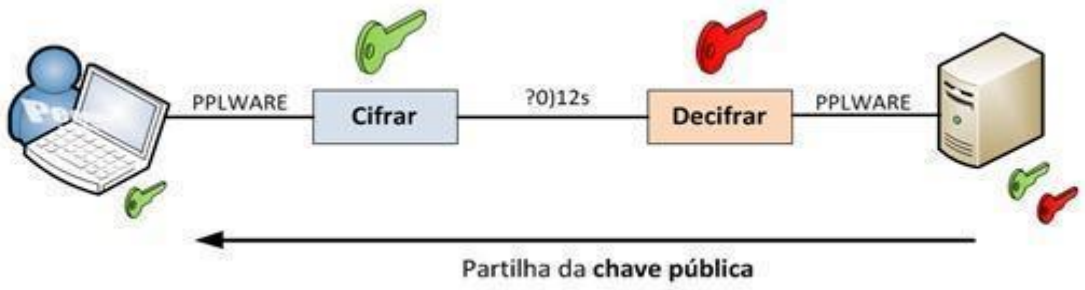
Fonte: Adaptação de Gunasundari e Elangovan (2014, p. 82, tradução nossa)

3.1.2 Criptografia assimétrica

Segundo Pinto (2010, online), "a criptografia assimétrica é também conhecida por criptografia de chave pública", pois emprega diferentes chaves para criptografar pelo emissor e decriptografar, pelo receptor (figura 12).

> Cada participante em um sistema de chave pública possui um par de chaves. Uma chave é nomeada como a chave privada e é mantida secreta. A outra chave é distribuída para quem deseja recebê-la; essa chave é a chave pública (IBM, 2015, online).

Figura 12 - Arquitetura da criptografia de chave pública (assimétrica)



Fonte: Pinto (2015, online)

Amaro (2007) afirma que as vantagens da mesma são: a chave não é compartilhada, autêntica de acordo com assinatura com a chave, permite o não-repúdio e é escalável de acordo com a hierarquia de controle e distribuição de chaves. Mas as desvantagens apresentadas, são: a lentidão no processo de leitura devido a sua origem matemática, exigindo alto desempenho computacional e requer autoridade de certificação para garantir a identidade e a chave confiável. Um exemplo de algoritmo de criptografia assimétrica pode ser citado, no tópico a seguir.

"Cabe salientar que a chave pública é geralmente distribuída e a chave privada mantida em segredo e armazenada em um *smart-card*, *token* ou em repositório em *software*" (NUNES, 2007, online). Os *tokens* são utilizados para validar "algo que você tem", que funciona para autenticar a validade da identidade de quem possui o mesmo e pode ser definido *token* como uma chave e é um objeto físico (REIS, 2015). É uma camada adicional e complementar de segurança utilizada, por exemplos, em bancos e em compras online e pode ser agregado a outras ferramentas, como a própria criptografia e Inteligência Artificial.

> O uso de *Token* como mecanismo adicional de autenticação tem se tornado cada vez mais comum no mercado e provê segurança de mais alto nível. Os *tokens* estão disponíveis em *hardware* e *software* e são utilizados no processo de autenticação de usuários, sistemas e processos (BRITO, 2009, online).

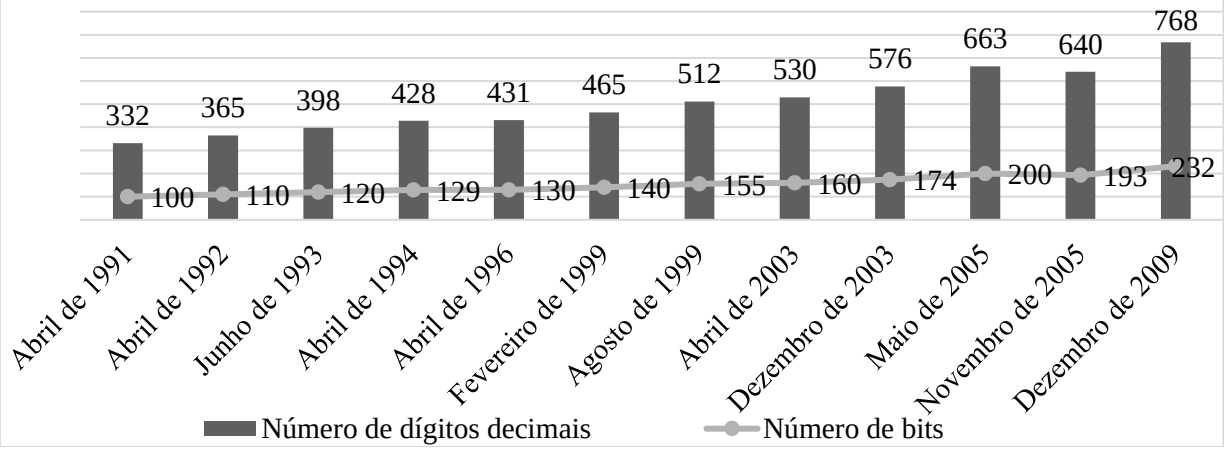
3.1.2.1 RSA

Foi criado na década de 70 no MIT, é o algoritmo de chave pública mais utilizado, afirma Villena (2012). Sua sigla é devido a iniciais dos sobrenomes dos responsáveis pela criação, Ron Rivest, Adi Shamir e Len Adleman. "Desde sua publicação, nenhum ataque conseguiu quebrá-lo, portanto não foi preciso mudar sua estrutura" (VILLENA, 2012, online).

Existem cinco possíveis técnicas para ataque: força bruta, ataques matemáticos, ataques de temporização, ataques baseados em falhas de *hardware* e ataques de texto cifrado escolhido. A seguir, uma breve descritiva a respeito de cada ataque e definição segundo Stallings.

- Força bruta: "envolve tentar todas as chaves privadas possíveis" (STALLINGS, 2015, p. 213). No caso de ataque de força bruta, a melhor forma de evitar é o tamanho da chave. Quanto maior o seu tamanho, isso quer dizer, maior número de *bits*, mais difícil de ser quebrada. Porém há uma ameaça, referente a esse tamanho da chave: seria uma evolução no poder da computação no decorrer dos anos e aperfeiçoamento dos algoritmos de fatoração.
- Ataques matemáticos: "existem várias técnicas, todas equivalentes em esforço a fatorar o produto por dois primos" (STALLINGS, 2015, p. 213). O gráfico 1, mostra alguns exemplos de ataque desse tipo, de acordo com o número de bits da chave.

Gráfico 1 - Processo de fatoração RSA



Fonte: Adaptado de Stallings (2015, p. 214)

- Ataques de temporização: “estes dependem do tempo de execução do algoritmo de decriptação” (STALLINGS, 2015, p. 213).
- Ataques baseados em falhas de *hardware*: “estes envolvem a indução de falhas de *hardwares* no processador que está gerando as assinaturas digitais” (STALLINGS, 2015, p. 213).
- Ataques de texto cifrado escolhido: “esse tipo de ataque explora as propriedades do algoritmo RSA” (STALLINGS, 2015, p. 213).

3.2 COMPARAÇÃO DE TIPOS DE CHAVES

Uma das comparações feitas entre os tipos é a respeito da chave, devido ao tamanho de chave maior significa maior segurança, mas pode diminuir a velocidade e criptografar/decriptografar (STALLINGS, 2015).

Os tamanhos de chave de 64 *bits* ou menos, agora são em grande parte consideradas inadequados, e 128 *bits* tornou-se um padrão comum. No quadro 2, compara-se os dois tipos de criptografia de acordo com a velocidade de leitura, chave para poder decriptografar e criptografar a mensagem e a comunicação entre emissor e receptor, que são servidor e cliente, respectivamente.

Quadro 2 - Comparação entre simétrica e assimétrica

CRIPTOGRAFIA	VELOCIDADE DE LEITURA	CHAVE	COMUNICAÇÃO
Assimétrica	Rápido	Uma só chave para cifrar e decifrar.	Problema para a troca de chaves, pois o cliente e servidor precisam conhecer a chave.
Simétrica	Lento	Usa um par de chaves. Onde uma chave cifra e outra decifrar.	O cliente precisa apenas conhecer a chave pública para cifrar e enviar os dados ao servidor, que por sua vez consegue decifrar a informação com a chave privada.

Fonte: Adaptado de Helvio (2012, online)

3.3 APLICAÇÕES ATUAIS DE CRIPTOGRAFIA

Nos dias atuais, existem diversas aplicações para a criptografia que variam desde a proteção de dados armazenados em nuvem a autenticação do usuário, e num mundo cada vez mais digital, procura-se proteger os dados independentemente da aplicação utilizada. Assim, um dos recursos que a criptografia oferece é o certificado digital e a assinatura digital, por exemplo.

Segundo Alecrim (2009), certificado digital é um tipo de tecnologia de identificação que permite que transações eletrônicas dos mais diversos tipos sejam realizadas considerando os aspectos da integridade, autenticidade e confiabilidade, de forma a evitar que a adulterações, interceptações de informações privadas ou outros tipos de ações indevidas ocorram.

"Uma assinatura é feita por um algoritmo criptográfico aplicado à mensagem ou a um pequeno bloco de dados que é uma função da mensagem" (STALLINGS, 2015, p. 205). Por exemplo, ao invés de apenas digitalizar a assinatura, corre-se o risco de haver uma modificação por via de alguns *softwares* de edição de imagem. Assim, a assinatura digital poderia ser usada para proteção do mesmo. A assinatura digital é um exemplo de aplicação utilizando a função de *hash* criptográfica, explicada no tópico a seguir.

3.3.1 *Hash*

Pode-se definir a função *hash* como "qualquer algoritmo que mapeie dados grandes e de tamanho variável para pequenos dados de tamanho fixo" (PISA, 2012, online). O mesmo menciona que são utilizados em grande escala para procurar um componente em um Banco de Dados (BD), ou verificar a totalidade de *download* de um arquivo ou para transmitir senha de um usuário a outro. Outra aplicação além da assinatura digital, é a busca de dados em BD. Existem alguns exemplos de algoritmos *hash*, como: MD5 (*Message-Digest algorithm* 5) e a família SHA (*Secure Hash Algorithm*): SHA-0, SHA-1, SHA-2 entre outras.

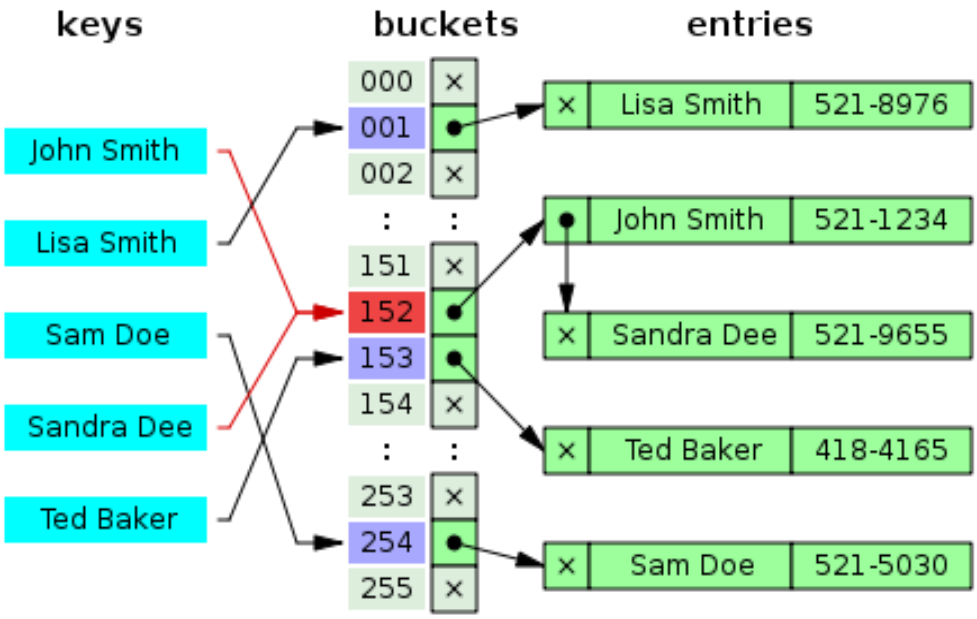
Pisa (2012) fala que a busca de elementos com base em resumo é tanto utilizada uma estrutura de dados em memória quanto é usada em BD. A sua performance baseia-se em uma construção de índice, similar à de livros. Por exemplo, imaginemos um livro que, para ler um tópico específico, iremos olhar antes o índice para procura a página referente ao mesmo para que então possa abrir na página exata, porém a pesquisa é realizada pelo resumo do conteúdo e não pelo dado.

Na figura 13 pode-se observar um exemplo de aplicação: a chave seria o nome do usuário e quando é associado com a tabela *buckets*, é então feita a ligação com o atributo de entrada, não sendo preciso gastar recurso procurando em cada endereço.

Existem algumas propriedades do *hash*: colisão e unidirecional. A seta vermelha na figura 13 representa um exemplo de colisão. A colisão pode ser uma consequência de duas chaves possuírem o mesmo endereço.

> O objetivo principal dos projetistas de função *Hash* é reduzir ao máximo a probabilidade de ocorrência das colisões. A ferramenta mais usada para reduzir essa probabilidade é o ajuste da distribuição dos resumos. Quanto mais uniforme e dispersa é a função resumo, menor é a sua probabilidade de colisão (PISA, 2012, online).

Figura 13 - Aplicação de *hash*



Fonte: Joyme (2017, online)

A tabela de dispersão ou tabela *hash* pode gerar colisões também, segundo Feofiloff (2017). Isso acontece quando se transforma uma chave correspondente a um endereço. A colisão depende de como a tabela de dispersão irá esquematizar as chaves. Assim, uma solução para esse problema é adotar o endereçamento aberto ou encadeamento (SAMPAIO, 2016).

O endereçamento aberto é a utilização da mesma tabela para guardar todas chaves, sem precisar armazenar fora da mesma ou de apontadores, assim procura por um espaço vazio na mesma tabela *hash*. Já o encadeamento é o processo de criar uma lista linear para guardar os endereços encadeados na mesma tabela.

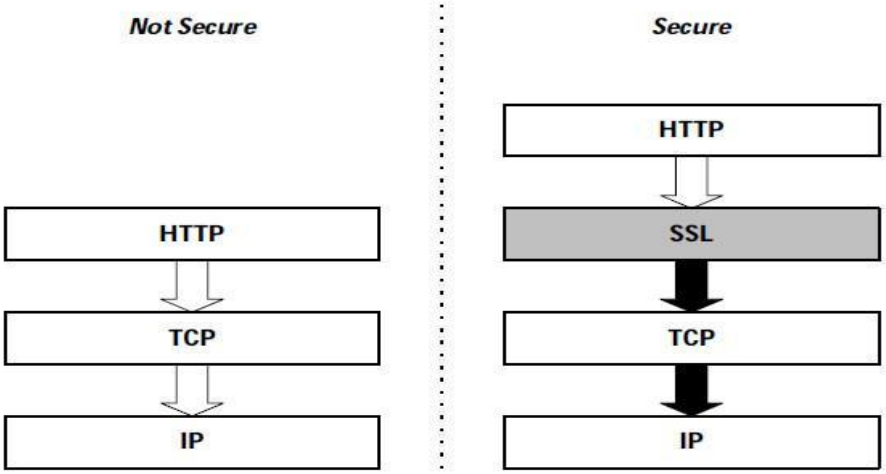
3.3.1.1 Protocolo de comunicação utilizados

Segundo Garrent (2016), os dois protocolos mais empregados para proteção de dados na Internet são, o SSL (*Secure Sockets Layer*) e o TLS (*Transport Layer Security*), assim com a ajuda da criptografia simétrica, protegem os dados transmitidos e armazenados. Protocolos "são formados por elementos-chave que os identificam e que definem como estas regras serão interpretadas pelas entidades componentes da comunicação" (CASTELUCCI, 2011, online).

3.3.1.2 SSL (Secure Sockets Layer)

Segundo Helvio (2012), o protocolo utiliza de criptografia, assimétrica e simétrica. A criptografia assimétrica é utilizada para estabelecer a conexão. Assim, por via de uma conexão segura realiza-se a troca da chave da criptografia simétrica. Essa comunicação dos dados continua com criptografia simétrica. "Permite que aplicativos cliente/servidor possam trocar informações em total segurança, protegendo a integridade e a veracidade do conteúdo que trafega na Internet" (MARTINS,2009, online).

Figura 14 - Utilização do protocolo SSL em um servidor *web*



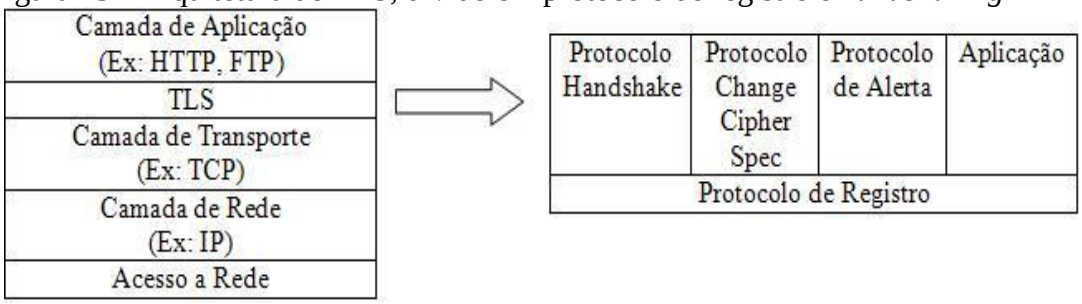
Fonte: Helvio (2012, online)

Na figura 14, tem-se um exemplo do uso do protocolo SSL em um servidor *web* no qual se insere um "s" (significando seguro ou *safe*) resultando em "https://" (MARTINS, 2009).

3.3.1.3 TLS

Pode-se definir TLS como um método que é meio que utiliza do conceito de criptografia para poder criptografar o canal que faz comunicação entre dois computadores (IBM, 2015). Já Coutinho, Machado e Silva (2006) dizem que esse protocolo objetiva a garantia da privacidade e a integridade dos dados, durante uma comunicação de uma ponta a outra. Esse protocolo possui duas camadas, sendo elas: protocolo de registro (TLS *Record Protocol*) e protocolos *Handshaking* (TLS *Handshaking Protocols*), como podemos observar na figura 15.

Figura 15 - Arquitetura do TLS, divido em protocolo de registro e *handshaking*



Fonte: Coutinho, Machado e Silva (2006, online)

Na figura 15, o protocolo *Handshaking* aparece mais detalhado, possuindo subcamadas: protocolo *Handshaking*, protocolo *Change Cipher Spec*, protocolo de alerta e aplicação.

O protocolo de registro, afirmam Coutinho, Machado e Silva (2006), é utilizado para poder fazer a encapsulação da camada anterior, a camada de aplicação. Esse protocolo possui etapas, no primeiro momento passa a ter as mensagens para poder conduzir, assim segmenta os dados em blocos e alternadamente realiza a concepção dos que adquiriu, coloca um endereço MAC (*Media Access Control*) e assim finalmente faz a encriptação e transporta o resultado das etapas.

Segundo Coutinho, Machado e Silva (2006), o protocolo *handshaking*, possui três subprotocolos, sendo eles: protocolo *handshake*, protocolo *chance cipher spec*, protocolo de alerta e aplicação. Os mesmos concedem um parâmetro de segurança entre ambas as partes, receptor e emissor, que serão usados na camada de registro para validar, comunicação e atribuir os estados de erros entre as partes.

No capítulo 3, foram demonstrados alguns conceitos de criptografia e exemplos algoritmos utilizados. Porém apenas a criptografia não é suficiente para garantir a segurança. Assim, buscamos aliar outros conceitos para melhorá-la. Com uso cada vez mais presente em nossas vidas e a evolução em passos largos, a inteligência artificial pode agregar valores a segurança da informação com os seus conceitos sobre redes neurais, *machine learning*, *data mining* e lógica nebulosa. No capítulo 4, iremos apresentar alguns conceitos de inteligência artificial e como eles contribuem com a segurança de informação.

4 INTELIGÊNCIA ARTIFICIAL

4.1 DEFINIÇÃO

De acordo com Joshi (2017) a Inteligência Artificial (IA) diz respeito aos estudos de teorias e metodologias para fazer com que a máquina seja capaz de realizar atividades do mesmo modo e eficiência de entendimento que os humanos teriam em situação análoga.

Ainda segundo Joshi (2017), a IA está intimamente relacionada ao estudo do cérebro humano. Diversos pesquisadores discorrem, em seus estudos, que ela é baseada na percepção de como o cérebro humano atua. Quando se consegue compreender como o cérebro humano pensa, aprende e age, se cria uma máquina que tem a capacidade de fazer o mesmo. Deste modo, de acordo com esta maneira de desenvolver sistemas inteligentes, podem ser criados programas com a capacidade de aprender.

Além do conceito tratado a cima, existem outras áreas da IA que fogem do escopo do pensamento, como a computação granular, computação evolucionária, entre outras, cada uma possuindo uma especificação particular.

Podemos dizer que a inteligência artificial é uma tentativa de copiar atividades que os humanos já realizam, como aprender, perceber, raciocinar, etc. Com isso, conseguem realizar tarefas como reconhecer imagens, reconhecer pessoas visualmente ou pela fala, entre outros. De acordo com Bolton, a IA é descrita como:

> Quanto mais inteligente uma pessoa é, mais a consideramos capaz de aprender, generalizar a partir deste conhecimento adquirido, capaz de raciocinar e deduzir considerando as possibilidades, aprendendo a partir dos erros. Podemos aplicar os mesmos critérios para uma máquina: uma máquina inteligente é aquela que é dotada da habilidade da razão (BOLTON, 2010, p. 371).

Porém, para identificarmos que aquele programa de computador realmente é uma IA, vários testes são feitos, como exemplo o Teste de Turing, que verifica a capacidade da máquina em demonstrar o comportamento análogo ao do ser humano ou idêntico a ele. Como para verificar este conhecimento são exigidos vários conhecimentos empíricos – acerca da realidade vivida – sobre diversos temas.

> Embora a maioria de nós esteja certo de que reconhecemos o que é comportamento inteligente quando o vimos, é muito improvável que alguém seja capaz de definir inteligência de uma maneira que seja específica o suficiente para auxiliar na avaliação de um programa de computador supostamente inteligente, e, ao mesmo tempo, capturando a vitalidade e a complexidade da mente humana (LUGER, 2004, p. 23).

Na Inteligência Artificial há diversas vertentes que podem ser abordadas, como a criação de sistemas que agem como humanos, que pensam e agem de maneira racional, entre outros e

neste âmbito já existem diversos protótipos de IA ao redor do mundo capazes de realizar atividades melhores que os próprios humanos, devemos isto a habilidade da razão da qual a IA é dotada.

> Uma máquina inteligente é aquela dotada da habilidade da razão. A percepção em um sistema inteligente é a coleção de informações usando sensores e a organização da informação obtida de forma que decisões possam ser tomadas. O raciocínio é o processo em que, a partir de situações conhecidas, a máquina lida com situações não conhecidas (BOLTON, 2010, p. 371).

A inteligência artificial nada mais é do que sistemas inteligentes que, segundo Simões:

> Os assim chamados 'sistemas inteligentes' são aqueles que fornecem respostas que solucionam problemas, tais respostas apropriadas às situações específicas destes problemas, mesmo que sejam novas ou inesperadas, fazendo com que tal comportamento seja 'único' ou até mesmo considerado 'criativo' (SIMÕES, 2007, p. 2).

Conforme Luger (2004) discorre em seu livro, para construirmos sistemas inteligentes precisamos organizar o conhecimento adquirido pela máquina e dar suporte a ela, por meio de ferramentas que representam conhecimentos de alto nível.

Continuando esta linha de pensamento "pode-se dizer que, para resolver um problema, é necessário ter algum conhecimento do domínio do problema e utilizar alguma técnica de buscar a solução" (BARRETO, 1999, p. 10).

Tendo em vista as considerações introdutórias feitas acerca da IA, devemos limitar nosso objeto de estudo. Com o intuito de adentrar no levantamento das principais técnicas de IA utilizadas no problema da segurança da informação, estudaremos acerca de Redes Neurais Artificiais, que, em síntese, são redes inspiradas em neurônios biológicos com a capacidade de aprendizado através do funcionamento semelhante ao das sinapses do cérebro humano.

Perpassando por outros conceitos primordiais como o da lógica nebulosa ou f*uzzy*, sendo inspirada no pensamento humano, o *data mining* com a extração de conhecimento através de grandes bancos de dados e o m*achine learning*, com a capacidade de aprendizado da máquina tendo em face os comandos gerados.

4.2 DATA MINING (DM)

Segundo Rezende (2003) e Colares e Carneiro (2006), a extração do conhecimento em base de dados é uma área que cresce a cada momento e tem beneficiado as necessidades econômicas, sociais, práticas, entre outras da sociedade.

A correlação que esta evolução tem com a tecnologia é o desenvolvimento das tecnologias de coleta, armazenamento e gerenciamento de grandes quantidades de dados. Tais dados possuem informações extremamente valiosas como tendências e padrões que podem ser usados para melhorar uma decisão de negócios.

Ainda segundo os autores:

> A definição de Mineração de Dados pode ser descrita como a união de diversas técnicas que têm como principal foco extrair conhecimento de grandes bases de dados, utilizando diversos algoritmos computacionais nas áreas de Classificação, Regras de Associação, Regressão ou Estimativa e Clusterização[13] (COLARES; CARNEIRO, 2006, p. 17).

Segundo Freitas (2002), o DM também pode ser definido como um campo interdisciplinar, que se utiliza de alguns métodos de diversas áreas de pesquisas – entre elas o m*achine learning* e a estatística – para então extrair uma gama de conhecimento advindo de conjunto de dados do mundo real. A etapa central de um processo mais amplo de mineração de dados é conhecida como descoberta de conhecimento em banco de dados.

Para realizar a descoberta do conhecimento, Rezende (2005) cita alguns processos de mineração de dados, sendo eles divididos em três grandes etapas: pré-processamento, extração de padrões e pós-processamento. Além das três etapas principais inclui-se duas etapas importantes no processo como identificação do problema e utilização do conhecimento.

Esse processo é centrado na interação de diversas classes de usuários, e seu sucesso dependente desta interação. As três classes de usuário são: especialista do domínio (usuário que conhece bastante do domínio da aplicação e que irá auxiliar a execução do processo); analista (usuário especialista que irá fazer a extração do conhecimento e a execução do mesmo); usuário final (aquele que irá utilizar o conhecimento extraído para assessorá-lo na tomada de decisão).

Em algumas situações o especialista do domínio também pode ser um usuário final ou até mesmo auxilie o analista ou que execute a mesma função (REZENDE, 2005).

Figura 16 - Etapas do processo de mineração de dados

Fonte: Rezende (2005, p. 312)

[13] **Clusterização**: "Trata-se de uma tentativa de aportuguesamento da palavra inglesa *clustering*, que designa, genericamente, um agrupamento de coisas semelhantes ou de coisas que funcionam de modo similar" (PINTO, 2004, online).

