FACULDADES DOCTUM DE CARATINGA

GRACE KELLY DA SILVA

ESTUDO DO FATOR HUMANO COMO VULNERABILIDADE PARA A SEGURANÇA DA INFORMAÇÃO NO FACEBOOK

CARATINGA

2017

FACULDADES DOCTUM DE CARATINGA

GRACE KELLY DA SILVA

ESTUDO DO FATOR HUMANO COMO VULNERABILIDADE PARA A SEGURANÇA DA INFORMAÇÃO NO FACEBOOK

Monografia apresentada ao curso de Ciência da Computação das Faculdades Doctum de Caratinga, como requisito parcial para obtenção do título de bacharel em Ciência da Computação.

Área de Concentração: Vulnerabilidade em Redes Sociais Digitais

Orientador: Prof.ª Msc. Fabrícia Pires Souza

CARATINGA

2017

FACULDADES DOCTUM DE CARATINGA

FOLHA DE APROVAÇÃO

O Trabalho de Conclusão de Curso intitulado: ESTUDO DO FATOR HUMANO COMO VULNERABILIDADE PARA A SEGURANÇA DA INFORMAÇÃO NO FACEBOOK, elaborado pela aluna GRACE KELLY DA SILVA foi aprovado por todos os membros da Banca Examinadora e aceita pelo curso de Ciência da Computação das Faculdades Doctum de Caratinga, como requisito parcial para a obtenção do título de:

BACHAREL EM CIÊNCIA DA COMPUTAÇÃO

Caratinga, 13 de dezembro de 2017

Prof. Orientador Fabrícia Pires Souza

Prof. Examinador 1 Elias Gonçalves de Souza

Prof. Examinador 2 Wanderson Miranda Nascimento

AGRADECIMENTOS

Agradeço primeiramente a Deus que me proporcionou saúde, sabedoria, perseverança e por ter me conduzido por esse caminho de grande amadurecimento.

Aos meus pais (Eny e Roberto), que sempre me apoiaram e me proporcionaram condições para que eu pudesse chegar até aqui. Às minhas irmãs (Geisy e Deisy), cujas colaborações foram de suma importância para a melhoria e conclusão deste trabalho.

Agradeço por sempre estarem presentes a meu lado, diante das alegrias e dificuldade, e sempre dispostos me ouvir, ou me aconselhar, pois sem minha família, minha caminhada seria muito mais difícil.

A minha orientadora, a professora Msc. Fabrícia Pires, por seu apoio na realização deste trabalho, por compartilhar seus conhecimentos, por seus conselhos, comentários e críticas, com os quais aprendi muito. Ampliando a minha visão deste trabalho ao mesmo tempo em que me motivou durante todo o processo de desenvolvimento do mesmo, sempre com atenção e simpatia.

Também agradeço a todos os professores com quais tive a oportunidade de estudar nesses quatro anos, agradeço por compartilhar suas experiências de vida acadêmica, profissional e pessoal, por toda a dedicação e atenção.

Aos colegas de graduação, pela cumplicidade, pelas novas amizades, pelos momentos de estudo e descontração. Em especial ao meu grupo de estudo: Cláudio, Djully e Glória.

Enfim, agradeço a todos que contribuíram direta ou indiretamente durante todo o período, desde as aulas iniciais do curso até as últimas linhas deste trabalho.

“Descobrir consiste em olhar para o que todo mundo está vendo e pensar uma coisa diferente”. (Roger Von Oech citado por Negrão e Camargo (2008, p. 143))

RESUMO

Este trabalho descreve os conceitos básicos relacionados à análise de redes sociais e a identificação de emoções em texto, contextualizando-os como ferramenta para engenharia social e Segurança da Informação. Considerando que, as emoções desempenham papel fundamental na comunicação e socialização humana interferindo nas relações interpessoais, e as redes sociais digitais passaram a fazer parte da vida das pessoas, tornando-se um local onde elas poderiam compartilhar informações e se expressar. E que devido ao grande número de usuários que as compõem, as redes sociais digitais, tornaram-se alvos de usuários mal-intencionados, os quais fazendo uso das técnicas de engenharia social buscam identificar e explorar usuários vulneráveis. Este trabalho tem por objetivo demonstrar a vulnerabilidade do fator humano nas redes sociais, identificando emoções básicas nos textos postados no Facebook, e como essas informações podem servir como base para ataques de engenharia social. Esta monografia apresenta algumas técnicas utilizadas para mineração de informação em textos com o intuito de identificar emoções em textos, embora não tenha sido utilizada uma ferramenta específica para esse fim. A metodologia adotada foi a de criar dois perfis no Facebook, enviar solicitações de amizade, analisar o nível de exposição de cada usuário que aceitou o convite, criar uma base textual com o conteúdo gerado pelo *Netvizz*. Identificar as emoções contidas nos textos baseando-se em características linguísticas e afetivas, por intermédio dos léxicos ANEW-BR e LIWC, bem como a representatividade das palavras no texto baseando-se em sua frequência (TF-IDF). Por último, desenvolver e aplicar uma técnica de phishing. O resultado do experimento, fazendo uso de características linguísticas e afetivas, por intermédio de léxicos, apresentaram valores de saída fortemente correlacionados às emoções básicas, mostrando assim, que as publicações dos usuários podem ser fontes de dados significativos para engenheiros sociais, uma vez que estes utilizam aspectos emocionais para elaborar estratégias que possam persuadir seus alvos a obedecê-los.

Palavras-chave: Engenharia Social, Fator humano, Emoções básicas, Rede Social, Segurança da Informação.

ABSTRACT

This paper describes the basic concepts related to social network analysis and identification of emotions in text, contextualizing them as tool for social engineering text and Information Security. Considering that emotions play fundamental role in human communication and socialization interfering in interpersonal relationships, and the digital social networks have become part of people's lives, making it a place where they could share information and express themselves. And that because of the number of users that make up the digital social networks, have become targets of malicious users, which making use of social engineering techniques, seek to identify and exploit vulnerable users. This work aims to demonstrate the vulnerability of the human factor in social networks, identifying basic emotions in texts posted on Facebook, and how that information can serve as base for social engineering attacks. This monograph presents some techniques used for mining information in texts in order to identify emotions in text, although it was not used a specific tool for this purpose. The methodology adopted was to create two profiles on Facebook, send friend requests, analyze the exposure level of each user who accepted the invitation, create a textual base with the content generated by Netvizz. Identify the emotions contained in the texts based on linguistic and affective characteristics, through the lexicons ANEW-BR and LIWC as well as the representativeness of words in the text based on their frequency (TF-IDF). Finally develop and apply a phishing technique. The result of the experiment, making use of linguistic and affective characteristics, by means of lexicons presented, output values strongly correlated to basic emotions, thus showing that user publications can be meaningful data sources for social engineers, since they use emotional aspects to devise strategies that can persuade their targets to obey them.

Key words: Social Engineering, Human Factor, Basic Emotions, Social Networking, Information Security

LISTA DE ILUSTRAÇÕES

LISTA DE GRÁFICOS

LISTA DE QUADROS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ANEW-BR	Normas Brasileiras para o Affective Norms for English Words
ARS	Análise de Redes Sociais
LIWC	Linguistic Inquiry and Word Count (Inquérito linguístico e Contagem de palavra)
TF-IDF	Term Frequency–Inverse Document Frequency
TI	Tecnologia da Informação

SUMÁRIO

1 INTRODUÇÃO

O surgimento e crescimento exponencial das redes sociais digitais transformou o relacionamento entre as pessoas, tornando-se uma ferramenta muito utilizada para fazer amigos e conhecer pessoas, e facilitando as interações sociais entre elas. Com o intenso uso das redes sociais e a diversificação dos usuários que as compõe, muitas são as possibilidades de exploração da mesma. Campanhas publicitárias por exemplo, fazem uso de técnicas de mineração de dados e descoberta de opinião, para saber o que oferecer a cada usuário.

Com isso áreas como marketing, economia, ciências sociais e comportamentais vêm utilizando a análise e extração de conhecimento de redes sociais para a compreensão do comportamento da sociedade. Trata-se da chamada análise das redes sociais, estudo que visa identificar diferentes formas de extrair informações das redes sociais digitais, identificando também as vantagens do uso dessas redes (POLONI; TOMAÉ, 2014).

Segundo Poloni e Tomaé (2014) algumas pesquisas sobre a análise das redes sociais, apontam para a construção de *software* robôs que percorrem os sites de relacionamentos em busca de informações de seus usuários. Mas também ressalta que redes sociais como o Facebook possuem proteção contra esses programas, para defender seus usuários contra a invasão de privacidade. No entanto, existem alguns aplicativos, que são executados na plataforma do Facebook, e que permite a extração de dados públicos disponibilizados por grupo públicos criados por usuários.

Por padrão as informações que são postadas pelos usuários, são de domínio público a menos que quem a postou restrinja o acesso às mesmas. Nesse caso os aplicativos seriam inúteis. Portanto para se ter acesso a essas informações restritas é que entra em cena a engenharia social. Uma técnica que visa entender o comportamento das pessoas e se aproveitar dele (SANTOS, 2004). Ela não se limita a área da computação, seus conceitos estão inseridos ou podem ser aplicados no ilusionismo, na medicina, na psicologia, e até mesmo em investigações policiais.

Um engenheiro social dentro da área da tecnologia da informação (TI), é alguém que precisa entender o comportamento dos usuários de uma rede, para que possa aplicar as técnicas mais apropriadas para alcançar seus objetivos. Para entender esse comportamento, ele precisa compreender como o usuário se sente diante de determinadas situações e prever todas as possíveis reações que esse usuário possa ter. E para facilitar esse processo de aquisição de dados referentes ao alvo, um engenheiro social, além de analisar perfis nas redes sociais, pode

vir a utilizar recursos como as técnicas de mineração de textos, com o intuito de descobrir de forma automática o estado emocional de seus autores. Uma vez que essas emoções podem vir a fornecer informações relevantes e podem ser estimuladas por fatores externos (ESPERIDIÃO- ANTONIO et al., 2008).

O foco deste trabalho se restringe ao Facebook devido à enorme quantidade de sites de relacionamentos. Seu objetivo geral é identificar prováveis alvos para ataques de engenharia social no Facebook, utilizando como técnicas de mineração de texto em grupos públicos da rede social para coletar dados que permita traçar um perfil emocional de possíveis vítimas em potencial. Sendo assim pode-se dizer que os objetivos específicos deste estudo foram:

- Estudar a possibilidade de se identificar as seis emoções básicas do ser humano (alegria, tristeza, nojo, medo, surpresa e raiva) a partir de texto publicados no Facebook, utilizando os léxicos ANEW-BR e LIWC, ferramentas usada para analisar os componentes cognitivos e emocionais em amostras textuais.
- Identificar o nível de exposição de usuários a partir de uma análise individual de cada perfil dentro da amostra selecionada.
- Abordar como um engenheiro social poderia fazer uso das informações publicada por usuários no Facebook para orquestrar um ataque.
- Discutir a fragilidade do fator humano para segurança da informação na rede social digital Facebook, destacando as principais vulnerabilidades exploradas pela engenharia social e o que pode ser feito para minimizar a probabilidade de se tornar uma vítima.

Portanto, neste estudo é apresentado não somente as principais técnicas de engenharia social, como também procurou identificar o nível de exposição dos usuários, e suas possíveis emoções com base nos textos publicados pelos mesmos.

Para isso, foram utilizados os léxicos ANEW-BR e LIWC, comparando os resultados obtidos pelos léxicos com os resultados obtidos a partir da identificação das seis emoções básicas proposta por Damásio (2003) nos textos coletados. A ideia é mostrar que além das informações acerca de si próprio as publicações do usuário também podem vir a ser fontes de dados valiosas, seja para fins comerciais, como o direcionamento de campanhas publicitárias como para fins maliciosos como ataques de engenharia social.

Este trabalho está estruturado da seguinte forma:

No capítulo 1 são descritos a introdução, os objetivos gerais e específicos e a justificativa geral da execução deste trabalho. O capítulo 2 apresenta a fundamentação teórica, tratando de descrever os assuntos relacionados à segurança da informação, redes sociais,

análise de sentimentos em textos, léxicos afetivos, mineração de texto, engenharia social, e as vulnerabilidades do fator humano.

No capítulo 3 a metodologia é descrita detalhadamente, com os passos que foram realizados para a execução da experimentação prática. O capítulo 4 apresenta a análise dos dados e os resultados obtidos. Por fim, são apresentadas às conclusões deste trabalho e sugestões para trabalhos futuros.

2 REFERENCIAL TEÓRICO

Compondo a revisão bibliográfica, este capítulo apresenta conceitos e teorias encontrados na literatura sobre o tema proposto.

De acordo com Creswell (2007), a revisão da literatura significa localizar e resumir os estudos sobre um tema, identificando os principais tópicos abordados na pesquisa, proporcionando uma estrutura para estabelecer a importância do estudo em questão. Sendo assim, são apresentadas argumentações que englobam os seguintes assuntos: segurança da informação, redes sociais digitais, engenharia social, mineração de textos, reconhecimento de emoções a partir de texto publicadas no Facebook, abordando a utilização dos léxicos afetivos ANEW-BR e LIWC.

2.1 Segurança Da Informação

O que é informação? Um bem de valor intangível. Um conjunto de dados cuja a organização constitui uma mensagem para um destinatário, permitindo-o solucionar problemas e tomar decisões (ALVES, 2010). Sendo assim perder ou ter informações roubadas pode causar grandes prejuízos a quem elas pertencem ou se refere. Por isso a informação precisa ser protegida, uma vez que:

> A informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e consequentemente necessita ser adequadamente protegida. [...] Como um resultado deste incrível aumento da interconectividade, a informação está agora exposta a um crescente número e a uma grande variedade de ameaças e vulnerabilidades (ABNT, 2005, p. x)

Isto posto, a Segurança da Informação ocupa-se dos processos e metodologias que foram planejados e implementados para proteger informações impressas, eletrônicas ou qualquer outra forma de informações confidenciais, privadas, e sigilosas contra uso indevido, divulgação, destruição, modificação ou interrupção não autorizados.

> O termo segurança da informação pode ser designado como uma área do conhecimento que salvaguarda os chamados ativos da informação, contra acessos indevidos, modificações não autorizadas ou até mesmo sua não disponibilidade. (Peixoto, 2006, p. 37)

A segurança da informação é formada por pilares básicos, que podem ser definidos da

seguinte maneira (PEIXOTO, 2006):

- Confidencialidade: É a garantia de que as informações transmitidas chegarão ao seu destino e que estarão acessíveis somente para as pessoas autorizadas a terem acesso a elas.
- Integridade: É a garantia de que as informações não passarão por nenhuma modificação durante o trajeto entre o emissário e o destinatário.
- Disponibilidade: É a garantia de que as informações estarão disponíveis para que os usuários autorizados obtenham acesso às mesmas sempre que necessário
- Alguns modelos chegam a incluir mais dois pilares básicos que seriam os seguintes:
- Não repúdio: É a garantia de que o autor não negará ter criado e assinado determinado documento.
- Autenticidade: visa estabelecer a validade da transmissão, da mensagem e do seu remetente, para que o destinatário possa comprovar a origem e autoria da informação.

Os pilares acima também envolvem três aspectos principais: pessoas, processos e tecnologia. Pessoas referem-se a usuários que utilizam os sistemas, e que deveriam ser bem orientados, treinados e conscientizados. Processo diz respeito às regras para utilização dos recursos tecnológicos e leis que objetivam punir de maneira rigorosa os infratores em caso de desvio de informações. E por fim tecnologia, trata-se dos sistemas utilizados e que deveriam ser bem implementados para garantir a proteção das informações. (SCHNEIER, 2013)

2.1.1 Incidentes relacionados à segurança da informação

Nos dias de hoje, a informação pode ser considerada um dos patrimônios mais importante, tanto para um indivíduo quanto para uma organização. E por causa disso as mesmas estão sob o constante risco, uma vez que sua perda ou roubo pode constituir em prejuízo para a pessoa ou para a empresa. Daí a importância em protegê-la, descobrindo os pontos vulneráveis da segurança, avaliando os riscos, os impactos e elaborando estratégias para minimizá-los (ARAÚJO, 2005).

Para Machado (2009, p.3). “grande parte dos incidentes contam com participação humana, diretamente ou indiretamente, intencionalmente ou não”. Por isso é essencial saber diferenciar quais informações são confidenciais e vitais, evitando que elas sejam divulgadas e expostas precipitadamente na internet. A mesma internet cujo uso crescente contribuiu para o aumento do índice de crimes virtuais.

De acordo com o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil foram 647.112 incidentes reportados entre janeiro a dezembro de 2016, dos quais 343.418 (55,49% dos incidentes) tiveram origem no Brasil (CERT, 2016b). Somente no Brasil 42,4 milhões de usuários foram afetados pelo cibercrime em 2016 e o prejuízo financeiro gerado foi de US$10.3 bilhões (NORTON, 2016). Dentre os tipos de fraudes virtuais mais comuns, estão o uso de sites falsos (90,85% dos incidentes); os trojans ou cavalos de Tróia (0,51%); violação dos direitos autorais (3,41%); e outras tentativas de fraudes possuem um percentual de 5,23% dos incidentes (CERT, 2016a).

Segundo o relatório da Norton (2010) quase dois terços ou 65% dos adultos mundialmente já foram vítimas de algum tipo de crime cibernético (golpes online, ataques de phishing, roubos de perfis de redes sociais e fraude de cartão de crédito). Sendo que 7% destes adultos se depararam até mesmo com predadores sexuais online. Mas apenas 68% dos entrevistados seriam capazes de detectar corretamente os *e-mails* de *phishing*. Isso significa que 32% das pessoas entrevistadas teriam maior possibilidade de ser vítima de um ataque de phishing por não saber como identificá-lo corretamente.

De acordo com Fernando Peres, advogado especialista em direito digital e crimes cibernéticos em uma entrevista ao jornal Gazeta do povo, afirmou que à medida que a quantidade de usuários de tecnologia aumentar, maior será o percentual da ocorrência de vírus. Peres afirma também que o aumento do número de usuários representa um aumento no número de aparelhos, de novas tecnologias, mas a educação digital desses usuários não muda. Para o especialista, os ataques de phishing são os crimes mais comuns porque são eficazes, e ele cita o seguinte exemplo: se um cibercriminoso enviasse 10 milhões de *e-mails* falsos, e que 1% destes *e-mails* fossem válidos; já seriam 100 mil *e-mails*. Supondo que deste 1%, 0,01% das pessoas impactadas clicou na isca, isso seria mil *e-mails*. E se metade dessas pessoas fornecesse informações como dados de cartão de crédito, já seriam 500 vítimas. Por isso esse tipo de ataque, além de ser simples pode ser muito vantajoso financeiramente para quem o utiliza (COELHO, 2017).

Aparentemente poucas pessoas parecem estar preocupadas com a facilidade com que suas informações são roubadas. Haja vista, o crescimento acelerado das redes sociais e o exibicionismo nas mesmas, a negligência às permissões de acesso à aplicativos desconhecidos em smartphone, e a dificuldade em seguir procedimento simples de segurança quando se está online. Vê-se inúmeros casos envolvendo invasão de sistemas, roubo ou sequestro de informações sendo noticiados. Como por exemplo, os casos envolvendo os *ransomwares*, um tipo de *software* nocivo, que tem causado prejuízo em todo o mundo, pois ao se infiltrar num

dispositivo ligado à internet sequestra os dados do mesmo e exige um pagamento em criptomoedas, como por exemplo, o Bitcoin, para que os dados sejam supostamente liberados e caso não ocorra o pagamento, arquivos podem vir a ser perdidos ou mesmo publicados (COELHO, 2017). Outro exemplo que pode ser citado também é o desafio denominado “baleia azul”. Um desafio compartilhado nas redes sociais que foi muito noticiado no primeiro semestre de 2017, e se baseava na relação entre os desafiantes e o administrador, este último define tarefas a serem executadas pelos desafiantes, essas incluem desde desenhos inofensivos a atividades de risco, passando por automutilações e incitação ao suicídio, e a maioria dos desafiantes resistia em sair do jogo por temer as ameaças e chantagens dos administradores (INFOGLOBO, 2017).