A figura 16 demonstra as etapas do processo de mineração de dados. O processo se inicia com a identificação do problema – feito neste o estudo do domínio e a definição de objetivos e metas, onde se entende o que será analisado. Começa-se, então, a extração do conhecimento, realizada pelo analista. Já a par do conhecimento realiza-se o pré-processamento – que consiste em adequar os dados à necessidade do sistema, seguindo algumas etapas, como extração e integração, transformação, limpeza e seleção e redução de dados.

Com os dados organizados é iniciada a fase de extração de padrões, "direcionada ao cumprimento dos objetivos definidos na identificação do problema. [...] compreende a escolha da tarefa de mineração de dados a ser empregada, a escolha do algoritmo e a extração dos padrões propriamente dita" (REZENDE, 2005, p. 317). Vem então a fase de pós-processamento – que está encarregada de verificar quais conhecimentos podem ser úteis para serem utilizados em problemas da vida real. Por fim, os conhecimentos obtidos são usados para resolução do problema encontrado inicialmente.

Informações como cadastros médicos, financeiros, escolares, entre outros meios de armazenamento em grande quantidade são de extrema importância tanto para os "donos" quanto para quem os manuseia. Por este motivo fazer o tratamento eficiente para assim tomar uma decisão é essencial, tendo em vista, que nos dias atuais saber como lidar com estes dados, assim como sua proteção, pode ocasionar o crescimento ou a queda de uma organização.

4.3 MACHINE LEARNING (ML)

Segundo Richert e Coelho (2013) e Colares e Carneiro (2006) ML é uma técnica que consegue 'ensinar' as máquinas a executarem tarefas sozinhas, fornecendo exemplos (como fazer ou não uma tarefa) para que ela consiga aperfeiçoar seus algoritmos com um treinamento, portanto, quanto mais repetições ela fizer melhor será seu desempenho e seu refinamento em relação aos seus testes bem-sucedidas.

Rezende (2005) cita em seu livro a existência de cinco paradigmas de aprendizado. O aprendizado simbólico que busca analisar exemplos e contraexemplos para assim os aprender e construir representações simbólicas de um contexto. O aprendizado estatístico consiste em usufruir de modelos estatísticos para obter uma correta aproximação do conceito induzido[14]. O aprendizado baseado em exemplos classifica padrões nunca vistos com base em padrões similares conhecidos. O aprendizado conexionista baseado em redes neurais, apresentaremos mais à frente. O aprendizado evolutivo originário do modelo biológico, faz a classificação de

[14]**Conceito induzido:** "É a forma de inferência logica que permite obter conclusões genéricas sobre um conjunto particular de exemplos" (REZENDE, 2005, p. 90).

elementos de uma população que competem entre si para conseguir a melhor performance e assim tomar a decisão.

Segundo Cánepa (2016) existem três tipos de ML sendo eles caracterizados pelos dados fornecidos e sua metodologia de treinamento: aprendizado supervisionado, aprendizado não supervisionado e aprendizado por reforço.

No aprendizado supervisionado, a máquina é treinada usando dados rotulados, sendo assim, cada elemento de entrada possui seu elemento de saída. Tendo essa relação, a máquina vai aprendendo e tomando decisões com base prévia nos dados de entrada.

O aprendizado não supervisionado é aplicado sem o uso de dados rotulados, como falado anteriormente, mas sim com o agrupamento de elementos com características semelhantes.

O aprendizado por reforço é similar ao aprendizado não supervisionado, porém ele difere no fato de ser baseado em recompensas e punições; quando a máquina obtém sucesso na atividade ela é recompensada, mas se não conseguir é punida, sendo formado um conjunto de estratégias para que ela sempre tenha sucesso.

Haja vista dos conceitos de DM e ML, as duas trabalham em conjunto, pois ao analisar os dados e tomar a decisão, a ML vai fazer com que esta decisão seja guiada para o caminho correto, ou o mais próximo disso. Como citado em DM, um bando de dados financeiro possui diversas informações importantes com ralação ao cliente e suas transações, para monitorar e tomar ações com base nas decisões a ML é de suma importância para o procedimento que a organização precisará fazer para proteger e gerir tais dados.

4.4 REDES NEURAIS

"Redes neurais artificiais se compõem de neurônios artificiais que se inspiram nos correspondentes biológicos e que são um tipo de célula" (BARRETO, 1999, p. 66). Este modelo de neurônio baseia-se em uma estrutura lógico-matemática[15] que faz com que ele seja comparado com o neurônio humano.

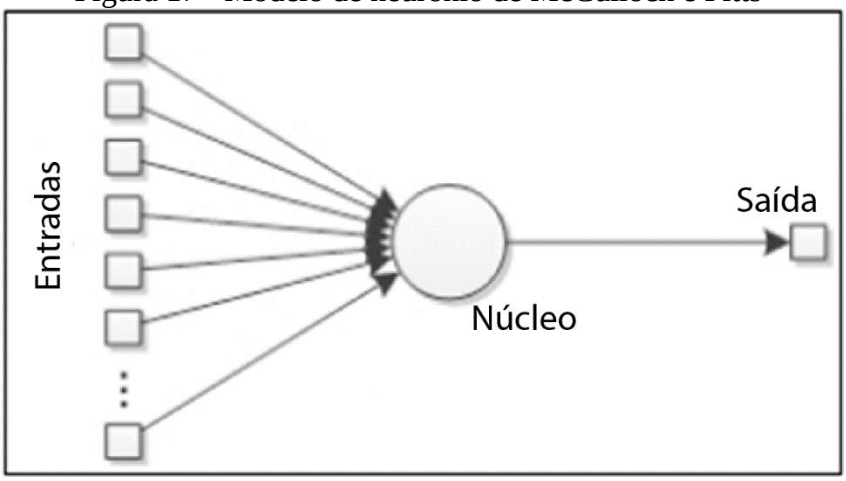
Seguindo essa linha, Haykin (2008) e Brumatti (2005) *apud* Silva (2016) explanam que as Redes Neurais Artificiais (RNA's) foram desenvolvidas na necessidade de representar uma das particularidades mais importantes dos seres humanos: a capacidade cognitiva. Tal funcionalidade decorre da aplicação no reconhecimento de padrões, na otimização e na previsão

[15] **Lógica Matemática** consiste em um sistema dedutivo de enunciados que tem como objetivo criar um grupo de leis e regras para determinar a validade dos raciocínios.

de sistemas complexos. Esse paradigma deriva de um conjunto de disciplinas como: matemática, física, estatística, engenharia, neurociência e ciência da computação.

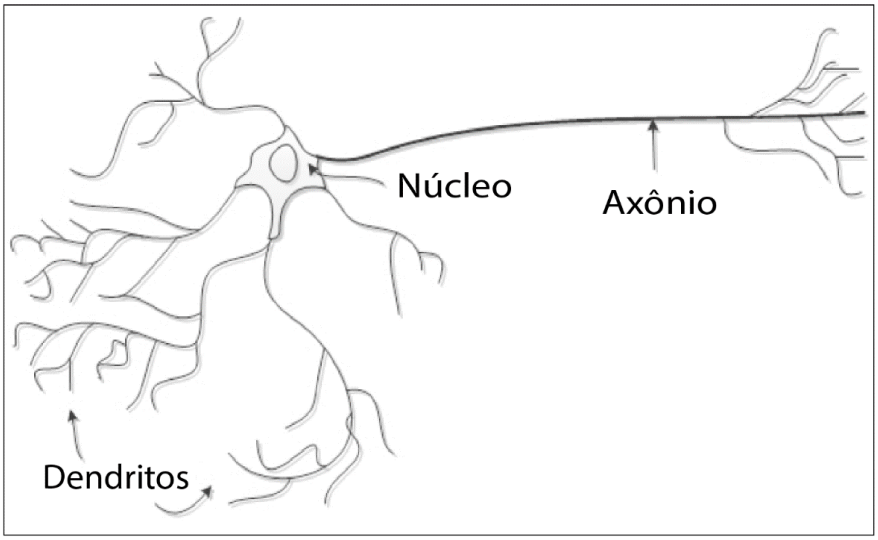
Podemos comparar a estrutura de um neurônio artificial (figura 17, a estrutura de um simples neurônio inspirado no neurônio de McCulloch e Pitts[16]) e um neurônio humano (figura 18). Sendo assim, os termos da estrutura de um neurônio artificial são análogos à estrutura de um neurônio humano como: dendritos (representam as entradas), sinapses (representam as conexões excitatórias ou inibitórias), o núcleo possui dois processos os estímulos captados (representa a função soma) e o limiar de disparo (representa a função de transferência ou de ativação) e por fim axônio (representa a saída).

Figura 17 - Modelo de neurônio de McCulloch e Pitts



Fonte: Adaptado de Soares e Sousa (2018, p. 4)

Figura 18 - Modelos do neurônio humano



Fonte: Adaptado de Soares e Souza (2016, p. 4)

[16] **McCulloch e Pitts** criadores do primeiro modelo do neurônio artificial, mais detalhes em Morais (2010).

O sistema funciona da seguinte maneira, caso alguma das conexões inibitórias seja 1, o neurônio retorna 0, ou seja, é vetado. Entretanto se nenhuma delas for acionada e pelo menos 1 conexão excitatória for acionada é feito a soma e assim comparada com θ, caso seja maior que seu limiar ela é disparada (MORAIS, 2010). As equações 1 e 2 demonstram este procedimento.

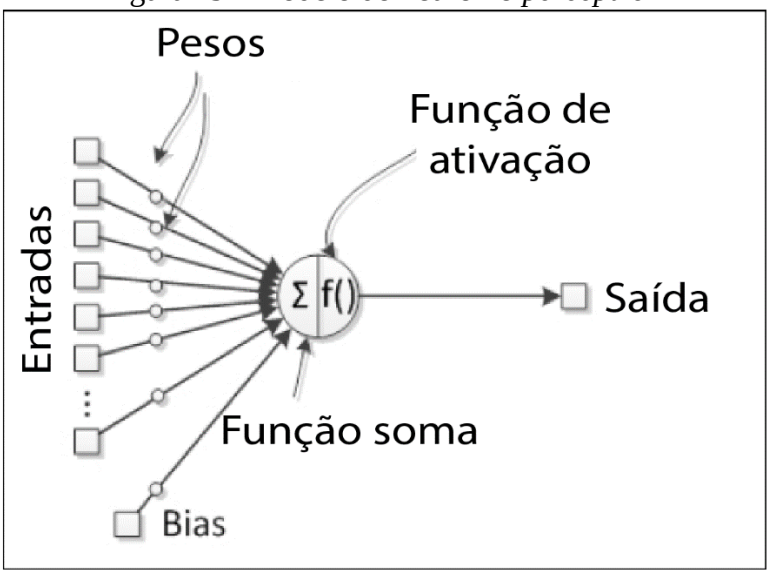
$$\sum_1^n (X_n) \tag{1}$$

$$\begin{cases} Saída = 1 \; se \; \Sigma \geq \theta; \\ Saída = 0 \; se \; \Sigma < \theta; \end{cases} \tag{2}$$

Com isto, Simon Haykin (2008) fala que com o impacto que os estudos de McCulloch e Pitts causaram na sociedade causando uma grande repercussão. Então, alguns anos depois, Rosenblatt propõe o modelo *perceptron*, que é o primeiro modelo com aprendizado supervisionado, criado para resolver problemas linearmente separáveis.

"Basicamente, ele consiste de um único neurônio com pesos sinápticos ajustáveis e *bias*" (HAYKIN, 2008, p. 143). Soares e Souza (2016) definem o *bias* como sendo um elemento independente que acrescenta um sinal extra a função de ativação, também possui um peso associado que faz com que ele ajude na concepção do conhecimento da rede.

Figura 19 - Modelo do neurônio *perceptron*



Fonte: Adaptado de Soares e Souza (2016, p. 5)

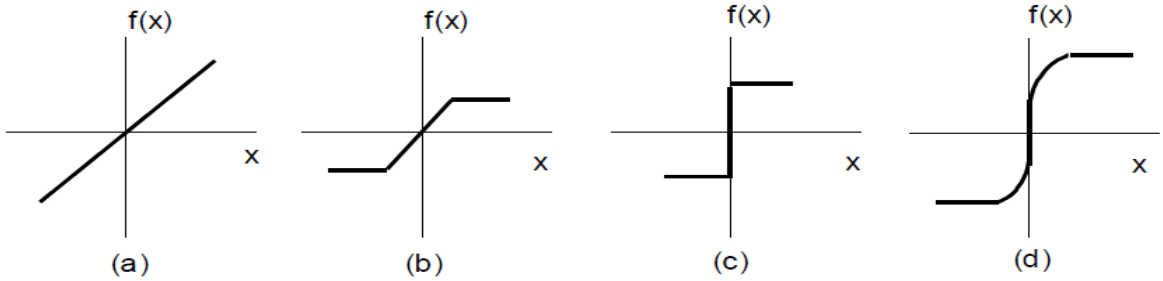
A figura 19 representa o modelo criado por Rosenblatt do neurônio *perceptron*. Este sistema possui entradas, pesos, função soma, o *bias*, função de ativação e uma saída. Sua similaridade com o neurônio de McCulloch e Pitts é perceptível, a diferença está na criação dos pesos que fazem com que o neurônio mude de acordo com um estímulo externo e a integração do *bias* ao sistema. Devido a isto a fórmula do sistema também muda, sendo assim,

acrescentamos os pesos e o valor da *bias* (representado pela letra b) na equação 1, ficando da seguinte forma:

$$\sum_1^n (En \times Pn) + b \quad (3)$$

A partir dos modelos criados, vários outros foram propostos proporcionando variados tipos de saídas, podendo ser ativada por uma função linear (figura 20a), função rampa (figura 20b), função degrau (figura 20c), função sigmoidal (figura 20d), entre outras.

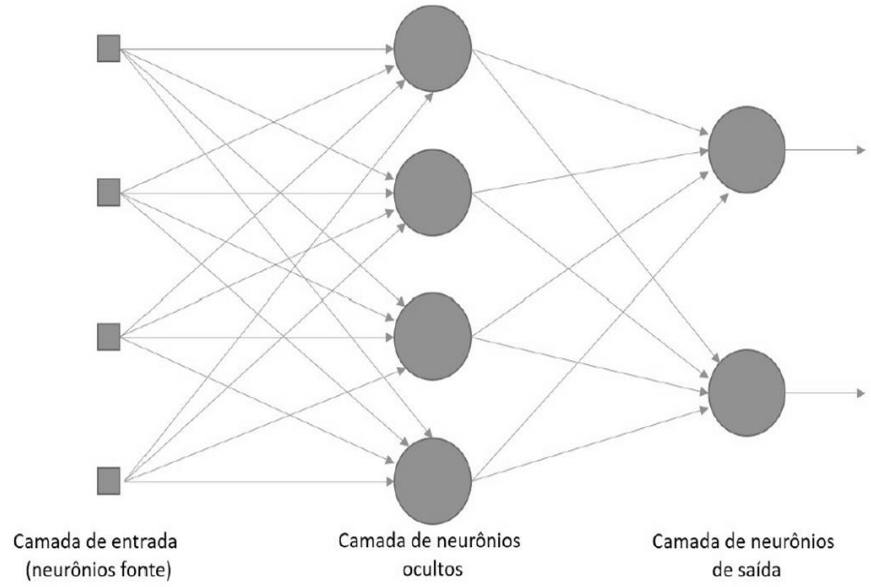
Figura 20 - Algumas funções de ativação



Fonte: Roque (2009, p. 51)

Tendo em vista os modelos de neurônios individuais, a figura 21 representa a formação de um exemplo rede neural em camadas.

Figura 21 - Exemplo de camadas de uma RNA



Fonte: Silva (2016, p. 47)

A figura 21 demonstra um exemplo de uma Rede Neural Artificial (RNA) com múltiplas camadas, tais camadas se diferem entre: camada de entrada onde vem as informações do meio externo, camada de neurônios ocultos (*hidden*), está camada é onde há o primeiro nível de processamento do neurônio podendo possuir mais de uma camada e pôr fim a camada de neurônios de saída onde é demonstrada a solução para o meio externo.

A utilização da quantidade de camadas do sistema depende do tipo de rede que será usada. “A topologia de uma rede neural é a forma como são conectados os elementos que compõem a mesma” (MARTINS, 1997, p. 43).

Braga, Carvalho e Ludemir (2000) *apud* Manica (2014) e Simon Haykin (2008) definem três parâmetros para determinar a arquitetura (estrutura) de uma RNA: o número de camadas – podendo ser dividida em uma única ou múltiplas camadas –, a topologia – sendo fragmentada em *feedforward* (redes nas quais as entradas de um neurônio de camadas anteriores não podem advir de uma saída de neurônio presente em qualquer camada da rede, sendo ela acíclica), e *feedback* (na qual tais entradas podem advir de saídas de neurônios de camadas anteriores, chama também de realimentação) – e a conectividade – podendo ter dois tipos desta: totalmente conectada (onde cada nó da camada se conecta com todos os nós da camada seguinte) e parcialmente conectada (aquela em que nem todos os nós estão conectados a alguma camada adjacente, podendo faltar alguma conexão).

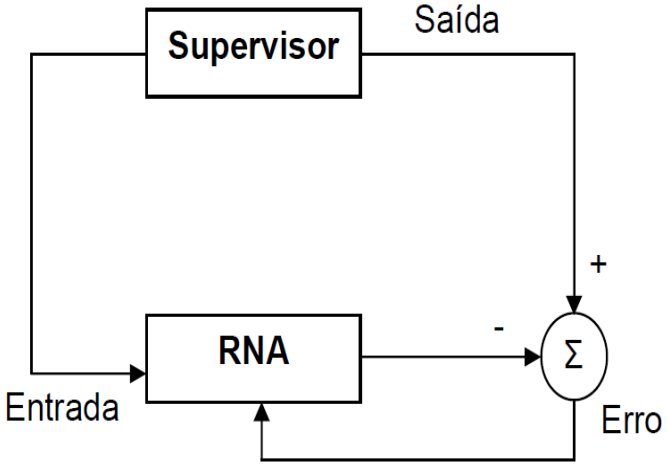
Para o funcionamento eficiente de um RNA alguns estudiosos criaram diversos algoritmos que fazem com que a rede aprenda os padrões requeridos no problema e possam tomar decisões, perante isto Morais dita:

> Redes neurais artificiais possuem a capacidade de aprender por exemplos e fazer interpolações e extrapolações do que aprenderam. Um conjunto de procedimentos definidos para adaptar os parâmetros de uma RNA para que a mesma possa aprender uma determinada função é chamado de algoritmo de aprendizado. Existe uma diversidade de algoritmos de aprendizado e estes diferem basicamente pela maneira na qual o ajuste de pesos é realizado (BRAGA; CARVALHO; LUDERMIR, 2000 *apud* MORAIS, 2010, p. 33).

Morais (2010) exprime que tal etapa de aprendizagem se compõe pelo ajustamento dos parâmetros da rede, os pesos das conexões entre as unidades de processamento e o conhecimento que a rede adquiriu do ambiente. Perante isso, vários métodos de treinamento foram desenvolvidos, sendo eles agrupados em dois grupos de paradigma, o aprendizado supervisionado e o não-supervisionado, que seguem os mesmos conceitos já apresentados no tópico sobre aprendizagem de máquina.

No aprendizado supervisionado, como o nome já diz, existe um supervisor que dita os dados de entrada e controla os dados de saída da rede, criando assim uma ligação entre os dados de entrada e saída. A figura 22 ilustra este mecanismo.

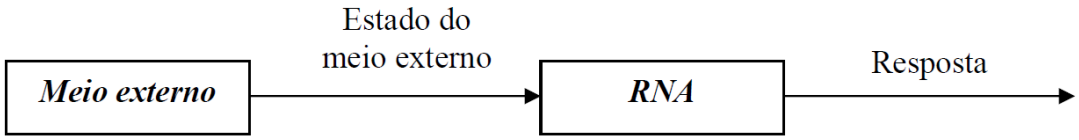
Figura 22 - Aprendizado supervisionado



Fonte: Morais (2010, p. 34)

No aprendizado não-supervisionado o algoritmo aprende sozinho, não possuindo um supervisor, apenas são disponíveis os dados de entrada, feito isto o sistema vai definir quais dados serão os dados de saída, aprendendo assim quais as melhores escolhas de forma independente. A figura 23 ilustra este mecanismo.

Figura 23 - Aprendizado não-supervisionado



Fonte: Morais (2010, p. 35)

Manica (2014), Martins (1997) e Prampero (1998) citam três tipos de redes mais utilizadas:

a) Redes *Perceptron* Multicamadas: são aquelas que possuem mais de uma camada em sua rede além das camadas de entrada e saída, sendo chamadas de camadas intermediárias ou escondida. Quanto mais camadas a rede possuir, mais esta ficará eficiente para determinadas situações, devemos aqui salientar ainda que suas conexões podem ser totais ou parcialmente conectadas (BRAGA; CARVALHO; LUDEMIR, 2000 *apud* MANICA, 2014).

b) Redes Recorrentes:

> São sistemas em que as entradas de cada elemento consistem de uma combinação das entradas da rede com as saídas de outros elementos da rede. Essas redes são apropriadas para sistemas com entradas que podem ser representadas por valores binários (MARTINS, 1997, p. 44).

Pampero (1998) complementa dizendo que em redes que possuem mais camadas, cada uma destas possui uma função específica. Sendo que a saída cada vez que recebe um estímulo de uma camada intermediária constrói o padrão de resposta para a rede, as camadas intermediárias como extratores de características, utilizando seus respectivos pesos para

construir essas características, fazendo com que a rede crie sua própria representação do problema de forma muito mais completa.

c) Redes auto organizáveis: De acordo com os ensinamentos de Manica (2014) são redes que fazem o agrupamento de seus dados encontrando características significativas nos mesmos, sem auxílio de um supervisor. Só pode ser usada quando for possível ter uma redundância em seus dados de entrada. A redundância das entradas faz com que a rede conheça a diferença e semelhança entre os dados, entretanto se não houver essa redundância a rede não consegue caracterizar esses padrões.

Em dessarte ao que diz respeito a topologia das redes neurais, Soares e Souza (2016), ditam que existem diversas possibilidades teóricas na resolução de tarefas, tanto simples quanto complexas, para isso o processo de aprendizado busca descobrir uma solução mais próxima de um resultado satisfatório.

A RNA é bastante utilizada pela sua habilidade de conseguir qualquer tipo de conhecimento, através dos estímulos de entrada que são os dados relevantes para o problema. Quando o treinamento da RNA é executado, produz um resultado aleatório e um erro. Utilizando-se deste erro, a rede vai alterando seus parâmetros até chegar em uma resposta satisfatória.

"Informalmente, uma Rede Neural Artificial (RNA) é um sistema composto por vários neurônios de modo que as propriedades de sistema complexo sejam usadas" (BARRETO, 1999, p. 66). Visto como funciona um neurônio artificial, ao juntarmos vários criamos o que é chamado de Rede Neural Artificial, que nada mais é do que a utilização de vários neurônios para chegar ao resultado esperado.

Os sistemas de RNA's procuram 'pensar' nas decisões que irão tomar com base nos dados obtidos pelo sistema. Para estas decisões garantir a integridade de dados e consequentemente das respostas é de suma importância para organizações, pois com todos os processos citados elas baseiam-se neles para guiar suas ações.

4.5 LÓGICA NEBULOSA

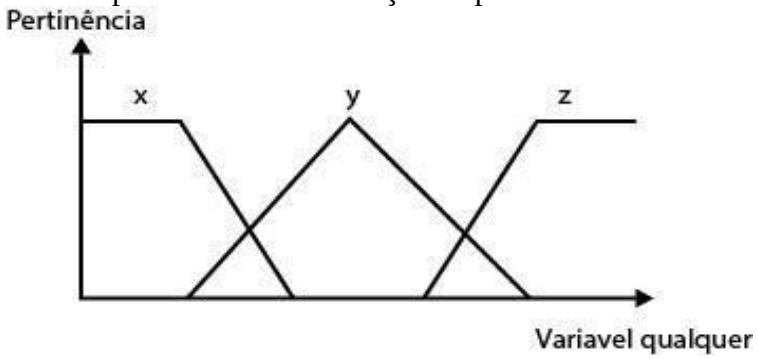
A lógica nebulosa ou *fuzzy* pode ser definida de várias formas e possuir diversos conceitos, mas para Simões (2007), Marro *et al*. (2010) e Chenci *et al*. (2011), ela se baseia no senso comum ou tomadas de decisão, sendo assim capaz de expressar de maneira sistemática atividades mal definidas, vagas ou imprecisas, onde não existe uma clareza de dados, em que cada valor de um conjunto possui um grau de pertinência dependendo do quanto ele tem a características do conjunto para assim chegar a uma resposta mais próxima do real.

Para fazer esta classificação cria-se uma variável linguística específica para cada situação para então gerar uma maneira sistemática de caracterizar os já citados fenômenos complexos ou mal definidos a partir do grau de pertinência (GONÇALVES, 2007).

"A forma de utilização das variáveis linguísticas depende basicamente da definição das propriedades sintáticas e semânticas que vão reger o comportamento do sistema de conhecimento *fuzzy*" (REZENDE, 2005, p. 178). Esse comportamento dependerá de onde o sistema será submetido.

A função de pertinência, pode possuir diferentes formas dependendo do contexto e do conceito que devem ser representados. Abaixo segue um exemplo de modelo de funções de pertinência em uma variável qualquer (figura 24).

Figura 24 - Exemplo de modelo de função de pertinência x variável qualquer



Fonte: Adaptado de Gonçalves (2007, p. 2)

Simões (2007) expõe alguns princípios básicos sobre lógica *fuzzy*, sendo eles: bivalência (na qual existem apenas dois valores para serem comparados, sendo a resposta verdadeira ou falsa, unicamente), multivalência (neste existe um mundo infinito de possibilidades de resposta, trabalhando com a incerteza e a verdade parcial), implicação lógica e regras de inferência (consiste em uma conexão de causa e efeito, como a inferência do SE...ENTÃO) e fuzzificação e defuzzificação natural (a fuzzificação é a transformação de números em conjuntos [número *fuzzy*], como no exemplo da figura 24: conjuntos x, y e z, já a defuzzificação é a transformação de um conjunto ou número *fuzzy* em um número real).

Vimos neste capítulo 4 algumas vertentes da inteligência artificial, como a procura de dados em um grande banco de dados, o aprendizado da máquina e como ela pode nos ajudar a entender alguns problemas do cotidiano. Lidar com problemas complexos exige estratégias de inteligência artificial que hoje se encontram nas mais diversas aplicações, incluindo aí a área de segurança da informação, na qual se pode, a partir de técnicas inteligentes, obter-se processos automáticos mais rápidos, mais flexíveis, mas ainda assim, seguros. Uma dessas aplicações é conseguir reconhecer padrões, podendo ser eles dados, pessoas ou até mesmo situações.

5 RECONHECIMENTO DE PADRÕES

5.1 DEFINIÇÃO

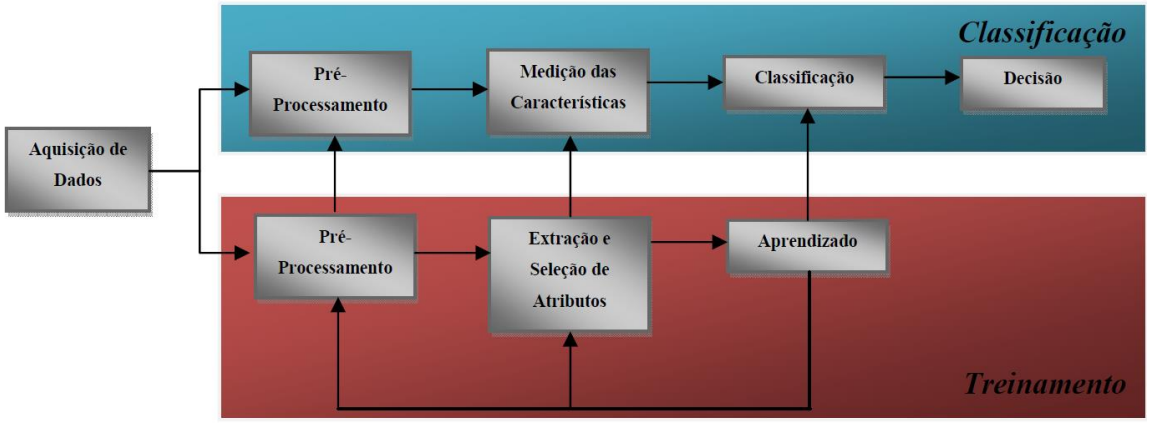
O Reconhecimento de Padrões (RP) consiste em reconhecer aquelas situações que se repetem com frequência, como por exemplo reconhecer a voz ou a face de uma pessoa. Para o ser humano parece ser uma atividade fácil, porém para a máquina ela se torna um pouco mais complexa.

Para Prampero (1998) e Theodoridis e Koutroumbas (2003), RP é reconhecer uma situação ou objeto classificando-as em classes ou categorias para assim gerar conhecimento a partir dos dados adquiridos e depois assimilá-los com os dados já conhecidos para assim chegar a uma conclusão.

> A abrangência do Reconhecimento de Padrões está na sua efetiva realização para as diversas áreas de pesquisas. A área abrange desde a detecção de padrões à escolha mais simples entre dois objetos, como a complexa realização da aprendizagem (MORAIS, 2010, p. 6).

A figura 25 representa um sistema genérico de RP. Tal sistema se divide em dois processos, sendo eles: treinamento e classificação.

Figura 25 - Sistema genérico de Reconhecimento de Padrões



Fonte: Moraes (2010, p. 9)

Antes de começar a funcionar, o sistema faz a aquisição dos dados, indo para a etapa de treinamento que, inicialmente, faz o pré-processamento dos dados adquiridos (que consiste em uma maneira de eliminar ruídos ou distorções) então passa para a fase de extração e seleção de atributos (que cria um vetor de características com dados extraídos dos objetos adquiridos, reduzindo os dados a atributos, propriedades ou características), para então fazer o aprendizado do sistema.

Já na etapa de classificação o sistema recebe os dados para o pré-processamento junto com alguns dados do treinamento. Feito isto, começa a fazer as medições das características (que analisa o conjunto de características e elimina as mais redundantes) e por fim classifica os

padrões obtidos que é realizada por um método de inteligência artificial, já citados no capítulo anterior, e toma uma decisão com base nos mesmos.

Krug *et al.* (2015), Prampero (1998), Morais (2010), Jain, Duin e Mao (1999) e Marin (2003) dizem que existe algumas abordagens de Reconhecimento de Padrões, sendo elas:

- Casamento ou associação (*template matching*): é um modelo usado para discriminar a similaridade entre dois dados do mesmo tipo;
- Conexionista (redes neurais): é um modelo que possui sistemas paralelos de processamento, utilizam os princípios organizacionais já citados anteriormente no tópico de redes neurais;
- Sintático: é o relacionamento da estrutura de padrões com a sintaxe de uma linguagem definida formalmente;
- Estrutural: organiza de uma forma hierárquica de padrões em sub padrão por meio de dados simbólicos;
- Lógica nebulosa: a teoria dos conjuntos nebulosos fornece um cenário mais natural para a formulação e solução dos problemas, principalmente os que envolvem indicadores subjetivos;
- Estatística: possui dois tipos de classificação, a classificação supervisionada onde possuiu uma classe pré-definida e a ajuda de um supervisor humano; e a classificação não supervisionada onde o sistema vai aprender formando um conjunto de classes.

Ainda segundo os autores supracitados, estas abordagens não são necessariamente independentes e às vezes a mesma abordagem de reconhecimento de padrão existe com diferentes interpretações. Para resolução deste presente documento falaremos sobre o reconhecimento biométrico, especificamente os reconhecimentos de impressão digital, da imagem da íris e da gravação da voz. Cada um deles pode utilizar-se de uma ou mais das técnicas citadas acima.

5.2 RECONHECIMENTO BIOMÉTRICO

Diversas tecnologias estão sendo criadas para autenticar e proteger dados ou dar acesso a eles. A biometria vem ganhando espaço por ser uma das mais efetivas e uma forte candidata a tomar conta da vida dos seus usuários que têm necessidade de autenticar alguma forma de informação ou que utilize acessórios físicos para tal (COSTA, 2009). Como vimos no tópico anterior, reconhecer padrões é reconhecer algo para assim classificá-lo e compará-lo com algo já conhecido.

O reconhecimento biométrico realiza a mesma função, porém utilizando as partes do corpo humano como padrão, para poder reconhecer e autenticá-lo. “O termo biometria deriva do grego *bios* (vida) + *metron* (medida) e, na autenticação, refere-se à utilização de características próprias de um indivíduo para proceder à sua autenticação e/ou identificação perante um SI[17] de uma organização” (MAGALHÃES; SANTOS, 2003, p. 5).

> A biometria veio revolucionar a identificação e a autenticação das pessoas. Até agora, a identificação e a autenticação têm-se baseado muito em elementos externos - palavras de passe, códigos (PIN, PUK), nomes de utilizador, cartões, etc. Com a biometria a invadir cada vez mais os sistemas de segurança, a identificação e a autenticação passam a ser algo mais pessoal e intrínseco aos indivíduos, de modo que muitas vezes até poderemos nem nos aperceber que estamos a ser autenticados e identificados (SINFIC, 2005, online).

Liu *et al.* (2001) *apud* Magalhães e Santos (2003) explicitam que existem várias abordagens utilizadas para caracterizar uma pessoa podendo ser isoladas ou em conjunto, sendo utilizados para realizar a autenticação ou identificação.

Tais métodos podem ser avaliados segundo os parâmetros de: grau de confiabilidade (considera-se a taxa de interseção de erros, sob o qual estão as taxas de falsos positivos e falsos negativos, quanto mais baixo for esta taxa mais preciso será o sistema), nível de conforto (relacionado a aceitação de usabilidade[18] do cliente), nível de aceitação (referente ao quanto o usuário aceita-o) e custo de implementação (referente a diversos fatores como: hardware, software, integração hardware/ software, entre outros).

> Perceber os níveis de precisão das tecnologias biométricas é uma tarefa difícil, não só pela complexidade dos testes necessários para os conhecer, mas pela dificuldade de obter esses dados do universo de empresas fabricantes destes dispositivos de autenticação (MAGALHÃES; SANTOS, 2003, p. 5).

Assim como todo o tipo de reconhecimento, o biométrico possui etapas e funciona fundamentado no registro e na verificação de dados. Como primeira etapa o usuário deve fazer um registro no sistema, com isso ele irá armazenar seus dados (por exemplo a impressão digital, a imagem da íris e a gravação da voz), que posteriormente será utilizada para a verificação do usuário.

A segunda etapa acontece na ocasião em que o usuário solicita uma autenticação, então é feita uma comparação entre o dado coletado com o modelo biométrico já armazenado na etapa

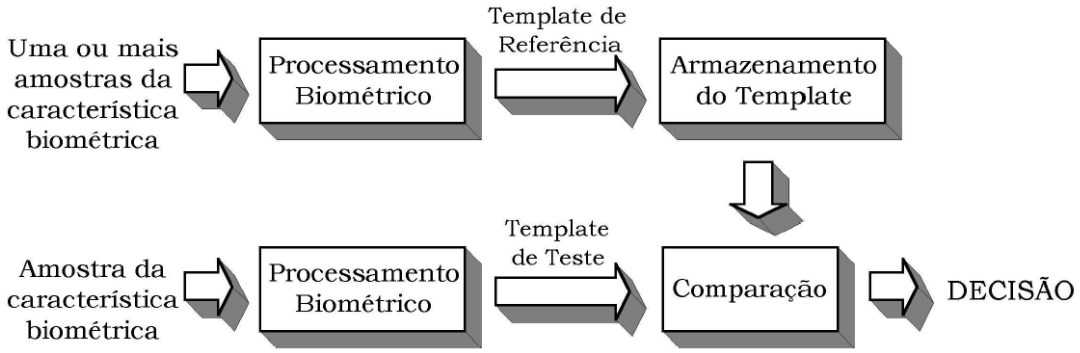
---

[17] **Sistema da informação**: “é o modelo, automatizado ou manual, de processos responsáveis por coletar e transmitir dados que sejam úteis ao desenvolvimento de produtos ou serviços das empresas, organizações e de demais projetos” (SIGNIFICADOS, 2016, online).

[18] **Usabilidade:** “está relacionada à forma como os sistemas são apresentados para a interação com os usuários, podendo ser simples e intuitivos ou complexos e difíceis” (Kawamura *et al.*, 2010, p. 23).

um, para então tomar uma decisão perante dos dados (confirmar ou não o dado) (COSTA, 2009). A figura 26 representa o funcionamento citado.

Figura 26 - Diagrama esquemático do sistema de verificação biométrica



Fonte: Carneiro (2010, p. 7)

5.2.1 Tipos de reconhecimento biométrico

Existem diversas maneiras de fazer o reconhecimento biométrico, entre estas, a impressão digital, voz, face, leitura da íris e/ou retina, geometria das mãos e a verificação da assinatura. Para fins deste documento, falaremos apenas da impressão digital, da íris e da voz.

Estes três tipos de padrões passam pelo mesmo processo de reconhecimento, já citado no tópico anterior, porém a informação que ele recebe é diferente, sendo a impressão digital, a imagem da íris e as ondas sonoras da voz, cada uma possuindo sua peculiaridade.

O reconhecimento de impressão digital, segundo Magalhães e Santos (2003), é o tipo de reconhecimento mais utilizado nos dias de hoje, pois possui um nível de satisfação muito alto devido já ser usado em vários locais, como nos registros civis.

Costa (2009) dita que esse tipo de reconhecimento necessita de um aparelho capaz de capturar, com uma boa qualidade de precisão, os traços que particularizam a impressão dos dedos, sendo esse sistema responsável por transformar as imagens em informações para serem reconhecidas.

A maioria dos sistemas analisam a posição detalhada chama de *minutiae* (que nada mais são do que pontos de interesse da impressão digital, como terminações e bifurcações). Sistemas mais novos, além dos traços citadas, utilizam características como arcos e voltas que aparecem no dedo. A figura 27 representa pontos característicos para reconhecimento a partir de impressão digital.

Figura 27 - Pontos característicos para reconhecimento a partir de impressão digital

Fonte: Matos (2011, p. 8)

O reconhecimento de íris consiste em utilizar os olhos humanos para fazer uma autenticação, para tal compreende a análise do anel colorido que cerca a pupila do olho humano (MAGALHÃES; SANTOS, 2003).

Para entender melhor a singularidade da íris é necessário explicar suas características estruturais. Na sua estrutura leva em consideração aspectos sendo alguns deles, o epitélio distinto e o estroma, não existe somente estes, mas sim um conjunto de aspectos, como vasos sanguíneos (FERREIRA, 1998). A figura 28 representa a imagem da íris humana, sob a qual é realizada o reconhecimento.

Figura 28 - Íris humana

Fonte: Bastos (2010, p. 15)

Reconhecer uma voz para os humanos é uma tarefa fácil, mas dependendo da sua entonação pode se tornar complicada, com o passar dos anos as máquinas começaram a adquirir esse poder. Devido ao indivíduo possuir características físicas únicas, cada um possui uma voz única. Então o processo, além de utilizar essas características da voz, utiliza uma palavra/frase chave para fazer a autenticação do indivíduo (MAGALHÃES; SANTOS, 2003).

Existe uma diferença entre reconhecer a voz e a fala, podendo chegar a confundir em certas situações. “A identificação é feita pela análise dos padrões harmônicos da voz e não

através de uma simples comparação entre reproduções de uma mesma fala" (COSTA, 2009, p. 13).

"O som da voz é produzido pela ressonância na região vocal, baseado no comprimento e no formato da boca e das cavidades nasais" (COSTA, 2009, p. 13). Seguindo esta linha, o autor complementa que, para capturar a voz, precisa-se usar um aparelho receptor. Posteriormente, o usuário pronuncia a palavra/frase chave diversas vezes, fazendo assim um prévio conjunto modelo, para que na próxima vez que for utilizar o sistema, este consiga reconhecê-lo. Para isto, deve possuir um tempo apropriado e ser feito em voz clara para melhor autenticação.

A tabela 1 representa algumas das principais características que os RP's citados necessitam ter para serem usados em autenticação da identidade (MATOS, 2011). São levados em conta sete pontos importantes, a universalidade (características que todas as pessoas têm que possuir), singularidade (característica única em cada pessoa), mensurabilidade (características quantitativas do sistema), permanência (característica que não varia com o tempo), desempenho (referencia-se a precisão, recursos, trabalho ou fatores ambientais que possam prejudicar a leitura), aceitabilidade (aceitação das pessoas), proteção (facilidade ou dificuldade de fraudar o reconhecimento).

Tabela 1 - Comparação das diferentes tecnologias biométricas quanto aos requisitos

Sistema Biométrico	Universalidade	Singularidade	Permanência	Mensurabilidade	Desempenho	Aceitabilidade	Proteção
Impressão digital	Média	Alto	Alto	Média	Alto	Médio	Alto
Íris	Alto	Alto	Alto	Médio	Alto	Baixo	Alto
Voz	Médio	Baixo	Baixo	Médio	Baixo	Alto	Baixo

Fonte: Adaptado de Matos (2011, p. 11)

Ainda referente a tabela 1 pode ser verificado que a impressão digital possui alto desempenho na maioria dos requisitos, sendo ela bem usual em diversas tarefas cotidianas, como por exemplo destravar o celular, a íris apesar de não ter uma aceitabilidade aceitável consegue ser melhor nos demais requisitos, enquanto a voz por ser uma característica humana que pode ser mudada facilmente, por motivos que serão explicados posteriormente, apresenta resultados não muito agradáveis perante os requisitos, entretanto, é a mais aceita entre os usuários e pode causar uma sensação de maior segurança entre eles.

5.2.2 Possíveis razões para o uso dos sistemas biométricos

Levando em consideração o devido trabalho proposto, que é a realização da autenticação de transações, o site Sinfic (2005) articula algumas vantagens do reconhecimento biométrico, sendo elas, o aumento da segurança na transação e do não repúdio (devido ser difícil contradizer transações fundamentadas em dados biométricos).

Sem contar que com a utilização atual dos cartões, os mesmos podem ser perdidos ou esquecidos, podendo ser usados por outras pessoas. Porém como as características biológicas são pessoais e intransmissíveis, na maioria dos casos, o seu uso exige a presença física do dono do cartão.

Vários autores ditam sobre os benefícios de utilizar sistemas biométricos, já que para autentica-los o portador do cartão tem que estar presente. Perante isso apresentaremos as razões para a utilização dos sistemas de reconhecimento de impressão digital, íris e voz.

Como visto na tabela 1, o reconhecimento de impressão digital uma alta proteção e singularidade únicas, sem contar com uma boa aceitação perante as pessoas, sendo utilizada, por exemplo, nas urnas eletrônicas do Brasil.

Magalhães e Santos (2003) informam que existem leitores que tentam ultrapassar o ‘efeito dedo morto’ recorrendo a sensores de tensão arterial, condutividade, temperatura e leitura de padrões existentes em camadas inferiores à epiderme. No entanto, estas tecnologias são caras e ainda não atingiram o nível de maturidade desejado.

Segundo Costa (2009), a impressão digital apresenta duas vantagens principais rapidez e confiança, conivente ao baixo custo e o pequeno tamanho dos leitores óticos.

O reconhecimento de íris segundo, Costa (2009) e Magalhães e Santos (2003), é um dos métodos mais eficientes pois apresenta taxas de acerto, precisão e segurança bem melhores do que as outras e um baixo custo de implementação pois uma câmera normal pode ser utilizada para realizar o reconhecimento.

“Em virtude de suas características, a íris oferece meios de identificar cada indivíduo de forma única em uma grande população de indivíduos” (ADLER, 1965 *apud* COSTA, 2009, p. 17). Mesmo com o grande grau de universalidade, singularidade e proteção muitas pessoas ainda possuem um certo preconceito, por ser um dos meios mais invasivos.

Com a utilização de sistemas de reconhecimento de voz é possível empregar uma ótima usabilidade, a um ponto de reduzir as lesões causadas por esforço repetitivo, estresse pela execução de tarefas complicadas, excessiva memorização de operações complexas e entre outras. Além de promover uma interação mais rápida com a atividade que o usuário realiza, por exemplo atendimento em *call center* no qual, o cliente ao falar comandos, o computador possua a capacidade de identificá-lo (KAWAMURA *et al,* 2010).

Costa (2009) e Magalhães e Santos (2003) falam que, o reconhecimento de voz é um método muito econômico, não necessitando de dispositivos especiais, apenas de um aparelho receptor de voz, como exemplo o microfone.

5.2.3 Possíveis razões para a falha dos sistemas biométricos

Thain (2001) *apud* Magalhães e Santos (2003) exprime que existem dois problemas ao estabelecer uma associação entre um indivíduo e sua identidade, sendo eles, autenticação e associação. A autenticação concerne a problemática de negar ou autenticar a identidade de um indivíduo. A identificação relaciona-se a estabelecer a identidade, desconhecida *a priori*, de um indivíduo.

Magalhães e Santos (2003) relatam que o reconhecedor de impressão digital é o que possui menor fiabilidade[19] dentre todos os outros. Isto é devido aos equipamentos normalmente utilizados não conseguirem distinguir, eficientemente, um dedo morto de um dedo vivo. Além do mais, hoje em dia é muito fácil fabricar uma impressão digital sintética, com ou sem ajuda do proprietário.

Costa (2009) diz que alguns ferimentos, sujeiras, ou ressecamento da pele podem dificultar ou até mesmo impedir a leitura da digital. Além de alguns usuários relacionarem este meio a fichas criminais, causando um grande desconforto. Levando em conta a grande divulgação tornou-se fácil burlá-la.

Além dos problemas citados para a identificação podemos apontar dedos com muita ou pouca umidade, o ângulo de colocação do dedo, pressão exercida no leitor, entre outros problemas que façam com que o leitor não consiga identificar a impressão digital.

[19] **Fiabilidade:** Particularidade do que é fiável (confiável); confiabilidade.

A íris possui obstáculos de utilização e integração com sistemas presentes na atualidade, necessitando de uma imagem com qualidade alta para que não haja problemas na identificação (MAGALHÃES; SANTOS, 2003).

Alguns outros motivos podem ocasionar no problema de identificação da íris como umidade do ambiente, curvatura na leitura, pálpebras, cílios, são susceptíveis a reflexos, contrações e dilatações da pupila.

Costa (2009) cita que este sistema que utilizam o reconhecimento de voz possuem algumas desvantagens como sensibilidade ao ruído, variações de canal e variações comportamentais humanas.

Alguns outros motivos como doença que afete a voz ou outros aspectos que alterem a voz, a utilização de diferentes equipamentos de captura e verificação da voz, diferentes ambientes de captura (no exterior ou no interior), alteração da forma de falar (de forma mais delicada ou rude, mais lenta ou rápida), deficiente captura da voz (por mau posicionamento do microfone, por exemplo) e a qualidade do equipamento de captura (SINFIC, 2005).

Falamos no capítulo 5 como reconhecer padrões e quais os tipos mais usuais de se autenticar algum dado que necessite de proteção. Alguns desses métodos são utilizados para realizar compras no lugar do uso do cartão de crédito/débito. A interação com o cartão como método de pagamento será tratada mais adiante, no capítulo 6.

6 CARTÃO DE CRÉDITO

Pode definir cartão de crédito como,

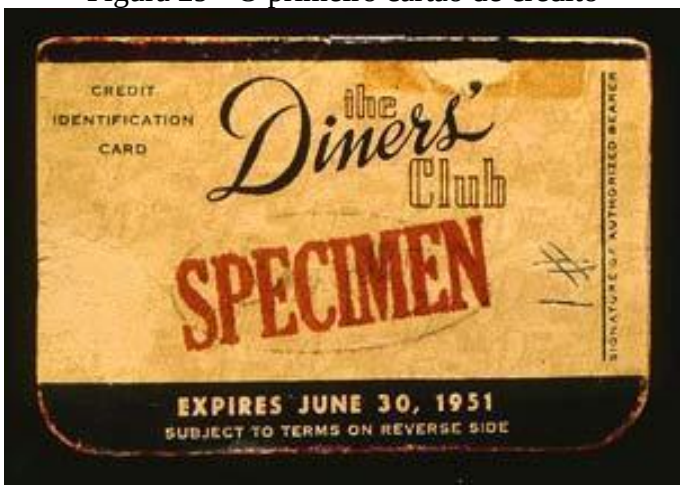
> Um meio que possibilita o pagamento à vista ou parcelado de produtos e serviços, obedecidos requisitos pré-determinados, tais como, validade, abrangência, limite do cartão, etc. Foi criado com a finalidade de promover o mercado de consumo, facilitando as operações de compra (FUNDAÇÃO PROCON SP, [200-?], online).

6.1 HISTÓRICO

Segundo o site Museu do Cartão de Crédito (2016, online), "já nos anos 20 alguns estabelecimentos davam créditos a alguns clientes, mas foi no início dos anos 50 que de fato foi criado o cartão de crédito". Os primeiros cartões de crédito eram fabricados em papel (figura 29), após os anos evoluiu a tecnologia do processo e o material do qual era feito.

Como exemplo da evolução no processo da segurança dos dados de cartões, a Associação Brasileira das Empresas de Cartão de Crédito e Serviços, ABECS afirma que "todas as transações trafegam por sistemas seguros, onde as informações das operações são criptografadas" (ABECS, 2016, online).

Figura 29 - O primeiro cartão de crédito



Fonte: Redação em Alta (2016, online)

Gadi (2008) reconhece que o empresário tcheco Hanus Tuaber foi o primeiro a trazer os cartões para o país. Nos EUA, comprou a franquia Diners Club, convidando o empresário Horacio Kablim para uma sociedade.

Afirma Gadi (2008) que o cartão de crédito chegou no ano 1956, no Brasil, o Diners Club. E "inicialmente funcionava como um cartão de compra[20] e não um cartão de crédito" (GADI, 2008, p. 15). Em 1968, foi lançado o primeiro cartão de crédito de banco, chamado ELO pelo Banco Bradesco. Entretanto, Em Alta (2016) declara que não remete a bandeira ELO que é comercializada no mercado atualmente pelo Bradesco, Banco do Brasil e Caixa

[20] **Cartão de compra:** nos dias atuais, é o cartão pré-pago.

Econômica. A ELO era uma parceira da BankAmericard, tornando futuramente a atual Visa, que atendia os turistas que portadores dos cartões que visitavam o Brasil.

No ano de 1971, foi criado a Associação Brasileira das Empresas de Cartões e Serviços (ABECS).

> Objetivo é contribuir para o fortalecimento e expansão da categoria, representando seus participantes junto ao mercado, poder público em suas diversas instâncias, órgãos de defesa do consumidor e sociedade em geral. [...] vem trabalhando para a intensificação do uso consciente dos meios eletrônicos de pagamento, através de uma campanha educativa voltada tanto para o portador do cartão quanto aos estabelecimentos comerciais [...] (ABECS, 2017, online).

Em 1983, "foi lançado o primeiro cartão de débito" (GADI, 2008, p, 15) no país (figura 30). No ano seguinte, a Credicard acabou sendo adquirida pela Diners Club, no Brasil.

Figura 30 - Primeiro cartão de débito no Brasil

Fonte: Bradesco (2013, online)

Gadi (2008) declara que um fato que colaborou para o uso internacional do cartão de crédito foi o Plano Real, pois houve abertura do mercado no governo Fernando Collor de Mello (1990 – 1992). O Plano Real também contribuiu para o uso internacional do cartão de crédito, devido à baixa inflação que reduziu e praticamente eliminou as sobretaxas relacionadas.

6.2 FUNCIONAMENTO DA MÁQUINA DE CARTÃO

Existem dois modos para iniciar o processo de transmissão de dados no uso do cartão de crédito/débito: tarja magnética e chip (EMV), como se observa na figura 31. A tarja magnética é uma forma de guardar as informações fundamentais para poder acontecer a transação e a mesma é composta por uma faixa que esconde três linhas, que são magnetizadas e possuem a orientação no sentido de 'baixo para cima'. Essas linhas possuem um código binário que o *software* da máquina interpreta (SANT'ANA, 2012, online).

> A tarja armazena memória que somente pode ser lida, já o chip além de ser lido pode ser gravado também e em alguns casos realizar processos como confirmação de transações, bloqueio e renovação de senhas, etc. Além de claro, prover segurança adicional usando complexas criptografias 3-DES (INFORMATÁVEL, 2013, online).

A tecnologia do chip, conhecido como EMV foi desenvolvida e gerenciada por bandeiras, segundo Squareup [201-?]: Europay, Mastercard, Visa, American Express, Discover, JCB e UnionPay. Porém a sigla é devido a três bandeiras: Europay, Mastercard e Visa.

Sant'Ana (2012) menciona alguns fatores de diferença do chip em relação a tarja magnética, como a capacidade de armazenamento maior e o fato de ser mais seguro, devido ser um microprocessador que criptografa os dados. Assim, por motivo de segurança, somente alguns *softwares* peculiares podem fazer a decriptação. Com o chip, o usuário precisa digitar a senha na máquina.