Assim como estes, existem muitos outros casos na internet, casos de empresa que tiveram prejuízos enormes, casamentos que terminaram em divórcio, funcionários que foram demitidos, amizades desfeitas, simplesmente porque alguém teve acesso indevido a informações privadas. Esses casos, assim como tantos outros, tiveram como elo fraco para a segurança, o fator humano. Fator este, que é amplamente explorado pela engenharia social. Supondo que a tecnologia seja avançada e utilizada da maneira correta, as estratégias de ataques recaem sobre as pessoas, isso porque seria muito mais fácil persuadir uma pessoa do que tentar invadir sistemas computacionais (MITNICK; SIMON, 2003). Sendo assim, o que é a engenharia social, e como ela tem se tornado um problema nas redes sociais digitais, quais os principais tipos de ataques, como a engenharia social é vista perante a lei e quais principais práticas que se deve adotar para minimizar a possibilidade de se tornar uma vítima, serão os temas discutidos na próxima seção.

2.2 Engenharia Social

Usada desde a origem do homem, a engenharia social, basicamente consiste em entender e se aproveitar do comportamento das pessoas construindo métodos para enganá-las usando informações cedidas por elas mesmas.

De acordo com Santos (2004) o termo “engenharia” é porque baseada em informações, são construídas táticas de acesso à informações sigilosas, e “social” porque se utiliza de pessoas que trabalham e vivem em grupos organizados.

> Engenharia Social é a ciência que estuda como o conhecimento do comportamento humano pode ser utilizado para induzir uma pessoa a atuar segundo seu desejo. Não se trata de hipnose ou controle da mente, as técnicas de Engenharia Social são

> amplamente utilizadas por detetives (para obter informação) e magistrados (para comprovar se um declarante fala a verdade). (KONSULTEX, 2004 apud PEIXOTO, 2006, p. 4).

Sendo assim a engenharia social não se restringe a área da computação. Ela pode ser aplicada, por exemplo, na medicina, ou na psicologia, quando o médico ou terapeuta precisa convencer seus pacientes a mudarem seu comportamento, e tomar assumir atitudes que os auxiliem no tratamento. Ou por policiais durante um interrogatório, quando se faz uso de reconhecimento de expressões faciais, linguagem corporal e técnicas de manipulações a fim de extrair o máximo de informações dos suspeitos. (CORTELA, 2013).

> A engenharia social usa a influência e a persuasão para enganar as pessoas e convencê-las de que o engenheiro social é alguém que na verdade ele não e, ou pela manipulação. Como resultado, o engenheiro social pode aproveitar-se das pessoas para obter as informações com ou sem o uso da tecnologia (MITNICK; SIMON, 2003)

Considerando que as informações pessoais fazem parte de um sistema que possui características comportamentais e psicológicas, no qual a engenharia social necessita ser auxiliada por técnicas como linguagem corporal e neurolinguística, para que tais informações possam ser obtidas por meio da persuasão, confiança, dissimulação ou ingenuidade, quem emprega a engenharia social deve estudar o comportamento de seus alvos fazendo uso de falhas ou brechas psicológicas e sociais, para compreendê-los melhor, monitorando seus horários, hábitos e círculos sociais, a fim de colher o maior número de dados possível. Esse e outros traços do perfil de um engenheiro social serão abordados a seguir.

2.2.1 Engenheiro Social

O engenheiro social usa sua criatividade simpatia, poder de persuasão, carisma para envolver sua vítima, sabendo explorar bem o ambiente, desvendando o comportamento de seu alvo, de tal forma que ele nem percebe que abriu as “portas” para uma invasão. Ele finge ser o que não é fazendo uso de estratégias que mudam de acordo com o ambiente em que está inserido e quais são seus objetivos.

> O profissional da arte de enganar pessoas utiliza-se de técnicas de persuasão e exploração da ingenuidade dos usuários, criando um ambiente psicológico perfeito para seu ataque, como por exemplo, utilizando identificações falsas, carisma e o apelo sentimental a fim de conquistar a confiança da vítima. (ALVES, 2010, p. 29)

Segundo Mitnick e Simon (2003,p.xiii) “quando você combina uma inclinação para

enganar as pessoas com os talentos da influência e persuasão, você chega ao perfil de um engenheiro social". Ainda segundo Mitnick e Simon (2003) trata-se de alguém que usa a fraude, a influência e a persuasão contra as empresas, em geral visando suas informações.

Quando se leva em consideração a relação entre o engenheiro social e seu alvo, no que se refere ao comportamento humano, é importante salientar que o engenheiro social deve sempre estar um passo à frente de sua vítima, para poder identificar qualquer reação da mesma. Seu alvo deve ser previsível aos seus olhos, para que seja possível identificar o momento em que as técnicas aplicadas trarão maior retorno ou não, de um jeito que a vítima não desconfie que esteja sendo manipulada. (SANTOS, 2014).

O engenheiro social é tão criativo, que muitas vezes, a vítima nem imagina que foi usada e muito menos que acabou de abrir o caminho para um invasor. Para que o ataque seja bem-sucedido, também é preciso que o engenheiro social seja muito paciente e persistente. (ALVES, 2010).

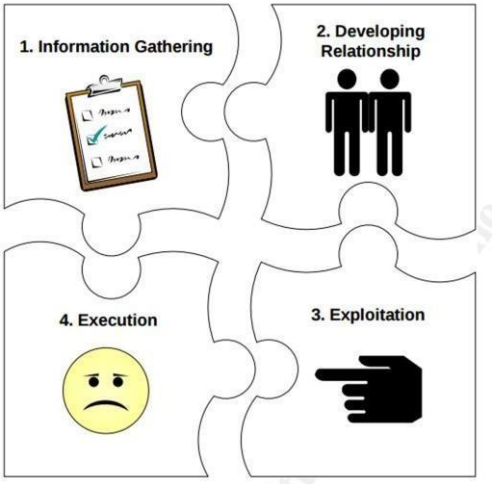
2.2.2 Ataques de Engenharia Social

Segundo Alves (2010) pode se dividir os ataques de engenharia social em dois grupos: Ataques diretos e ataques indiretos. Os ataques diretos se caracterizam, pelo contato direto da vítima com o engenheiro social, requerendo dele muita criatividade, muita preparação e prática, um planejamento antecipado e bem detalhado, para poder prever reação da vítima, além de um segundo plano caso o primeiro falhe. Tais ataques podem ser executados por telefone, fax ou pessoalmente. Já nos ataques indiretos, o engenheiro social, irá utilizar algum *software* ou alguma ferramenta que possa fazer o intermédio entre ele e a vítima. Pode ser vírus, cavalos de Tróia, *e-mails* falsos, sites falsos, o que for preciso para obter as informações desejadas.

Segundo Santos (2004, p.24) os ataques do engenheiro social podem ocorrer através de uma boa conversa, seja numa mesa de bar, ao telefone ou, em casos mais sofisticados, através da sedução. Para ele a engenharia social é mais utilizada "para o levantamento de informações preliminares que possam tornar a tentativa de invasão mais eficiente". Geralmente as pessoas acreditam que mentiras elaboradas são usadas nos ataques de engenharia social, no entanto devido a ingenuidade ou a confiança de um usuário, basta simplesmente o engenheiro social pedir a informação desejada e pronto (SANTOS, 2004). Mesmo com a possibilidade de envolver múltiplas fases/ciclos e/ou pode até mesmo agregar o uso de outras técnicas, cada

ataque de engenharia social é único. Segundo Allem (2006, p. 5), o ciclo de ataques da engenharia social consiste em quatro fases, como mostrado na Figura 1:

Figura 1 - O Ciclo da Engenharia Social



Fonte: Allem (2006, p. 6)

- Reunir Informações - Buscar o máximo de informações possíveis sobre o alvo Desenvolver o Relacionamento com a vítima - Se aproximar da vítima, pessoalmente ou não.
- Exploração - identificar e explorar as principais vulnerabilidades do alvo.
- Execução - Definir e executar as melhores estratégias para conseguir do alvo o que se deseja.

Mas o que leva alguém a estudar, arquitetar e realizar um ataque de engenharia social? Segundo Allem (2006, p. 6) existe uma variedade de motivações:

- Ganho financeiro: por diversas razões, um indivíduo pode ficar obcecado em ganhos monetários. Por exemplo, ele pode acreditar que ele merece mais dinheiro do que ganha ou talvez precise satisfazer um vício.
- Interesse próprio: um indivíduo pode, por exemplo, querer acessar e / ou modificar informações associadas a um membro da família, amigos ou um vizinho.
- Vingança: por razões que só indivíduo conhece, ele pode procurar um amigo, colega, organização ou mesmo um completo estranho para satisfazer o desejo emocional de vingança.
- Pressão externa: um indivíduo pode receber pressão de amigos, familiares ou crime organizado por razões como ganho financeiro, interesse próprio e / ou vingança.

E uma vez que uma pessoa tenha um ou mais desses interesses em mente, ela poderia

vir escolher dentre as técnicas a seguir a que melhor se enquadra ao ataque que se deseja realizar. Abaixo se encontram as técnicas, meios e métodos de ataque mais comuns usados pelos engenheiros sociais:

- Cartas/Correspondência: embora não seja um meio muito atual, é certamente um ótimo recurso para ser utilizado com pessoas que resistem aos avanços tecnológicos como pessoas idosas por exemplo. O método consiste em enviar cartas falsas para enganar as vítimas. (PEIXOTO, 2006).
- Chats (bate papo): o atacante tenta se passar por outra pessoa em salas de bate-papo, chegando a enviar fotos atrativas para seduzir as vítimas e obter as informações desejadas (POPPER; BRIGNOLI, 2002).
- *E-mails* falsos: é um dos meios mais comuns, a técnica consiste em enviar *e-mails* falsos com o intuito de induzir seu alvo a clicar em um link que irá instalar um vírus, cavalo de Tróia ou redirecionará a vítima a uma página falsa que irá capturar os dados inseridos pela mesma. Geralmente esses *e-mails* tratam de assuntos como promoções, premiações, recuperação de dados, contas bancárias, ou seja, qualquer assunto que possa despertar a curiosidade e o interesse do alvo. (JUNIOR, 2006; POPPER; BRIGNOLI, 2002).
- Contato Telefônico: Seja simulando um atendimento ou uma ação de emergência, ou para complementar uma das técnicas anteriores, o engenheiro social utiliza essa abordagem para ludibriar a vítima e obter acesso não autorizado ou informações sigilosas, podendo se passar por qualquer pessoa que preste algum tipo de serviço a vítima como um funcionário de uma empresa, fornecedor, amigo de um colega de trabalho, ex-colega de classe. (POPPER; BRIGNOLI, 2002).
- Disfarce: Nesse método, o engenheiro social pode fazer uso de disfarce para poder entrar em estabelecimentos restritos. Geralmente os disfarces mais comuns são os de equipe de manutenção e de entregadores. (SANTOS, 2004).
- Divisão de responsabilidades: trata-se de uma técnica muito comum, e consiste em convencer alguém a compartilhar informações e senhas objetivando dividir alguma tarefa ou responsabilidade. (JUNIOR, 2006).
- Engenharia Social Inversa: é trata-se de uma técnica um pouco mais elaborada, exigindo muita preparação e pesquisa. Consiste em fazer com que a vítima acredite que o atacante é alguém que possui autoridade e conhecimento, de modo que a vítima passe a pedir informações ao atacante, até que, sem que ninguém perceba, o

criminoso consiga extrair as informações valiosas de que precisava. (JUNIOR, 2006).

- Fax ou internet-fax: trata-se de um meio cuja finalidade é obter informações através de formulários de preenchimento, pedidos da requisição, dentre outros, para posteriormente fazer um ataque mais elaborado. (PEIXOTO, 2006).
- Footprint: Esta técnica visa descobrir informações sobre os recursos tecnológicos utilizados pelo alvo em questão, para isso faz-se necessário a utilização de *softwares* especializados, que irão coletar as informações desejadas (JUNIOR, 2006).
- Internet e Redes sociais: A internet e em especial as redes sociais, são excelentes ferramentas para se coletar informações relevantes a respeito de um alvo. O anonimato ou a possibilidade de se passar por outra pessoa nos sites de relacionamentos, tem contribuído muito para o sucesso dos ataques de engenharia social (PEIXOTO, 2006; POPPER; BRIGNOLI, 2002).
- Intranet (acesso remoto): Essa técnica consiste em acessar remotamente um computador, assumindo o controle do mesmo, objetivando se passar por alguém que na realidade não é (PEIXOTO, 2006; POPPER; BRIGNOLI, 2002).
- P2P (*Peer-to-Peer*): tecnologia empregada para o compartilhamento de arquivos entre diversos computadores. E o atacante pode usar essa tecnologia para espalhar pragas virtuais. (POPPER; BRIGNOLI, 2002).
- Pessoalmente: A técnica consiste em realizar uma visita pessoalmente ao alvo. Utilizando um disfarce, o atacante usa todo seu poder de persuasão, charme, carisma, habilidade de comunicação e ingenuidade da vítima para convencê-la a dar-lhe informações restritas ou acesso a essas informações (PEIXOTO, 2006).
- *Phishing*: trata-se de uma técnica que utiliza links que redirecionam a vítima a sites falsos criados para se passar por sites reais a fim induzir a vítima a inserir informações pessoais (JUNIOR, 2006).
- Programação neurolinguística: conjunto de técnicas que utiliza a comunicação verbal e não verbal, para entender e modificar o comportamento da outra pessoa. Na engenharia social, essa técnica visa ganhar a confiança da vítima, criando nela uma sensação de afinidade com o atacante. E uma vez estabelecida essa confiança o atacante persuadir a vítima e obter as informações desejadas (JUNIOR, 2006).
- *Spoofing*: com essa ferramenta o atacante pode manipular o número exibido pelo

identificador de chamadas. Exibindo aquele que ele desejar (JUNIOR, 2006).

- Surfar sobre os ombros (*shoulder surfing*): consiste em olhar o que a pessoa está digitando para descobrir as senhas dela enquanto ela digita no teclado (JUNIOR, 2006).
- *Spyware*: É um *software* espião usado de modo oculto, para monitorar o computador sem que a vítima perceba. (PEIXOTO, 2006).
- Varredura do Lixo: Geralmente as pessoas têm pouco cuidado com o que vai para o lixo. Muitos documentos contendo informações relevantes são jogados no lixo por falta de atenção. Uma conta de água ou de luz, por exemplo, nela está o nome, endereço, CEP, CPF; um extrato pode expor a situação financeira de alguém. Essas informações nas mãos de pessoas erradas podem causar sérios transtornos (JUNIOR, 2006; PEIXOTO, 2006; POPPER; BRIGNOLI, 2002).

Algumas dessas técnicas podem ser utilizadas isoladas ou em conjunto, isso vai depender da habilidade do engenheiro social e da resistência da vítima.

2.2.2.1 Phishing

Dentre as técnicas citadas na seção 2.2.2, deu-se uma atenção mais detalhada ao phishing, por ser a técnica escolhida para ser aplicada no estudo de caso. Isso porque diariamente são espalhadas pela internet milhões de ameaças virtuais, podendo ser a maioria classificada como phishing.

O termo "*phishing*" vem do inglês "*fishing*" e significa "pescando", pois, o objetivo é "pescar" as informações pessoais. Os ataques de phishing podem ocorrer de várias formas, desde uma simples mensagem por *e-mail* ou mensageiro instantâneo induzindo o usuário a clicar em um link suspeito, até páginas inteiras implementadas com o intuito de imitar sites reais como bancos, instituições financeiras, redes sociais entre outras. Assim os cibercriminosos podem obter senhas e nomes de usuários de um determinado site, ou obter dados de cartões de crédito e contas bancárias (DANHIEUX, 2013).

De acordo com Danhieux (2013) os ataques de *phishing* acontecem de quatro maneiras:

- Coletar Informações: O objetivo do atacante é o usuário clicar em um link que o levará a uma página de Internet que pedirá o nome de usuário e senha, ou talvez dados do cartão de crédito ou débito. Tais páginas embora pareçam legítimas, são

falsas e foram desenvolvidas pelos cibercriminosos apenas para roubar informações;

- Infectar o computador com links maliciosos: semelhante ao anterior, o objetivo dos atacantes é faz o usuário clicar em um link, visando infectar o computador da vítima ao invés de colher informações. Se a vítima clicar no link, ela é direcionada a uma página de Internet que lança silenciosamente um ataque contra o navegador de Internet e, se bem-sucedido, dará acesso total ao computador da vítima, via Internet;
- Infectar o computador com anexos maliciosos: São *e-mails* com anexos maliciosos como arquivos PDF ou imagens. Quando se abrem estes anexos, eles atacam o computador e, se quando bem-sucedidos, dão controle total ao computador da vítima;
- Fraudes (Scam): São tentativas dos cibercriminosos para defraudar suas vítimas. Entre os exemplos clássicos estão: notícias de que a vítima ganhou na loteria (mesmo que nunca tenha jogado), pedidos de ajuda financeira sejam logo após desastres recentes ou para alguém que supostamente está doente e precisa de ajuda.

No Facebook as “iscas” frequentemente podem ser lançadas em forma de sorteios, promoções, mensagens pessoais, disfarçadas de perfis e páginas falsos. O usuário mais desatento tende a cair facilmente nessas armadilhas.

2.2.3 Engenharia social nas redes sociais

Desde a popularização da internet diversas plataformas foram criadas com o intuito de aproximar as pessoas. Seja para ensinar, aprender, trabalhar ou se relacionar, cada dia as pessoas encontram mais motivos para permanecer conectadas na internet. Devido a simplicidade e facilidade de uso, as redes sociais se popularizaram rapidamente, possibilitando o relacionamento com parentes, amigos e desconhecidos. No entanto, como qualquer ferramenta, existe os prós e contras, a facilidade de se localizar em poucos minutos informações pessoais como nome, endereço, telefone, é o lado negro das redes sociais. Tornando evidente que qualquer pessoa que possua um perfil ativo numa rede social pode se tornar uma vítima de um ataque de engenharia social. (SANTOS, 2014).

Por exemplo, uma das principais características que o Facebook possui é a facilidade para encontrar novos amigos. E essa possibilidade acaba se tornando uma técnica comumente

utilizada por engenheiros sociais. Se uma solicitação de amizade é aceita por um usuário, seu grupo de amigos certamente receberá notificações referentes a isso, e também receberão recomendações do próprio Facebook para incluir aquele “amigo” que foi aceito, em sua rede de amigos. Assim poderão estar aceitando a amizade de um engenheiro social sem se dar conta disso. E por causa do grande volume de dados publicados e compartilhados em redes sociais pelos próprios usuários, os engenheiros sociais tem se atraído cada vez mais pela plataforma. Pois ele pode se aproveitar da relação de confiança que existe entre ele e vítima, conquistada devido a uma simples solicitação de amizade, para capturar as informações que estão disponíveis no perfil da vítima, podem vir a fazer uso de outras técnicas de ataque. (SANTOS, 2014).

Embora as redes sociais sejam implementadas com um alto nível de segurança, a fragilidade da segurança das mesmas se encontra no fator usuário, uma vez que ele é quem tomará a decisão de seguir ou não as regras básicas de segurança. Mas o que diz a legislação brasileira quanto a engenharia social? Esse é o tema da próxima seção.

2.2.4 A Engenharia Social Perante a Lei

Cada vez mais pessoas estão se conectando à internet. Seja pelo computador, celulares ou tablets, diariamente pessoas no mundo todo usam a internet para diversos fins, realizam transações bancárias, transferência de documentos, troca de mensagens etc. Por causa disso os chamados crimes virtuais têm se tornado uma ameaça cada vez maior. Mas, afinal, os que são crimes virtuais e quais leis se aplicam a eles? E como os crimes causados pelas técnicas de engenharia social são tratados a vista da lei?

Diferente de outros crimes, o crime virtual também é conhecido como crime eletrônico, cibercrime, ou crime cibernético. Trata-se de crimes praticados por pessoas com certo conhecimento em tecnologia, que geralmente utilizam a internet para cometê-los. Dentre os objetivos dos cibercriminosos estão: roubar identidade, praticar fraudes, acessar contas bancárias, chantagear, coagir, ameaçar, extorquir, pressionar, caluniar e assediar pessoas (AVAST, 2017).

As técnicas de engenharia social são consideradas crimes, portanto passíveis de punição. Tais punições podem ir desde o pagamento de multas até a detenção. Como por exemplo, as técnicas em que o engenheiro social se passa por outra pessoa, nesse caso ele poderia ser enquadrado no Art. 299 do Código Penal (Brasil. Decreto-Lei n. 2.848, 1940),

como falsidade ideológica.

> Art. 299. - Omitir, em documento público ou particular, declaração que dele devia constar, ou nele inserir ou fazer inserir declaração falsa ou diversa da que devia ser escrita, com o fim de prejudicar direito, criar obrigação ou alterar a verdade sobre fato juridicamente relevante:
>
> Pena - reclusão, de 1 (um) a 5 (cinco) anos, e multa, se o documento é público, e reclusão de 1 (um) a 3 (três) anos, e multa, se o documento é particular. (Brasil. Decreto-Lei n. 2.848, 1940, p. 76)

Della Valle e Ulbrich (2004, p. 124) citam que: "A interpretação legal baseia-se na configuração dos atos de engenharia social como falsidade ideológica, caracterizada pela incorporação de uma identidade alheia (impostura) seguida de fraude".

E no que diz respeito a fraudes os engenheiros sociais poderiam ser enquadrados no Art. 171 do Código Penal dependendo do que o invasor fizer com as informações, respondendo pelo crime de estelionato. (DELLA VALLE; ULBRICH, 2004, p. 124)

> Art. 171 - Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento.
>
> Pena - reclusão, de 1 (um) a 5 (cinco) anos, e multa (Brasil. Decreto-Lei n. 2.848, 1940, p. 45).

No entanto já está em vigor a lei 12.737/2012 que insere no Código Penal crimes ocorrem na internet ou por meio eletrônicos, os crimes cibernéticos. A lei foi apelidada de "Carolina Dieckmann", depois que a atriz teve 36 fotos íntimas disponibilizadas na internet sem autorização, e prevê pena de seis meses a dois anos de reclusão nos casos em que a invasão resultar em invasão de privacidade, obtenção de conversas privadas ou informações sigilosas, segredos comerciais ou industriais (SANTOS, 2004).

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
>
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa. (Brasil. Decreto-Lei n. 12.737, 2012)

Caso haja divulgação, comercialização ou transmissão a terceiro, a pena pode ser aumentada de um a dois terços. Aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão à terceiro, a qualquer título, dos dados ou informações obtidas.

> § 3° Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
>
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
>
> § 4° Na hipótese do § 3o, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos. (Brasil. Decreto-Lei n. 12.737, 2012).

Podendo aumentar ainda de um terço a metade se as vítimas forem políticos como vereadores, prefeitos, deputados federais, deputados estaduais, senadores, governadores, e presidente da República.

> § 5° Aumenta-se a pena de um terço à metade se o crime for praticado contra: I - Presidente da República, governadores e prefeitos;
>
> - Presidente do Supremo Tribunal Federal;
>
> - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
>
> - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal. (Brasil. Decreto-Lei n. 12.737, 2012).

Mesmo que o código penal não utilize o termo “engenharia social”, é possível perceber que devido às técnicas empregadas pelos engenheiros sociais, eles poderiam ser enquadrados em outros artigos sofrendo as punições correspondentes aos crimes cometidos.

2.2.5 Boas práticas contra a engenharia social

Segundo Mitnick e Simon (2003, p. 195) “a verdade é que não existe uma tecnologia no mundo que evite o ataque de um engenheiro social”. Tecnologia pode ser que não, mas boas práticas e medidas de defesa, certamente. E nesta seção algumas dicas básicas de como se proteger dos engenheiros sociais, minimizando ou dificultando as possibilidades de ataque. Para uma navegação segura, não apenas nas redes sociais, mas na internet, é essencial:

- Ter bom senso, sendo capaz de considerar as consequências de seus atos, como por exemplo, saber que ao clicar num link desconhecido, existe a possibilidade de ter informações coletadas.
- Saber o risco que se corre ao preencher um formulário online com dados pessoais ou fornecer informações confidenciais, como senhas, a estranhos.

- Distinguir qual a melhor decisão a ser tomada diante de uma situação de risco, como por exemplo, quando um navegador de internet identifica que um determinado site não é seguro, é responsabilidade do usuário abrir a página e permanecer nela ou não.

Além disso, existem algumas práticas que se aplicadas podem auxiliar os usuários a se manter seguro diante de alguma tentativa de ataque de engenharia social, são elas (CERT.BR, 2017):

- No que diz respeito ao que se deve fazer quando estiver navegando na internet, o usuário deve: observar se os sites acessados utilizam protocolos de segurança como o https; verificar a barra de status do navegador antes de se clicar em um link, observando se o endereço de destino do link corresponde com a descrição do mesmo; prestar a atenção no regulamento de sorteios e promoções, verificando se estão de acordo com a lei; tomar cuidado com os redirecionamento de páginas, pois podem vir a se tratar de páginas falsas; quando necessário o preenchimento de formulários, observar atenciosamente se existe a uma real necessidade de coletar essas informações; antes de se realizar compras pela Internet deve-se procurar por sites reconhecidamente seguros; deve-se ter cautela com *e-mails* falsos de bancos, lojas e cartões de crédito;
- Quanto a senhas, não se deve disponibilizá-las, nem as escrever em locais onde há fluxo de pessoas, evitando inclusive mencioná-las por telefone também se deve usar uma senha diferente para cada site ou sistema. Para a criação de senhas, deve-se combinar números, letras maiúsculas e minúsculas, e símbolos. A senha será mais forte quando houver uma variedade de caracteres, mas caso haja uma menor variedade de caracteres então maior deve ser a senha. Pode-se usar frases ou palavras que, embora sejam conhecidas para quem está criando a senha, deve ser difícil de ser adivinhada por um estranho, mas não se deve utilizar sequências repetidas, parte do nome, nome de *login*, data de aniversário, número de documentos, pois são as primeiras a serem testadas pelos invasores.
- Com relação aos recursos computacionais, deve-se evitar deixar a máquina ligada com usuário logado disponível para alguém não autorizado; evitar exibir informações confidenciais, como por exemplo, senha, *login* de usuário; também é necessário que se instale bons antivírus realizando uma verificação completa do computador no mínimo uma vez por semana, usando sempre uma cópia original do programa, uma vez que as cópias falsificadas além de não funcionar corretamente, já estão infectadas

por vírus e malwares; deve-se manter o sistema operacional e os programas instalados sempre atualizados, para protegê-los contra as falhas de segurança, que diariamente são descobertas;

Essas práticas auxiliam à medida que minimizam a possibilidade de se tornar uma vítima de um engenheiro social. Embora geralmente não se possa ter certeza das intenções de um site ou de uma pessoa, a desconfiança pode vir a ser uma aliada, pois excesso de confiança é um dos aspectos amplamente explorado pela engenharia social.

Como dito anteriormente as redes sociais digitais têm chamado a atenção dos engenheiros sociais, por esse motivo a próxima seção abordará os conceitos concernente à rede social e seu contexto na área da tecnologia da informação.

2.3 Redes Sociais Digitais

O termo rede social, se refere a uma estrutura englobada por pessoas e organizações que se conectam por diferentes tipos de relações, relações de amizade, relações familiares, comerciais, entre outros, compartilhando valores e objetivos comuns (SILVA, 2007, p. 66).

Segundo Recuero (2009) rede social, é um conjunto de dois elementos básicos: atores e suas conexões – onde atores podem ser pessoas, organizações ou instituições:

> Os atores são o primeiro elemento da rede social, representados pelos nós (ou nodos). Trata-se das pessoas envolvidas na rede que se analisa. Como partes do sistema, os atores atuam de forma a moldar as estruturas sociais, através da interação e da constituição de laços sociais. (RECUERO, 2009, p. 25).

E conexões as interações entre esses atores:

> Em termos gerais, as conexões em uma rede social são constituídas dos laços sociais, que, por sua vez, são formados através da interação social entre os atores. De um certo modo, são as conexões o principal foco do estudo das redes sociais, pois é sua variação que altera as estruturas desses grupos. (RECUERO, 2009, p. 30).

No contexto digital, uma rede social se baseia nas relações online entre o indivíduo e as pessoas ou organizações com quem têm alguma conexão ou interesse em comum. Nesse ambiente virtual, os usuários podem criar um perfil com informações pessoais sobre situações de sua vida atual, situação familiar, parcerias, interesses como filmes, livros, política, música, etc.

Sendo a socialização uma das necessidades básicas do ser humano assim como comer e dormir (BARBOSA, 2016). Um dos reflexos dessa necessidade é a popularização dos sites

de relacionamentos, como LinkedIn, Twitter, Instagram, e o Facebook que é o mais acessado entre eles (KEMP, 2017). Todos os dias milhões de pessoas acessam o Facebook para trocar informações, atualizar perfis, postar fotos, e divulgando informações que são de sua preferência. Assim, as redes sociais digitais atuam sobre a auto expressão de seus usuários, bem como a rede de amigos dos mesmos através das listas de amigos.

Um termo comumente utilizado nas definições de redes sociais é o termo relacionamento. De acordo com Dimantas (2010), se relacionar com alguém faz parte da natureza humana, compondo assim um dos principais valores da sociedade.

> Pessoas querem, precisam, conversar com outras, apesar de tantos desencontros, guerras, mortes e catástrofes sociais. Insistimos em querer conversar. A relação é um valor importante e genuíno na sociedade. Concerne à natureza humana estar em relação com outros seres humanos, construindo mundos, compartilhando ideias e gerando inovações. (DIMANTAS, 2010, p. 20).

Para o autor, uma rede social representa uma imensa possibilidade de troca com qualquer ator envolvido na rede:

As redes sociais prescindem de ações para se configurar como espaço de troca. São propriamente redes sociais quando nos conectamos com os amigos dos amigos e, além disso, procuramos compartilhar as informações com mais gente (DIMANTAS, 2010, p. 22).

Segundo Recuero (2009, p.19), inserida no contexto das ciências sociais, a abordagem científica sobre o conceito de redes remete ao século XVIII, quando “a metáfora da rede foi utilizada pela primeira vez como semente de uma abordagem científica pelo matemático Leonard Euler” em 1736. A autora usa a teoria dos grafos para representar uma rede e suas conexões, constituídas por arestas e nós, pois “indivíduos e suas interações também podem ser observados através de uma rede ou grafo”. Isso levou a diversos estudos empíricos “que deram origem ao que hoje é referenciado como Análise Estrutural de Redes Sociais”. (RECUERO, 2009, p.20)

Para esta pesquisa, e considerando o contexto de TI, foi adotado o termo rede social digital, pois de acordo Wellman (1996), quando uma rede de computadores conecta pessoas, ela é uma rede social.

2.3.1 Características das redes sociais

Embora existam inúmeras redes sociais digitais (*LinkedIn, Youtube, Instagram, Facebook*...), cada uma possui tanto característica básica - como por exemplo um perfil

> de usuário que exibe uma lista dos perfis aos quais esse está conectado - quanto características particulares que as tornam diferentes das demais, como por exemplo, os interesses de cada público alvo e o tipo de conteúdo a ser compartilhado. O *LinkedIn* está mais focado no tema profissional, o *Youtube* permite a publicação de vídeos, o *Instagram* é focado no compartilhamento de fotografias e o Facebook, que permite partilhar vídeos, fotos, páginas, eventos etc. (SANTOS, 2014, p. 18).
>
> Além de permitir o compartilhamento de conteúdo, outra característica que a maioria das redes sociais digitais possui, é a possibilidade de os usuários comentarem as publicações de rede de amigos. Também é possível a troca de mensagens, as quais apenas emissoras e receptoras poderão acessar. Algumas redes sociais digitais possibilitam que postagens específicas sejam compartilhadas de acordo com o interesse de determinados grupos, sejam de amigos, família, grupos de estudo, entre outros. Também viabiliza ao usuário a sua participação em grupos de interesse comum, proporcionando conexões que vão além daquela relacionadas à sua lista de contatos na rede (SANTOS, 2014). Mas para que um usuário possa fazer tudo isso, antes é preciso que ele crie um perfil personalizado. E esse será o assunto abordado a seguir.

2.3.2 O perfil pessoal nas redes sociais

O perfil pessoal é o principal ponto de partida de quem deseja entrar numa rede social. Sua finalidade é traçar uma descrição do usuário em questão, a partir de informações disponibilizada pelo mesmo, como seu status de relacionamento (solteiro, casado, divorciado etc.), sua data de aniversário, seu *e-mail* pessoal, endereço residencial, cidade, estado. É nesse perfil que se encontrará sua lista de contatos, gosto musical, comunidades a qual pertence, religião, seu álbum de fotos e vídeos, opção sexual, atualizações feitas nos perfis de amigos, livros preferidos, estilo de vida. Podendo informar desde traços físicos (como cor do cabelo, dos olhos, altura etc.) a dados trabalhistas e/ou acadêmicos como empresas trabalhadas, ramos de atuação, escolas e cursos feitos etc. (CAVALCANTE JR, 2011, p. 19).

Com base nas informações publicadas pelo usuário, teoricamente, seus novos amigos poderão ter uma noção de quem se trata, quais são suas preferências pessoais e qual o nível de compatibilidade entre eles. Também é baseando-se nessas informações que os mecanismos internos das redes sociais digitais pesquisam a respeito de outros perfis que possuam traços de personalidades em comum, informando ao usuário, por meio de sugestões de amizades, as possíveis compatibilidades entre ele e novos usuários. (CAVALCANTE JR., 2011, p. 19).

Até este ponto foram abordados os conceitos de segurança da informação, engenharia

social e suas técnicas de ataque principalmente nas redes sociais digitais. Porquanto, será abordado na próxima seção o porquê e como se dá a extração de conhecimento nas redes sociais, em especial no Facebook.

2.4 Análise e extração de conhecimento em redes sociais

Compreender o comportamento do indivíduo na sociedade, tentando explicar como se dá as interações humanas e a realidade social dos grupos, se tornou estratégico. Por isso, houve nos últimos anos, um considerável aumento de estudos cujo foco se tornou a análise das redes sociais. Devido ao grande volume de dados que estão disponíveis diariamente, as redes sociais digitais, se tornaram um dos mais complexos e importantes desafios para aqueles buscam estudá-las e extrair informações das mesmas. Muitos dos estudos voltados para redes sociais, tratam da construção de *softwares* que percorrem os sites em busca dessas informações. (ROSA; SILVA; SILVA, 2012; MARTINAZZO, 2010).

No entanto algumas redes sociais apresentam proteção para a execução desses *softwares*, como por exemplo o Facebook, visando de proteger e defender seus usuários de invasões de privacidade. Isso acaba resultando numa certa dificuldade para a obtenção dos dados. Uma alternativa para solucionar o problema de como obter informações em redes sociais digitais como o Facebook, é o uso de técnicas de mineração de dados. Com tais técnicas, será possível extrair dados de grupos públicos da rede social Facebook e, a partir desses dados, realizar a análise dos resultados obtidos (ROSA; SILVA; SILVA, 2012; FREIRE, 2015).

2.4.1 Mineração de textos

Também conhecida como *Knowledge Discovery in Texts* (KDT), em português, Descoberta de Conhecimento em Textos, a mineração de Textos refere-se ao processo de extração, em documentos de textos não estruturados, informações que possam ser úteis. Mineração de textos é um conjunto de métodos usados para navegar, organizar, achar e descobrir informações em bases de textos. Pode ser vista como uma extensão da área de *Data Mining*, focada na análise de textos (BARION; LAGO, 2008).

É importante lembrar que existe uma diferença entre Mineração Textual e

Recuperação de Informações. Segundo Baeza e Ribeiro (1999 apud BARBOSA,2012,p.38) "a Mineração Textual busca a descoberta de padrões implícitos, enquanto Recuperação de Informação visa à recuperação de forma automática de documentos que satisfaçam as necessidades de informação do usuário" (BAEZA; RIBEIRO, 1999 apud BARBOSA,2012,p.38).

2.4.1.1 Pré-processamento

O pré-processamento se refere a aplicação de técnicas necessárias para captação, organização, tratamento e a preparação dos dados. Formatando a informação de modo a torná-la acessível aos métodos de mineração. Compreendendo desde a correção dos dados errados até o ajuste da formatação dos dados. A seguir encontram-se descritas as principais etapas de pré-processamento segundo Cervi (2008).

- Seleção dos dados - Trata-se de um processo complexo, pois os dados podem possuir diversos formatos e podem vir de diferentes fontes como, por exemplo: planilhas, *data warehouses*, *e-mails*, sistemas legados, bibliotecas digitais, e mais especificamente como foco deste trabalho, texto de publicações em redes sociais. Sendo assim a qualidade do resultado do processo sofrerá impacto significante devido essa etapa (BARBOSA, 2012).
- Limpeza dos dados e transformação dos dados - a limpeza de dados é um processo que visa assegurar a qualidade dos dados. Eliminando dados errados, dados duplicados, valores ausentes, e padronizando os dados: formatando datas, abreviações, atributos (ex. sexo: M ou F, 0 ou 1, Mas e Fem...). Quanto a transformação e enriquecimento dos dados, trata-se de um processo consiste em reduzir a quantidade de dados agrupando- os por atributos que representem as características principais dos dados das bases (BARBOSA, 2012).

2.4.1.2 Mineração de dados

Atualmente a mineração de dados é utilizada em muitas áreas, e possui diferentes aplicabilidades, como por exemplo, em marketing, finanças, comércio on-line, ou controle de crime. Segundo Braga (2005, p. 11) “a mineração de dados provê um método automático para descobrir padrões em dados, sem a tendenciosidade e a limitação de uma análise baseada

meramente na intuição humana". Tal método é utilizado para investigar grandes volumes de dados e os padrões identificados podem auxiliar na tomada de decisões para determinados problemas, tornando-a mais fácil.

> A "mineração de dados" compreende um conjunto de técnicas para "descrição" e "predição" a partir de grandes massas de dados. Por este motivo ela está geralmente associada a bancos de dados especiais denominados data warehouse. Estes bancos de dados viabilizam a integração rápida de dados oriundos de diferentes fontes. (BRAGA, 2005, p. 12).

Para Côrtez, Lifschitz e Porcaro (2002) a mineração de dados é um processo no qual homem e máquina trabalham juntos visando "a exploração de grandes bancos de dados, com o objetivo de extrair conhecimentos através do reconhecimento de padrões e relacionamento entre variáveis, conhecimentos esses que possam ser obtidos por técnicas comprovadamente confiáveis e validados pela sua expressividade estatística".

> Mineração de Dados é parte de um processo maior de pesquisa denominado Busca de Conhecimento em Banco de Dados (Knowledge Discovery in Database - KDD), o qual possui uma metodologia própria para preparação e exploração dos dados, interpretação de seus resultados e assimilação dos conhecimentos minerados. No entanto, se tornou mais conhecida do que o próprio processo de KDD em função de ser a etapa onde são aplicadas as técnicas de busca de conhecimentos. (CÔRTEZ ; LIFSCHITZ; PORCARO, 2002, p. 3).

Hoje praticamente não existe nenhuma área de conhecimento em que técnicas de data mining não possam ser usadas. Entretanto existem áreas onde o uso tem sido mais frequente, como por exemplo: para reduzir os custos no marketing direto a partir da identificação de grupos de clientes potenciais; detecção de fraude identificando reclamações, compras fraudulentas ou compras fraudulentas; em investimentos com modelos de redes neurais aplicados no mercado de ações; e em produção "desenvolvem sistemas para detectar e diagnosticar erros na fabricação de produtos" (PRASS, 2012, p.4).

A mineração de texto possui várias etapas, composto pelas etapas de pré-processamento, mineração de dados e pós-processamento (CERVI, 2008).

2.4.1.3 Pós Processamento

Esta fase visa a melhorar a qualidade do texto. Pois conhecimento adquirido na fase de mineração de dados precisa ser interpretado e avaliado pois possui grande quantidade de padrões que podem ou não se importantes ou interessantes. Daí a necessidade da fase de pós-processamento, pois o que importa são os resultados que realmente possam ser significativos.

E caso os resultados não sejam satisfatórios pode-se iniciar todo processo, modificar o conjunto de dados iniciais ou trocar o algoritmo de mineração de dados (PRASS, 2012).