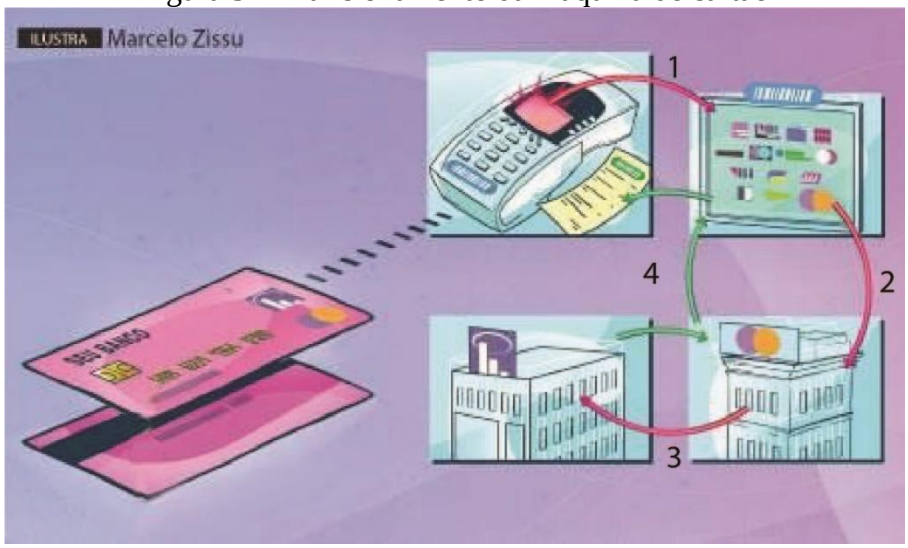
Figura 31 - O cartão de tarja magnética e o EMV

Fonte: Canal no YouTube *Follow The Coin* (2015, online)

O processo de compra utilizando o cartão é dado em uma série de etapas (SANT'ANA, 2012). Inicialmente, os dados são convertidos pela máquina em sinal transmitido pelo mesmo sinal que o sistema de telecomunicações utiliza nos celulares.

Assim, esse sinal é enviado para a credenciadora, que é aquelas "empresas que habilitam estabelecimentos fornecedores de bens e/ou prestadores de serviços para aceitarem cartões", (ABECS, 2017, online). Para continuar o processo, a credenciadora faz a ponte com a bandeira do cartão, como por exemplo Visa e DinersClub, pois a mesma determina regras e políticas de uso. Por fim, a credenciadora entra em contato com o emissor do cartão que são, na sua maioria das vezes os Bancos que tem a função de autorizar o processo todo e retorna a resposta para a máquina com uma mensagem dizendo o status da transação. Todo esse processo da transação pode ser observado na figura 32 a seguir.

Figura 32 - Funcionamento da máquina de cartão



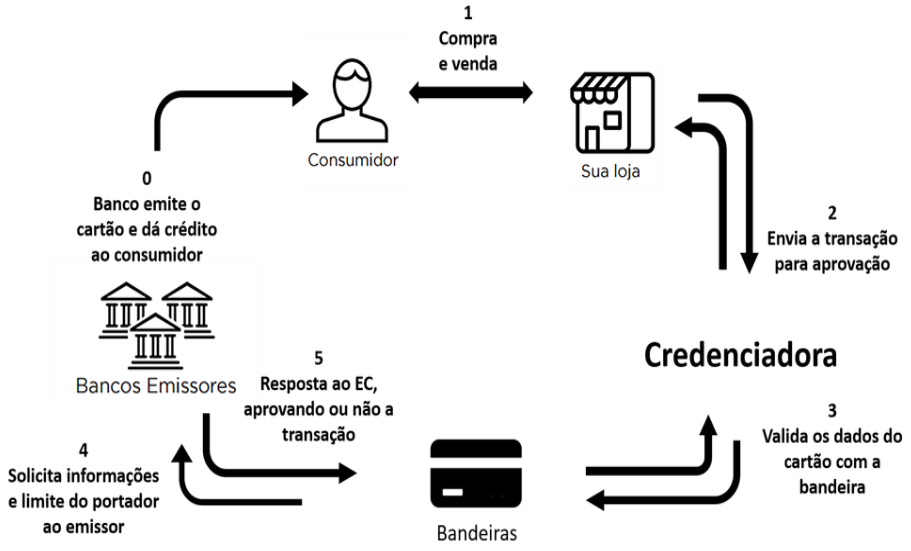
Fonte: Adaptado de Sant'Ana (2012, online)

6.3 AGENTES

Em torno do funcionamento do cartão, existem cinco agentes: portador, estabelecimento, adquirente, bandeira e emissor. A interação entre os agentes acontece quando uma transação ocorre.

A figura 33 mostra como os agentes participam de todo o processo, desde a emissão do cartão até a resposta de aceitação ou negação da transação. Esse processo evoluiu devido a tecnologia, não somente no Brasil, mas no mundo. Um exemplo de evolução nesse processo, durante os anos, é a máquina de cartão, pois antes era utilizado a máquina de papel carbono.

Figura 33 - Esquema dos agentes no processo da transação



Fonte: Associação Brasileira de Instituições de Pagamentos ([201-?], online)

A seguir, uma descrição mais detalhada do processo da figura 33, de acordo com a conceituação de agentes feita por Gadi (2008).

6.3.1 Portador ou Consumidor

O cliente é chamado portador, e é quem possui o cartão. É o agente responsável por iniciar o processo do sistema de transações.

O cliente precisa pôr uma senha numérica para validar a transação, que é uma autenticação baseada no conhecimento, em outras palavras “o que se sabe” (BRITO, 2009). Outra forma de autenticação é o *token*, já mencionado no capítulo de criptografia.

6.3.2 Estabelecimento ou Loja

O estabelecimento é qualquer empresa ou pessoa jurídica devidamente qualificada para aceitar o cartão por via de um equipamento como forma de pagamento.

6.3.3 Adquirente ou Credenciadora

Segundo ABECS (2016). O adquirente é o responsável pela instalação e suporte das máquinas de cartão que realização as transações como: POS e POO, por exemplo, e dos *softwares* de transações. “A função principal dessa empresa é credenciar, supervisionar e repassar os valores de compras/saques aos estabelecimentos que aceitam cartão de crédito” (GADI, 2008, p. 17).

No Brasil, a maioria das bandeiras como, Visa e MasterCard, possuem o adquirente específico, ou seja,

> Cada Adquirente possui monopólio da filiação para uma determinada Bandeira, de modo que cada pequeno ou grande estabelecimento comercial tem que negociar e locar dispositivos de capturas de transação de cada um destes monopólios (GADI, 2008, p. 17).

6.3.4 Bandeira

Gadi (2008) afirma que a bandeira é o agente que administra as regras, políticas e o uso que regem o cartão. Também está ligado com a relação entre emissores e adquirentes. Na tabela 2, são alguns exemplos de bandeiras existentes, no Brasil e em outros países.

Tabela 2 - Primero dígitos correspondentes com suas respectivas bandeiras

BANDEIRAS	BIN	INTERVALO DE DÍGITOS	MÁXIMO DE CVC
American Express	34, 37	15	4
Diners Club	301, 305, 36, 38	14 ou 16	3
JCB	35	16	3
HiperCard	38, 60 (exceto 6011)	13, 16 ou 19	3
Amex	34 e 37	15	4
Visa	4 (exceto 438935, 451416, 4576, 4011)	13 ou 16	3
Aura	50 (exceto 504175, 5067)	19	3
MasterCard	51, 52, 53, 54 ou 55 2 (a partir de 2017)	16	3
Discover	6011, 622126 até 622925, 644, 645, 646, 647, 648, 649, 65	16	4
ELO	636368, 438935, 504175, 51416, 636297, 5067, 4576, 4011 e 506699	16	3

Fonte: Autores (2018)

6.3.5 Emissor

Emissor é o distribuidor dos cartões, sendo na sua maioria das vezes os Bancos (GADI, 2008). Cada Banco tem a sua política de aprovação que o oferece aos seus clientes.

> Podem figurar de duas formas no arranjo. Podem ser Banco Emissor dos cartões de débito e de crédito, como também podem aparecer como Instituição Domicílio, ou seja, o banco em que o estabelecimento comercial mantém sua conta (ABIPAG, [201-?], online).

6.4 TIPOS DE CARTÃO

No mercado, são oferecidos alguns tipos principais de cartões podendo ter bandeiras diversas: crédito, débito, pré-pago, múltiplo e de loja (ABECS, 2017). Esses tipos de cartões, divergem principalmente na parte lógica no funcionamento, porém são idênticos fisicamente.

> Sabemos bem que praticamente quase todo cartão hoje possui essa conhecida função crédito, mas existem outros tipos de cartões também, tais como débito, refeição, alimentação, convênio, farmácia, clube, fidelidade, crediário, presente, etc… Cada "tipo" de transação que o cartão pode fazer é chamado de modalidade (INFORMATÁVEL, 2013, online).

As principais modalidades de operação podem ser diferenciadas da seguinte maneira:

- **Crédito**: Esse tipo de cartão permite fazer uma transação durante o mês e no momento do pagamento será perante a uma fatura, na data definida pelo portador;
- **Débito**: Nessa forma de operação, o cartão é associado a uma conta bancária. Assim, no momento de uma transação é automaticamente debitado da mesma, partindo da premissa de dispor de saldo;
- **Pré-pago**: o portador do cartão irá 'carregar' um valor X no mesmo *a priori* e, na hora da transação, será subtraído a partir do valor da 'carga'. O usuário possui controle nos valores máximo e mínimos. Algumas empresas especializadas em cartões dessa modalidade, disponibilizam aplicativos para seus clientes, como, por exemplo, Brasil Pré-Pagos;
- **Múltiplos**: Este tipo é a junção do funcionamento do cartão de crédito e débito em um único local, podendo o portador escolher qual modalidade quer usar para fazer o pagamento, a cada vez;
- **De loja**: Funciona como um cartão de crédito normal, porém foi criado para ser usado naquela loja, embora, hoje em dia, já existam cartões de loja que são aceitos em estabelecimentos diferentes da loja que os emitiu.

6.5 COMO SÃO CRIADOS OS NÚMEROS DE CARTÃO DE CRÉDITO

Existe dezesseis números na frente do cartão, sendo que cada um tem seu propósito, criados por um algoritmo que os identifica como validos. Esta sequência é reconhecida por todos os países do globo, sendo definida pela ISO/IEC 7812-1[21] (VENTURA, 2013).

A figura 34 ilustra qual o significado de cada um dos dezesseis dígitos do cartão. Os seis primeiros números identificam a instituição que emitiu o cartão, os nove subsequentes identificam o cliente do cartão (gerados aleatoriamente) e o último número é o dígito verificador.

[21] **ISO / IEC 7812-1**: 2017 especifica um sistema de numeração para a identificação dos emissores de cartões, o formato do número de identificação do emissor (IIN – *Issuer Identification Number*) e o número da conta principal (PAN – *Primary Acount Number*) (*International Organization for Standardization*, 2017, online, tradução nossa).

Figura 34 - Informações correspondentes a cada um dos números do cartão de crédito

Fonte: Ventura (2013, online)

Segundo Held (2017), os seis dígitos iniciais do cartão correspondem ao BIN (*Bank Identification Number*), devendo ser ressaltado que estes números iniciais sempre se referem à bandeira representada, e trazem informações como emissor, tipo de cartão e classe (como *gold*, *platinum*, entre outros).

O último dígito do cartão é o chamado algoritmo de Luhn ou dígito verificador que serve (VENTURA, 2013), para prevenir quando cliente errar a sequência numérica e para não deixar *hackers* criarem números aleatórios para cartões que funcionem.

> Você não escolhe este último dígito: ele é determinístico. A fórmula matemática exata para gerá-lo foi inventada por Hans Peter Luhn, um engenheiro da IBM, em 1954. Originalmente patenteado, o algoritmo está agora no domínio público… o algoritmo de Luhn é inteligente na medida em que detecta qualquer erro único (de um único dígito), tal como trocar o 9 por um 6 (VENTURA, 2013, online).

Lage (2018) demonstra o algoritmo de Luhn da seguinte forma: os números em posições impares são multiplicados por um peso 2, caso este valor exceda dois algoritmos soma-se os valores absolutos dos mesmos – por exemplos: 9 por 2, seu valor dará 18, sendo formado por dois algoritmos, faríamos 1 + 8 = 9. Ou pegamos o resto da divisão deste número por nove –, e seus números pares multiplicados por um peso 1. Feito isto, soma-se a cada combinação e então combina-se a reposta das posições pares com as posições impares. Então o número verificador será o número que falta para chegar a um múltiplo de dez.

As equações abaixo representam este cálculo, sendo a equação 1 representa os dígitos do cartão, a equação 2 é o vetor de pesos, e a equação 3 o produto da soma entre eles.

$$C = [c_1\ c_2\ c_3\ c_4\ \dots\ c_{15}] \quad (1)$$

$$P = [2\ 1\ 2\ 1\ 2\ 1\ 2\ 1\ 2\ 1\ 2\ 1\ 2\ 1\ 2\ ] \quad (2)$$

$$C\ .\ P^t = 2c_1 + c_2 + 2c_3 + c_4 + \dots + 2\ c_{15} \quad (3)$$

O resultado da equação 3 será o dígito verificador do cartão.

Além do dígito verificador, tratado anteriormente, existe mais um código que é gerado pelo emissor do cartão, que é calculado ao se criptografar o número do cartão e sua data de validade.

> O código de verificação do cartão (CVC) são os três ou quatro dígitos do código de segurança do cartão de crédito e que não está gravado no cartão junto aos números frontais, impedindo sua impressão do recibo e que alguém sem esses números tente realizar alguma transação utilizando seu cartão de crédito (CRÉDITO OU DÉBITO, 2012, online).

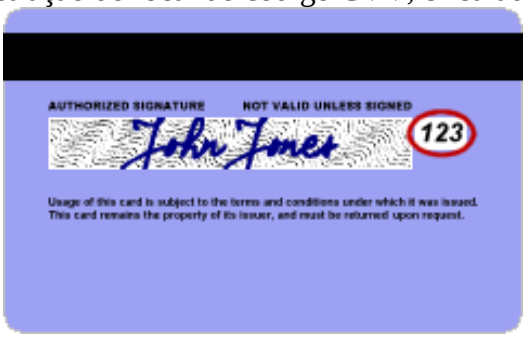
O CVC é utilizado para aumentar a proteção contra fraudes e para evitar também que o cartão seja clonado ou algum outro tipo de golpe. Tem sua aplicação em transações online pois dá uma maior proteção, já que exige que o usuário o tenha em mãos e em nenhum momento a loja física tem autorização de requerer o CVC, apenas as lojas online.

Este código pode ter diversos nomes e apresentar algumas diferenças na sua verificação, dependendo da empresa da bandeira que o utiliza, como exemplo de códigos:

- CAV (*Card Authentication Value* - Valor de Autenticação do Cartão): cartões de pagamento JCB, possui também o CAV2;
- PAN CVC (*Primary Account Number Card Validation Code* - Número de Conta Principal Código de Validação do Cartão): cartões de pagamento MasterCard, possui também o PAN CVC2;
- CVV (*Card Verification Value* - Valor de Verificação de Cartão): cartões de pagamento Visa e Discover;
- CSC (*Card Security Code* - Código de Segurança do Cartão): American Express);
- CID (*Card Identification Number* - Número de Identificação de Cartão): cartões de pagamento American Express e Discover;
- CVV2 (*Card Verification Value* 2 - Valor de verificação de cartão 2): cartões de pagamento Visa.

A figura 35 ilustra o local a parte de trás do cartão onde pode ser encontrado o CVC, circulado.

Figura 35 - Ilustração do local do código CVV, circulado em vermelho



Fonte: Ventura (2013, online)

6.6 TIPOS DE MÁQUINA DE CARTÃO

A máquina de cartão é responsável fazer a transmissão dos dados financeiros, se tornando o intermédio do processo entre o cliente e o Banco, e é responsável pelo retorno do resultado da transação.

Hoje em dia existem diversos tipos de máquinas de cartão, tanto aquelas conectadas a fio, quanto as que utilizam o smartphone e também que aceitam ou não certos tipos de cartão (crédito e/ou débito). Falaremos apenas das principais maquinas utilizadas que são: POS (*Point of Sale*), POO (*Point of Outdoor*), TEF (Transferência Eletrônica de Fundos) e Cartão *Mobile*.

6.6.1 POS (*Point of Sale*)

Pode-se define POS como o "h*ardware* e/ou *software* usados para processar transações com cartão de pagamento nos endereços do comerciante" (PCI *SECURITY STANDARDS COUNCIL*, 2016, p. 20).

É a máquina mais conhecida dentre todas. Utilizam a linha telefônica para conexão, sendo ela discada. São capazes de imprimir os recibos sem utilizar nenhum outro tipo de equipamento. Ela também pode ser do tipo POS *wireless* que tem mesma funcionalidade da de linha, porém restringe-se ao alcance do *wi-fi* (KONKERO, 2017).

Na figura 36 é mostrada a máquina desse tipo, possuindo uma tela LCD para poder ver as ações, como: ver ser a transação foi negada ou aprovada ou o valor inserido para poder realizar o pagamento, por exemplo; e um teclado para pôr a senha e fazer a configuração. "Alguns tipos de POS ainda podem ter um *firmware* que se comunicam com um servidor TEF, fazendo com que o POS aproveite também a estrutura de TEF dedicado" (INFOMATÁVEL, 2013, online).

Figura 36 - Modelo da máquina de cartão do tipo POS

Fonte: *El Observador* (2015, online)

6.6.2 POO (*Point of Outdoor*)

São máquinas que utilizam um chip de celular para a transmissão das informações da compra, tendo seu funcionamento similar com o da POS. Devido a utilizar o chip possuem um maior alcance, sendo mais utilizadas, por exemplo, em pedidos *delivery*, ou qualquer transação a longa distância (KONKERO, 2017).

A figura 37 apresenta a máquina de cartão POO, possui uma estrutura muito parecida com o POS, entretanto ela pode ser utilizada sem conexão a cabo e longe do terminal.

Figura 37 - Modelo da máquina de cartão do tipo POO

Fonte: Aquário (2016, online)

6.6.3 TEF (Transferência Eletrônica de Fundos)

Hoje em dia as empresas possuem um grande fluxo de transações. Devido a isto, precisam ter uma boa gestão e controle financeiro, e a máquina TEF vem para proporcionar este benefício.

> É a comunicação que ocorre entre o lojista e as administradoras de cartões para a realização de transações financeiras de cartões de crédito/débito que são integradas com software de gestão da loja para a emitir cupons fiscais. Essa solução facilita a vida dos lojistas por garantir maior agilidade, segurança e economia para o negócio próprio, além de reduzir drasticamente as porcentagens de erro (TW SISTEMAS, 2017, online).

Ela pode ser encontrada em três modelos: discado, dedicado e IP (*Internet Protocol*). Modelos estes que serão tratados logo em seguida. A figura 38 mostra um modelo da máquina de cartão tipo TEF.

Figura 38 - Modelo da máquina de cartão do tipo TEF

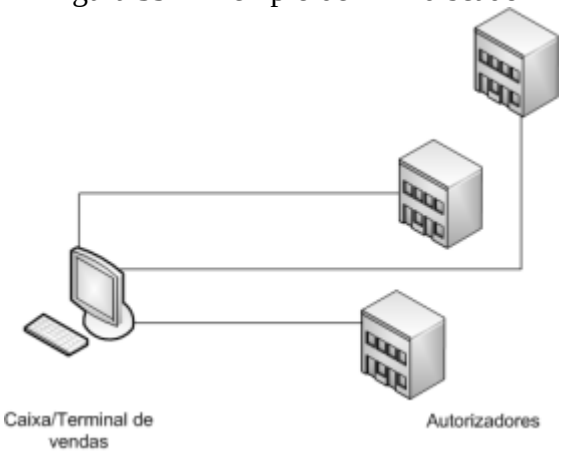
Fonte: Inventti (2017, online)

6.6.3.1 Discado

Usualmente usada em negócio de pequeno e médio porte, pois não necessita de grande quantidade caixas. A cada transação a máquina manda um pulso telefônico, sendo assim, se o negócio possuir uma grande quantidade de transações poderá ocorrer perdas (INFORMATÁVEL, 2013; MEGASUL SISTEMAS, 2009).

Seu funcionamento aproveita-se de uma conexão baseada em linhas telefônicas para compartilhar as informações, mas costumam ser lentas no retorno de uma resposta (INVENTTI, 2017). Na figura 39, observa-se um exemplo de TEF discado onde o terminal de vendas comunica-se com os autorizadores respectivos do cartão a fim de retornar o resultado da operação.

Figura 39 - Exemplo de TEF discado



Fonte: Informatável (2013, online)

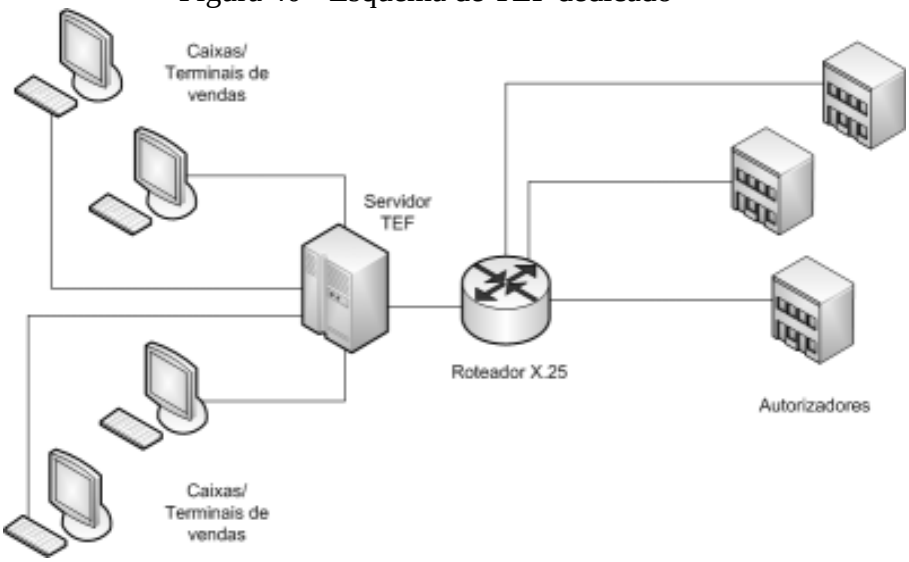
6.6.3.2 Dedicado

Bem como diz respeito ao nome, precisa-se ter uma conexão dedicada fazendo assim com que as informações sejam centralizadas em um único ponto, podendo ser uma linha X.25 ou uma conexão VPN (*Virtual Private Network*) pela Internet (INFORMATÁVEL, 2013).

Este tipo de conexão possibilita uma maior agilidade e rapidez no processo da transação, além de uma maior segurança (INVENTTI, 2017).

A figura 40 retrata o esquema de funcionamento dedicado. Representa a conexão dos terminais com um servidor TEF, centralizado em um roteador X.25, que faz a conexão com os autorizadores.

Figura 40 - Esquema de TEF dedicado



Fonte: Informatável (2013, online)

6.6.3.3 IP

Este tipo de TEF dispõe de uma conexão através da internet utilizando o Protocolo IP para compartilhar as informações. Utilizado por grandes empresas, onde o fluxo de transações

é muito alto, impossibilitando a utilidade do TEF discado e do POS. É a solução mais veloz devido sua conexão com a Internet (INVENTTI, 2017).

6.6.4 Máquina de Cartão *Mobile*

Este tipo são leitores que se conectam com smartphones, através de cabo ou conexão *bluetooth*. Sua forma de transação é via Internet, através de um aplicativo baixado no *smartphone* da empresa. A figura 41 mostra um modelo de máquina tipo cartão *mobile*, conectada por *bluetooth* com dois *smartphones* diferentes por um aplicativo.

Figura 41 - Modelo da máquina de cartão do tipo Cartão *Mobile*

Fonte: Higa (2016, online)

6.7 PCI DSS (*Payment Card Industry – Data Security Standard*)

Segundo Mota (2017), o PCI DSS é um padrão de normas de segurança com o foco na indústria de cartões de crédito, válido tanto para comércio físico quanto virtual, e um formado uma cúpula por bandeiras como MasterCard, Visa e American Express. Essas normas empregam a todos os envolvimentos no processo de pagamento (portador, estabelecimento, adquirente, bandeira e emissor) e daqueles que armazenam e transmitem os dados.

Após 2016, o assunto segurança da informação é cada vez mais importante, pois muitas empresas foram centro de invasão como SnapChat e Dropbox, por exemplo e devido à importância desses dados, Mota (2017) afirma que foi elaborado o PCI DSS em 2006.

> Essa certificação é necessária para qualquer empresa que armazene, transmita ou processe informações sigilosas de portadores de cartões. Dados como nome, número do cartão e código de segurança devem ser criptografados para a segurança dos portadores de cartões. É muito importante destacar que a contratação de um antifraude é essencial para o *e-commerce*, mas ele não substitui a necessidade de um certificado PCI (MOTA, 2017, online).

O Brasil se encontra entre os mercados mundiais mais importantes na utilização do PCI-DSS, “com 12,3 bilhões de transações em 2016 (débito e crédito) e, recentemente, atingiu o

segundo lugar em ciberataques" (TIINSIDE ONLINE, 2017, online). Em 2017, foi celebrado um ano no Brasil e o PCI DSS encontra-se na versão 3.2, desde de abril de 2016.

Essa regulamentação é composta por 12 normas (ou requerimentos) que são subdivididas em 6 categorias, como podemos observar na figura 42. Em cada requisito, existem procedimentos de teste e assim uma respectiva orientação a ser cumprida. Alguns termos apresentam descritivos como: requisitos (padrão de segurança dos dados), procedimentos de teste (testes utilizados para validar os requisitos, se estão sendo atendidos e vigentes) e orientação (tem como propósito amparar o motivo de cada requisito) (PCI *SECURITY STANDARDS COUNCIL*, 2016).

Figura 42 - Padrão de segurança de dados do PCI – Visão geral de alto nível

Construir e manter a segurança de rede e sistemas	**1.** Instalar e manter uma configuração de firewall para proteger os dados do titular do cartão **2.** Não usar padrões disponibilizados pelo fornecedor para senhas do sistema e outros parâmetros de segurança
Proteger os dados do titular do cartão	**3.** Proteger os dados armazenados do titular do cartão **4.** Criptografar a transmissão dos dados do titular do cartão em redes abertas e públicas
Manter um programa de gerenciamento de vulnerabilidades	**5.** Proteger todos os sistemas contra malware e atualizar regularmente programas ou software antivírus **6.** Desenvolver e manter sistemas e aplicativos seguros
Implementar medidas rigorosas de controle de acesso	**7.** Restringir o acesso aos dados do titular do cartão de acordo com a necessidade de conhecimento para o negócio **8.** Identificar e autenticar o acesso aos componentes do sistema **9.** Restringir o acesso físico aos dados do titular do cartão
Monitorar e testar as redes regularmente	**10.** Acompanhar e monitorar todos os acessos com relação aos recursos da rede e aos dados do titular do cartão **11.** Testar regularmente os sistemas e processos de segurança
Manter uma política de segurança de informações	**12.** Manter uma política que aborde a segurança da informação para todas as equipes

Fonte: PCI *Security Standards Council* (2016, p. 5)

É recomendado por Lanna (2010) que sejam cumpridos pelo menos 3 dos requerimentos: 6, 11 e 12. Para um melhor entendimento, a seguir será represento os 12 requerimentos e suas respectivas especificações.