2.4.2 Mineração de textos em redes sociais

Sabe-se que a mineração de texto pode ser aplicada em diferentes áreas, sejam elas científicas ou comerciais. Mas a ideia de se coletar dados em grande quantidade se tornou mais interessante após o surgimento das redes sociais digitais. No entanto como afirma Silva e Stabile (Orgs.) (2016, p. 71) “coletar esses dados pode ser uma tarefa complicada” devido aos diversos fatores que precisam ser considerados: “plataforma, volume, tratamento, objetivos, métricas, análise, operacionalização e orçamento”. Por causa disso, houve um crescimento considerado do número de sites, serviços e *softwares* cuja finalidade é monitorar, analisar, e extrair dados das redes sociais. (SANTOS, 2014)

Um exemplo que pode ser citado é o Facebook Topic Data, uma ferramenta que pode recolher e agrupar, e posteriormente apresentar, sem revelar as identidades dos usuários, tudo o que eles estão fazendo na rede social. E de posses desses dados pode se tomar as melhores decisões no que tange ao o quê publicar e o quê anunciar no Facebook (SILVA; STABILE (ORGS.), 2016).

Mas além desse tipo de sistema, também se encontram disponíveis gratuitamente uma grande quantidade de aplicações de código aberto e scripts com a finalidade de extrair dados de redes sociais. De acordo com Silva e Stabile (Orgs.) (2016) alguns desses aplicativos são “interfaces que se conectam às APIs e facilitam o processo de coleta de dados”. Essas APIs (do original *Application Programming Interface* – API) são uma série de comandos que possibilitam tanto que aplicativos quanto usuários possam se comunicar com sites ou fazer requisições de dados de seus servidores (SILVA; STABILE (ORGS.), 2016). Um exemplo desse tipo de API, é o Netvizz, uma ferramenta de que possui múltiplas funções, como por exemplo: coleta de dados de grupos abertos, de páginas, relação de páginas curtidas entre outras. E vinculado ao Facebook oferece análise de dados da rede social exportando os resultados para arquivos no formato .tab que pode posteriormente ser executado em *softwares* de edição de planilhas como o *Microsoft Excel* ou *BrOffice Calc*. Esses dados permitem uma análise mais detalhada a respeito de como as pessoas se comportam nas redes sociais. E abordar acerca do fator humano e suas vulnerabilidades são o assunto da próxima seção.

2.5 Fator Humano

A necessidade humana de comunicação e socialização é a razão para o uso crescente das redes sociais digitais. Por se tratar de uma ferramenta de comunicação muito poderosa, ela agrega grandes volumes de informação.

Segundo Fernandes e Souza (2016) as pessoas que publicam informações na rede, muitas vezes não têm ideia do tipo de controle que essas informações recebem. Ainda segundo eles, essas informações podem "ser usadas para interesses comerciais, controle de opinião" bem como a utilização por pessoas mal-intencionadas. Assim como as redes sociais deram ao usuário comum o privilégio de expor suas opiniões, também permite que essa exposição seja utilizada para prejudicar quem as expôs. É inegável que toda informação possui um valor, não apenas econômico, mas também sentimental, para quem a produziu e/ou para quem é destinada, por isso a importância em protegê-la de acessos indevidos. Como as informações na maioria das vezes são destinadas às pessoas, o fator humano acaba se tornando o principal alvo da engenharia social. As pessoas que publicam informações na rede, muitas vezes não têm ideia do tipo de controle que essas informações recebem (ALVES, 2010).

Uma famosa frase diz que "uma corrente é tão resistente quanto seu elo mais fraco". (MARCIANO, 2006). Considerando a segurança da informação "a corrente", qual seriam seus elos e dentre eles qual é o mais fraco?

Schneier (2013) afirma que os elos dessa corrente seriam a tecnologia, os processos e as pessoas, sendo estas últimas o elo mais fraco. Pois muitos dos incidentes relacionados à segurança têm intervenção humana, podendo assim afirmar que segurança tem a ver com pessoas e processos antes de ter a ver com tecnologia (SCHNEIER, 2013).

Segundo Kevin Mitnick:

> Uma empresa pode ter adquirido as melhores tecnologias de segurança que o dinheiro pode comprar, pode ter treinado seu pessoal tão bem que eles trancam todos os segredos antes de ir embora e pode ter contratado guardas para o prédio na melhor empresa de segurança que existe. Mesmo assim essa empresa ainda estará vulnerável. Os indivíduos podem seguir cada uma das melhores práticas de segurança recomendadas pelos especialistas, podem instalar cada produto de segurança recomendado e vigiar muito bem a configuração adequada do sistema e a aplicação das correções de segurança. Esses indivíduos ainda estarão completamente vulneráveis (MITNICK; SIMON, 2003, p. 3).

Algumas pessoas não acreditam que possam ser enganadas, outras não têm consciência a respeito das técnicas empregadas por um engenheiro social, esses e outros aspectos que

serão tratados a seguir favorecem, e muito o sucesso da Engenharia Social. (ALCOFORADO; RIBEIRO; CUNHA, 2012).

2.5.1 Vulnerabilidades

Muitos usuários de uma rede social digital não sabem que as informações publicadas por ele podem servir de base inicial para o ataque mais complexo como fraude financeira roubo de identidade, ou espionagem (CORTELA, 2013).

O fator humano e sua ignorância tem sido um dos maiores problemas enfrentados atualmente pelos especialistas em segurança da informação. Uma vez que o comportamento de uma pessoa pode afetar consideravelmente as medidas de segurança (SILVA; COSTA, 2009).

Entre as principais características encontradas nos indivíduos que se expõe em redes sociais se encontram (CORTELA, 2013):

Necessidade de expressar-se – Muitos usuários, principalmente os mais jovens, possuem uma grande necessidade de se expressarem publicamente.

Necessidade de atenção – Alguns usuários utilizam esse espaço virtual para obter a atenção de outros usuários.

Necessidade de popularidade – Esta característica, muito conhecida no mundo real, não é diferente no mundo virtual. Os usuários postam fotos provocativas ou ostentando objetos de valor apenas para alcançar popularidade na rede, sendo que algumas vezes essa exibição não é condizente com a realidade desses usuários. (CORTELA, 2013).

Segundo o filósofo Luiz Felipe Pondé, “a exposição extrema nas redes sociais tem mais a ver com narcisismo do que com qualquer nova noção de privacidade, assim, as pessoas escrevem besteiras no Facebook apenas para serem vistas, é só uma questão de autoestima.” (FERRARI et al., 2013).

Isto posto, pode-se destacar ainda, os seguintes traços comportamentais e psicológicos, que segundo Junior (2006) tornam o ser humano vulnerável e suscetível a ataques de engenharia social:

- Vontade de se tornar útil: O ser humano procura ser gentil e cortês, ajudando os outros sempre que preciso com isso ele se sente realizado.
- Buscar amizades: Há pessoas que não se sentem bem e nem feliz se não tiver amigos. Precisam ser elogiados e apreciados por quem estão próximos a elas. De

modo que acabam se abrindo emocionalmente para aqueles que mais as elogiam.

- Prorrogar responsabilidades: Muitas vezes o ser humano tem dificuldades de assumir os próprios erros, e tentam culpar outras e pessoas ou situações por seu comportamento ou por não alcançar os resultados que esperavam.
- Persuasão: em geral as pessoas possuem características comportamentais que as tornam vulneráveis à manipulação.

"Não há Patch contra a Burrice Humana." Sabendo disso os engenheiros sociais se aproveitam dessas fraquezas ou dos gostos pessoais de seus alvos para conseguir se aproximar deles e efetuar seus ataques (MARCELO; PEREIRA, 2005).

Que todos os usuários desejam segurança, isso é indiscutível. No entanto, os seres humanos são seres imperfeitos, e quando precisa tomar decisões que envolvem procedimentos de segurança, acham-na inconveniente. Como por exemplo, se precisam de um *software* cuja licença é paga, preferem fazer o download e instalar uma versão pirata da internet, as vezes ignorando os alertas de segurança, mesmo sabendo que correm o risco de instalar um malware em sua máquina. E conhecendo esse comportamento dos usuários, "os engenheiros sociais criam situações para que a segurança seja quebrada." (SANTOS, 2004).

Segundo Mitnick e Simon (2003) os ataques da engenharia social tem sucesso quando as pessoas são estúpidas ou apenas desconhecem as boas práticas da segurança.

Todos que acham que os produtos de segurança sozinhos oferecem a verdadeira segurança estão fadados a sofrer da ilusão da segurança. Esse é o caso de viver em um mundo de fantasia: mais cedo ou mais tarde eles serão vítimas de um incidente de segurança. (MITNICK; SIMON, 2003).

Mitnick e Simon (2003) afirmam ainda que os atacantes exploram cada vez mais o elemento humano, uma vez que os especialistas têm contribuído para o desenvolvimento de melhores tecnologias de segurança, tornando a exploração de vulnerabilidades técnicas ainda mais difícil. Afinal é quase sempre mais fácil quebrar a "*firewall* humana" do que um sistema computacional avançado, pois além do risco ser mínimo, não exige muito investimento por parte do atacante.

> [...] clicar em links suspeitos, escrever senhas em bilhetes colados à máquinas, sucumbir a um pedido mais gentil de informações sobre acesso estratégicos ou não instalar um patch de atualização de programa aplicativo ou Sistema Operacional alegando que "deixará mais lento o computador", são algumas das formas de caracterizar a falha humana. Estas mesmas pessoas que falham são as que utilizam os recursos tecnológicos. E esta tecnologia, sem correta utilização, pouco servirá com tamanhas brechas causadas pela falha humana. (MACHADO, 2009, p. 13).

Como é possível observar, um engenheiro social pode comprometer esse sistema

apenas forçando a confiança entre ele e a vítima, uma vez que o fator humano “possui interferência fundamental na estabilidade de um sistema de segurança”. CAVALCANTE JR., 2011).

Reforçando o que já foi dito anteriormente o Facebook permite que seus usuários compartilhem textos que expressam não apenas opiniões pessoais, mas também sentimentos. Isto posto, na próxima seção serão apresentados os conceitos de emoção e quais são as seis emoções básicas do ser humano, independente da sua nacionalidade, e como essas emoções podem ser identificadas em textos nas redes sociais.

2.5.2 Identificando de emoções em textos do Facebook

Em termos psicológicos, a emoção pode ser definida como uma reação momentânea que coloca o indivíduo pronto para ação, ou seja, uma resposta do organismo perante um estímulo externo, que está relacionada ao temperamento, a personalidade e motivação, alterando a atenção e a intensidade de determinado comportamento dentre as possíveis respostas do indivíduo (MARTINAZZO, 2010, p. 6), sendo composta por pelo menos duas dimensões perpendiculares, uma de valência (que vai do desagradável ao agradável) e uma de alerta (que vai do relaxado ao estimulado), em uma concepção definida como a teoria dimensional da emoção (KRISTENSEN et al., 2011, p. 3).

> Os estímulos que evocam uma emoção discreta de raiva podem ser classificados como de valência desagradável e alerta alto; estímulos que evocam uma emoção discreta de tristeza podem ser classificados como de valência desagradável e alerta baixo; estímulos que evocam uma emoção discreta de felicidade podem ser classificados como de valência agradável e alerta alto (KRISTENSEN et al., 2011, p. 3).

Devido ao fato das emoções serem elementos extremamente importantes da natureza humana, em qualquer sociedade e cultura, elas acabem se tornando objeto de pesquisas em diversas áreas, tais como a psicologia e outras ciências cujo foco é o estudo do comportamento. E recentemente a atenção de pesquisadores da Ciência da Computação tem se voltado esse tipo de estudo, principalmente os interessados na recuperação de informação, processamento de textos, e na interação humano-computador. (MARTINAZZO, 2010).

Um dos fatores fundamentais para tais estudos, foi crescimento das redes sociais digitais, pois possibilitou que o usuário expressasse sua opinião e discutisse suas ideias, e até mesmo se posicionasse diante de determinadas situações. Assim a evolução computacional possibilitou a análise de grandes quantidades de texto, objetivando descobrir automaticamente

os traços de personalidade de seus autores (PAIM, 2016, p. 1).

Segundo Martinazzo (2010, p.7) o "estudo das emoções se divide em várias áreas distintas", e neste trabalho foi utilizado o conceito proposto por Paul Ekman e Wallace Friesen na década de 1970 (EKMAN; FRIENSEN, 1978), conhecido como Emoções Básicas (ou Puras), e são elas: alegria, tristeza, desprezo (nojo ou desgosto), medo, raiva e surpresa.

Pesquisadores (EKMAN; FRIENSEN, 1978) realizaram estudos em diferentes países, onde pediam aos nativos que, por meio de fotografias de expressões faciais, identificassem quais eram as respostas emocionais apresentadas. E nesses estudos as seis emoções foram facilmente identificadas em todos os países onde o teste foi aplicado. (MARTINAZZO, 2010)

2.5.3 Emoções Básicas ou Primárias

As emoções são processos que ocorrem as vezes de modo inconsciente, estimulados por pessoas, acontecimentos ou situações, elas fornecem informações importantes sobre o indivíduo acerca da relação deste com os outros e consigo mesmo (ESPERIDIÃO-ANTONIO et al., 2008).

Segundo Ekman et al. (2003) existem sete emoções básicas ou primárias, sendo elas: a alegria, a tristeza, o medo, a surpresa, o nojo, o desprezo e a raiva.

Já Damásio (2003) afirma que existem seis e não sete emoções básicas: a alegria, a tristeza, o medo, a surpresa, o nojo e a raiva. A seguir a definição de cada uma delas:

- Alegria: Trata-se de uma emoção prazerosa, a qual os seres humanos buscam diariamente. Pequenos gestos, elogios, gentilezas, atenção, podem fazer alguém feliz. Essa emoção provoca bem-estar e satisfação, conduzindo a sentimentos positivos e inibindo pensamentos negativos. Ela não se manifesta apenas num sorriso, ela pode ser expressa no comportamento, numa conversa, num texto escrito durante um momento de felicidade (FREITAS-MAGALHÃES, 2013).
- Desprezo e Aversão/Nojo/Desgosto: Essa emoção ocorre quando se observa matéria deteriorada ou eventos que demonstram uma degradação dos valores aceitos pela sociedade (FREITAS-MAGALHÃES, 2011). Gosto e cheiros, não são os únicos a provocarem essa emoção, ações e ideias também podem desencadeá-la (EKMAN et al., 2003). Segundo Strongman (1998) esta emoção pode estar relacionada com qualquer coisa que o indivíduo acredite que seja desagradável ou que possa prejudicá-lo. Ele associa esta emoção a um sentimento de rejeição ou desprezo. No entanto para Ekman et al. (2003), desprezo se diferencia de aversão, uma vez que o desprezo pode ser sentido somente relação a pessoas ou suas ações, e não perante

gostos, cheiros ou toques.

- Medo: É uma emoção que proporciona um estado de alerta e é despertada diante de um perigo ou à ameaça, seja ela física ou psicológica (EKMAN et al., 2003). Embora sua função seja proteger e fazer uma pessoa reagir diante do perigo obrigando-a enfrentá-lo ou a fugir dele, o medo também pode bloquear e impedir o indivíduo. Algumas vezes o medo pode ser confundido com a ansiedade. Mas diferença é que o medo ocorre no momento do perigo, sendo uma reação ao mesmo, e a ansiedade ocorre antes de um perigo que pode ou não ocorrer, é sentir "medo" por antecipação. Mesmo o medo sendo considerado com uma emoção negativa, ele é essencial para a sobrevivência de uma pessoa (FREITAS-MAGALHÃES, 2013). Ele possui diferentes intensidades, desde uma leve insegurança ou ansiedade até o terror total. Podendo estar presente na "insegurança, preocupação, ansiedade, fobias, ataques de pânico e transtorno do estresse pós-traumático" (ALVES, 2017).
- Raiva: A raiva surge quando alguma coisa contraria as intenções da pessoa, fazendo-a se sentir fraca e frustrada por reconhecer seu limite interno e externo. É uma emoção que prepara o indivíduo para a defesa, inspirando comportamentos agressivos, permitindo a ele lutar e se defender quando é atacado (STRONGMAN, 1998). Muitas vezes ela pode ser associada ao medo, a aversão ou até mesmo a vergonha de sentir a própria raiva (EKMAN et al., 2003). Também está associada a ela "a revolta, a hostilidade, a irritabilidade, o ressentimento, a indignação, o ódio e a violência" (FREITAS-MAGALHÃES, 2013).
- Surpresa: Trata-se de uma breve emoção que ocorre mediante acontecimentos inesperados. Segundo Ekman et al. (2003) a emoção surpresa é rápida e difícil de ser captada em uma fotografia facial. De acordo com Freitas-Magalhães (2013) diversos autores alegam que as emoções devem ser agradáveis ou desagradáveis, positiva ou negativa, e por não a conseguirem classificar a surpresa dessa maneira acabam por não a considerar uma emoção. No entanto Ekman et al. (2003) consideram a surpresa uma emoção. Ele argumenta que a surpresa pode fazer com que outras emoções sejam despertadas, e mesmo que isso não ocorra, uma vez que ela possa ser definida como boa ou má, pode ser classificada como positiva ou negativa (EKMAN et al., 2003).
- Tristeza: Falta de disposição, falta de alegria, de ânimo, insatisfação, estas são as principais características de quem está triste. O grau de intensidade e o tempo de duração dessa emoção varia de alguns minutos ou horas para a tristeza passageira, até dias ou semanas, podendo ser o início de uma depressão (ESPERIDIÃO-ANTONIO et al., 2008). A tristeza pode ser desencadeada por vários motivos, como uma demissão, a morte de um familiar, uma desilusão amorosa, qualquer outra situação que afete a pessoa psicologicamente, e que seja encarada de forma negativa pela mesma, provocando desespero, desencorajamento, culpa e rejeição (FREITAS-MAGALHÃES, 2013).

Para que fosse possível identificar essas emoções por meio de textos, fez-se necessário o estudo a respeito de léxicos, esse é o próximo tema a ser abordado.

2.6 O uso de léxicos para identificar emoções em textos

Léxico é o conjunto de termos próprios de um idioma. Trata-se de um dicionário cujos termos as pessoas utilizam para se expressar, seja por escrito ou oralmente, ou seja, é o conjunto de vocabulários de uma língua. (TRASK, 2004). No entanto há uma diferença entre léxico e vocabulário. O vocabulário é uma seleção de termos que uma pessoa faz com base no léxico de seu idioma, ou seja, o vocabulário é o fragmento do léxico. Sua estrutura é formada por um banco de dados contendo termos ou conjunto de termos isolados, que foi utilizado ao longo do tempo no processo de comunicação. Isso significa que o léxico de um idioma, como o português por exemplo, é mutável, pois novos termos estão sempre surgindo, e outros entrando em desuso (AZEREDO, 2008). O intuito desse trabalho não é construir um léxico, pois essa seria uma tarefa árdua, devido ao tempo que se gastaria e ao grande volume de informações que deveriam ser processados. Pretende-se utilizar léxicos já existente, criados e/ou aperfeiçoados por outros autores.

2.6.1 ANEW-BR - Normas Brasileira para o Affective Norms for English Words

Desenvolvido por Bradley e Lang (1999), o léxico ANEW (Affective Norms for English Words), é um conjunto de classificações emocionais normativas para um grande número de palavras na língua inglesa, e conceitua a emoção como uma relação temporal breve, de três dimensões: valência, alerta e dominância. A primeira dimensão, denominada valência representa a avaliação do quão agradável ou desagradável um estímulo é percebido. A segunda dimensão, conhecida como alerta, consiste na avaliação do quão motivador ou relaxante um estímulo pode ser. A terceira dimensão, chamada de dominância, consiste na avaliação da intensidade do estímulo sobre o indivíduo, o quanto este controla ou é controlado por aquele (KRISTENSEN et al., 2011, p. 3).

Assim, segundo Paim (2016, p. 2) seria possível “caracterizar um estímulo de uma palavra, medindo o quão desagradável ou agradável, referindo-se à valência e ao quão relaxado ou estimulado ficamos perante a palavra, referindo-se ao alerta”.

2.6.2 LIWC - Linguistic Inquiry and Word Count

O *Linguistic Inquiry and Word Count*(LIWC), que numa tradução direta significa Inquérito linguístico e Contagem de palavra, foi criado por James W. Pennebaker (PAIM, 2016). Segundo Paim (2016, p.21) trata-se de "uma ferramenta de análise de texto que avalia componentes emocionais, cognitivos e estruturais de um determinado texto". Pretende-se com a utilização do LIWC, obter uma confirmação das características textuais que corroboram as encontradas com o ANEW-BR e com o identificador de emoções básicas criado para esse trabalho.

2.6.3 TF-IDF - Term Frequency–Inverse Document Frequency

Tf-idf é uma abreviação para a expressão em inglês "*term frequency–inverse document frequency*" e significa "frequência do termo–inverso da frequência nos documentos" (PAIM, 2016). Trata-se de um valor muito utilizado na mineração de texto e na recuperação de informações. Com esse valor é possível avaliar estatisticamente a importância de uma palavra um documento. O aumento dessa importância é diretamente proporcional ao número de vezes que uma palavra aparece no documento (ALAM; STEPANOV; RICCARDI, 2013). Geralmente o valor de TF-IDF é composto por dois termos:

- TF (Frequência do termo): que calcula o número de vezes que uma palavra aparece em um documento. Devido ao fato de que um documento pode ser diferente de outro, por ser mais longo ou mais curto, e que é possível que um termo apareça mais vezes nos documentos longos do que naqueles mais curtos, o TF geralmente é dividido pelo comprimento do documento, ou seja, pelo número total de termos no documento, como forma de normalização (TF-IDF..., 2017):
    - TF (t) = (Número de vezes que o termo t aparece em um documento) / (Número total de termos no documento).
- IDF (inverso da frequência nos documentos): calcula a importância do termo. Quando se calcula o TF, todos os termos são considerados igualmente importantes. No entanto alguns termos podem aparecer com muita frequência no texto e ter pouca importância, como por exemplo: os artigos definidos e indefinidos; as preposições; expressões como "é", "que", "de" entre outros. Sendo assim o IDF é calculado como o logaritmo do número de documentos no corpus dividido pela quantidade de documentos onde o termo específico aparece (TF-IDF..., 2017):

- IDF (t) = log_e (Número total de documentos / Número de documentos com termo t nele).

Supondo que um documento possua 200 palavras e que dor aparece 7 vezes neste documento. O termo frequência (TF) para dor é então (7/200) = 0,035. Agora, considerando que se tenha 300 documentos, e que a palavra dor aparece em 53 desses documentos, a frequência inversa do documento (IDF) é calculada como log (300/53) = 0,752. Assim, o valor TF-IDF é: 0,035 *0,752 = 0,02632.

3 METODOLOGIA

Este capítulo descreve os procedimentos aplicados nos experimentos realizados no estudo exploratório. Neste contexto, a primeira seção apresenta os materiais e métodos utilizados. Em seguida, são apresentados os estudos exploratórios e as aplicações desses métodos.

3.1 Materiais e Métodos

Método pode ser definido como o "conjunto de atividades sistemáticas e racionais que permitam alcançar um objetivo, baseando-se no raciocínio dedutivo, no indutivo, no hipotético-dedutivo ou no dialético." (CIRIBELLI, 2000, p. 24). Este estudo se trata de uma pesquisa qualiquantitativa por apresentar uma abordagem mista.

> Assim, para o pesquisador que usa métodos mistos, o pragmatismo abre as portas para métodos múltiplos, diferentes visões de mundo e diferentes suposições, além de diferentes formas de coleta e análise de dados no estudo de métodos mistos. (CRESWELL, 2007, p. 30).

Tal abordagem, segundo Creswell (2007), baseia a investigação na pressuposição de que a coleta de diferentes tipos de dados possibilita uma melhor compreensão do problema de pesquisa.

> Essa técnica emprega estratégias de investigação que envolvem coleta de dados simultânea ou sequencial para melhor entender os problemas de pesquisa. A coleta de dados também envolve a obtenção tanto de informações numéricas (por exemplo, em instrumentos) como de informações de texto (por exemplo, em entrevistas), de forma que o banco de dados final represente tanto informações quantitativas como qualitativas (CRESWELL, 2007, p. 35).

Foi adotado como universo de pesquisa as redes sociais digitais devido ao grande fluxo de dados que são compartilhados e disponibilizados nas mesmas. E dentro desse universo, o Facebook foi a rede social selecionada como objeto de estudo, devido ao seu crescimento exponencial nos últimos anos (KEMP, 2017).

Como técnica de pesquisa foi adotado a pesquisa de campo, levando em conta as considerações de Lakatos e Marcone (2003), dentre elas a de que:

> Pesquisa de campo é aquela utilizada com o objetivo de conseguir informações e/ou conhecimentos acerca de um problema, para o qual se procura uma resposta, ou de uma hipótese, que se queira comprovar, ou, ainda, descobrir novos fenômenos ou as relações entre eles (LAKATOS; MARCONE, 2003, p. 186).

A proposta ao se utilizar essa técnica é estudar o conteúdo textual de grupos da rede social em questão, fazendo um uso maior das técnicas de observação do que de interrogação. Os instrumentos de coleta de dados foram os seguintes:

Utilizou-se a observação sistemática direta de grupos públicos da rede social digital Facebook. Conforme afirma Lakatos e Marcone (2003, p.193) nesse tipo de observação, "o observador sabe o que procura e o que carece de importância em determinada situação" devendo ser objetivo, reconhecendo possíveis erros e eliminando sua influência sobre o que vê ou recolhe.

- Para essa observação sistemática, fez-se uso dos seguintes artefatos tecnológicos:
- Computador, Smartphone, Internet.
- Canva, uma ferramenta para criação de conteúdos gráficos. Ele é gratuito e online e está disponível em: https://www.canva.com
- Editor de planilhas Microsoft Office Excel.
- NetBeans IDE, *software* de desenvolvimento usado para implementar os códigos em Java utilizados neste trabalho.
- Aplicativo Netvizz, cuja função é coletar diferentes tipos de dados do Facebook, principalmente de Páginas, Grupos e Eventos. Possibilitando a extração de conteúdo textual de postagens e comentários, bem como dados de *likes*, compartilhamentos e reações. Para Rosa, Silva e Silva (2012, p. 9) "este aplicativo pode gerar o arquivo necessário para visualização dos grafos, tanto do perfil do usuário, quanto dos grupos ao qual o usuário pertence". Funciona como um rastreador de dados para o Facebook, mas respeitando as configurações de privacidade de usuários do Facebook. Resultado de tentativas práticas de estudar API's no site de rede social e avaliar o potencial da utilização de métodos digitais obteve repercussão positiva como extrator de dados que oferece saídas de informação para diferentes seções do Facebook em formatos normalizados. O aplicativo disponibiliza os seguintes módulos:
    - Dados de grupo - cria redes e arquivos tabulares para a atividade do usuário em torno de postagens em grupos.
    - Dados da página - cria redes e arquivos tabulares para a atividade do usuário em torno de postagens nas páginas.
    - Página como rede - cria uma rede de páginas conectadas através dos gostos entre elas. Imagens da linha de tempo da página - cria uma lista de todas as imagens do álbum "Imagens da linha de tempo" nas

páginas.

- Pesquisa - interface para a função de pesquisa do Facebook Estatísticas de link - fornece estatísticas para links compartilhados no Facebook.

Para que o aplicativo *Netvizz* possa rastrear o conteúdo, extrair os dados é necessário escolher um dos módulos acima, e informar o ID da página ou grupo a ser pesquisado.

3.2 Estudos Exploratórios

Para a elaboração desse estudo foi preciso a criação de perfis no Facebook, o envio de solicitações de amizade, a coleta e a análise dos textos das postagens públicas para se identificar as emoções básicas expressadas por seus autores, bem como a simulação de um ataque de phishing não prejudicial.

3.2.1 Criação dos perfis

A primeira etapa consistiu na criação de dois perfis dentro da rede social Facebook. Tais perfis foram utilizados para testar a interação entre os usuários da rede. Simulando situações em que os usuários se tornam vulneráveis as ações de um engenheiro social. Essas situações envolvem desde convidar ou aceitar um convite de amizade, trocar mensagens, compartilhar fotos, participar de grupos, participar de promoções e sorteios, a ser redirecionado a uma página em que se pede dados pessoais.

Os dois perfis receberam informações para se parecem com perfis de usuários reais. Essas informações incluem a adição de fotos nos perfis manipuladas e modificadas digitalmente para não ir contra as políticas de segurança e privacidade, postagens fictícias, a adição de grupos e por fim, o preenchimento completo do "perfil pessoal". Portanto qualquer semelhança das imagens que seguem com usuários reais é apenas coincidência. E após a conclusão desse estudo ambos os perfis foram desativados e excluídos, pois a justificativa para cria-los era demostrar a facilidade com que as pessoas podem se deixar enganar nas redes sociais.

O primeiro perfil a ser criado fio um perfil masculino, de 26 anos, psicólogo. O objetivo foi montar um perfil participativo, que mostrasse empatia, e fosse persuasivo o suficiente para derrubar as barreiras de comunicação. Assim ele poderia se aproximar de

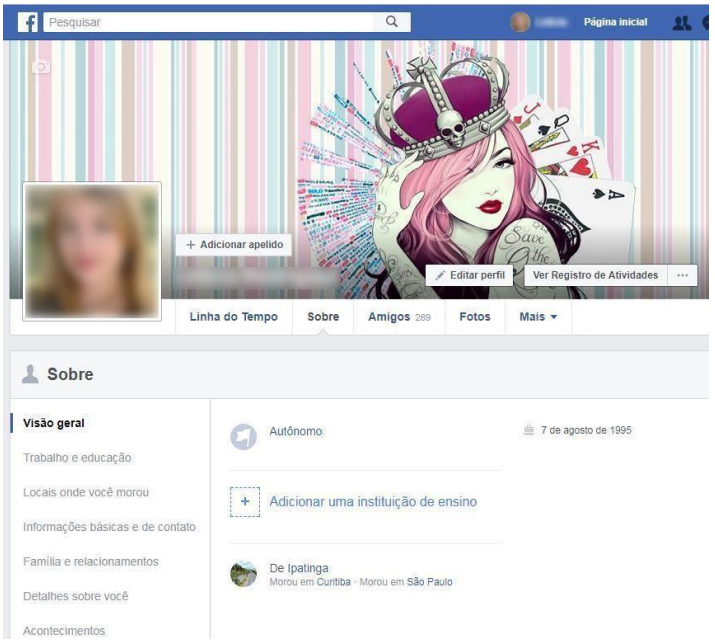
outros usuários mais facilmente.

Figura 2 - Perfil Masculino, o primeiro usuário criado para a experimentação

Fonte: O autor (2017)

O segundo perfil foi baseado em uma mulher de 22 anos, loira, que já morou em diferentes cidades, e que trabalha autonomamente como consultora de cosméticos. O objetivo foi montar um perfil bem feminino, com um grande interesse nas pessoas de modo geral. Este perfil possui 186 “amigos” no Facebook, somando as solicitações de amizade enviadas com as recebidas.

Figura 3- Perfil feminino, o segundo usuário criado para a experimentação.



Fonte: O autor (2017)

Cada perfil entrou em 10 diferentes grupos na rede social Facebook, dentre os quais 5 eram grupos públicos (não precisa de confirmação do administrador para participar) e 5 eram grupos privados (aqueles em que é preciso a confirmação do administrador para participar).

3.2.2 Solicitações de Amizades

Uma vez inseridos nos grupos cada perfil enviou 200 solicitações de amizades para os usuários reais participantes desses grupos. Sendo 100 homens e 100 mulheres de diferentes faixas etárias, graus de escolaridades (quando informados) e localidades. No total foram 200 para usuários do sexo masculino e 200 para usuários do sexo feminino. Totalizando 400 solicitações enviadas. Não houve nenhuma tentativa de facilitar a aceitação de uma solicitação por meio de contatos ou tentativas subsequentes. No entanto, à medida que os perfis se tornaram ativos na rede social, diversos usuários lhes enviaram solicitações de amizade, sendo 65 para o perfil masculino e 137 para o perfil feminino. Na seção 4.1 é mostrada uma análise sobre a reação dos usuários a essas solicitações de amizade, quantos aceitaram, quantos recusaram e as solicitações foram recebidas pelos perfis criados.

Foi dado um prazo de duas semanas para que as solicitações fossem aceitas ou não. Terminado o prazo, foi realizado um levantamento das informações disponíveis nos perfis que aceitaram a solicitação. Para fim de análise, as solicitações que não foram aceitas serão tratadas como recusadas ou ignoradas.

3.2.3 Nível de exposição dos usuários

Para definir o nível de exposição dos usuários foi criado uma escala que vai de 1 (menos exposto) a 4 (mais exposto). No perfil foram analisados: nome, idade, sexo, endereço residencial, estado civil, trabalho, telefone, e outros dados como: gostos pessoais, lazer, grupos e comunidades afiliadas. E nas fotos pessoais, foram analisados: hábitos sociais, presença de parentes, amigos íntimos, locais de visita constante.

Segundo Cortela (2013, p. 14) tais informações embora não seja o objetivo primário de um engenheiro social, são utilizadas para “esquematizar um ataque mais intrusivo, geralmente focado na conta bancária ou empresa na qual a vítima trabalha”.

Os níveis dessa escala são explicados abaixo:

Nível 1 - Pertencem a esse nível os perfis que não possuem informação específica a respeito do usuário. Sendo difícil de definir local de trabalho ou de residência, data de nascimento, relacionamentos.

Nível 2 - Pertencem a esse nível os perfis que poucas informações específicas a seu respeito. Geralmente informações genéricas, como cidade onde mora, local de trabalho, data de nascimento com apenas dia e mês, poucas fotos pessoais, poucos gostos ou hábitos pessoais.

Nível 3 - Pertencem a esse nível os perfis que exibem atividades profissionais, gostos ou hábitos pessoais, grupos musicais, times de futebol, lazer, grupos e comunidades afiliadas.

Nível 4 - Pertence a esse nível os perfis que exibem hábitos pessoais, residência, local de trabalho ou estudo.

Nível 5 - Pertencem a esse nível os perfis que possuem dados mais específicos a respeito dos usuários. Como endereço residencial completo, telefone, *e-mail* pessoal, código de endereço postal, membros da família, álbuns de fotos muitas publicações.

3.2.4 Base de dados Textual para mineração de texto

A base de dados textual deste trabalho é composta por textos publicados pelos usuários que aceitaram a solicitação amizade ou enviaram solicitações e pelos textos publicados em grupos abertos do Facebook, cujo foco fosse desabafos pessoais. Seguindo as especificações do Termo de serviço do Facebook (FACEBOOK, 2017), as publicações coletas foram aquelas que os usuários disponibilizaram como pública.

> Quando você publica conteúdos ou informações usando a opção Público, você está permitindo que todos, incluindo pessoas fora do Facebook, acessem e usem essas informações e as associem a você (isto é, ao seu nome e foto do perfil). (FACEBOOK, 2017, p.1)

Dos 380 usuários considerados válidos por possuir as informações mínimas necessárias para este estudo foi retirada uma amostra de 200 perfis para análise mais detalhada dos textos, com o intuito de definir seu estado emocional através dos conteúdos postados. Para extrair os textos desses grupos foi utilizada a API Netviz. O Quadro 1 apresenta uma amostra dos textos que compõem a base de dados.

Quadro 1- Amostra dos textos coletados na rede social Facebook.

Usuários	Texto Publicado
Usuário 1	Há marcas que nunca serão apagadas existem feridas que vão doer pra sempre na alma da gente
Usuário 2	Será que alguém aqui pode me ajudar ... Preciso muito me desabafar com uma pessoa q eu não conheça... ?????????? Preciso arrancar essa dor de dentro de mim... Só queria um amigo ou
Usuário 3	Nesta vida suportei tantas coisas q agora só me levam a chorar normalmente chorar tornou-se o meu passatempo pois nada para mim dá certo as vezes penso q Deus ñ tem olhos para mim,
Usuário 4	Sei que preciso mudar o rumo do meu barco mais não tenho força Sei que mereço amor
Usuário 5	Tem uma Hora que VC cansa das decepções e começa se afastar das pessoas ...e fecha seu
Usuário 6	A vida é como as portas Quando está escrito puxar Não adianta empurrar.....
Usuário 7	acontece não porque deixaste de te importar mas sim para tentar diminuir as dores e cicatrizar
Usuário 8	E pensar que algumas pessoas já foram tão importantes pra mim e hoje elas não são nada...Que
Usuário 9	O pior tipo de fracassado é aquele que não voa e nem te deixa voar não vence e nem te deixa
Usuário 10	E você se encanta pela doçura da pessoa se apaixona e ela depois de um tempo muda passa a

Fonte: O autor (2017)

Baseando-se nos dados coletados, se obteve uma base textual composta por 64.652 palavras, presentes em 9.236 publicações realizadas por 200 usuários que aceitaram as solicitações de amizade e por 100 usuários que postaram ou comentaram em grupos abertos no Facebook, mas que não pertence aos “amigos” dos perfis falsos.

Tabela 1- Informações sobre o conjunto de dados

Informações	Total
Usuários	300
Publicações	9236
Média de publicações por usuário	46
Palavras	64.652
Média de palavras por usuário	323

Fonte: O autor (2017)

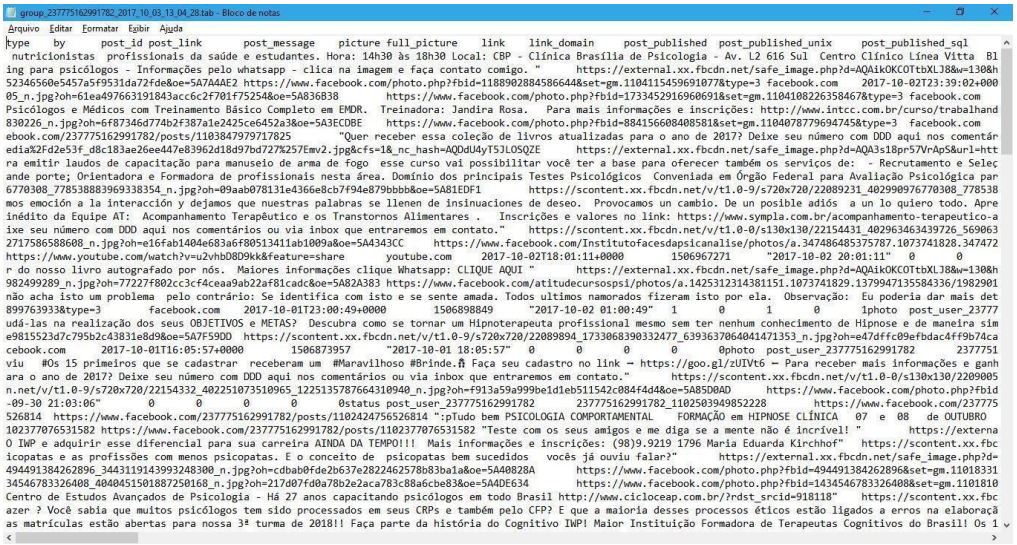
3.2.4.1 Coleta de dados utilizando a ferramenta Netvizz

Para realizar a coleta de textos de grupos públicos e páginas no Facebook, foi utilizado o aplicativo *Netvizz* (RIEDER, 2013). E para a construção da base textual deste trabalho foram utilizadas três páginas e três grupos ambos identificados como abertos ou públicos. Essa técnica permitiu a saída de dados em arquivos com extensão .tab, que posteriormente foram copiados e colados em planilhas, o que permitiu trabalhar com dados de acordo com os diferentes objetivos da pesquisa.

3.2.4.2 Transformando arquivos do Netvizz em planilhas

Foi preciso abrir os arquivos com extensão .tab em um editor de texto, neste trabalho optou-se pelo bloco de notas, que por padrão já vem instalado no sistema operacional Windows. A figura 5 ilustra a abertura de arquivos originados do *Netvizz*.