- **Requerimento 1**:

  > Um *firewall* examina todo o tráfego da rede e bloqueia aquelas transmissões que não atendem aos critérios de segurança específicos. Todos os sistemas devem ser protegidos do acesso não autorizado de redes não confiáveis, seja acessando o sistema por meio da Internet como *e-commerce*, acesso à Internet através dos navegadores na área de trabalho por parte dos funcionários, acesso via e-mail dos funcionários, conexão dedicada como conexões entre negócios, por meio de redes sem fio ou de outras fontes (*SECURITY STANDARDS COUNCIL*, 2016, p. 20).

- **Requerimento 2**:

  > Indivíduos mal-intencionados (dentro e fora de uma empresa) com frequência usam senhas padrão do fornecedor e outras configurações padrão do fornecedor para comprometer os sistemas. Essas senhas e configurações são bastante conhecidas pelas comunidades de *hackers* e facilmente determinadas por meio de informações públicas (*SECURITY STANDARDS COUNCIL*, 2016, p. 29).

- **Requerimento 3**:

> Métodos de proteção como criptografia, truncamento, mascaramento e codificação *Hash* são componentes essenciais para proteção de dados do titular do cartão. [...]. Outros métodos eficientes de proteção dos dados armazenados também devem ser considerados como oportunidades potenciais de minimização dos riscos. Por exemplo, os métodos para minimizar riscos incluem não armazenar dados do titular do cartão, a menos que seja absolutamente necessário, truncar dados do titular do cartão se o PAN completo não for necessário e não enviar PAN usando tecnologias de mensagens ao usuário final, como e-mails e mensagens instantâneas (*SECURITY STANDARDS COUNCIL*, 2016, p. 37).

- **Requerimento 4**:

> As informações confidenciais devem ser criptografadas durante a transmissão nas redes que são facilmente acessadas por indivíduos mal-intencionados. Redes sem fio configuradas de forma incorreta e vulnerabilidades na criptografia herdada e nos protocolos de autenticação permanecem como alvos contínuos de indivíduos mal-intencionados que exploram vulnerabilidades para obtenção de acesso privilegiado aos ambientes de dados do titular do cartão (*SECURITY STANDARDS COUNCIL*, 2016, p. 52).

- **Requerimento 5**:

> O *software* de antivírus deve ser usado em todos os sistemas comumente afetados pelo *malware* para proteger os sistemas de ameaças atuais e potenciais de *softwares* mal-intencionados. Soluções adicionais contra *malware* podem ser consideradas como suplemento ao *software* de antivírus; no entanto, estas soluções adicionais não substituem a necessidade de o *software* de antivírus estar adequado cartão (*SECURITY STANDARDS COUNCIL*, 2016, p. 55).

- **Requerimento 6**:

> Indivíduos inescrupulosos usam as vulnerabilidades da segurança para obter acesso privilegiado aos sistemas. Muitas dessas vulnerabilidades são solucionadas pelos *patches*[22] de segurança disponibilizados pelos fornecedores, que devem ser instaladas pelas entidades que gerenciam os sistemas. Todos os sistemas devem contar com os *patches* de *software* adequado para a proteção contra a exploração e o comprometimento dos dados do titular de cartão por indivíduos e *softwares* mal-intencionados (*SECURITY STANDARDS COUNCIL*, 2016, p. 59).

- **Requerimento 7**:

> Para assegurar que os dados críticos possam ser acessados somente por uma equipe autorizada, os sistemas e processos devem estar implementados para limitar o acesso com base na necessidade de divulgação e de acordo com as responsabilidades da função. A 'necessidade de divulgação' é quando os direitos de acesso são concedidos somente ao menor número possível de dados e privilégios necessários para realizar um trabalho (*SECURITY STANDARDS COUNCIL*, 2016, p. 76).

- **Requerimento 8**:

> Atribuir uma identificação exclusiva (ID) a cada pessoa com acesso assegura que cada indivíduo seja exclusivamente responsável pelas suas ações. Quando tal responsabilidade estiver em vigor, as ações desempenhadas nos dados e sistemas críticos serão realizadas e podem ser rastreadas, por usuários e processos conhecidos e autorizados (*SECURITY STANDARDS COUNCIL*, 2016, p. 79).

- **Requerimento 9**:

> Qualquer acesso físico aos dados ou sistemas que armazenam dados do titular do cartão conferem a oportunidade para que pessoas acessem dispositivos ou dados e removam sistemas ou cópias impressas, e deve ser restrito de forma adequada. Para as finalidades do Requisito 9, 'funcionário' refere-se a funcionários que trabalham em

[22] ***Patch***: "Atualização de um *software* existente para agregar funcionalidades ou para corrigir defeitos" (PCI *SECURITY STANDARDS COUNCIL*, 2016, p. 18)

> período integral e meio-período, funcionários e equipes temporárias e prestadores de serviços e consultores que atuem com presença física no endereço da entidade. Um ‘visitante’ refere-se a um fornecedor, convidado de um funcionário, equipes de serviço ou qualquer pessoa que precise adentrar as dependências por um breve período, normalmente um dia, no máximo. ‘Mídia’ refere-se a todas as mídias impressas ou eletrônicas que contenham dados do titular do cartão (*SECURITY STANDARDS COUNCIL*, 2016, p. 91).

- **Requerimento 10**:

> Mecanismos de registro e a capacidade de monitorar as atividades dos usuários são fundamentais na prevenção, detecção ou minimização do impacto do comprometimento dos dados. A presença de registros em todos os ambientes permite o monitoramento, o alerta e a análise completa quando algo dá errado. Determinar a causa de um comprometimento é muito difícil, se não impossível, sem registros das atividades do sistema (*SECURITY STANDARDS COUNCIL*, 2016, p. 101).

- **Requerimento 11**:

> As vulnerabilidades estão sendo continuamente descobertas por indivíduos mal-intencionados e pesquisadores e são apresentadas por novos *softwares*. Os componentes do sistema, processos e *softwares* personalizados devem ser testados com frequência para assegurar que os controles de segurança continuem refletindo um ambiente em transformação (*SECURITY STANDARDS COUNCIL*, 2016, p. 111).

- **Requerimento 12**:

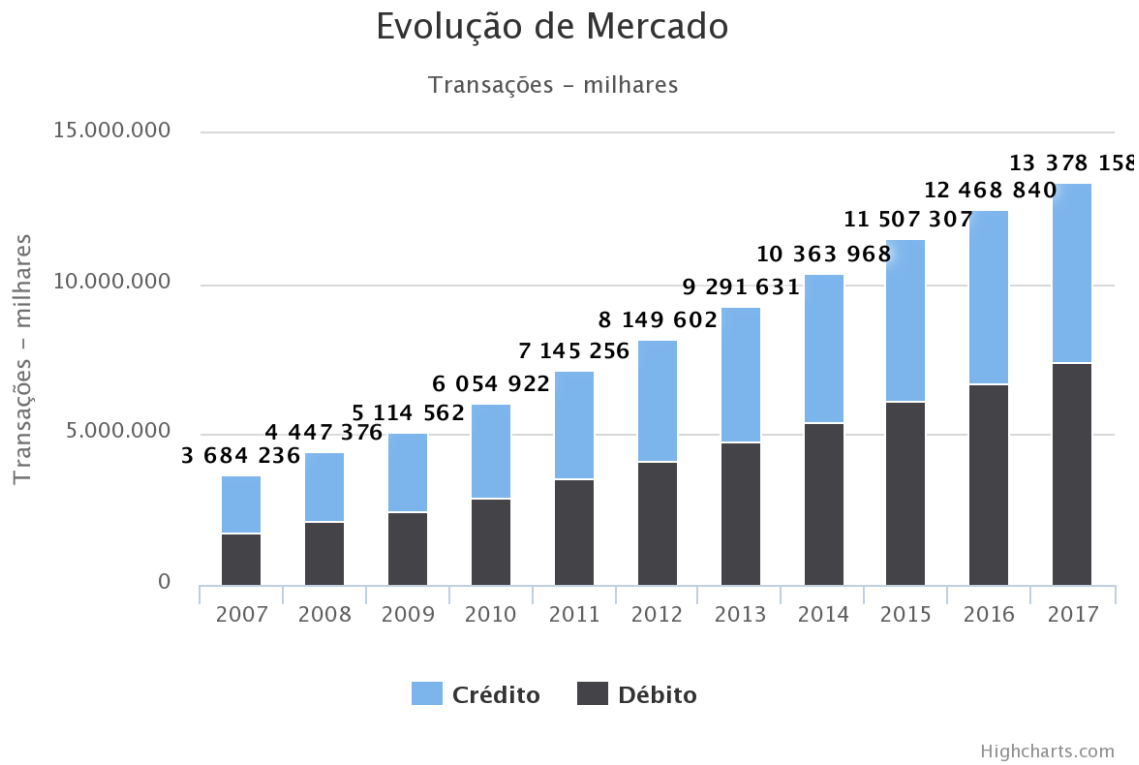
> Uma política de segurança sólida determina o tom da segurança para toda a empresa e informa aos funcionários o que é esperado deles. Todos os funcionários devem estar cientes da confidencialidade dos dados e de suas responsabilidades para protege-los Para as finalidades do Requisito 12, ‘funcionário’ refere-se a funcionários que trabalham em período integral e meio-período, funcionários e equipes temporárias e prestadores de serviços e consultores que ‘residem’ no endereço da entidade ou têm acesso ao ambiente de dados titular de cartão (*SECURITY STANDARDS COUNCIL*, 2016, p. 121).

6.8 Consumidor brasileiro e a forma de pagamento

Com o decorrer dos anos, o consumidor brasileiro começou a optar cada vez mais pelo cartão como forma de pagamento, pela praticidade e segurança já que não precisava andar com o dinheiro no bolso, e isso acarretou no aumento da variedade de formas de pagamento em alguns setores do mercado.

Isso acarretou a um aumento do número de transações durante os anos, de acordo com os dados da ABECS. A figura 43 mostra que há uma diferença da quantidade de números de transações entre crédito e débito no mercado. Em 2017, foram cerca de 13.378.158 de transações, divididas entre crédito (5.955.663 de transações, na cor azul) e débito (7.422.495 de transações, na cor preta). Os dados apresentados são referentes a 12 meses do ano anterior, já que devido a análise de todos os meses, porém a publicação desses dados só divulgados em 2018.

Figura 43 - Número de transações de crédito e débito (2007-2017)

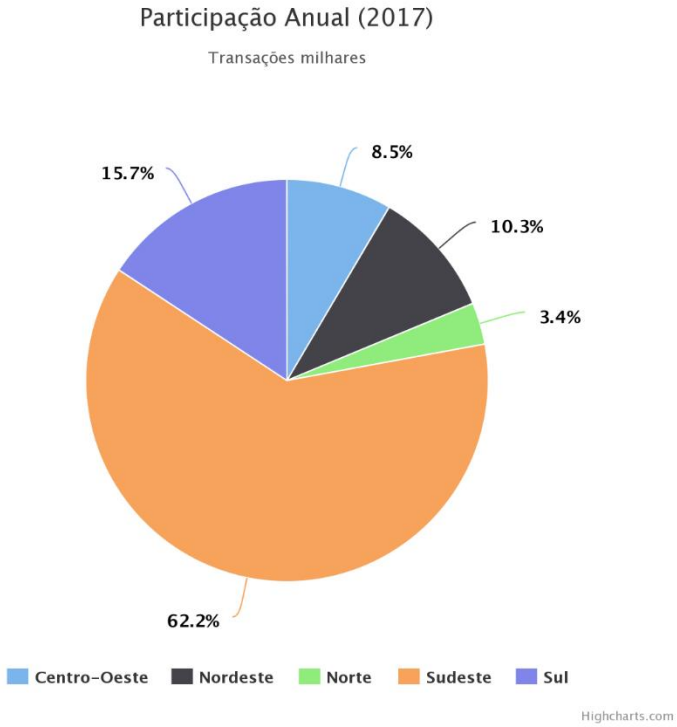


Fonte: ABECS (2017, online)

A figura também deixa clara a divisão do mercado a que se refere a forma de pagamento, crédito ou débito. Em cada região do país são diferentes os números de transações, já que a distribuição da população no território brasileiro é variável.

Como, pode ser visto na figura 44, a maior porcentagem de transações de cartão de débito é na região Sudeste (na cor laranja). Essa região representa 62,2%, com 4.613.899 de transações de débito no ano de 2017 (ABECS, 2017). Em seguida, tem-se a região Sul com 15,7%, com 1.67.871 transações.

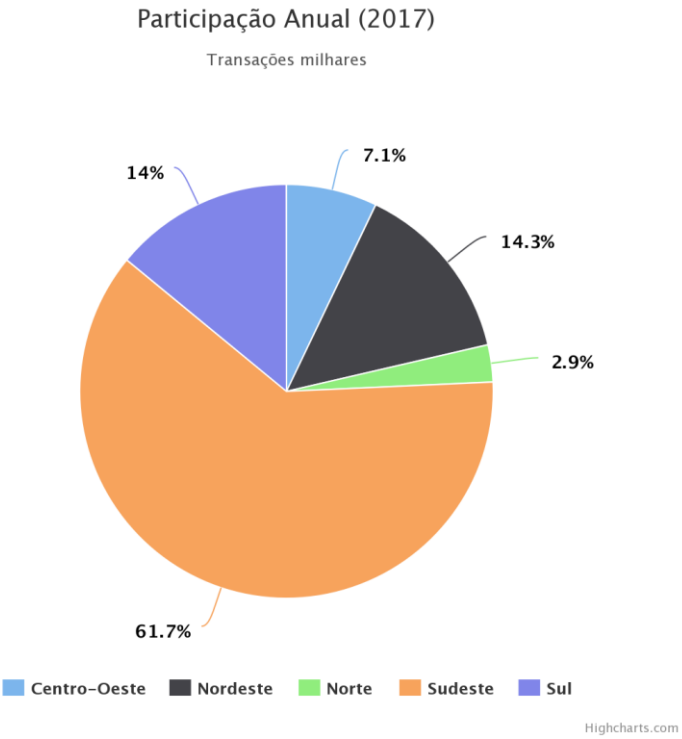
Figura 44 - Utilização de cartão de débito como forma de pagamento, de acordo com a região



Fonte: ABECS (2017, online)

Na modalidade de crédito (figura 45) há uma predominância na região Sudeste também, representando cerca de 61,7%, aproximadamente 3.596.102 de transações em 2017. O segundo lugar é ocupado pela região Sul, 14% representados com 818.828 transações.

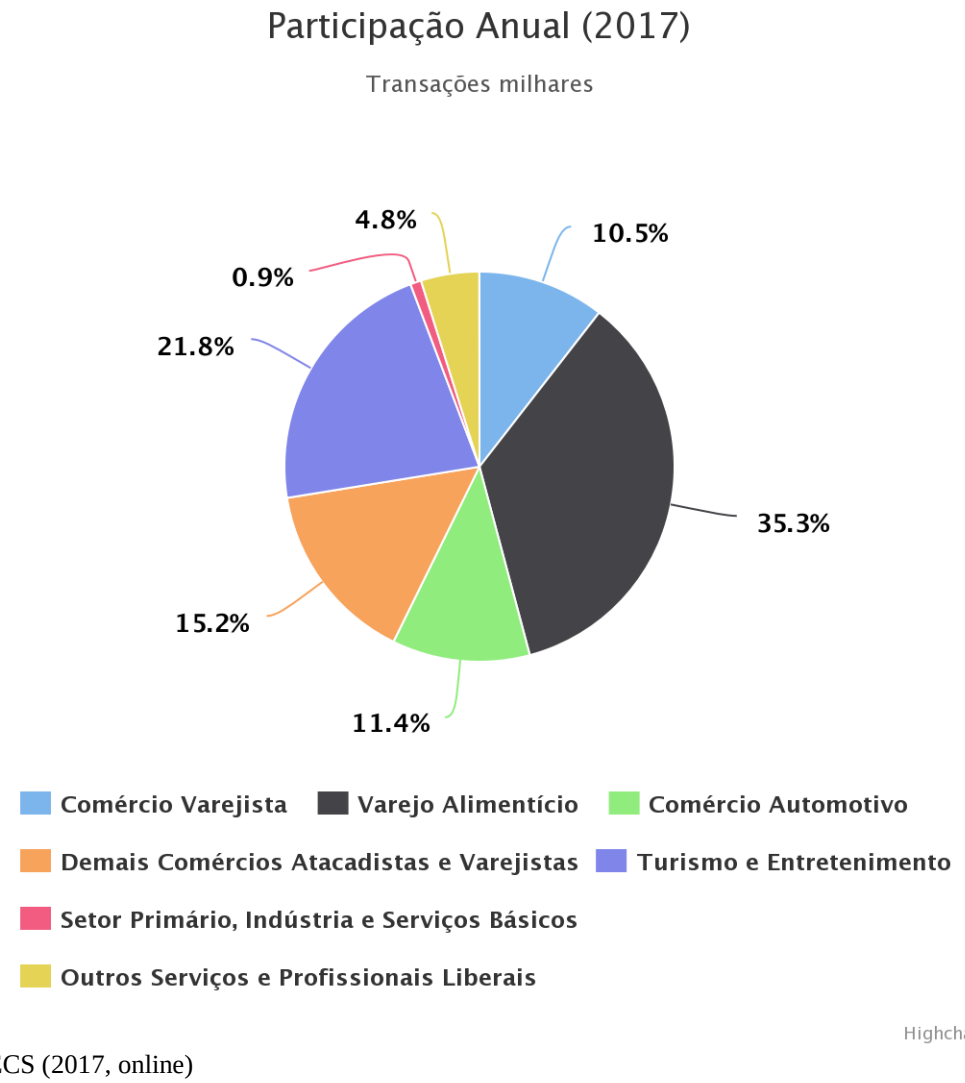
Figura 45 - Utilização de cartão de crédito como forma de pagamento, de acordo com a região



Fonte: ABECS (2017, online)

Essas transações ainda podem ter divisões que variam entre setores do mercado como por exemplo, entretenimento e alimentício. Em 2017, na figura 46 é observado que a atividade que o consumidor mais opta é o varejo alimentício (na cor preta), na forma de débito. Cerca de 35,3%, equivalente a 2.623.162 de transações. Em segundo lugar, o ramo de demais comércios atacadistas e varejistas (na cor laranja), com 15,2% (1.125.800 transações). Comparando os números do mesmo setor com 2016 houve um aumento de 0,03%, representando isso em números, foram cerca de 273.601 transações a mais em 2017.

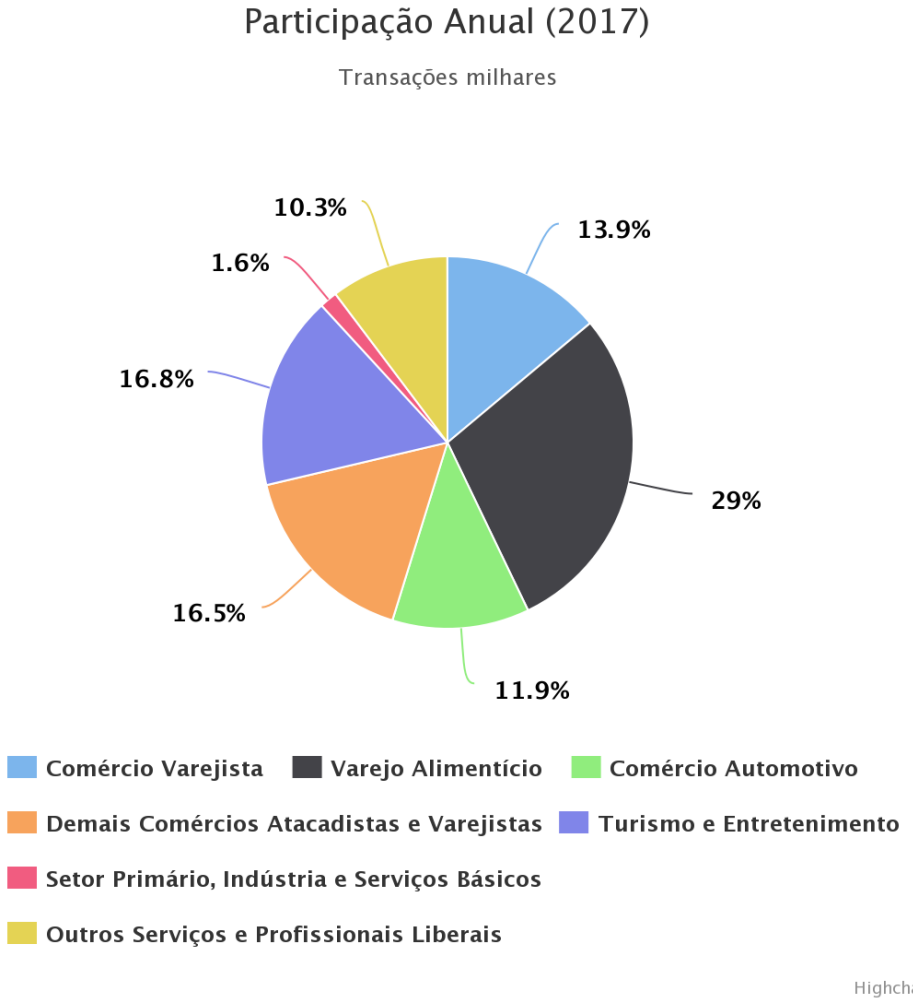
Figura 46 - Atividades que predomina débito



Fonte: ABECS (2017, online)

Já na opção crédito, em 2017, aconteceram 1.688.701 de transações, representando 29% das atividades no setor de varejo alimentício (cor preta). No mesmo setor mencionado, houve um aumento de 0,9% em relação ao ano anterior, sendo 95.787 de transações a mais do que 2016 (figura 47).

Figura 47 - Atividades que predomina crédito



Fonte: ABECS (2017, online)

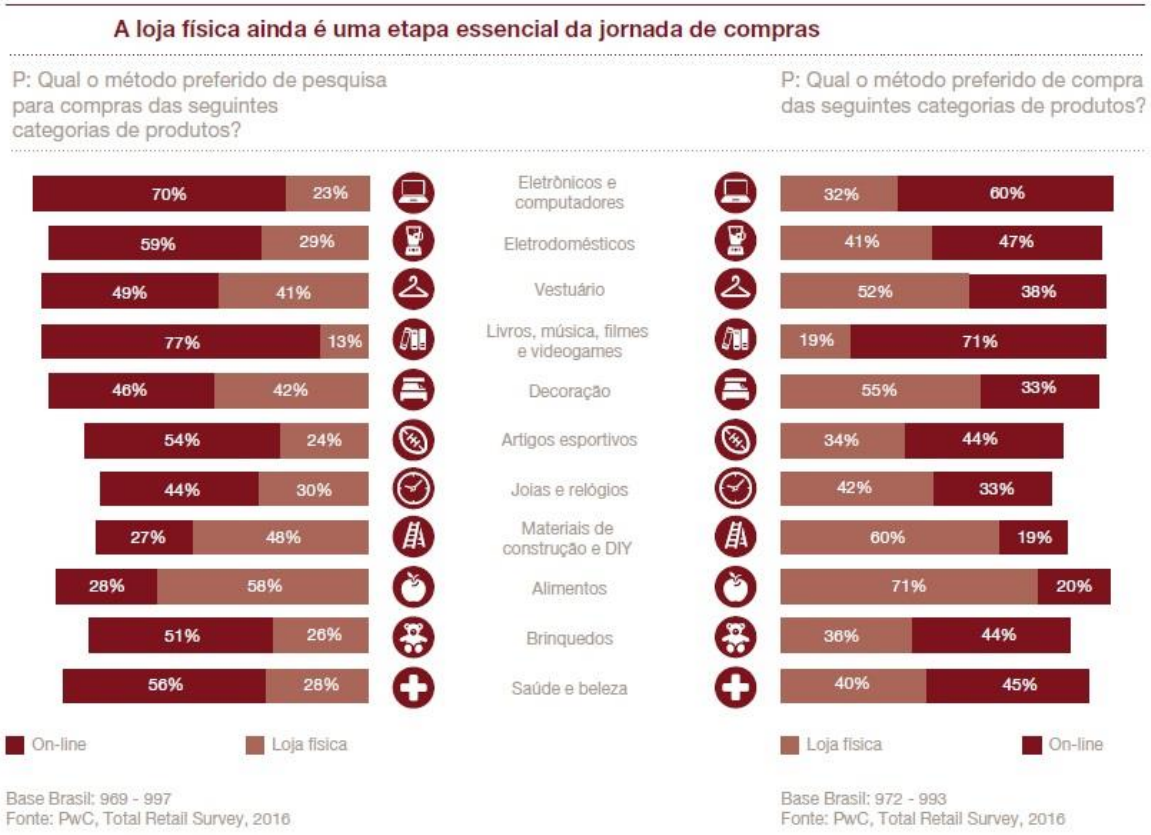
Com a facilidade que possui agora, o consumidor munido de cartão procura por outras maneiras de realizar uma compra. Isso gerou um aumento no mercado *m-commerce* (*mobile commerce*), que ganharam espaço além das lojas físicas. Dois exemplos bem-sucedidos são lojas Americanas e Saraiva. Com propagandas atraentes em sites e redes sociais que acessamos, procura chamar a atenção do maior número de cliente para esse mercado. Com alguns toques na tela no *smartphone* é possível realizar uma compra que poderia ser feita em uma loja física sem enfrentar filas, por exemplo.

Apesar de existir um grande aumento da procura pela compra online, as lojas físicas ainda são essenciais. Clientes optam por pesquisar os preços antes de ser efetuar uma compra online e analisar os produtos como a melhor opção de compra podendo visualizar o produto em mão, por exemplo.

Na figura 48, é mostrado como o cliente se comporta na hora de pesquisar e comprar, tanto em lojas físicas quanto de maneira online. O setor que tem mais demanda pela compra física é o setor alimentício, com cerca de 71% de preferência. Já o eletrônico e computadores,

o cliente opta pela pesquisa e compra online, representa 70% e 60% respectivamente. Parte dos consumidores ainda preferem compras em loja física, mas por outro lado, por mais facilidade e comodidade, online.

Figura 48 - Comportamento do cliente em relação a loja física e online, de acordo com setores



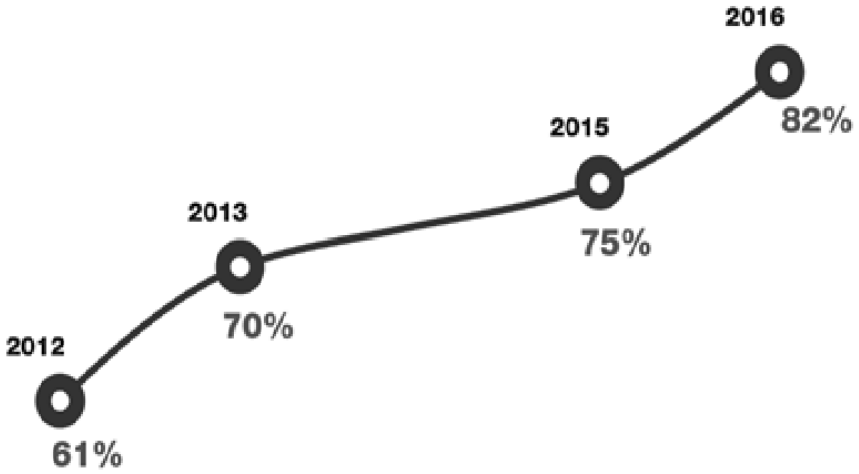
Fonte: *Total Retail* 2016 (2016, p.15)

6.9 FRAUDE

Com o avanço do mercado financeiro durante os anos, houve a necessidade de realizar a melhoria da forma de pagamento tanto no processo quanto no serviço oferecido para o cliente, mas consequentemente surgiram problemas, como a fraude e clonagem de cartões, problemas esses que são enfrentados em todo o mundo: por exemplo, no Brasil, a cada 16 segundo acontece uma tentativa de fraude, em 2017 (MELO, 2018).

Na figura 49, vemos que 82% dos entrevistados em 2016 pela Kroll (2018) relataram algum incidente de fraude no último ano. Desde 2012, é observado um aumento desse índice e apresentando uma tendência de crescimento acentuada, em 2012 apresenta com 61% de incidência de fraudes.

Figura 49 - Índice de fraude



Fonte: Relatório Global de Fraude e Risco 2016/17 (2017, p. 4)

Podemos definir a fraude para esse trabalho como,

> Alguém usa seu cartão de crédito ou conta de crédito para fazer uma compra que você não autorizou. Os fraudadores também podem roubar seu número de conta de cartão de crédito, PIN e código de segurança para realizar transações não autorizadas, sem precisar do seu cartão de crédito físico. Transações ilegais como essas são conhecidas como fraude de cartão [...] (TATHAM, 2018, online).

6.9.1 Tipos de fraude

A fraude pode apresentar alguns tipos que podemos citar (como contato das administradoras de cartão, clonagem de cartões, fraudes internas), mas focaremos para cartões de forma geral (SPEZIALI, 2016).

Na fraude por contato das administradoras, o cliente recebe alguma ligação, solicitando CPF, número de cartão, data de validade e outras informações do cartão. Justificam que os dados pedidos são para uma análise de dados, porém os Bancos nunca pedem dados de cartão por telefone. Grande parte das vítimas são idosos que, sem muitas perguntas, repassam essas informações.

A clonagem também é um tipo de fraude. Não existem uma única maneira de clonar um cartão, porém, um tipo mais comum é o ‘chupa-cabra’: dispositivos que são acoplados no leitor de ATM’s (*Automatic Teller Machine* - caixas eletrônicos). Outra maneira de clonar é com geradores de números de cartão, apresentado no próximo tópico.

As fraudes internas partem de dentro da própria empresa, quando, por exemplo, por algum funcionário no momento de cobrança de algum valor de seus clientes, observam e decoram as senhas digitadas e depois imprimem os recibos na máquina para coletar os dados pessoais de cada cliente.

6.9.1.1 Geradores de números de cartão

Existem vários sites que prestam o serviço de gerar cartões de forma fácil e gratuita. Com apenas uma pesquisa rápida sobre essa ferramenta, encontra-se diversos exemplos. Segundo Held (2017) não é necessário clonar um cartão para ter um número válido, basta de se utilizar do gerador de cartão. Não existem apenas geradores de cartão, mas também de CFP, CNPJ, placa de carro, CNH entre outros. Utilizando linguagem de programação, como PHP e Java, que geram os números que dentro de uma combinação que pode ser válida, com os parâmetros certos para cada bandeira, as ferramentas geradoras usam os *proxy's* para checarem os cartões, e quanto menor a latência, mais rápida a resposta da validação. Os principais prejudicados com o uso de geradores são:

> Lojas online que vendam produtos com um baixo ticket médio, *e-commerce* novos ou vulneráveis a ataques de testadores, lojas online com modelo de *checkout* que informe instantaneamente se o pagamento foi aprovado ou negado e ONGs e instituições de caridade que recebam doação por cartão de crédito (KONDUTO, 2016, p. 3).

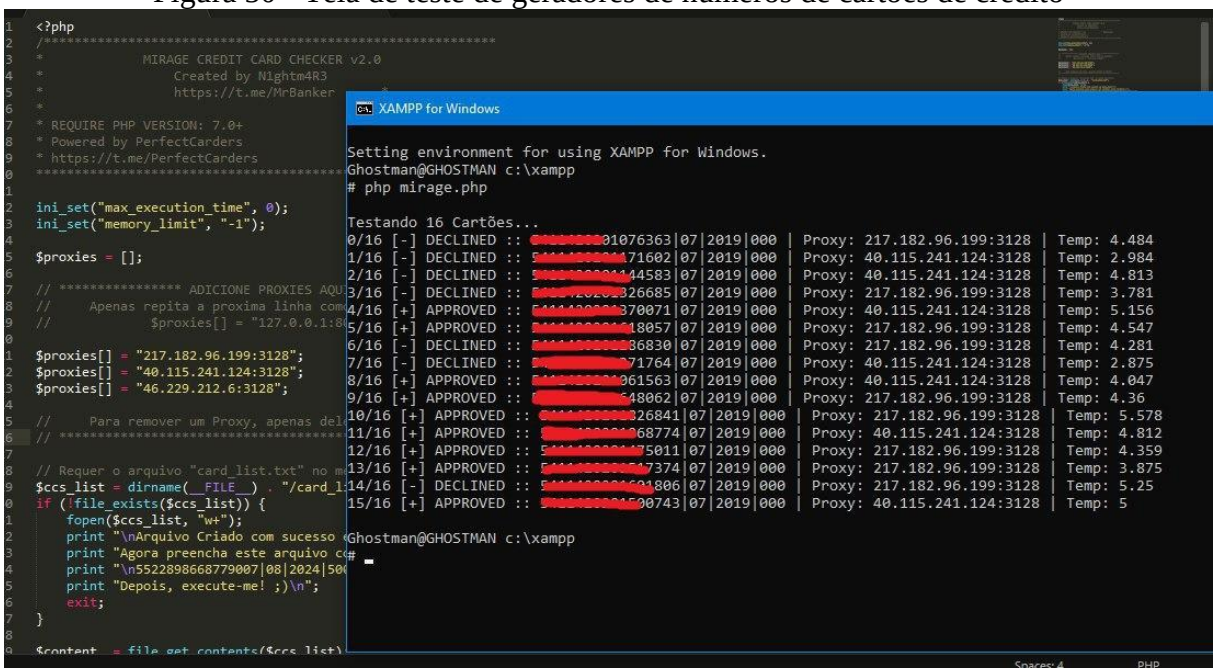
Antes de utilizar os cartões clonados, precisam ser testados, assim os criminosos classificam os cartões entre quentes (aceitos nos testes) e frios (foram clonados ou foram bloqueados em algum teste). Os testadores funcionam da seguinte maneira (KONDUTO, 2016, p. 2):

1 – O fraudador adquire um lote com dados de milhares de cartão de crédito que foram vazados ilegalmente;

2 – O criminoso encontra um *e-commerce* vulnerável, ou até mesmo uma instituição de caridade que aceite doação via cartão de crédito, e realiza várias compras em um curto espaço de tempo. Em alguns casos ele consegue até automatizar esta tarefa.

Outra possibilidade é o fraudador criar um sistema que gere dados aleatórios e cartão de crédito e simule teste por teste em sua tela de *checkout*, até obter alguma informação que seja válida. Na figura 50, após automatizar em linhas de código PHP, são feitos testes com os números de cartões, CVV e data de validade do cartão para validar ou negar o mesmo, antes de utilizar em compras online, por exemplo.

Figura 50 - Tela de teste de geradores de números de cartões de crédito



Fonte: *PerfectCarders* (2018, online)

3 – Os testes são transações (ou doações) de baixo valor, pois não levantaram suspeitas e não comprometem os limites de fatura. Os cartões ‘quentes’ (aceitos nos testes) são separados, e o fraudador despreza os que foram negados. Já os cartões “frios” são aqueles que já foram clonados ou foram bloqueados em algum teste.

O uso de cartões clonados dessa maneira acarreta alguns problemas como por exemplo: mancham na imagem do negócio *online* e geram um grande volume de *checkout* que seria o valor de reembolso como forma de validação. Existem maneiras de minimizar esse tipo de fraude:

> Implementar um sistema antifraude que emita respostas em tempo real. Criar um fluxo de integração que não entregue ouro: quando a transação for legítima, a resposta é imediata; se a recomendação for recusada, ocultar a resposta sobre o pagamento (se não for possível refazer o fluxo, ao menos não informar instantaneamente que o pagamento foi autorizado/negado). Impedir o usuário de colar dados de cartão de crédito no *checkout*, para dificultar a vida do fraudador (KONDUTO, 2016, p. 3).

6.9.2 A fraude no mundo

A fraude é um problema enfrentado pelo mundo todo em diversos setores: serviços financeiros, bens de consumo, tecnologia, mídia e telecomunicações entre outros. Apesar de ser o mesmo problema enfrentado, em cada país é diferente a maneira como é encarado, devido a defesa e investimento contra esses ataques. Os países que possuem maior preocupação com fraude são na China (25%) e Índia (19%), América Latina, onde localiza o Brasil, possui apenas 13% (KROLL, 2018). Esse problema afeta não só o consumidor, mas também a economia, que

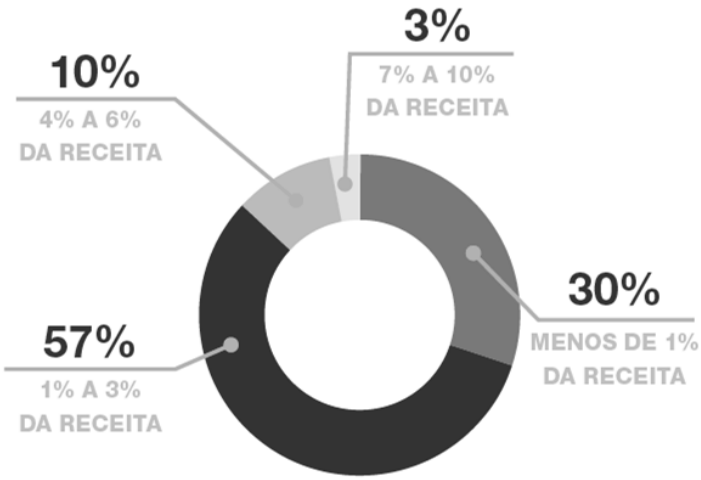
evitam levar seus serviços e/ou produtos para determinados países devido ao alto índice de fraude.

> A globalização de negócios trouxe oportunidades de expansão estratégica, e também uma grande variedade de riscos regionais. De fato, 69% dos executivos disseram que foram aconselhados a não operar em um determinado país ou região no ano passado, porque isso aumentaria sua exposição à fraude. Da mesma forma, 63% dos entrevistados se afastaram de determinadas regiões devido a preocupações com segurança (KROLL, 2018, p. 6).

6.9.2.1 Brasil

Durante a pesquisa feita pela Kroll (2018, p. 14), entre entrevistados "94% acreditam que a exposição à fraude aumentou". Esse problema afeta economicamente empresários, cerca de 10% afirma que registrou uma perda de 4% a 6% de suas receitas, e 57% dos empresários afirma que estima prejuízos que influenciam 1% a 3% de suas receitas, como mostra a figura 51.

Figura 51 - Porcentagem de perdas das receitas durante 12 meses



Fonte: Kroll (2018, p. 5)

O Brasil tem tido um aumento no número de fraudes ao longo dos anos, fator influenciado, entre outros, pelo aumento na procura de crédito, aumentando o número de transações. Durante o todo o cenário explicado, o consumidor precisa usar seus dados em todo o processo. Desta forma, aparecem vulnerabilidades para utilizar das informações de forma ilícita e realizar a fraude (BRANT, 2017).

> No primeiro semestre, a demanda do consumidor por crédito cresceu 2,1% em relação ao mesmo intervalo de 2016 – em julho, a alta foi de 11,4% ante igual mês do ano passado. A expectativa é que continue aumentando, acompanhando a consolidação da retomada econômica, e os fraudadores devem tentar se aproveitar desse movimento [...] (ARAGÃO, 2017, online).

Os principais responsáveis pela fraude no Brasil são pessoas que podem ser, respectivamente com a média brasileira e global: ex-funcionários (43% - 27%), funcionários de

baixo escalão (22% - 39%), vendedores/fornecedores (17% - 26%), clientes (17% - 19%), por exemplo (KROLL, 2018). A principal maneira de descobrir é através de auditorias externas que equivale a 43% da média nacional, em comparação à média global possui um aumento de 7%. Auditoria pode ser definida como:

> (...) um processo de verificação de todos os registros financeiros e de operações de uma empresa, com o objetivo de certificar aquilo que está correto ou identificar falhas que necessitem de correções. A auditoria externa é realizada por profissionais independentes, sem nenhuma ligação com a empresa, e que possuem esse tipo de especialização e regulamentação. Essa auditoria serve como uma medida de segurança que a empresa passa aos seus investidores, pois é realizada uma certificação dos registros contábeis e análise operacional da empresa, e o resultado emitido em relatórios (DICIONÁRIO FINANCEIRO, [201-?], online).

Algumas medidas serão adotadas este ano, segundo Kroll (2018). As principais são (com a média nacional e global, respectivamente): *due diligence* em parceiros, clientes e fornecedores (74% - 56%); controle financeiros e combate à lavagem de dinheiro (71% - 63%); monitoramento de mídia, controle de conformidades, revisão legal (65% - 58%) entre outras.

Como visto no capítulo 6, evoluiu a forma de pagamento e com isso hoveram muitos pontos negativos e positivos. Percebeu-se uma grande aceitação da parte do consumidor e assim, levou algumas empresas a adotarem. Com isso acarretou uma evolução, que resultou a junção do reconhecimento biométrico e a essa forma de pagamento. Assim será apresentado no capítulo seguinte algumas empresas que já utilizam a biometria em seu meio.

7 ESTRATÉGIAS DE SEGURANÇA PARA TRANSAÇÕES DE CARTÃO: ESTADO DA ARTE

Com o crescente avanço das tecnologias utilizadas atualmente vêm se pensando em maneiras de maior usabilidade e segurança para todos os meios, principalmente para pagamento. Os capítulos explanados neste documento encaminham para esta nova proteção que é a utilização da biométrica em vários níveis para autenticar as transações e outras métricas que utilizam a 'pessoa' como senha. Várias grandes empresas, como: Visa, Mastercard, Banco do Brasil, Bradesco, Gemalto e Alibaba, vêm dando o passo inicial para o novo futuro com a biometria. Este capítulo pretende fazer um apanhado das tecnologias que estão sendo utilizadas na realidade presente, neste ano de 2018.

A Visa iniciou os testes, no começo do ano de 2018, de um modelo de EMV com dupla interface (chip e *contactless*[23]), em conjunto com os bancos *Mountain America Credit Union* e o *Bank of Cyprus*, que utilizará a impressão digital no lugar da senha digitada, que é a opção mais usual (IDGNOW, 2018). A figura 52 mostra o cartão citado.

Figura 52 - Cartão *contactless*

Fonte: Natalie Bruins (2016, online)

O sistema funcionará da seguinte forma:

> Quando o portador de cartão coloca o dedo no sensor, sua impressão digital é comparada ao modelo previamente cadastrado e armazenado de forma segura no cartão, para que a transação seja autenticada. Uma luz verde e uma vermelha integrada ao cartão indicam se o resultado da comparação foi positivo ou negativo (IDGNOW, 2018, online).

[23] ***Contactless***: "pagamento por proximidade [...] é necessário que o usuário tenha um celular com um chip e antena *Near Field Communication* (NFC), que armazena as informações da conta do usuário e realiza a comunicação com um leitor Ponto de Venda (PDV), de propriedade do estabelecimento, ou seja, não é necessária a presença de um vendedor" (SEBRAE NACIONAL, 2018, online).

Este modelo faz com que a ação fique mais segura, pois os dados são armazenados e comparados no próprio cartão, além de oferecer uma maior velocidade e conveniência ao usuário.

Acompanhando a Visa nesta empreitada, a Mastercard iniciou o processo de teste do Mastercard *Identity Check* no Brasil, que já é utilizado em mais de 14 países. Este modelo utiliza o reconhecimento facial para autorizar as transações, e atua utilizando *smartphones*, *tablets* e computadores conectados à Internet. Ao efetuar a transação, o usuário tira uma *selfie* e confirma assim a operação. (*E-COMMERCE* BRASIL, 2016).

Continuando esta linha a Gemalto, empresa de tecnologias de autenticação, criou um cartão EMV com a biometria da impressão digital. “Com um simples toque do dedo, sem a necessidade de digitar uma senha (PIN) no terminal POS (Ponto de Venda) para finalizar o pagamento, seja no modo com ou sem contato” (GEMALTO, 2018, online). A figura 53 simboliza este modelo.

Figura 53 - Modelo do cartão da empresa Gemalto

Fonte: Gemalto (2017, online)

Uma das afiliadas da empresa Alibaba, criou um sistema de pagamento biometria facial chamado de *Smile to Pay* que está sendo usado nos caixas da Founded 1952 *Kentucky Fried Chicken* (KFC) na cidade de Hangzhou, na China. Neste sistema, basta o usuário tirar uma *sefie* sorrindo e sua compra será autorizada.

O Banco do Brasil e Bradesco optaram para utilizar a biometria na utilização de seus caixas eletrônicos, tendo suas datas de implementação em 2012 e 2006, respectivamente (GOVERNO DO BRASIL, 2017). O primeiro utiliza a impressão digital como facilitador, aumentando a proteção para os clientes ao fazer as movimentações em suas contas. Já o segundo utiliza a autenticação biométrica da palma da mão, como forma de seus usuários fazerem saques e consultar suas contas bancárias.

> Bancos de todo o mundo estão optando cada vez mais pela biometria para autenticar os clientes que acessam seus serviços. Esta tendência não se limita aos bancos; outras empresas financeiras também estão adotando autenticação biométrica para identificar clientes e proteger recursos (THAKKAR, 2017, online, tradução nossa).

Alguns países ao redor do mundo já possuem a biometria como método de autenticação nos caixas eletrônicos, dentre estes, Brasil, Polônia, Japão e Índia. Países dos continentes africano e asiático estão dispostos a utilizar esta nova tecnologia em um futuro próximo (THAKKAR, 2017).

O quadro 3 e 4, a seguir apresentam 56 bancos mundiais e empresas financeiras que já adotam o sistema biométrico e qual padrão biométrico que utilizam. O padrão biométrico mais utilizado é a impressão digital com 20 empresas utilizando-o, seguido da face e a voz com 11 empresas e não tão utilizado os padrões de íris com 6, comportamento com 4 e palma da mão com 2 empresas. Algumas empresas não possuem um padrão biométrico especifico, mas sim utilizam plataformas que fazem este processo.

Quadro 3 - Implementação de padrões biométricos em Bancos mundiais (A até F)

Banco / Empresa Financeira	**Padrão Biométrico**						
	Plataforma	**Digital**	**Face**	**Comportamento**	**Voz**	**Palma da mão**	**Íris**
ABN AMRO			X				
Atom Bank			X		X		
Australia and New Zealand Banking Group					X		
Banco Azteca		X					
Banco Inbursa			X				
Banco Industrial SA		X	X				X
Bank Leumi	Secured Touch						
Bank of Scotland		X					
Barclays		X					
BBVA Compass		X					
BNP Paribas	IdentityX						
Bunq		X					
Citi Group Inc.					X		
Commercial Bank of Qatar (CBQ)		X					
Commonwealth Bank of Australia		X					
DBC Bank	Aadhaar						
Deutsche Bank				X			
Digibank by DBS	Aadhaar						
Fifth Third Bank		X					
First Bank		X					
First International Bank of Israel	Transmit Security						

Fonte: Adaptado de Thakkar (2017, online)

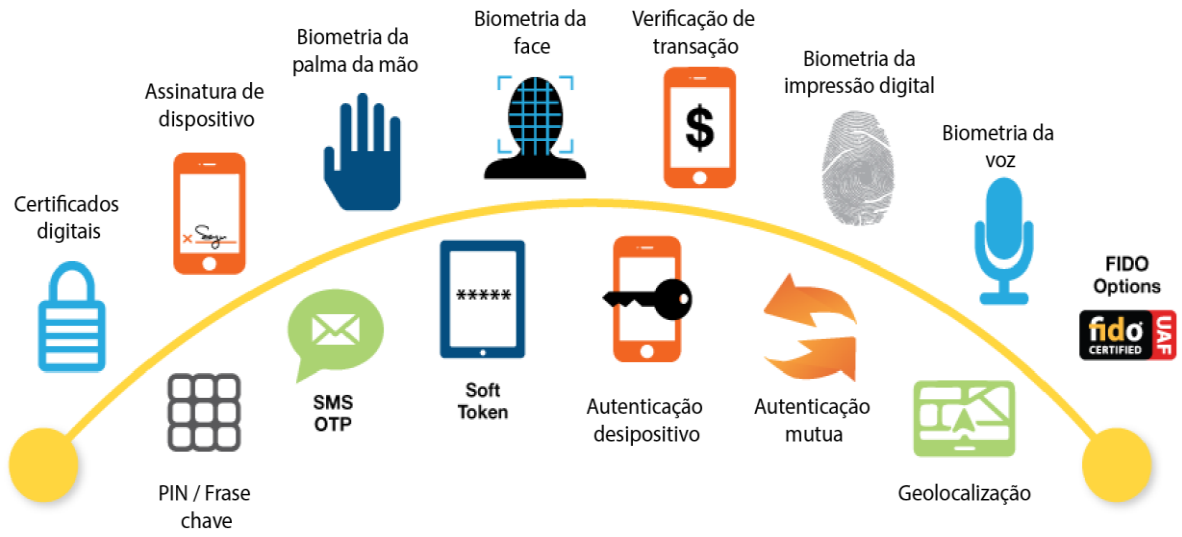
Quadro 4 - Implementação de padrões biométricos em Bancos mundiais (G até Y)

Banco / Empresa Financeira	Padrão Biométrico						
	Plataforma	**Digital**	**Face**	**Comportamento**	**Voz**	**Palma da mão**	**Íris**
Gesa Credit Union	DNA					X	
Guaranty Trust Bank Kenya		X					
Gulf Bank	IdentityX						
HSBC Hong Kong		X					
HSBC USA					X		
IDFC (Infrastructure Development Finance Company)		X					
JP Morgan Chase		X					
Jumio			X				
KB Kookmin Bank							X
KEB Hana							X
Lloyds Banking Group plc		X	X				
Mashreq		X					
Mastercard			X				
NatWest				X			
Nequi	IdentityX						
Now Money			X	X			
OCBC Bank		X					
PyraMax Bank	DNA					X	
Reparo			X				
Royal Bank of Scotland Group plc				X			
Santander UK					X		
Sberbank of Russia			X		X		
SilkBank Limited		X					
Standard Chartered		X			X		
Sumitomo Mitsui Banking Corporation (SMBC)	IdentityX						
The Qatar National Bank (QNB)							X
TIAA (Teachers Insurance and Annuity Association)					X		
Ujjivan	Aadhaar						
Union Bank of Philippines	IdentityX						
USAA	IdentityX						
Virginia Credit Union					X		
Visa		X	X		X		
Wells Fargo					X		
Woori Bank							X
Yapi ve Kredi Bankasi							X

Fonte: Adaptado de Thakkar (2017, online)

Um sistema que está sendo bastante utilizado no mundo é a plataforma *IdentityX*, da empresa *Daon*. Ela utiliza da unicidade do homem para deixar seus processos mais flexíveis. Além do sistema garantir segurança, ele também oferece a liberdade para que o usuário (no caso, o Banco) implemente novas tecnologias conforme elas vão surgindo. A figura 54 representa esta dinamicidade do sistema.

Figura 54 - Integração da plataforma IdentityX



Fonte: Adaptado de Daon ([201-?], online)

A empresa brasileira Acesso utiliza a pessoa e suas características (biometria facial, por exemplo) para facilitar o acesso a documentos. Assim, busca desburocratizar e facilitar o acesso a esses documentos, quando preciso, em diferentes ocasiões e com essa solução já atingidas 36.166.142 brasileiros, até o momento dessa pesquisa. Empresas de diversos setores já são atendidas e acreditam essa facilidade, como por exemplo, Tim, Magazine Luiza, Citibank, Bradesco, Claro entre outras (ACESSO, 2018).

O capítulo 7 demonstrou a ampla aceitação de grandes empresas com a entrada do reconhecimento biométrico como meio de autenticação. Pensando neste fato, no capítulo 8 será apresentado uma nova proposta de metodologia para autenticação de transação.

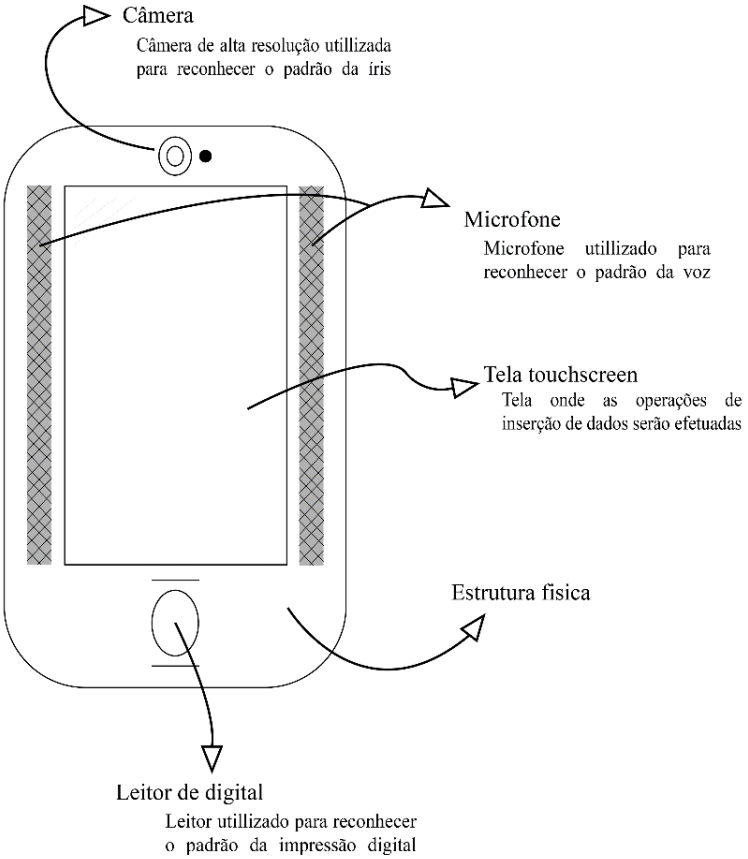
8 METODOLOGIA

A partir da revisão bibliográfica feita, foi possível levantar os motivos de se fazer uma comunicação segura visando a proteção dos dados durante o envio dos mesmos, independente do meio e da informação. A criptografia, juntamente com outras tecnologias, traz a segurança necessária, já que a real melhoria vem através dessa união. Utilizada como ferramenta de autenticação, a inteligência artificial entra no processo para reconhecer os padrões gerados pelos usuários – esses padrões, por dependerem de uma característica que o usuário possui em si, minimizam problemas decorrentes do esquecimento de um cartão físico. É necessário, no entanto, estar atento na verificação de alguma alteração em um dos meios de autenticação, pois isso pode ocasionar problemas nas leituras.