Figura 4 - Arquivo tab aberto no bloco de notas



Fonte: O autor (2017)

Inicialmente parece um caos. Segundo Freire (2014) “essa é a fase que espanta ou causa desistência na maioria de pesquisadores acadêmicos em tentativas de utilizar a técnica”. Daí a necessidade para importar os dados para o formato de planilha. Para isso, basta selecionar todo o arquivo .tab aberto, clicar com o botão esquerdo do mouse, clicar em copiar, abrir planilha no Excel e colar a informação copiada. Quando o programa de planilha solicitou

como as variáveis seriam organizadas nas colunas, optou-se por separá-las por espaço e por vírgulas. O resultado foi uma planilha com informações sobre conteúdos por gerados por usuários do grupo do escolhido.

Posterior a etapa de seleção e criação da base de dados textual, passou-se para a etapa de pré-processamento, efetuando as fases já exploradas na seção 2.4. O resultado foi uma representação dos dados em formato vetorial, possibilitando que os léxicos fossem explorados.

3.2.5 Pré-processamento do texto

Finalizando a coleta dos textos e construindo da base de dados, se fez necessário o pré-processamento dos dados, para que estes fossem organizados e formatados de modo adequado inferência de personalidade. Nessa fase o texto foi preparado para a mineração dos dados, sendo extraídas as características emocionais e linguísticas que foram empregadas no texto, com isso é uma matriz de termos relevantes é criada para a inferência. Nessa fase o texto foi preparado para a mineração dos dados, sendo extraídas as características emocionais e linguísticas que foram empregadas no texto, com isso é uma matriz de termos relevantes é criada para a inferência.

A fase do pré-processamento em mineração de texto geralmente consiste em três etapas que podem variar sua ordem ou simplesmente não ocorrer, dependendo da aplicação de domínio, são elas: análise léxica, eliminação de termos considerados irrelevantes e normalização morfológica dos termos (BARBOSA, 2012).

A análise léxica é responsável pelas adaptações do texto, e foi aplicada nesse estudo da seguinte maneira: os sinais de pontuação foram eliminados, letras maiúsculas foram convertidas para maiúsculas, e os termos (tokenização) foram isolados (BARBOSA, 2012).

A remoção de termos irrelevantes ou stop words tem por objetivo remover termos de pouca importância, sem valor semântico na frase. Sendo essas preposições, artigos, pontuações e verbos auxiliares (BARBOSA, 2012). No entanto, o léxico LIWC categorizar palavras como verbos, verbos auxiliares e artigos, portanto elas foram mantidas. Sendo assim a elaboração de uma lista de stop words fez-se necessária. A seguir, no Quadro 2 é apresentado alguns exemplos de stop words que foram utilizados para essa etapa.

Quadro 2- Exemplos de stop words

a, agora, alguém, algum, alguma, algumas, alguns, ampla, amplas, amplo, amplos, ante, antes, ao, aos, após, aquela, aquelas, aquele, aqueles, aquilo, as, assim, até, através, cada, coisa, com, como, de, e, ele, em, esse, este, eu, isso, mas, o, ou, para, por, porque, que, se, sua., também, um, uma, você,

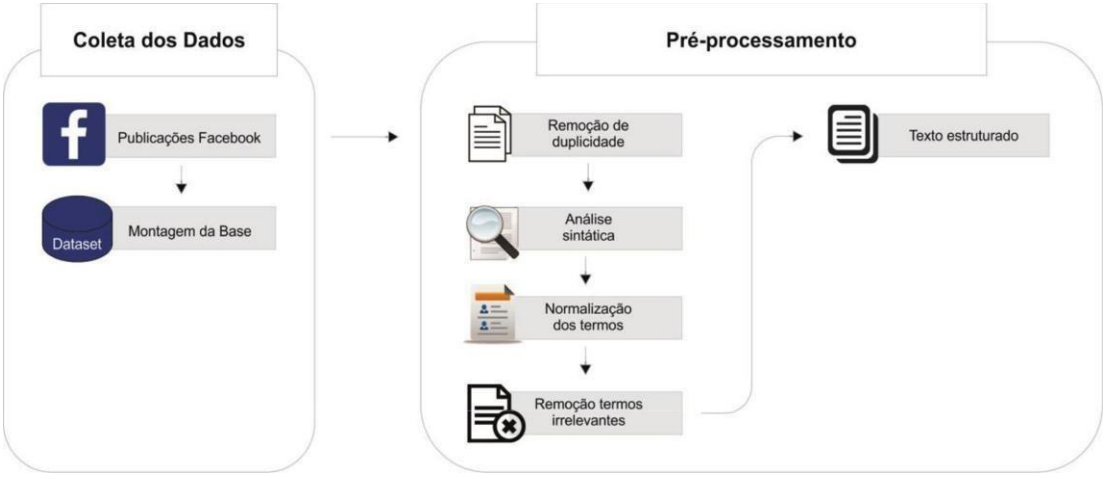
Fonte: Martinazzo (2010, p. 23)

Objetivando a redução de esforço dos processos subsequentes, mensagens geradas pelo mesmo autor que fossem repetitivas foram eliminadas do processo.

Como os textos utilizados pelos usuários nas redes sociais, é de caráter informal em sua maioria, tornou-se um desafio normalizar algumas palavras. A informalidade das redes sociais permite que algumas palavras possam ser escritas abreviadamente ou com certa variação, como por exemplo: vc (você), amg (amigo), vdd (verdade), bjs (beijos), kkkkk (risos), muiiiiitooo booooooomm (muito bom), d+ (demais), d-(de menos), p/ (para), sdds (saudades) entre outros. Tais expressões podem dificultar o tratamento dos textos. Portanto foi realizada implementação em java simples de normalização para a maioria dos jargões encontrados nos textos, com o intuito de melhorar o desempenho dos classificadores.

É possível visualizar na Figura 4 cada etapa do tratamento que foi realizado na base textual, cujo resultado foi a estruturação do texto.

Figura 5- Etapas do pré-processamento



Fonte: Paim (2016, p. 82)

Também foram removidos todos os caracteres que não possuem relação com as palavras e que não foram normalizados, como operadores aritméticos (*, +, -, /); barras (/ ou \), operadores relacionais (>, <, =). Quanto aos *emoticons* (Imagens e símbolos que

representam uma expressão facial) para caracterizar o estado emocional contido na mensagem, eles foram eliminados do escopo deste trabalho, por se tratar de imagens. Bem como, o procedimento conhecido como lematização ou *stemming*, que se refere à normalização morfológica, e reduz os radicais dos termos irrelevantes. Pois, este trabalho se utiliza léxicos, e reduzir uma palavra a seu radical certamente afetará a comparação das palavras do texto com os termos dos léxicos.

Para a execução dessas etapas de pré-processamento (limpeza e transformação) dos textos coletados foi criado e utilizado um algoritmo em Java. Além disso, esse mesmo algoritmo possibilitou analisar os textos sob a ótica do ANEW-BR, para identificar qual seria a média ponderada da valência e do alerta dos textos em questão. Bem como possibilita uma comparação entre as palavras do texto as bases textuais das seis emoções básicas (alegria, tristeza, medo, surpresa, nojo e raiva), determinando assim o tipo de emoção predominante no texto.

Concluída as etapas anteriores, os termos resultantes foram submetidos ao léxico LIWC e ao léxico afetivo ANEW-BR, bem como à apuração das palavras baseando em sua frequência (TF-IDF), implementando assim, um vetor de características textuais para a identificação da emoção predominante no texto.

3.2.6 Reconhecimento de emoções com ANEW-BR e LIWC

Para extrair emoções em textos foi utilizado o léxico afetivo ANEW-BR, objetivando de aperfeiçoar a associação da emoção em textos. Também foi utilizado o método TF-IDF para o aperfeiçoamento do o método de inferência da emoção, com o intuito de associar aos léxicos os termos extraídos que possuem uma representatividade maior no texto.

Posteriormente foi criada uma base textual para cada uma das seis emoções básicas descritas por Damásio (2003), tendo como base os anexos do trabalho de Martinazzo (2010). Comparando os textos coletados com a base textual das emoções básicas, foi possível identificar a emoção predominante no texto.

3.2.6.1 ANEW-BR

A base do léxico ANEW-BR possui 1.046 temos para a língua portuguesa com valores de valência e alerta. Dentre esses termos estão as palavras afetivas, que foram usadas na

comparação com o dos termos da base textual criada anteriormente, com o intuito de obter o nível emocional que foi empregado nos textos. Os experimentos utilizando o léxico ANEW-BR, se dividiram em duas abordagens.

A primeira abordagem tratou de computar a média ponderada de valência e alerta utilizadas nos textos de cada usuário. Segundo a teoria dimensional da emoção, as emoções podem ser compostas por ao menos duas dimensões ortogonais, uma de valência (do desagradável ao agradável) e outra de alerta (do relaxado ao estimulado) (KRISTENSEN et al., 2011).

Esses valores variam de 1 a 9. Com isso palavras respectivamente desagradáveis e relaxadas apresentaram valência e alerta baixos, próximos de 1, e as palavras agradáveis e estimuladas, apresentaram valência e alerta altos, próximos de 9 (KRISTENSEN et al., 2011).

Por exemplo, a frase: “Fico abalado com os crimes absurdos, mas tento acreditar na justiça de Deus e dos homens”, quando confrontadas com a lista de termos do ANEW-BR, apresenta a seguinte classificação:

Tabela 2- Frase confrontada com o ANEW-BR

Frase	**Valência**	**Alerta**
Fico abalado	2,58	5,11
com os crimes	1,72	6,45
absurdos	2,79	5,81
mas tento acreditar	8,29	5,04
na justiça	6,52	5,61
de Deus	8,11	3,8
e dos homens	6,85	4,47
Media da Frase toda	**5,27**	**5,18**

Fonte: O autor (2017)

Para a sentença acima, para cada termo contabilizado no léxico (abalado, crime, absurdo, acreditar, justiça, Deus e homem) foram criadas duas colunas num vetor, uma para armazenar o peso de valência e outra para armazenar o peso de alerta, contendo a multiplicação da frequência dos termos: abalado, crime, acreditar, justiça Deus, e homem. Portanto essa frase teria como valência 5,27 e alerta de 5,18, o que poderia classificá-la como uma frase que expressa sentimentos mais positivos do que negativos, valores representam valência e alerta moderados.

Para identificar os valores de valência e alerta do ANEW-BR, foram utilizados modelos matemáticos capaz de estimar a média ponderada de valência (MV) e alerta (MA), conforme as equações 1 e 2 de Enembreck et al., 2014:

Equação matemática para identificar a média para valência e alerta:

$$M_V = \frac{q_i \ * \ V_i + \ldots q_n \ * \ V_n}{q_i + \cdots \ q_n} \quad (1)$$

$$\mathrm{M_A} = \frac{\mathrm{q_i} * \mathrm{A_i} + \ldots \mathrm{q_n} * \mathrm{A_n}}{\mathrm{q_i} + \ldots \mathrm{q_n}} \quad (2)$$

Fonte: Enembreck et al. (2014)

No qual:

M_V é a média ponderada para a valência;

M_A a média ponderada para o alerta;

q_i, para i = 1,...,n, a quantidade de vezes que uma palavra é encontrada;

V_i, para i=1,...n, o valor de valência de uma palavra;

A_i, para i=1,...n, o respectivo valor de alerta de uma palavra.

Essas equações foram implementadas em linguagem Java, para comparar um ou mais arquivos de texto com a base textual do ANEW-BR, minerando as palavras afetivas em comum, e retornando a média ponderada para a valência e para o alerta do texto contido no arquivo.

3.2.6.2 LIWC

A finalidade em se utilizar esse léxico é computar cada categoria do léxico LIWC a fim de contabilizar a polaridade (positivos, negativos e neutros) dos termos que foram empregados nos textos.

Para contabilizar essa polaridade fez-se uso do site http://www.liwc.net/tryonline.php, nesse sistema basta inserir um texto para se obter uma saída básica para o LIWC. Aplicando a frase da seção 3.2.6.1 ao LIWC obtêm-se a tabela a seguir:

Tabela 3- Resultados do LIWC

Dimensão LIW	Seus Dados	Textos Pessoais	Textos Formais
Auto referências (eu, eu, meu)	0.00	11.4	4.2
Palavras sociais	0.00	9,5	8.0
Emoções positivas	0.00	2,7	2.6
Emoções negativas	0.00	2.6	1.6
Palavras cognitivas gerais	0.00	7.8	5.4
Artigos (a, um, o)	5.88	5.0	7.2
Grandes palavras (> 6 letras)	17,65	13.1	19.6

Fonte: O autor (2017)

Com a aplicação dessas duas abordagens, será possível comparar o ANEW-BR com o LIWC e o TF-IDF, e investigar se a inclusão do léxico ANEW-BR. possibilitou um melhoramento na precisão da inferência de emoções em textos.

3.2.7 Análise das seis emoções básicas

Para realizar a análise das emoções foram utilizadas seis listas de palavras em seis arquivos diferentes, sendo cada uma delas relacionada com uma emoção básica descrita anteriormente, tal lista foi disponibilizada por Martinazzo (2010).

Tabela 4- Exemplos de palavras contidas nas listas de emoções.

Emoção	**Alegria**	**Nojo/Desgosto**	**Medo**	**Raiva**	**Surpresa**	**Tristeza**
Exemplos	amor amizade brincadeira esperança	enjoo feio náusea nojo	assombrado cruel medroso pânico	assassinar cólera destruir diabólico	deslumbrar embasbacar fantástico pasmo	arrepender chorar derrota desamparo
Quantidade	**278**	**72**	**104**	**168**	**40**	**184**

Fonte: Adaptado de Martinazzo (2010, p. 34)

O objetivo é comparar o documento de texto de cada usuário e os textos coletados nos grupos públicos com as bases textuais das seis emoções básicas, a fim de identificar, baseado na quantidade de palavras relacionadas as emoções e a frequência delas no documento, qual emoção é predominante no documento. Por exemplo, um texto pode ter algumas palavras que expressam tristeza ou raiva, mas ainda ser considerado um texto alegre por ter uma frequência maior de palavras que expresse alegria. Também é possível que o mesmo texto demonstre

mais de uma emoção, mas geralmente uma irá ser predominante. Como pode ser observado no Quadro 3, que exemplifica três documentos que foram coletados para a análise.

Quadro 3- Pré-processamento dos textos

ID	Texto
1	A todos meus amigos que são papai, um feliz dia dos pais cheio de paz pra vocês...e sim todos os dias da sua vida, eu torço pela sua felicidade, meu pai, pois você merece...
2	Alguém me ajuda estou beirando o suicídio. Eu só queria que alguém notasse que eu não tô legal, que alguém me notasse. Quero muito ajuda, tudo está dando errado, não sei mais o que fazer...
3	Fico furioso com gente idiota. Elas me tiram do sério. Sei que o ódio não é um sentimento bom, mas para certas coisas e pessoas não consigo ter paciência...

Fonte: O autor (2017)

Após realizar as etapas de pré-processamento, obteve-se os resultados exibidos no quadro a seguir:

Quadro 4 - Exemplo de palavras contidas no texto

ID	**Alegria**	**Nojo/Desgosto**	**Medo**	**Raiva**	**Surpresa**	**Tristeza**
1	**0,65**	-0,02	-0,14	-0,01	**0,23**	-0,31
2	-0,15	0,17	0,16	0,33	-0,1	**0,71**
3	-0,32	**0,41**	0,09	**0,54**	0,11	0,14

Fonte: O autor (2017)

Ao se avaliar os resultados observa-se foram identificadas as emoções alegria e surpresa no documento 1; tristeza e raiva no documento 2; e raiva e desgosto no documento 3. Para se chegar a esses valores utilizou-se o coeficiente de correlação de Pearson (r), cuja a interpretação se encontra na Tabela 5.

Tabela 5-Valores de referência para a interpretação do coeficiente de correlação Pearson

Valores da Correlação	Interpretação
0,0 até 0,19	Muito Fraca
0,20 até 0,39	Fraca
0,40 até 0,69	Moderada
0,70 até 0,89	Forte
0,90 até 0,99	Muito Forte
1	Absoluta

Fonte: Adaptado de Shimakura (2006)

Esse coeficiente é usado para quantificar o grau de associação linear entre duas variáveis quantitativas, ou seja, quantifica a semelhança que existe entre dois vetores de valores. O valor de r varia entre e -1 e +1 sendo que r = 0 significa que não existe relação linear entre os valores. E quanto maior o valor de r (positivo ou negativo), mais forte a associação. (SHIMAKURA, 2006)

Optou-se por utilizar esse teste para verificar a relação entre os léxicos LIWC e ANEW- BR as seis emoções básicas identificada nos textos coletados, podendo assim classificá-los adequadamente. Após a etapa de classificação dos textos de acordo com as emoções predominantes neles, passou-se para a etapa em que seria realizado um ataque de phishing a fim de identificar o comportamento do usuário diante de uma publicação atrativa com um link disfarçado supostamente malicioso.

3.2.8 Ataque de phishing

Para demonstrar como a falta de informação dos usuários pode torná-los vulneráveis nas redes sociais, foi lançado no Facebook um ataque de phishing não prejudicial, com o intuito de levantar quantos usuários iriam clicar no link disponibilizado. Esta é uma parte importante para esse trabalho, pois clicar num link pode redirecionar um usuário a um site realmente falso e malicioso criado por engenheiros sociais, cuja finalidade é induzir o usuário a liberar informações sigilosa e/ou comprometer a segurança de seu computador.

Figura 6 - Código PHP para realização do experimento

```php
<?php
$ip= $_SERVER['REMOTE_ADDR'];
$host = gethostbyaddr($ip); //guarda o mome do host
$data = date("d/m/Y"); //formata data
$hora = date("H:i"); //formata hora
$arq = fopen("visitas.txt","a+");
     fwrite($arq,"\n$host;$ip;$data;$hora");
fclose($arq);
?>
```

Fonte: Cortela (2013, p. 36)

Nessa etapa do trabalho um ataque do tipo phishing foi lançado através de uma publicação na linha do tempo de cada um dos perfis falsos, com uma mensagem apelativa. Como a finalidade era apenas estudar o comportamento dos usuários, observando quantos usuários clicaram no link, não foram utilizados códigos maliciosos na página referente à publicação, apenas um código para capturar, o nome do host, o ip, a data e hora em que o link

foi clicado. Para que não houvesse suspeitas por parte das vítimas, foi utilizado um encurtador de URL.

Ao clicar no link malicioso, foi criado um log em um arquivo texto denominado visitas.txt, com as informações básicas do visitante. Em seguida o usuário foi redirecionado para a página do Google. Como nenhuma página relacionada ao anúncio foi aberta, alguns usuários clicaram várias vezes, ocasionando entradas repetidas no arquivo de log, no entanto esses cliques repetidos foram eliminados. Posteriormente um quadro com os logs gerados pelo link malicioso, foi criado para mostrar o desempenho do ataque.

Quadro 5 - Logs gerados pelo link malicioso

IP	DATA	HORA
XXX.XXX.XXX.XXX	04/set	12:35
XXX.XXX.XXX.XXX	04/set	10:07
XXX.XXX.XXX.XXX	05/set	12:02
XXX.XXX.XXX.XXX	05/set	15:05
XXX.XXX.XXX.XXX	05/set	12:02

Fonte: O autor (2017)

Esse link ficou disponível entre os dias 4 de setembro e 4 de novembro de 2017, e publicado a cada 15 dias, objetivando atrair ainda mais a atenção dos usuários. Para atrair esta atenção a plataforma Canva.com foi utilizada para criar os anúncios.

Figura 7 - Anúncios utilizada nas postagens

Fonte: O autor (2017)

O primeiro anúncio trata a respeito de uma receita, assim como tantas outras que são compartilhadas no Facebook. E sendo em nível de informação, transmitia a ideia de que bastaria clicar para se ter acesso a receita sem que o usuário precisasse inserir dados pessoais. Já o segundo anúncio trata de uma suposta promoção de perfumes, ficando implícita a ideia de que caso o usuário se interesse por um dos produtos, precisaria inserir dados pessoais para um possível cadastro e posteriormente concluir a venda.

4 RESULTADOS

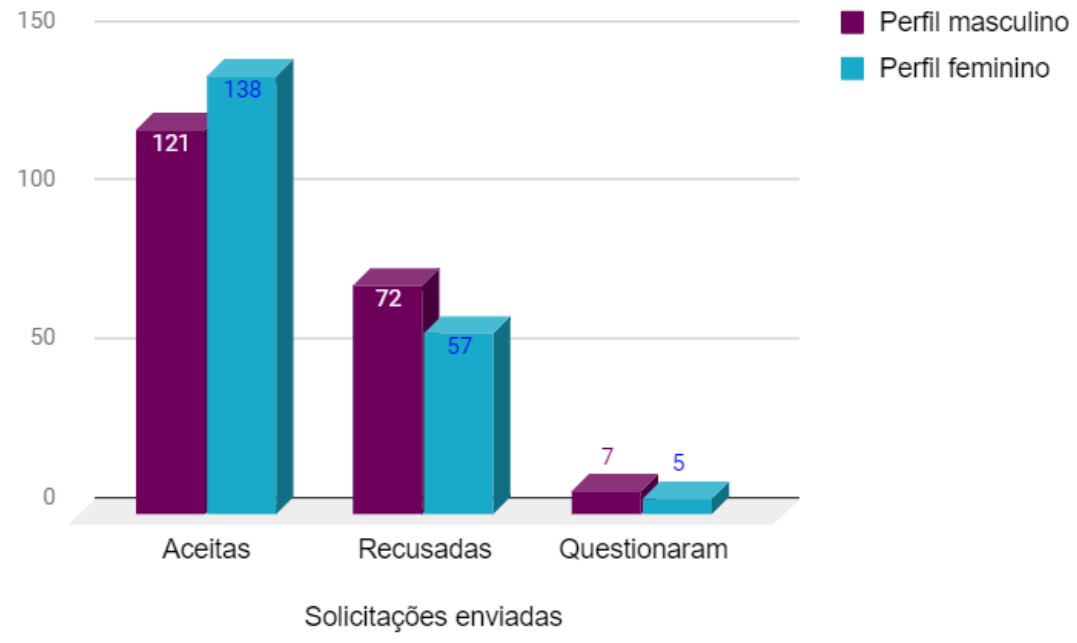
Este capítulo descreve os resultados obtidos nos experimentos realizados no estudo exploratório. Neste contexto, a primeira seção apresenta a criação dos usuários, as solicitações de amizades enviadas e o nível de exposição dos usuários que aceitaram os convites de amizade. Em seguida, são apresentados a formação da base textual, os resultados da aplicação dos léxicos afetivos ANEW-BR e LIWC, bem como os resultados da análise das seis emoções básicas contidas nos textos coletados. Por fim, são avaliados os resultados obtidos na aplicação do ataque de phishing.

4.1 Reação dos usuários quanto a solicitação de amizade

Mesmo não estando incluída no escopo deste trabalho, a primeira pergunta a ser respondida após o término do prazo de espera para a aceitação ou rejeição das solicitações foi: quantas pessoas aceitariam uma solicitação de amizade enviada por um desconhecido (a)?

Pode ser observado no Gráfico 1 que, 121 das solicitações de amizade foram aceitas, isso corresponde a 60,5% pessoas das 200 que receberam as solicitações do perfil masculino.

Gráfico 1- Quantidade de pessoas que aceitaram o convite dos dois perfis



Fonte: O autor (2017)

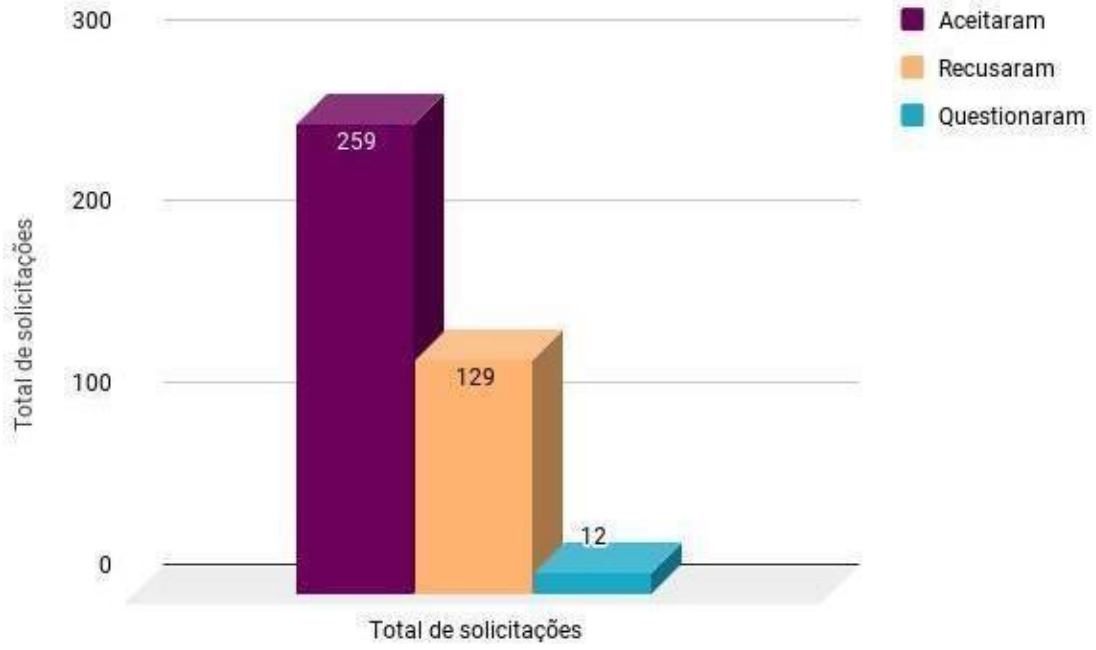
Somente 7 pessoas questionaram a solicitação, ou seja, apenas 3,5% entraram em

contato para saber se o perfil era real ou falso. Quanto às solicitações não aceitas, foram 36%, isso significa de 72 pessoas, ou recusaram, ou ignoraram o convite para fazer parte da rede de amigos do perfil masculino.

Quanto ao perfil feminino, como mostrado no Gráfico 1, das 200 pessoas que receberam a solicitação de amizade, 69% dos usuários aceitaram a solicitação sem conhecê-la, em números seria 138 pessoas. Apenas 2% questionaram a solicitação, alegando não conhecer o perfil, isso equivale a 5 pessoas. Os outros 28,5% não aceitaram e nem questionaram a solicitação, portanto entram no grupo das solicitações recusadas ou ignoradas, sendo um total de 57 usuários. Valendo ressaltar que apenas uma solicitação foi enviada para cada usuário, ou seja, não foram realizadas segundas tentativas.

Analisando o Gráfico 2 pode-se chegar às seguintes constatações: das 400 solicitações de amizades enviadas pelos dois perfis, 64,8% foram aceitas. Isso significa que 259 usuários, aceitaram o convite de um completo desconhecido. Apenas 3% (12 pessoas) tiveram dúvidas quanto a aceitar a solicitação de um desconhecido, e entraram em contato para saber se o perfil se tratava de alguém real ou não. O restante, 129 pessoas, ou 33% dos usuários, ignoraram ou recusaram a solicitação de amizade.

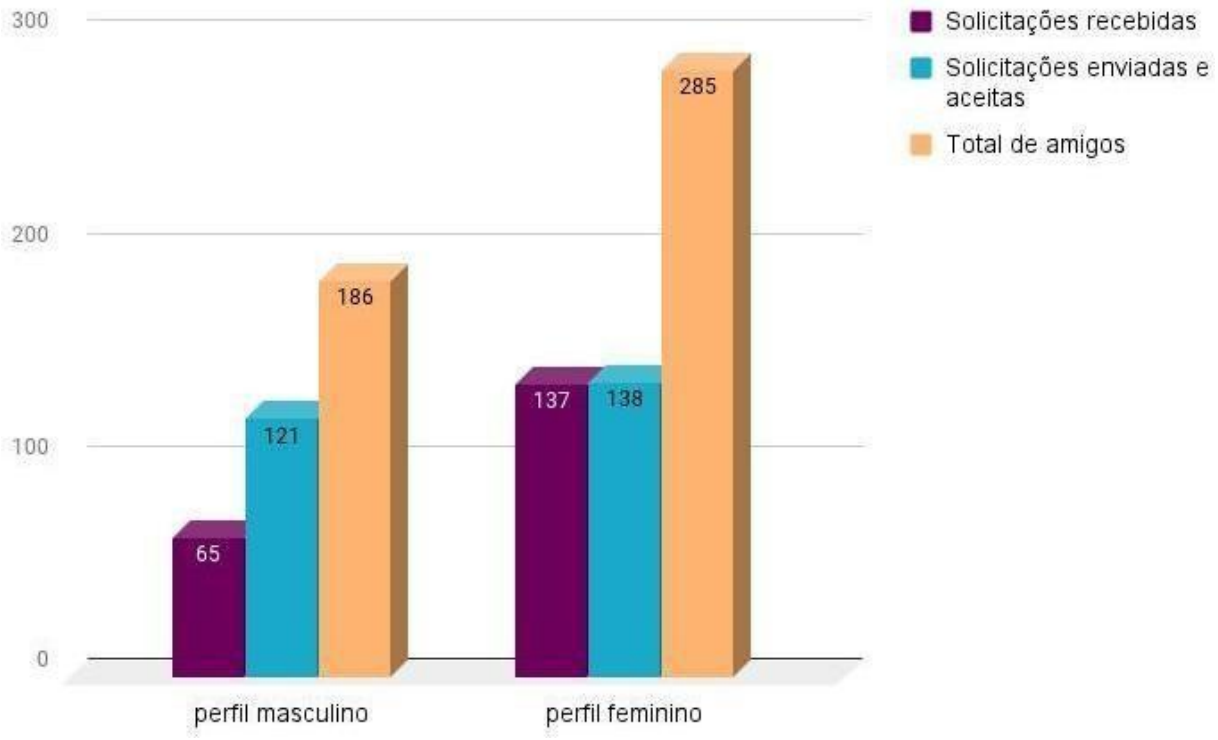
Gráfico 2- Total de solicitações



Fonte: O autor (2017)

No Gráfico 3 foi feita uma comparação entre a quantidade de solicitações enviadas e aceitas, a quantidade de solicitações recebidas, e a soma do total de amigos de cada perfil.

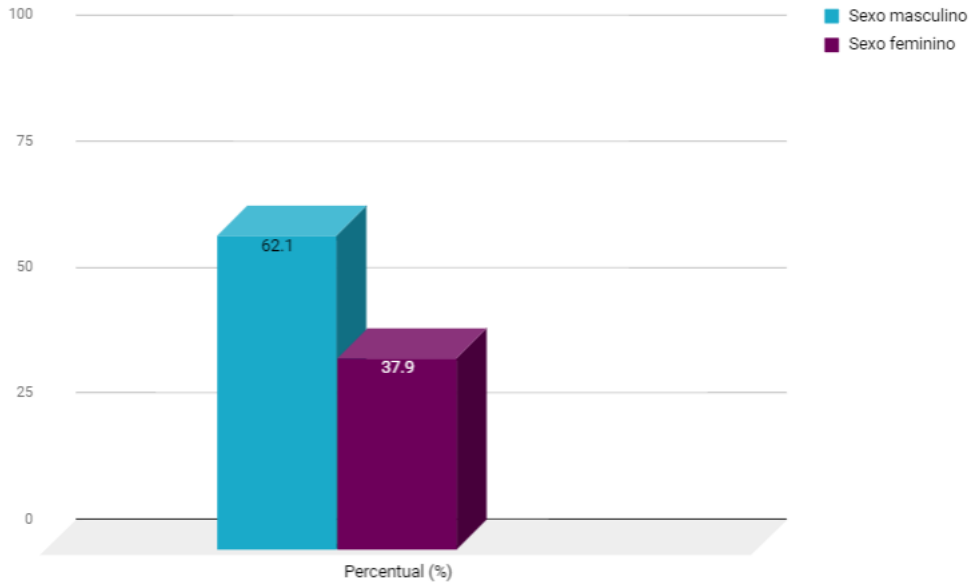
Gráfico 3 - Comparação entre o total de amigos



Fonte: O autor (2017)

O perfil masculino recebeu e aceitou 65 solicitações de amizade de usuários desconhecidos, totalizando 186 amigos no Facebook, sendo que 36% são do sexo masculino e 64% são do sexo feminino.

Gráfico 4 - Sexo dos usuários nos dois perfis



Fonte: O autor (2017)

Quanto ao perfil feminino criado, das 200 solicitações de amizade que foram enviadas 138 foram aceitas, 137 solicitações foram recebidas de outros usuários, totalizando 285

“amigos” no Facebook, sendo 79% do sexo masculino e 21% do sexo feminino.

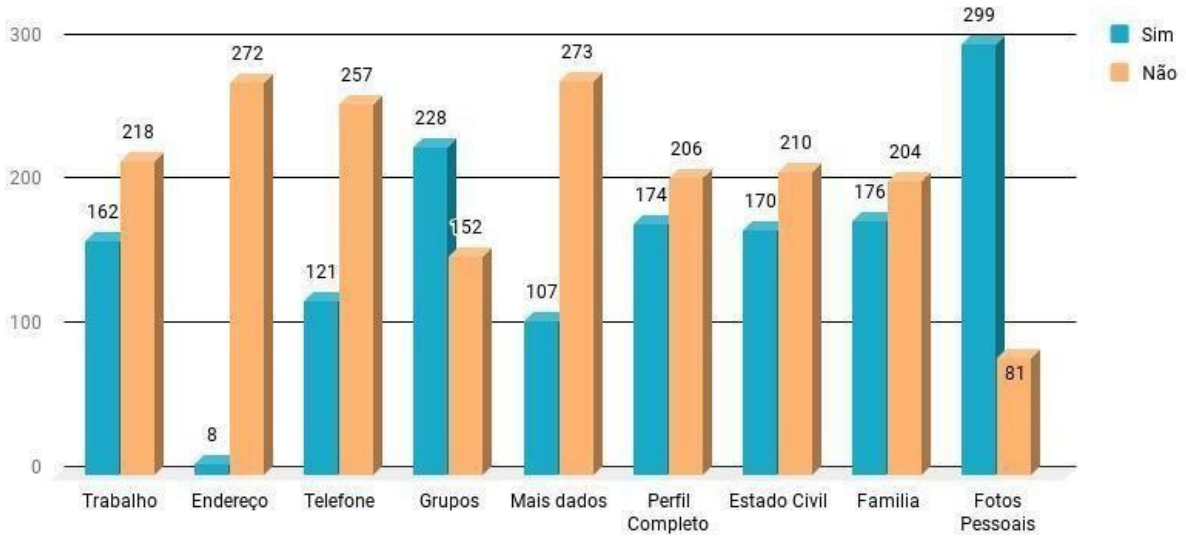
A quantidade de pessoas que compõem a lista de “amigos” dos dois perfis corresponde a 471 usuários. Sendo que 62,1% são do sexo masculino e 37,9% são do sexo feminino.

Os resultados obtidos permitem concluir que existe uma tendência em se aceitar mais facilmente a amizade de perfis femininos do que a amizade perfis masculinos, e demonstrou que os homens são muito mais propensos a aceitar as solicitações de estranhos do que as mulheres.

4.2 Análise do nível de exposição dos usuários que aceitaram a solicitação

Após a análise das solicitações enviadas e recebidas pelos perfis feminino e masculino, foram analisados detalhadamente os 80,6% dos perfis de cada um totalizando 380 perfis analisados, em busca de informações pessoais e específicas como endereço, local de trabalho telefone, relacionamentos, ou seja, informações que poderiam ser usadas por um engenheiro social. Tal análise pode ser observada no Gráfico 5.

Gráfico 5- Análise das informações disponíveis



Fonte: O autor (2017)

Desse universo, foi analisada a porcentagem de usuário que possuem o perfil pessoal preenchido com informações pessoais de forma completa ou incompleta.

Sendo que 174 (45,8%) dos usuários preencheram de forma completa seu perfil, contendo informações a respeito de si como: família, relacionamentos, várias fotos pessoais,

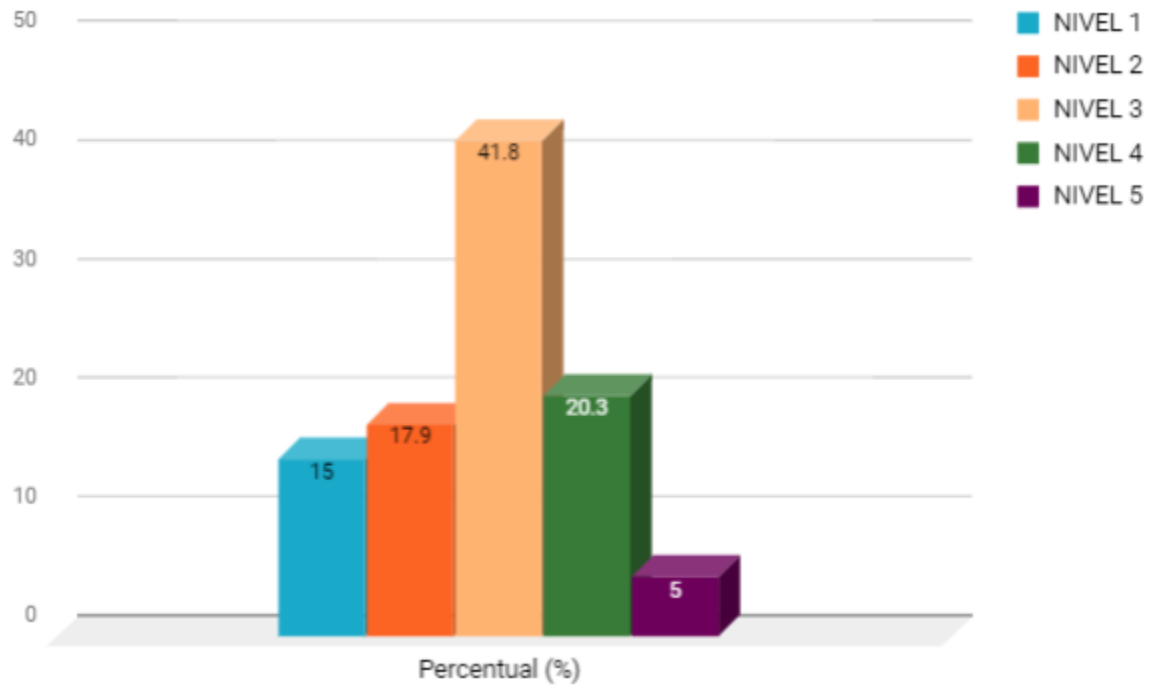
atividades de interesses, trabalho, cidade onde mora ou já morou, religião, escola. No entanto 206 (54,2%) dos usuários preencheram seu perfil com pouca ou nenhuma informação. Mesmo para estes, as informações extraídas das fotos poderiam ser o bastante para colocá-los em riscos.

Alguns casos chamaram a atenção, pois, além de preencherem seus perfis completamente, também colocaram telefone, *e-mail* pessoal, local de trabalho, endereço residencial completo, CEP e telefone.

Dos 380 usuários analisados, 60% (228 deles) pertencem a grupos cujas descrições poderiam ser usadas para montar um perfil psicológico dessas pessoas. Por último, os 380 perfis foram analisados na sua totalidade e foram agrupados por nível de exposição segundo a escala elaborada na metodologia deste estudo.

Como pode ser observado 15% dos usuários possuíam um perfil que não oferecem riscos, portanto ficaram no nível 1. No nível 2 foram 17,9%, pois possuem poucas informações pessoais, e consequentemente o risco oferecido é mínimo.

Gráfico 6 - Nível de exposição dos usuários analisados



Fonte: O autor (2017)

Também é possível perceber que a maior parte dos usuários ficam no nível 3, pois estes perfis possuem informações como locais de trabalho ou residência, parentes e amigos, gostos pessoais, o que permite a um engenheiro social pode obter informações básicas sobre o usuário. Ou seja, 41,8% possuem um nível de exposição considerado normal dentro da escala.

Dentro do nível 4 estão os perfis que ofereciam um grau de risco maior que os perfis do nível 3, por disponibilizarem informações que os deixavam mais expostos. Sendo 20,3% dos perfis analisados. Por fim, no nível 5, estão os perfis que ofereciam o maior grau de risco, por possuírem informações detalhadas como endereço residencial, telefone, lista de amigos íntimos, família, *e-mail* pessoais, estado civil, local de trabalho, interesses pessoais, religião, e álbum com muitas fotos.