O objetivo desta pesquisa é apresentar uma especificação que agregue segurança ao processo que é utilizado atualmente no pagamento de compras em lojas físicas, na modalidade de cartão de crédito.

Tal especificação segue algumas etapas de desenvolvimento padronizadas. Para que o sistema funcione, propõe-se, primeiramente, a criação de um novo modelo de processo e máquina de pagamento que efetuará as etapas pensadas, a figura 55 expressa este modelo.

Figura 55 - Modelo proposto para o *hardware* da máquina de cartão



Fonte: Autores (2018)

Ao enviar as solicitações de autenticação para o sistema, a máquina enviará em conjunto um código *token* que funcionará como seu ID, uma verificação de autenticidade da própria máquina, uma camada de segurança a mais para minimizar ocorrência de clonagem do dispositivo.

Antes mesmo de começar o processo, é preciso fazer a aquisição dos dados. Com a nova metodologia, o cliente precisará ir ao Banco para realizar essa etapa e assim será feito o credenciamento dos seguintes dados biométricos: impressão digital, íris e voz. Com os dados validados, o cliente poderá fazer compras em algum estabelecimento que possuir a máquina adequada.

Para realizar o processo de captura e aprendizado dos dados biométricos são executadas as etapas demonstradas na figura 26, no capítulo 5 no tópico 5.2. Dado que cada uma das biometrias possui sua particularidade, elas são gravadas por meios diferentes, impressão digital pelo sensor de digital, a íris por uma câmera e a voz por um microfone. O portador do cartão poderá escolher entre uma palavra-chave ou frase-chave, para autenticar a voz aumentando assim a segurança, já que além de reconhecer a voz do cliente (algo que o cliente ‘é’) o sistema também reconhecerá a fala/senha (algo que o cliente ‘sabe’). A aquisição desses dados deve ser feita com um número de amostras apropriadas para que o erro seja mínimo.

O processo de tratamento e administração dos dados será feito utilizando técnicas de inteligência artificial, mais especificamente, utilizando as redes neurais artificiais com base em um aprendizado supervisionado, por ser uma das estratégias consolidadas para reconhecimento de padrões em diferentes mídias (imagem e som, por exemplo). Ao longo do processo, que será explicado mais adiante, o sistema poderá solicitar tanto a impressão digital quanto a íris ou senha falada. É necessário, portanto, que o usuário tenha cadastrado os três padrões, para que o sistema tenha em posse todos os dados para validar a transação ou não, dependendo da sua interpretação.

A digital é a primeira verificação do processo, podendo ser comparada ao chip no cartão EMV, pois será associada à bandeira do cliente. A digital pode ter ligação com mais de uma bandeira conforme o cliente desejar, trocando os cartões físicos pela digital do portador. A digital foi escolhida como primeira verificação devido a sua usabilidade, grande aceitação e por ser considerada pouco invasiva.

A máquina de cartão, na nova metodologia, possui um *token* criptografado embutido no sistema, e assim gera um ID único para cada máquina, como uma maneira de evitar a troca de máquinas para fraude ou adultério. Cada máquina, irá possui uma chave pública para validar e comparar junto com a chave privada (criptografia assimétrica) do Banco de Dados (BD) de máquinas autorizadas para realizar a transação em lojas físicas.

Quando os dados (impressão digital, íris ou voz) forem adquiridos eles alimentarão as entradas dos sistemas de redes neurais artificiais correspondentes e, se os códigos obtidos forem os mesmos dos que já estão no BD a transação é validada. Os BD são separados lógica e fisicamente para cada meio de autenticação, dando assim mais segurança e confiabilidade ao sistema.

Para conseguir realizar a transação de modo seguro precisa-se ter em mente os doze requisitos do PCI DSS, explanados no capítulo 6, no tópico 6.7. Entretanto, dependendo do uso do sistema nem todos os requisitos serão almejados. Foram priorizados os seguintes requerimentos: 1, 3, 4, 8 e 12. O quadro 5 fará a correspondência de cada etapa com cada requisito, após a apresentação de cada etapa da metodologia proposta.

As etapas de funcionamento do processo de operação do cartão propostas neste trabalho serão descritas, explanadas e justificadas no decorrer do capítulo. Os procedimentos ocorrem na seguinte ordem:

1) O funcionário insere o seu ID, para assim utilizar a máquina. Assim insere o tipo de transação (crédito ou débito), o valor da compra e confirma em um botão no visor, para seguir para a etapa dois.

   Obs.: Caso o ID não seja reconhecido, a máquina não irá funcionar.

2) O cliente insere a impressão digital via o sensor da máquina.

   Obs.: Caso o código da impressão digital não seja encontrado, o sistema pede para repetir o processo. O cliente tem até três tentativas para que funcione, caso contrário a ação é cancelada.

3) A máquina espera a resposta de confirmação do sistema, para assim apresentar o valor da compra e as opções da bandeira que o cliente possui, e o cliente escolhe a bandeira e confirma a ação;

   Obs.: Caso o cliente só possua uma bandeira, o sistema passará direto para a etapa 04.

4) Após confirmação, o cliente usará a íris como último modo de autenticação para confirmar a transação;

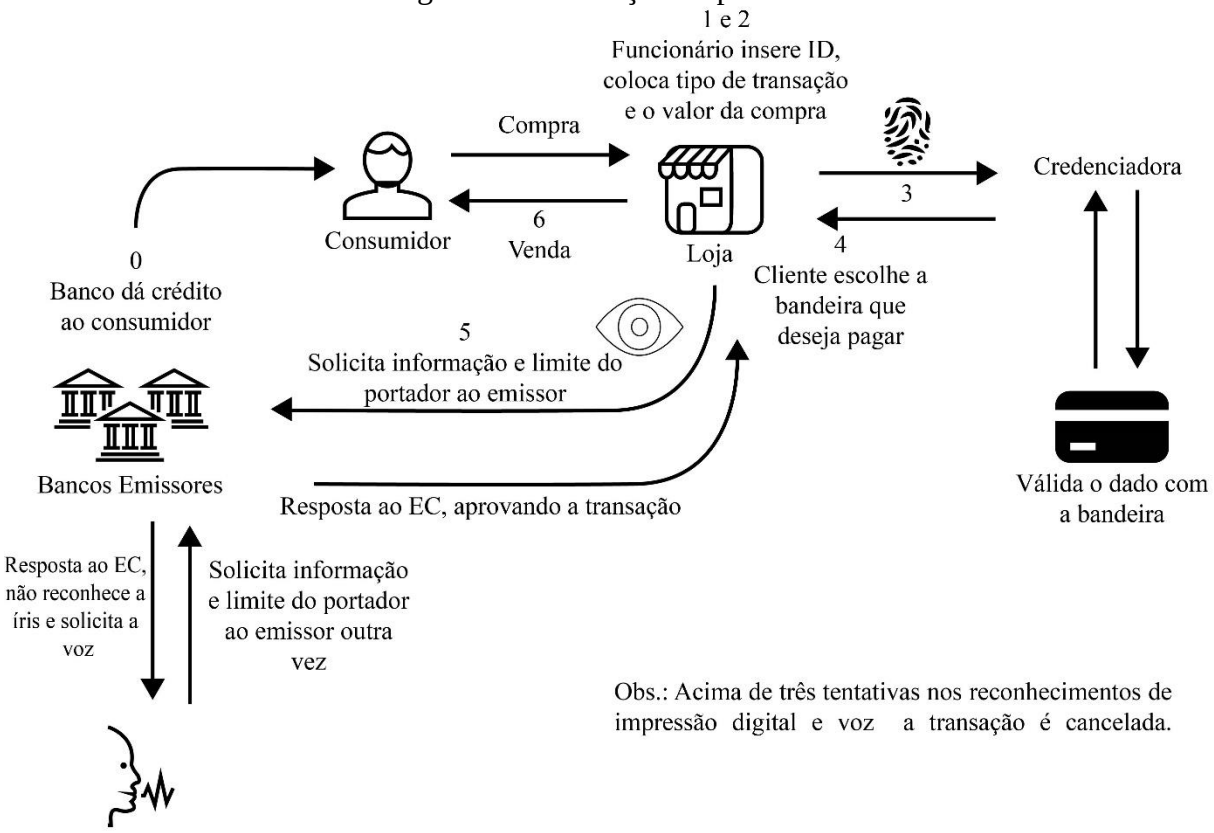
   Obs.: caso a íris seja negada três vezes o sistema pedirá ao cliente que fale a sua senha por voz, para assim confirmar a transação, sendo ela averiguada até três vezes, passando disto a operação é cancelada.

5) Finalizada a transação, uma mensagem será enviada para o celular com a confirmação da compra e para o e-mail cadastrado, a nota fiscal.

   Obs.: nota fiscal deverá ter as informações de forma geral que já possui na via do cliente emitido pela máquina atualmente: bandeira, tipo do cartão, a vista / parcelado, últimos números do cartão, nome cliente e Banco.

A figura 56 ilustra a descrição do processo citado de forma mais completa, contendo as observações e operações do sistema. Baseado no processo da figura 33 do capitulo 6, segundo a ABIPAG.

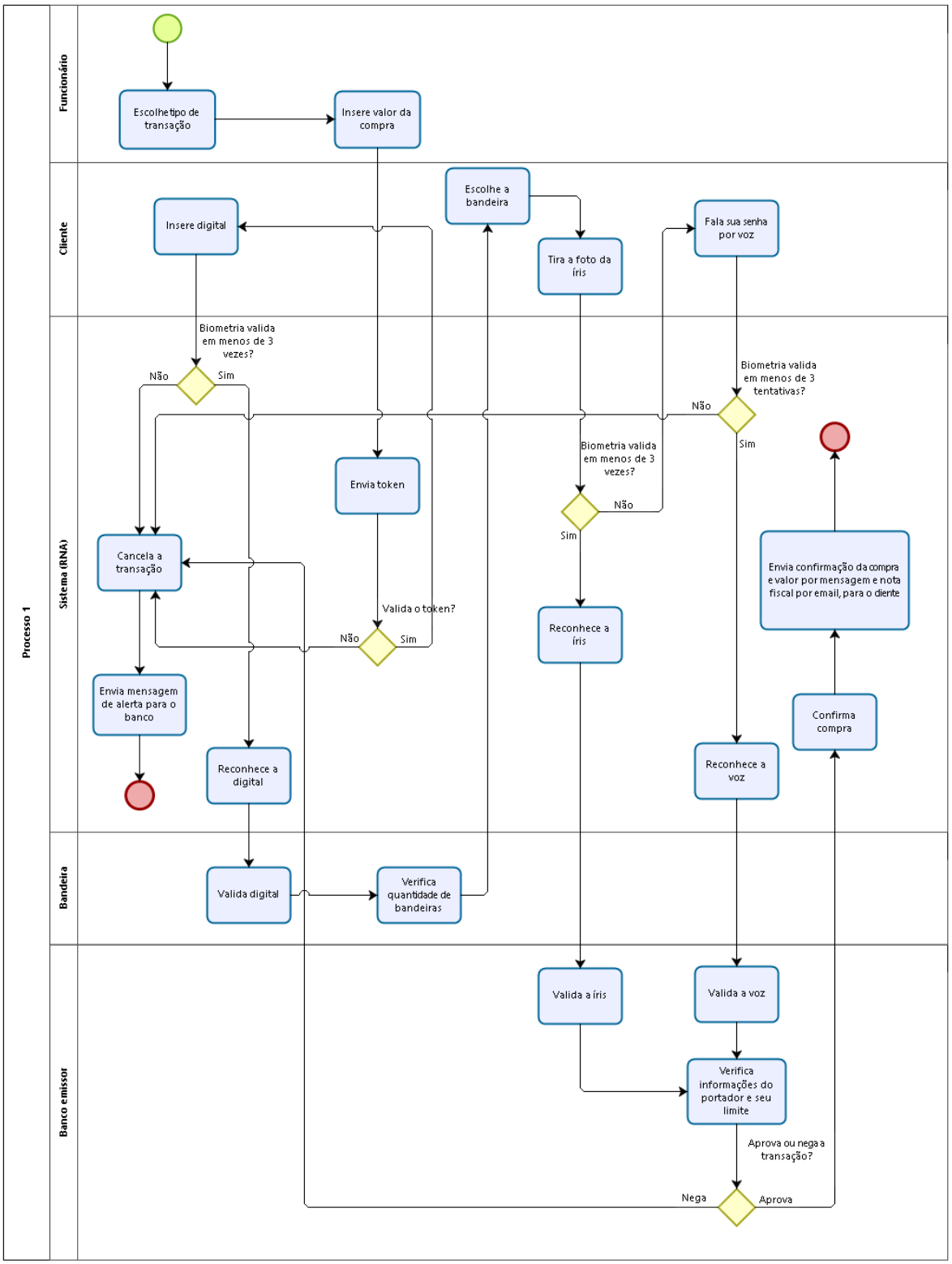
Figura 56 - Descrição do processo



Fonte: Adaptado de Associação Brasileira de Instituições de Pagamentos ([201-?], online)

Para uma melhor a representação do processo acima foi elaborado um diagrama de processo, representado pela figura 57, com as devidas etapas citadas e suas observações.

Figura 57 - Diagrama de processo



Fonte: Autores (2018)

O quadro 5 representa a modelagem proposta para efetuar a transação explanada acima, ela está subdividida em cinco colunas, sendo elas, etapa (número da etapa explanada acima), agente (quem realizara a ação), PCI DSS (requisitos de segurança), ação tomada (ação tomada pelo sistema), ação que o sistema inteligente irá realizar. As etapas que apresentam o asterisco

ao lado do número possuem observações que foram apresentadas no fluxograma do processo e nos textos anteriores.

Quadro 5 - Metodologia proposta para efetuar transações

Etapa	**Agente**	**PCI DSS**	**Ação tomada**	**Ação do Sistema inteligente**
1	Funcionário	8	Insere ID do funcionário	Verifica o ID
2	Funcionário	1 4 12	Salvar tipo (crédito ou débito) e valor da compra	-
3*	Cliente	3 4	Envia uma solicitação de confirmação da digital	Verificar a impressão digital
4*	Cliente	3 4	Apresenta o valor da compra e verifica com qual bandeira será feito o pagamento	-
5*	Cliente	3 4	Envia uma solicitação de confirmação da íris	Verificar a íris
6	Sistema	3	Enviar para o celular do cliente a confirmação da compra e para o e-mail cadastrado, a nota fiscal	-

Fonte: Autores (2018)

Além dos processos ditados anteriormente, o sistema será capaz de identificar quantas vezes o usuário efetua apenas a verificação de segurança da voz. Feita esta análise, o sistema enviará uma mensagem ao Banco com o informativo e o mesmo deverá averiguar com o cliente o motivo de estar ocorrendo, pois, o cliente pode estar sofrendo algum tipo de fraude ou seus dados biométricos precisam de atualização.

O sistema também fará o monitoramento de compra do cliente, sendo estas compras aprovadas e negadas, levando em consideração o critério de identificação ou não da biometria. Em relação a compras aprovadas, o sistema sempre fará uma análise - que também pode utilizar-se de rede neural artificial - de padrão de comportamento, para o caso de atividades fora do normal, avisar o Banco e ao cliente.

Quanto a compras negadas, enviará avisos ao banco para verificar o que está acontecendo, pois devido a intempéries do clima, a necessitar de alta precisão o equipamento pode apresentar má leitura ou os dados biométricos do cliente precisam ser atualizados.

Com as estratégias demonstradas neste capítulo, tem-se uma descrição completa dos procedimentos de transação proposta. Com a pesquisa feita no estado da arte procuramos desenvolver uma metodologia que já é presente no mercado. Buscando assim, agregar valores que já existem com a metodologia proposta.

As empresas na sua maioria, no presente momento da pesquisa, utilizam no máximo dois padrões biométricos, devido a isto, procuramos aumentar a segurança com três padrões de reconhecimento, sendo eles impressão digital, íris e voz.

9 CONSIDERAÇÕES FINAIS

No decorrer deste trabalho de curso, obtivemos conhecimentos a respeito de diversas áreas, como criptografia e inteligência artificial. Porém, através de estudo e análise feitas, em sites e documentos, foi adquirido um conhecimento de forma mais profunda na parte de forma de pagamento, mais precisamente em cartões.

Desde a origem do cartão, o percentual de clientes que adotaram este tipo de pagamento aumentou com o decorrer da aceitação, devido a comodidade e facilidade que trouxe o mesmo. Assim houve a necessidade de evoluir o processo de transação junto com o cliente, aumentando a segurança e o meio de autenticação.

Durante o estudo, percebeu-se que é possível criar novos métodos de segurança, utilizando os fundamentos já existes e aliados com outras áreas e com isso, tornar a tecnologia mais segura.

Pretendeu-se desenvolver uma metodologia para autenticação do portador do cartão e proteção do processo abrangendo aspectos de *hardware* e *software*. Considera-se que os objetivos foram atingidos com sucesso, devido a conseguirmos aliar a criptografia e a inteligência artificial para a forma de pagamento.

No processo atual de cartão, nota-se a necessidade de um contínuo estudo e pesquisa para o tornar mais seguro, já que com a tecnologia evoluindo cada vez mais procura-se elevar a segurança, independentemente do meio. A proposta indicada é viável, devido do ponto de vista que alguns Bancos já utilizarem a tecnologia combinada de reconhecimento. Nessa metodologia, buscou-se minimizar os riscos de fraude com a implementação do *token* na máquina para validar a mesma. E os três tipos reconhecimento biométrico, na parte do cliente, é para autenticar o portador, garantindo assim uma segurança no processo.

Durante a pesquisa, percebeu-se algumas fontes que se contradizem, principalmente na parte de cartão, por falta de um especialista. E no que desrespeito a metodologia, houve dificuldade em decidir quais padrões biométricos seriam utilizados e qual sequência de processos ficaria mais adequada levando em conta proteção e confiabilidade.

De forma geral conseguimos aprender e absorver conhecimento sobre essa forma de pagamento tão evidente no cotidiano. A respeito de criptografia e inteligência, pudemos aprimorar o conhecimento ensinado em sala de aula.

Para trabalhos futuros, buscaremos melhorar e desenvolver, o *software* e o *hardware*, de acordo com a demanda da segurança e para isso, visamos a construção do protótipo funcional para validar *hardware* e *software*. Com isso, iremos aprofundar as especificações para o mercado, com estudos e pesquisas relacionadas a essa temática. Visamos o aprimoramento de requisitos e atualizações, como um todo dessa metodologia, tornando assim uma realidade mais próxima.

Outra proposta de trabalhos futuros é adaptar a metodologia de *software* apresentada para o *hardware* de *smartphones*/celulares, visto que isso poderia baratear o custo final de implementação para o cliente e difundir a metodologia com maior rapidez.

REFERENCIAL BIBLIOGRÁFICO

ACCEO TENDER RETAIL TEAM. 2017. ***The impact of contactless EMV technology in South America***. Disponível em: < https://tender-retail.acceo.com/blog/the-impact-of-contactless-emv-technology-in-south-america//>. Acessado em 14 maio 2018.

ACESSO. **O que fazemos**. [201-?]. Disponível em:<http://www.acesso.io/>. Acesso em: 21 maio 2018.

AMARO, George. Criptografia simétrica e criptografia de chaves públicas: vantagens e desvantagens. **Revista Negócios e Tecnologia da Informação**, Curitiba, v.2, n.1, p.1-11, 2007.

APPLYEBY, Tyra. ***Phishing Definition, Prevention, and Examples***. [201-?]. Disponível<http://resources.infosecinstitute.com/category/enterprise/phishing/#gref>. Acesso em: 07 abr. 2018.

AQUÁRIO. **Falha de sinal na máquina de cartão**: veja o que fazer em sua empresa. [S.l.], 21 set. 2016. Disponível em:< http://blog.aquario.com.br/falha-de-sinal-na-maquina-de-cartao/ />. Acesso em: 21 maio 2018.

ASSOCIAÇÃO BRASILEIRA DAS EMPRESAS DE CARTÕES DE CRÉDITO. **Gráficos**. 2017. Disponível em:<http://www.abecs.org.br/indicadores-graficos>. Acesso em: 06 maio 2018.

_____. **Perguntas frequentes**. 2016. Disponível em:< http://www.abecs.org.br/consumidores-perguntas-frequentes>. Acesso em: 08 abr. de 2018.

ASSOCIAÇÃO BRASILEIRA DE INSTITUIÇÕES DE PAGAMENTOS. **Fluxograma da indústria**. [201-?]. Disponível em:< http://www.abipag.com.br/>. Acesso em: 05 maio 2018.

AUSTRILIAN CYBER SEGURITY CENTRE. ***Threat Report 2017.*** 2017.

BANCO DO BRASIL. **Biometria**. [201-?]. Disponível em:<http://www.bb.com.br/pbb/pagina-inicial/bb-seguranca/biometria#/>. Acesso em: 12 maio 2018.

BÄR, Hugo. ***Botnet*****:** o que são *bots* e para que são usados?. 2017. Disponível em: <http://triplait.com/bot-botnet-zombie/#.WtVCKZch3IU>. Acesso em: 16 abr. 2018.

BARRETO, Jorge Muniz. **Inteligência Artificial no Limiar do Século XXI**. 2 ed. Florianópolis: J. M. Barreto, 1999.

BASTOS, Carlos Alberto Carneiro Marinho. **Segmentação e Reconhecimento de Íris**. 2010. 110 f. Dissertação (Mestrado em Ciência da Computação) - Universidade Federal de Pernambuco. Recife, 2010.

BBC BRASIL. ***Bitcoin***: o que é e como funciona a moeda virtual. 2017. Disponível em: <www.bbc.com/portuguese/brasil-42313567>. Acesso em: 16 abr. 2018.

BOLTON**,** Willian. **Mecatrônica:** Uma abordagem multidisciplinar. 4 ed. Porto Alegre: Bookman, 2010. 664 p.

BRADESCO. **Biometria (Segurança Bradesco na Palma da Mão)**. [201-?]. Disponívelem:<https://www.bradescoseguranca.com.br/html/seguranca_corporativa/pf/canais-digitais/maquinas-de-autoatendimento/biometria.shtm>. Acesso em: 12 maio 2018.

_____. **Pioneirismo e liderança em tecnologia e atendimento ao cliente.** 2013. Disponível em:< https://banco.bradesco/html/classic/sobre/nossa-historia.shtm>. Acesso em: 10 abr. 2018.

BRANT, Danielle. Consumidor brasileiro é alvo de tentativa de fraude a cada 17 segundos. **Folha de São Paulo** 2017. Disponível em:<http://www1.folha.uol.com.br/mercado/2017/09/1917285-consumidor-brasileiro-e-alvo-de-tentativa-de-fraude-a-cada-17-segundos.shtml>. Acesso em: 10 maio 2018.

BRITO, Amilton. **Entendo a Autenticação com *Tokens***. 2009. Disponível em:<https://olhardigital.com.br/fique_seguro/noticia/entendendo-a-autenticacao-com-tokens/10049>. Acessado em: 19 maio 2018.

BRUINS, Natalie. ***Contactless Payments making a Real Connection***. 2016. Disponível em:<https://www.k3retail.com/en/contactless-payments-making-a-real-connection/>. Acesso em: 14 maio 2018.

CÁNEPA, Gabriel. **What You Need to Know about Machine Learning**. Birmingham: Packt Publishing , 2016.

CAPGEMINI; BNP PARIBAS. ***World Payments Report* 2017**. 2017

CAPUTO, Victor. **De olho no passado, chefe de riscos da Visa garante futuro seguro**. 2017. Disponível em:< https://exame.abril.com.br/tecnologia/de-olho-no-passado-chefe-de-riscos-da-visa-garante-futuro-seguro/>. Acesso em: 13 maio 2018.

CARDOSO, Pedro. **O que é *ransoware*?**. 2016. Disponível em: <http://www.techtudo.com.br/noticias/noticia/2016/06/o-que-e-ransomware.html>. Acesso em: 16 abr. 2018.

CARNEIRO, Milena Bueno Pereira. **Reconhecimento de íris utilizando algoritmos genéticos e amostragem não uniforme.** 2010. 178 f. Tese (Doutorado em Engenharia Elétrica) - Universidade Federal de Uberlândia, Uberlândia, 2010.

CASTELUCCI, Daniella. **Protocolos de comunicação em redes de computadores**. Disponível em:<https://daniellacastelucci.wordpress.com/2011/04/08/protocolos-de-comunicacao-em-redes-de-computadores/>. Acessado em 19 maio 2018.

CHENCI, Gabriel P.; RIGNEL, Diego GS; LUCAS, Carlos A. Uma introdução á lógica Fuzzy. **Revista Eletrônica de Sistemas de Informação e de Gestão Tecnológica**, v. 1, n. 1, 2011.

COLARES, Adolfo Francesco de Oliveira; CARNEIRO, Allan Guerreiro. **Uma Aplicação de Descoberta de Conhecimento para Auxiliar o Profissional da Área Médica na Tomada de Decisão**. 2006. 84 f. Trabalho de Conclusão de Curso (Bacharelado em Ciência da Computação) - Centro Universitário do Pará, Belém, 2006.

COMPUTERWORLD **Ataques como do WannaCry são apenas o começo, dizem especialistas**. 2017. Disponível em: <computerworld.com. br/ataques-como-do-wannacry-sao-apenas-o-comeco-dizem-especialistas>. Acesso em: 02 maio 2018.

CONCILIADORA. **Quais os tipos mais comuns de fraudes com cartões de crédito?**. 2016. Disponível em:<http://www.conciliadora.com.br/blog/quais-os-tipos-mais-comuns-de-fraudes-com-cartoes-de-credito/>. Acessado em: 09 maio 2018.

COSSETTI, Melissa. **O que você precisa saber sobre o ransomware WannaCrypt**. 2017. Disponível em: <https://www.techtudo.com.br/listas/2017/05/o-que-voce-precisa-saber-sobre-o-ransomware-wannacrypt.ghtml>. Acesso em: 12 abr. 2018.

COSTA, Ronaldo Martins da. **Uma nova abordagem para reconhecimento biométrico baseado em características dinâmicas da íris humana**. 2009. 101 f. Tese (Doutorado em Engenharia Elétrica) - Universidade de São Paulo. Escola de Engenharia de São Carlos, 2009.

COUTINHO, Gustavo Lacerda; MACHADO E SILVA, Renan Galvão. **Funcionamento do TLS**. 2006. Disponível em:< https://www.gta.ufrj.br/grad/06_1/ssl/func_tls.htm>. Acesso em: 26 abr. 2018.

CRÉDITO O DÉBITO. **O que é o Código de verificação do cartão de crédito? CVC**. 2012. Disponível em:<https://www.creditooudebito.com.br/que-codigo-verificacao-cartao-credito-cvc/#comment-38341>. Acesso em: 12 maio 2018.

DAON. **IDENTITYX® PLATFORM**. Disponível em: <https://www.daon.com/products/identityx-platform>. Acesso em: 20 maio 2018.

DICIONÁRIO FINANCEIRO. **Auditoria**. [(201?)]. Disponível em:<https://www.dicionariofinanceiro.com/auditoria/>. Acesso em: 10 maio 2018.

DUARTE, Henrique. **O que é um Trojan ou Cavalo de Troia?**. 2014. Disponível em: <http://www.techtudo.com.br/noticias/noticia/2014/06/o-que-e-um-trojan-ou-cavalo-de-troia.html>. Acesso em: 16 abr. 2018.

E-COMMERCE BRASIL. **Mastercard lança solução de checkout baseada em biometria e reconhecimento facial no Brasil**. 2016. Disponível em:<https://www.ecommercebrasil.com.br/noticias/mastercard-lanca-solucao-de-checkout-com-biometria-e-reconhecimento-facial/>. Acesso em: 14 maio 2018.

EL OBSERVADOR. ***La bancarización de los salarios ignora un derecho constitucional a que empresas o personas***. 2015. Disponível em:< https://www.elobservador.com.uy/inclusion-pero-no-la-fuerza-n698551>. Acesso em: 13 maio 2018.

ENGAGEMENT BUREAU. ***MasterCard Identity Check, nuevo servicio que simplifica el proceso de compra online***. 2016. Disponível em:<https://newsroom.mastercard.com/eu/es/press-releases/mastercard-identity-check-nuevo-servicio-que-simplifica-el-proceso-de-compra-online/>. Acesso em: 18 de maio 2018.

FEOFILOFF, Paulo. ***Hashing***. *2017. Disponível em:* < https://www.ime.usp.br/~pf/estruturas-de-dados/aulas/st-hash.html>. Acesso em: 08 de maio 2018.

FERREIRA, Denilson Palhares. **Identificação de Pessoas por Reconhecimento de Íris Utilizando Decomposição em Sub-bandas e uma Rede Neuro-Fuzzy.** 1998. Mestre em Engenharia Elétrica. Campinas, São Paulo.

FOLLOW THE COIN. ***What Are The New EMV Chip Credit Debit Cards***. 2015. Disponível em:<https://www.youtube.com/watch?v=WHkkRe4KBBg>. Acesso em: 04 abr.2018.

FREITAS, Alex A. ***Data mining and knowledge discovery with evolutionary algorithms*.** Berlin: Springer-Verlag, 2002. 264p.

GADI, Manoel. **Uma comparação de métodos de fraude em cartões de crédito**. 2008. São Paulo.

GARRETT, Filipe. **O que é criptografia?**. 2012. Disponível em:< http://www.techtudo.com.br/artigos/noticia/2012/06/o-que-e-criptografia.html>. Acesso em: 26 abr. 2018.

GEMALTO. **Cartão EMV com biometria de impressão digital**. [201-?]. Disponível em:<https://www.gemalto.com/brasil/servicos-financeiros/cartaos/cartao-biometrico-emv>. Acesso em: 20 maio 2018.

GONÇALVES, André Paim. **Aplicação de Lógica *Fuzzy* em Guerra Eletrônica**. {S.l}, Instituto Tecnológico da Aeronáutica, 2007.

GOVERNO DO BRASIL. **Bancos se preparam para o uso da biometria**. 2011. Disponível em:<http://www.brasil.gov.br/cidadania-e-justica/2011/10/bancos-se-preparam-para-o-uso-da-biometria>. Acesso em: 9 maio 2018.

GRIMES, Roger A. ***The 5 types of cybeer attack you're most likely to face***. 2017. Disponível em: <https://www.csoonline.com/article/2616316/data-protection/the-5-types-of-cyber-attack-youre-most-likely-to-face.html>. Acesso em: 02 abr. 2018.

GUNASUNDARI, T., and K. ELANGOVAN. A comparative survey on symmetric key encryption algorithms. ***International Journal of Computer Science and Mobile Applications*****.** v. 2, n. 2. 2014.

HAYKIN, Simon. **Redes neurais:** princípios e práticas. 2.ed. – Porto Alegre: Bookman, 2008.

HELD, Felipe. KONDUTO. **Ferramentas da Fraude:** geradores de cartão de crédito. 2017. Disponível em:<https://blog.konduto.com/pt/2017/06/ferramentas-da-fraude-gerador-de-cartao/>. Acesso em: 28 abr. 2018.

HIGA, Paulo. **Como não fazer uma máquina de cartão "moderninha"**. 2016. Disponível em:<https://tecnoblog.net/191099/maquina-cartao-acessibilidade-cegos/>. Acesso em: 13 maio 2018.

_____. ***WhatsApp* usa criptografia de ponta a ponta para suas mensagens no *Android***. 2015. Disponível em:<https://tecnoblog.net/169936/whatsapp-criptografia-ponta-a-ponta-android/>. Acesso em: 16 abr. 2018.

IBM. ***Transport Layer Security* (TLS)**. 2015. Disponível em:< https://www.ibm.com/support/knowledgecenter/pt-br/SSWU4L/Deliverability/imc_Deliverability/003_TLS.html>. Acesso em: 2 abr. 2018.

INFO WESTER. **Criptografia**. 2005. Disponível em:< https://www.infowester.com/criptografia.php>. Acesso em: 01 abr. 2018.

INFORMATÁVEL. **Como funciona um cartão de crédito (conceito de TEF)**. 2013. Disponível em:< https://informatavel.wordpress.com/2013/07/23/como-funciona-seu-cartao-de-credito/>. Acesso em: 29 abr.2018.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO/IEC 7812-1:2017**. 2017. Disponível em:< https://www.iso.org/standard/70484.html>. Acesso em: 26 abr. 2018.

INVENTTI. **O que é TEF e como funciona?**. 2017. Disponível em:<https://www.inventti.com.br/o-que-e-tef-e-como-funciona/>. Acesso em: 13 maio 2018.

JAIN, Anil K.; DUIN, Robert P.. W..; MAO, Jianchang. *Statistical pattern recognition: A review*. ***IEEE Transactions on pattern analysis and machine intelligence***, v. 22, n. 1, p. 4-37, 1999.

JOSHI, Prateek. ***Artificial Intelligence with Python:*** *Build real-world Artificial Intelligence applications with Python to intelligently interact with the world around you*. Birmingham: Packt Publishing, 2017.

JOYME. ***LevelDB.*** 2017. Disponível em: https://www.myway5.com/index.php/2017/08/20/leveldb%E6%BA%90%E4%BB%A3%E7%A0%81%E9%98%85%E8%AF%BB%EF%BC%88%E5%9B%9B%EF%BC%89-table-cache%E7%9A%84%E5%AE%9E%E7%8E%B0/>. Acesso em: 30 mar. 2018.

JUNIOR, Helvio. ***Transport Layer Security*** **(TLS) e** ***Secure Sockets Layer*** **(SSL)**. 2012. Disponível em: <http://www.helviojunior.com.br/it/security/transport-layer-security-tls-e-secure-sockets-layer-ssl/>. Acesso em: 15 abr. 2018.

JUROSBAIXOS**. Conheça todos os modelos de Máquina de Cartão do mercado**. 2017. Disponível em:< https://jurosbaixos.com.br/conteudo/conheca-todos-os-modelos-de-maquina-de-cartao-do-mercado/>. Acesso em: 12 maio 2018.

KASPERSKY LAB DAILY. **O que é um ataque *spear phishing*?**. 2017. Disponível em: <https://www.kaspersky.com.br/blog/what-is-spearphishing/9933/>. Acesso em: 08 abr. 2018.

_____. **O que é um *exploit*?**. 2013. Disponível em: <https://www.kaspersky.com.br/blog/o-que-e-um-exploit/740/>. Acesso em: 16 abr. 2018.

KAWAMURA, David Naoki N.; COSTA, Luciano de Oliveira; SAWADA, Renan Toda; NISIMURA, Thiago de Moraes. **Sistema inteligente com reconhecimento de fala na geração de comandos compostos para controle de agentes robóticos**. 2010. 68 f. Trabalho de Conclusão de Curso (Bacharelado em Ciência da Computação) - Centro Universitário do Pará, Belém, 2010.

KNIEFF, Ben. ***Global Consumer Card Fraud:*** *Where Card Is Coming From*. Boston: 2016.

KONKERO. **Máquina de cartão:** conheça todos os modelos do mercado. 2017. Disponível em:< https://www.konkero.com.br/cartao/maquina-de-cartao/maquina-de-cartao-conheca-todos-os-modelos-do-mercado>. Acesso em: 12 maio 2018.

KROLL. **Relatório Global de Fraude e Risco**: Construindo Resiliência em um Mundo Volátil. 2016/2017.

KRUG, Álisson Bohnert et al. Análise e Reconhecimento de Padrões usando processamento de imagens e inteligência artificial. **Revista de Iniciação Científica da ULBRA,** v. 7, n. 7, 2015.

KURTZ, João. **O que é engenharia social?**. 2016. Disponível em: <http://www.techtudo.com.br/dicas-e-tutoriais/noticia/2016/11/o-que-e-engenharia-social.html>. Acesso em: 16 abr. de 2018.

LAGE, Francisca Daniella Andreu Simões Moraes. **Um estudo de aritmética modular para a educação básica** [manuscrito]. - 2018. 61f.

LANNA, Eduardo. **Recomendações do PCI-DSS (**Cópia).2010. Disponível em:<http://www.redesegura.com.br/2010/10/recomendacoes-pci-dss-ii/>. Acesso em: 29 abr. 2018.

LOPES, Elias. **Protocolo Ponto-a-Ponto (PPP)**. [201-?]. Disponível em:< http://www.artigos.com/artigos/706-protocolo-ponto-a-ponto-ppp>. Acesso em: 03 maio de 2018.

LUGER, George F. **Inteligência artificial**: estruturas e estratégias para a solução de problemas complexos. 4. ed. Porto Alegre: Bookmann, 2004.

MAGALHÃES; SANTOS. **Biometria e autenticação**. 2003. Conferência da Associação Portuguesa de Sistemas de Informação, 4. Porto. Portugal. CD-ROM.

MANICA, Cezar Leandro. **Implementação de um módulo de reconhecimento de fala como interface de comando para robôs LEGO R MINDSTORMS R NXT 2.0**. 2014. 39f. Trabalho de Conclusão de curso (Bacharelado em Ciência da Computação) - Universidade Estadual do Oeste do Paraná, Cascavel, 2014.

MARIN, L.O. **Investigações sobre redes neurais artificiais para o reconhecimento de faces humanas na forma 3D**. 2003. 118 f.. Dissertação (Mestrado) - Universidade Federal de Santa Catarina, Florianópolis, 2003.

MARRO, Alessandro Assi et al. **Lógica *fuzzy*:** conceitos e aplicações. Natal: Universidade Federal do Rio Grande do Norte, 2010.

MARTIN, Alison. ***The global risks lasndscape* 2018**. 2018. Disponível em: <https://www.zurich.com/en/knowledge/articles/2018/01/the-global-risks-landscape-2018> Acesso em: 03 fev. 2018.

MARTINS, Elaine. **O que é SSL?**. 2009. Disponível em:< https://www.tecmundo.com.br/seguranca/1896-o-que-e-ssl-.htm>. Acesso em: 15 abr. 2018.

MARTINS, José Antônio. **Avaliação de Diferentes Técnicas para Reconhecimento de Fala**. Campinas , SP: [s.n], 1997.

MATOS, Hélder José da Silva. **Reconhecimento Biométrico Baseado na Geometria da Mão**. 2011. 115f Trabalho de Conclusão de Curso (Bacharelado em Engenharia Eletrotécnica e de Computadores) - Faculdade de Engenharia da Universidade do Porto, Porto, 2011.

MEGASUL SISTEMAS. **TEF (Transferência Eletrônica de Fundos).** 2009. São Paulo.

MILLER, Michael. ***Data Theft: How Big a Problem*?**. 2008. Disponível em: <http://www.informit.com/articles/article.aspx?p=1220308>. Acesso em: 15 abr. 2018.

MORAIS, Emerson Cordeiro. **Reconhecimento de Padrões e Redes Neurais Artificiais em Predição de Estruturas Secundárias de Proteínas**. Rio de Janeiro: UFRJ/COPPE, 2010. 135 p.

MOTA, Miguel. **PCI-DSS**: O que é e por que preciso dele**?**. 2017.Disponível em:< https://www.mundipagg.com/blog/o-que-e-pci/>. Acesso em: 28 abr. 2018.

MUSEU DO CARÃO DE CRÉDITO. **Linha do Tempo**. 2016. Disponível em:<http://www.museudocartao.com.br/linha_interna.php?id=78>. Acesso em: 02 abr. 2018.

NETWORKING. PPLWARE. **Criptografia simétrica e assimétrica:** Sabe a diferença?. 2010. Disponível em:< https://pplware.sapo.pt/tutoriais/networking/criptografia-simetrica-e-assimetrica-sabe-a-diferenca>. Acesso em: 15 abr. 2018.

NUNES, Délio Silva. **Criptografia assimétrica**. 2007. Disponível em:https://www.gta.ufrj.br/grad/07_2/delio/Criptografiaassimtrica.html>. Acessado em: 19 maio 2018.

PASSERI, Paolo. **2017 *Cyber Attacks Statistics***. 2018. Disponível em: <https://www.hackmageddon.com/2018/01/17/2017-cyber-attacks-statistics/>. Acesso em: 16 abr. 2018.

PINTO, Cláudia. **clusterização [Definição]**. 2004. Disponível em:<https://www.flip.pt/Duvidas-Linguisticas/Duvida-Linguistica/DID/730>. Acesso em: 14 maio 2018.

PINTON, Luiz Henrique. **Preservação de informações sensíveis**: aspectos sobre segurança, privacidade e integridade. 2016. Disponível em:<http://www.conteudojuridico.com.br/artigo,preservacao-de-informacoes-sensiveis-aspectos-sobre-seguranca-privacidade-e-integridade,56788.html> Acesso em: 19 abr. 2018.

PISA, Pedro. **O que é *hash*?**. 2012. Disponível em:<http://www.techtudo.com.br/artigos/noticia/2012/07/o-que-e-hash.html>. Acesso em: 27 abr.2018.

POZZEBOM, Rafaela. **Diferença entre:** vírus, *spam*, *spyware*, *worm*, *phishing*, *botnet*, *rootkit*. 2014. Disponível em: <https://www.oficinadanet.com.br/post/12991-diferenca-entre-virus-spam-spyware-worm-phishing-botnet-rootkit>. Acesso: 16 abr. 2018.

PRAMPERO, Paulo Sérgio. **Combinação de classificadores para Reconhecimento de Padrões**. 1998. Mestrado em Ciências de Computação e Matemática Computacional - Universidade de São Paulo, 1998.

PRICEWATERHOUSECOOPERS BRASIL. **A revolução que os consumidores almejam com a execução que os conquista:** *Total Retail* 2016. 2016.

REDAÇÃO EM ALTA. **A história dos cartões de crédito**. 2016. Disponível em:< http://emalta.com.br/historia-dos-cartoes-de-credito/>. Acesso em: 05 maio 2018.

REDAÇÃO OLHAR DIGITAL. **Rússia está por trás do ataque *NotPetya*, diz governo dos EUA**. 2018. Disponível em: <https://olhardigital.com.br/fique_seguro/noticia/russia-esta-por-tras-do-ataque-notpetya-diz-governo-dos-eua/74119>. Acesso em: 12 abr. 2018.

REDAÇÃO, TIINSIDE ONLINE SEGURANÇA. **Padrão PCI cresce para além dos mercados de cartões de débito e crédito**. 2017. Disponível em:< http://tiinside.com.br/tiinside/seguranca/mercado-seguranca/15/08/2017/padrao-pci-cresce-para-alem-dos-mercados-de-cartoes/>. Acesso em: 29 abr. 2018.

REDAÇÃO. IDGNOW FORM ING. **Visa inicia projeto piloto de cartão de pagamento biométrico**. 2018. Disponível em:< http://idgnow.com.br/mobilidade/2018/01/17/visa-inicia-projeto-piloto-de-cartao-de-pagamento-biometrico/>. Acesso em: 13 maio 2018.

REDESEGURA. **Recomendações do PCI-DSS**. 2011. Disponível em: https://www.redesegura.com.br/gerenciamento-de-vulnerabilidades/recomendacoes-do-pci-dss/>. Acesso em: 05 maio 2018.

REIS, Fábio dos. **Criptografia – Paradigmas e Técnicas de Autenticação**. 2015. Disponível em:<http://www.bosontreinamentos.com.br/seguranca/criptografia-paradigmas-e-tecnicas-de-autenticacao/>. Acessado em: 19 maio 2018.

REZENDE, Solange Oliveira. **Sistemas Inteligentes**: Fundamentos e Aplicações. Barueri, São Paulo: Manole. 2005.

RICHERT, Willi; COELHO, Luis Pedro. ***Building Machine Learning Systems with Python***. Birmingham: Packt Publishing, 2013.

RODARTE, Christiano. **Criptografia MD5**. [201-?]. Disponível em:< https://www.devmedia.com.br/criptografia-md5/2944>. Acesso em: 27 abr. 2018.

ROHR, Altieres. ***'Petya' x WannaCry*:** veja diferenças do novo ataque cibernético. 2017. Disponível em: <http://g1.globo.com/tecnologia/blog/seguranca-digital/post/petya-x-wannacry-veja-diferencas-do-novo-ataque-cibernetico.html>. Acesso em: 12 abr. 2018.

_____. ***WhatsApp* começa a identificar conversas com criptografia**. 2016. Disponível em:<http://g1.globo.com/tecnologia/blog/seguranca-digital/post/whatsapp-comeca-identificar-conversas-com-criptografia.html>. Acesso em: 07 abr. 2018.

ROMAGNOLO, Cesar Augusto. **O que é Criptografia?**. 2007. Disponível em:https://www.oficinadanet.com.br/artigo/443/o_que_e_criptografia>. Acesso em: 04 abr.2018.

ROQUE, Reginaldo do Carmo. **Estudo sobre a empregabilidade da previsão do índice BOVESPA usando Redes Neurais Artificiais**. 2009. 102 f. Trabalho de Conclusão de Curso (Bacharelado em Engenharia Eletrônica e de Computação) - Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2009.

RUSSELL, Jon. ***Alibaba debuts 'smile to pay' facial recognition payments at KFC in China***. 2017. Disponível em:< https://techcrunch.com/2017/09/03/alibaba-debuts-smile-to-pay/>. Acesso em: 10 fev. 2018

SAMPAIO NETO, Nelson Cruz. **Tabela de Dispersão (ou Hash)**. 2016. Disponível em:<http://www2.unifap.br/furtado/files/2016/11/Aula7.pdf>. Acesso em: 27 abr. 2018.

SANCHES, Pedro. ***Deep Web* e suas famosas "camadas"**. 2015. Disponível em: <https://thegeekstorm.wordpress.com/2015/08/12/deep-web-e-suas-famosas-camadas/> Acesso em: 16 abr. 2018.

SANT'ANA, Thais. **Como funciona um cartão de crédito?**. 2012. Disponível em:< https://mundoestranho.abril.com.br/tecnologia/como-funciona-um-cartao-de-credito/>. Acesso em: 23 abr. 2018.

SEBRAE NACIONAL. **O que são meios eletrônicos de pagamentos?**. 2018. Disponível em:< http://www.sebrae.com.br/sites/PortalSebrae/artigos/o-que-sao-meios-eletronicospagamentos,3a085415e6433410VgnVCM1000003b74010aRCRD>. Acesso em: 20 maio 2018.

SECURE TRADING FINANCIAL SERVICES. ***What are AVS, CVV, CCV and CVV2?***. [201-?]. Disponível em:<https://www.securetradingfs.com/faq/faq-10/#>. Acesso em: 26 abr. 2018.

SECURITY STANDARDS COUNCIL. ***Requirements and Security Assessment Procedures***. *Version* 3.2. 2016.

SEGURANÇA DO WHATSAPP. **Privacidade e segurança estão no nosso DNA**. [(201?)]. Disponível em:<https://www.whatsapp.com/security/>. Acesso em: 01 abr.2018.

SERASA EXPERIAN. **Tentativas de fraude contra o consumidor crescem 7,1% em janeiro, revela indicador da Serasa**. 2018. Disponível em:< https://www.serasaexperian.com.br/sala-de-imprensa/tentativas-de-fraude-contra-o-consumidor-crescem-71-em-janeiro-revela-indicador-da-serasa>. Acesso em: 09 maio 2018.

SIGNIFICADOS. **Significado do Sistema de informação**. [201-?]. Disponível em:<https://www.significados.com.br/sistema-de-informacao/>. Acesso em: 15 abr. 2018.

SILVA, Edmar Albino da. **Controle e monitoramento para consumo eficiente de energia elétrica em uma smart home utilizando redes neurais artificiais.** 2016. 86 p. Trabalho de Conclusão de Curso (Bacharel em Engenharia da computação) – Universidade Federal de Santa Catarina, Santa Catarina, 2016.

SIMÕES, Marcelo Godoy; SHAW, Ian. **Controle e modelagem fuzzy**. São Paulo: E. Blucher; FAPESP, 2007. 186p.

SINFIC. **Vantagens e Problemas da Biometria**. 2005. Disponível em:<http://www.sinfic.pt/SinficWeb/displayconteudo.do2?numero=24095>. Acesso em: 15 abr. 2018.

SOARES, Fábio M.; SOUZA, Alan M.f.. ***Neural Network Programming with Java***: Unleash the power of neural networks by implementing professional Java code. Birmingham: Packt Publishing, 2016.

SOS SERVIÇO ONLINE DE SEGURANÇA. UOL SEGURANÇA DIGITAL**. O que é *malware*, *adware*, cavalo de Troia e *spyware***. 2013. Disponível em: <https://seguranca.uol.com.br/antivirus/dicas/curiosidades/o-que-e-malware-adware-cavalo-troia-spyware.html#rmcl>. Acesso em: 16 abr. 2018.

SOUZA, Samira. **Afinal, o que é a *Due Diligence*?**. 2018. Disponível em:<http://www.contabeis.com.br/artigos/4523/afinal-o-que-e-a-due-diligence/>. Acesso em: 10 maio 2018.

SQUAREDUP. ***What is EMV*?**. [201-?]. Disponível em:< https://squareup.com/townsquare/emv>. Acesso em: 23 abr. 2018.

STALLINGS, William. **Criptografia e segurança de redes.** São Paulo: Pearson Pretice Hall, 2008.

_____. **Criptografia e segurança de redes:** princípios e práticas. 6. ed. São Paulo: Pearson Education do Brasil, 2015.

TATHAM, Matt. **20 *Types of Identity Theft and Fraud***. 2018. Disponível em: <https://www.experian.com/blogs/ask-experian/20-types-of-identity-theft-and-fraud/>. Acesso em: 15 abr. 2018.

TECHTERMS. ***Cryptography***. 2015. Disponível em:<https://techterms.com/definition/cryptography>. Acesso em: 01 abr. 2018.

TESTADORES DE CARTÃO. Lista de discursão mantida pela Perfectcards para discursão dos testadores de cartão. 2018. 19 de abr.. Disponível em:<https://t.me/PerfectCarders>. Acesso em: 19 abr. 2018.

THAKKAR, Danny. ***Adoption of Biometrics in Banking and Financial Service Industry***. 2017. Disponível em:<https://www.bayometric.com/biometrics-in-banking-and-finance/>. Acesso em: 9 maio 2018.

THEODORIDIS, Sergios; KOUTROUMBAS, Konstantinos. ***Pattern recognition***. 2. ed. San Diego: Elsevier, 2003.

TREND MICRO CYBER SAFETY SOLTIONS TEAM. ***FighterPOS PoS Malware Gets Worm Routine***. 2016. Disponível em: <https://blog.trendmicro.com/trendlabs-security-intelligence/fighterpos-gets-worm-routine/>. Acesso em: 20 mar. 2018.

TREND MICRO. ***Smart protection network***. 2013.

_____. ***Spear Phishing 101: What is Spear Phishing?***. 2015. Disponível em: <https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/spear-phishing-101-what-is-spear-phishing>. Acesso: 15 abr.2018.

_____. **Vulnerabilidades são as melhores amigas dos cibercriminosos**. 2018**.** Disponível em: <http://blog.trendmicro.com.br/vulnerabilidades-sao-as-melhores-amigas-dos-cibercriminosos/>. Acesso em: 16 abr.2018.

TW SISTEMAS. **TEF – Saiba o que é e como funciona**. 2017. Disponível em:< http://twsistemas.com.br/blog/2017/04/18/tef-saiba-o-que-e-e-como-funciona/>. Acesso em: 01 maio 2018.

VENTURA, Felipe. **Como são criados os números de cartão de crédito**. 2013. Disponível em:< http://gizmodo.uol.com.br/como-sao-edituicriados-os-numeros-de-cartao-de-credito/>. Acesso em: 08 maio 2018.

VILLENA, Reynaldo C. **Reconstrução da chave privada RSA**. 2012. Disponível em:<https://www.ime.usp.br/~reynaldo/sem/sem_3.pdf>. Acesso em: 19 abr. 2018.

VISA. ***Is biometrics the next frontier of mobile payments?***. [201-?]. Disponível em:<https://usa.visa.com/visa-everywhere/innovation/biometrics-next-frontier-payments.html>. Acesso em: 14 maio 2018.

WORLD ECONOMIC FORUM. ***Global Risks Report 2018***. 2018. 13th edition.

ZOCHIO, Marcelo Ferreira. **Introdução à criptografia**. São Paulo: Novated, 2016.

ZURIANRRAIN, José Mendiola. **O que é a criptografia no *WhatsApp* e porque é tãoimportante.2016**. Disponível em:<https://brasil.elpais.com/brasil/2016/04/06/tecnologia/1459942001_217614.html>. Acesso em: 03 abr. 2018.