Os resultados obtidos levam à conclusão de que a maior parte dos usuários 62, 1% (41,8% do nível 3 e 20,3% do nível 4) possuem informações como locais de trabalho ou residência, parentes e amigos, gostos pessoais, que dariam a informações a base necessária para tornar os usuários alvos de ataques. Observando o Gráfico 6 percebe-se uma falta de preocupação no que diz respeito a privacidade por parte dos usuários do Facebook. E de posse destes dados um engenheiro social seria capaz de realizar diferentes tipos de ataque, podendo variar de roubo de identidade até a simulação de um sequestro, uma vez que ele possui dados sobre localização, familiares, amigos, e hábitos da vítima.

Durante a fase de análise dos resultados, os usuários foram listados de 1 a 380 (usuário 1, usuário 2, usuário 3...) para facilitar a identificação dos mesmos. Após a análise dos resultados alguns usuários foram selecionados segundo três critérios:

- Os que publicaram textos com emoções negativas mais recentes: como por exemplo, o usuário 29, que após uma desilusão amorosa e um rompimento conturbado, postou frases de como ele se sentia desolado, e decepcionado com a vida. Suas postagens tiveram certa repercussão obtendo 32 comentários, alguns com frases de apoio outros com pedidos para que ele superasse e seguisse em frente.
- Os que foram classificados no nível 5 de exposição como explicado na seção 3.2.3: como por exemplo os usuários 111 e 326 que publicaram número de telefone, *e-mail* e endereço residencial, possibilitando uma abordagem mais direta de um usuário mal-intencionado.
- Os que demonstraram interesse pelos perfis falsos criados: Os usuários 65 e 92 demonstraram forte interesse pelo perfil feminino, ambos se ofereceram para pagar todas as despesas necessárias para que ela se mudasse para a cidade dele. Já o usuário 47 assediou o perfil feminino chegando a lhe enviar fotos de conteúdo adulto. Quanto ao perfil masculino, o usuário 271 demonstrou interesse em conhecer pessoalmente o perfil, mas a abordagem foi mais discreta, apenas por meio de conversas simples, sem conotação sexual, mais com a intenção em desabafar o que estava sentindo.

Os resultados dessa abordagem indicaram que estes usuários possuíam uma

necessidade de aprovação e reconhecimento por parte dos usuários no Facebook, expresso através de publicações, esperando a aprovação dos outros através dos *likes* e comentários que elevassem a autoestima sua autoestima. E essa necessidade de aprovação faz com que esses usuário se abram emocionalmente para um desconhecido, tornando-os vulneráveis num ambiente em que a legitimidade de um perfil pode ser questionada.

4.3 Resultados da união dos léxicos LIWC e ANEW-BR com as emoções básicas

Justifica-se a utilização de pelo menos dois léxicos com o propósito de comparar qual deles apresenta melhor resultado, podendo até mesmos serem combinados entre si. E por meio dos resultados obtidos com os dois léxicos, validar a possibilidade de que a forma como as pessoas escrevem nas redes sociais, fornece uma abertura para a observação de aspectos emocionais. Seguem-se os resultados obtidos a partir da análise das seis emoções básicas identificadas por meio da utilização dos léxicos ANEW-BR e LIWC. Como foi especificado na seção 3.2.4 foi construída uma base textual para os textos coletado nas publicações dos usuários que compunham a lista de "amigos" dos dois perfis criados no Facebook. Uma base textual apenas para os textos publicados em grupos abertos do Facebook também foi criada. Outras seis bases de textos foram criadas, sendo uma para cada emoção básica. O objetivo era passar os textos coletados pelas etapas de mineração de texto descrito na seção 3.2.4, para posteriormente compará-los com as bases textuais referentes aos léxicos e as emoções básicas.

No quadro a seguir podem ser observados algumas das frases que foram coletadas e o tipo de emoção que elas expressam.

Quadro 6- Exemplos de frases coletadas

Emoção	Frases
Alegria	Que Deus abençoe seu dia
Tristeza	Eu não sei se choro, se sumo, ou se finjo que estou bem
Raiva	Odeio crises ciumes, mas não consigo me controlar
Medo	Tenho pavor da velhice e da morte
Surpresa	É o inesperado que muda nossas vidas
Nojo / Desgosto	Tenho repulsa da falsidade e aversão a julgamentos

Fonte: O autor (2017)

Após comparar os documentos textos dos usuários e os textos coletados nos grupos públicos com as bases textuais das seis emoções básicas, fez-se uso dos léxicos para estabelecer o coeficiente de correlação a fim de identificar as emoções predominantes nos textos. E a Tabela 6 mostra os resultados do coeficiente de correlação entre as emoções básicas e o léxico ANEW-BR.

Tabela 6-Coeficiente de correlação de Pearson para o ANEW-BR

Emoção	Textos dos usuários	Textos dos Grupos
Alegria	0,31304712	0,31958563
Medo	-0,1764599	-0,15114754
Nojo/desgosto	-0,0119915	-0,02663387
Raiva	0,27531789	0,288758507
Surpresa	0,14691104	-0,18968430
Tristeza	0,30337385	0,343520821

Fonte: O autor (2017)

E para compreendê-la deve-se relembrar que a escala o coeficiente de correlação vai de -1 a 1. Isso significa que quanto mais perto de 1 estiver o coeficiente maior a relação entre as variáveis, e quanto mais perto de -1 mais distante é a relação entre as variáveis, ou seja, quando uma variável aumentar a outra obrigatoriamente irá diminuir.

No caso da Tabela 6, observa-se que para todas as emoções coletadas dos textos dos usuários obteve-se uma correlação que se apresenta no intervalo interpretado muito fraca ou fraca (Tabela de interpretação na seção 3.2.8), com resultados entre 0.01 a 0.30 nos testes com o léxico ANEW-BR.

Isso significa que embora o ANEW-BR possa ser usado para identificar emoções, não é possível afirmar que ele – ao menos para esse estudo – é suficiente para identificar as seis emoções básicas nos textos coletados.

Já a correlação nos testes realizados com o léxico LIWC, os resultados obtidos mostram uma correlação que se apresenta no intervalo interpretado como muito fraco para as emoções de medo, raiva e surpresa com resultados entre 0.02 a 0.19; e fraco para as emoções de alegria, nojo, e tristeza com resultados entre 0.23 a 0.29.

Tabela 7 - Coeficiente de correlação de Pearson para o LIWC

Emoção	Textos dos usuários	Textos dos Grupos
Alegria	0,2879979	0,26972864
Medo	-0,02398356	-0,0573599602
Nojo/desgosto	-0,28946281	-0,29839094
Raiva	0,18053461	0,139351551
Surpresa	-0,02468703	-0,010848651
Tristeza	0,26995198	0,255000697

Fonte: O autor (2017)

Assim como ocorreu com o ANEW-BR, o léxico LIWC, usado isoladamente também permitiu afirmar que ele não seria o suficiente para identificar as seis emoções básicas nos textos coletados, ao menos para esse estudo. Isso porque embora houvesse uma correlação ela não era forte o bastante para confirmar que se é possível usar apenas um dos léxicos para identificar as seis emoções básicas.

Já a Tabela 8 mostra a correlação entre a união dos léxicos e as emoções básicas.

Os resultados obtidos mostram uma correlação forte na união dos léxicos o LIWC e o ANEW-BR para identificar as emoções alegria e tristeza, uma correlação moderada para identificar raiva e surpresa, e uma correlação fraca para identificar as emoções de medo e nojo/desgosto, como pode ser observado na Tabela 8. No entanto a situação mudou quando se usou os dois léxicos simultaneamente e em conjunto com o TF-IDF.

Tabela 8- Coeficiente de correlação de Pearson para o ANEW-BR e o LIWC

Emoção	Textos dos usuários	Textos dos Grupos
Alegria	0,51080743	0,60569947
Medo	0,3203694	0,44484502
Nojo/desgosto	0,2678222	0,392182383
Raiva	0,45181478	0,302142578
Surpresa	0,31513944	0,348239104
Tristeza	0,65669777	0,541653783

Fonte: O autor (2017)

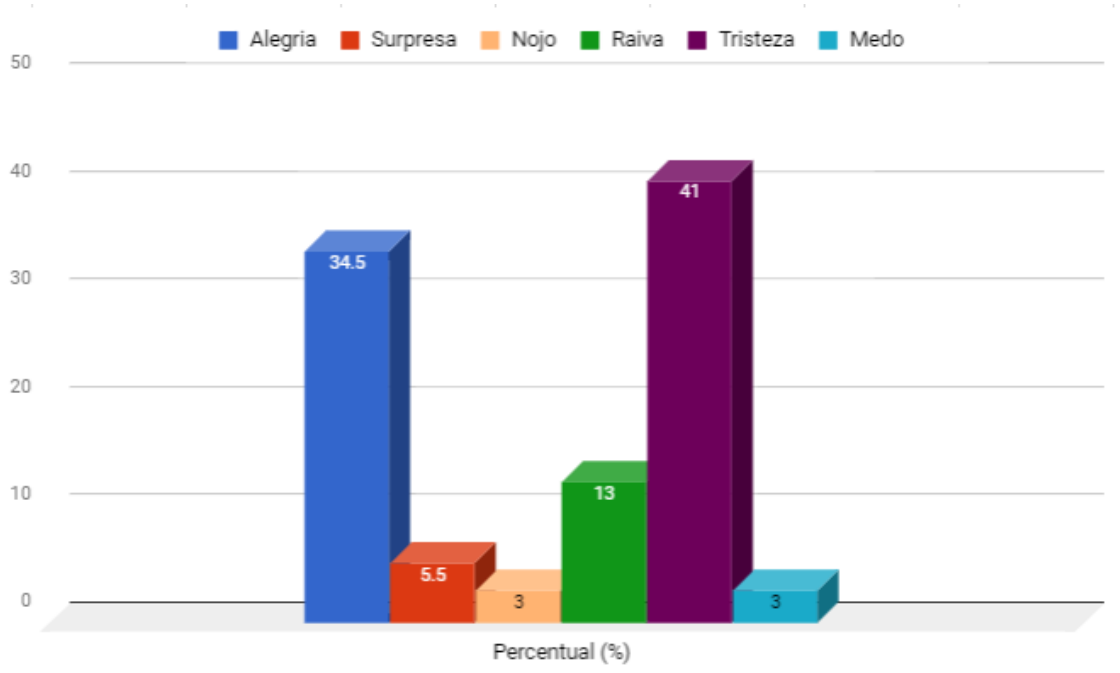
A união dos léxicos com o TF-IDF possibilitou uma correlação cujo intervalo é interpretado como:

- Fraco: para as emoções de medo, nojo e surpresa para os textos dos usuários; e nojo raiva e surpresa para os textos dos grupos;

- Moderado: para as emoções alegria, raiva e tristeza para os textos dos usuários; e alegria, medo e tristeza para os textos dos grupos.

Isso significa que, em comparação com os resultados da Tabela 6 e 7, os resultados mostrados na Tabela 8 foram superiores, indicando que quando unidos os léxicos LIWC e ANEW-BR juntamente com o TF-IDF possibilitam resultados que corroboram a hipótese da utilização dos mesmos para o reconhecimento de emoções por meio de texto. Com base nos resultados obtidos foi gerado os gráficos 7 e 8 a fim de demonstrar as emoções predominantes nos textos coletados, os documentos com os textos dos usuários foram classificados de acordo com as emoções. Com isso os gráficos 7 e 8 foram criados para demonstrar o percentual das principais emoções que se podem encontrar nas redes sociais. O Gráfico 7 mostra o percentual das emoções identificadas nos textos publicados em grupos abertos no Facebook coletados por meio do aplicativo *Netvizz*.

Gráfico 7 - Emoções identificadas nos textos dos grupos públicos



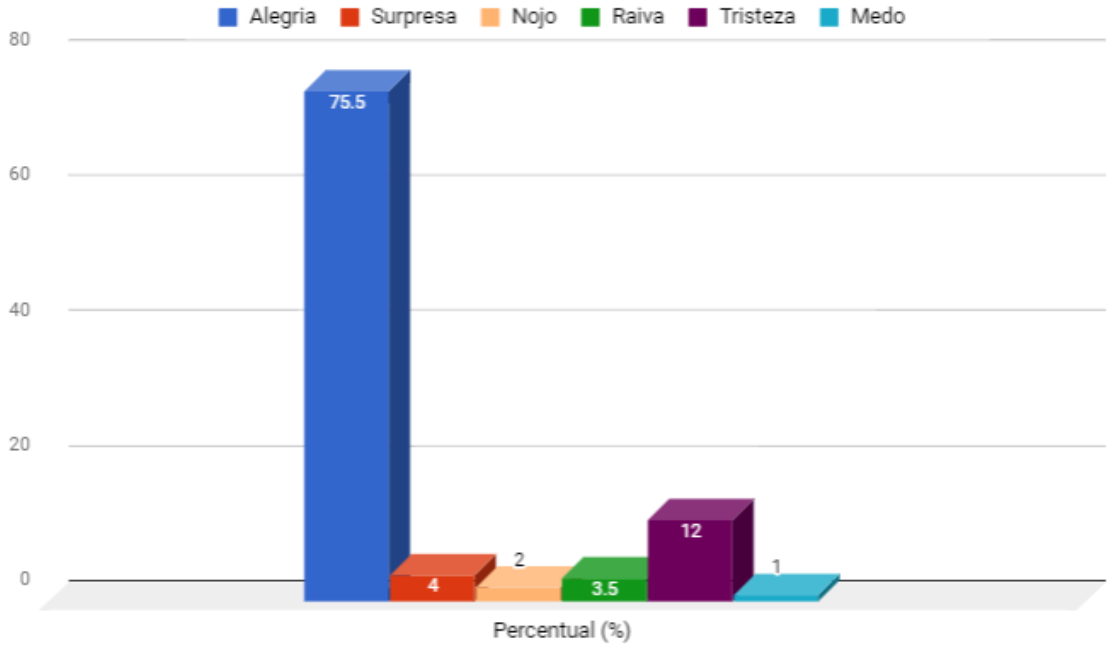
Fonte: O autor (2017)

Como o objetivo de um engenheiro social é encontrar alvos emocionalmente vulneráveis para manipulá-los mais facilmente, optou-se por escolher grupos cujo teor das publicações fosse voltado para desabafos pessoais. Por causa disso pode-se observar uma expressividade maior dos sentimentos negativos, tristeza (41%), raiva (13%), medo (3%), nojo (3%) em comparação com os sentimentos positivos, alegria (34,5%) e surpresa (5.5%).

Com base nesse gráfico pode-se conjecturar que, um engenheiro social poderia se conectar com as pessoas que expressaram mais tristeza do que alegria, e tentar persuadi-la a fazer algo ruim contra algo ou alguém, ou até contra si mesma, bem como poderia se passar por alguém amigo e solidário para tirar vantagem da fragilidade emocional da vítima.

A análise seguinte diz respeito aos textos coletados dos usuários que pertenciam a lista de amigos dos dois perfis criados para este estudo. O Gráfico 8 mostra a predominância das emoções nos textos que foram coletados de 200 usuários dentre os 380 disponíveis como "amigos" nos dois perfis criados. Como podem ser observados 77,5% dos documentos expressam alegria, contentamento, ou seja, frases com emoções positivas.

Gráfico 8- Emoções identificadas nos textos dos usuários



Fonte: O autor (2017)

Já restante dos documentos expressam outras emoções, sendo a tristeza predominante em 12% dos textos, através de frases de insatisfação; a surpresa em 4% expressa a partir de texto relativos a coisas estranhas ou inesperadas; a raiva em 3,5% através de frases de protestos contra a própria situação ou contra a situação econômica e política do país, em alguns casos o texto foi classificado como triste devido a insatisfação ou frustração de quem o escreveu, ainda que o sentimento inicial tenha sido de raiva; o desgosto ou nojo foi identificado em apenas 2% dos textos através de frases nas quais seus autores expressaram sobre aquilo que consideravam desagradável. Quanto ao medo, foi identificado em 1% dos

textos por meio de frases que demonstravam o receio dos usuários em fazer algo, ou alguma atividade.

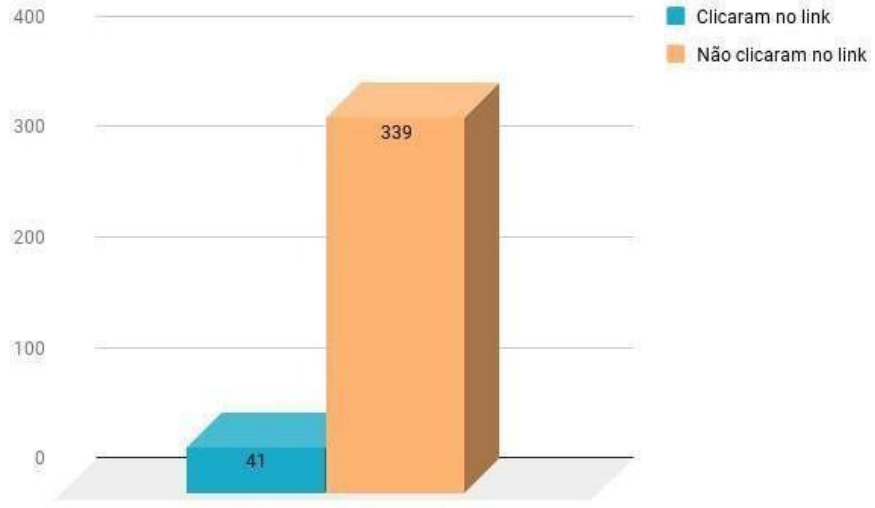
Esses resultados demonstram que os usuários do Facebook em sua maioria, procuram transmitir na rede social uma imagem positivar acerca de si mesmo, e isso pode ser identificado também nos conteúdos compartilhados e nos textos publicados, sejam em forma de imagens, vídeos, notícias compartilhadas ou através de textos, estando estes na linha do tempo do próprio usuário ou como comentário à publicação de algum outro usuário. Ao longo do desenvolvimento deste estudo, ficou claro que, a forma como as pessoas se sentem e como elas percebem o mundo, influencia nas decisões que elas tomam em seu dia a dia.

4.4 Resultados do ataque de phishing

Como detalhado na seção 3.2.9, foi lançado no Facebook um ataque de phishing não prejudicial, para quantificar quantos usuários clicariam num link disponibilizado numa postagem.

Como pode ser observado no Gráfico 9, das 380 possíveis vítimas 41 clicaram no link malicioso, sendo que alguns deles clicaram até mais de uma vez.

Gráfico 9- Quantidade de pessoas que clicaram no link malicioso



Fonte: O autor (2017)

Isso mostra que se um site falso fosse montado, esses usuários possivelmente enviaram informações sigilosas como senha, documentos ou números de cartões de créditos. Ainda que o usuário percebesse que não se tratava de algo real e fechasse seu navegador, *exploits* poderiam ser embutidos numa página simples e comum. Com esses *exploits* um

hacker poderia ter acesso ao computador afetado sem ter contato direto com a vítima, pois tais *exploits* se aproveitam de falhas presentes nos próprios *softwares* que a vítima possa possuir.

A princípio pretendia-se com esse ataque, relacionar os usuários cujos textos foram identificados com emoções negativas (raiva, tristeza, medo e nojo) com os usuários que clicaram no link malicioso. No entanto, isso não foi possível por causa da dificuldade em se extrair automaticamente o identificador de usuário, dos usuários do Facebook. Apesar do código em PHP ser capaz de capturar o nome do host, o IP, isso não foi o suficiente para associar usuários cujos textos foram coletados com os usuários que clicaram no link. No entanto isso não invalida os resultados do ataque para esse trabalho, pois o phishing ainda é uma técnica muito utilizada para coletar dados de usuários em diferentes plataformas.

5 CONCLUSÃO

Este trabalho teve por objetivo abordar o tema da engenharia social no Facebook, com o intuito de identificar possíveis alvos para a mesma, a partir de uma análise das informações coletadas em perfis de usuários e as suas publicações, com o auxílio das técnicas básicas de mineração de textos e o uso de léxicos para identificar emoções em textos.

Para realização do estudo, foram efetuadas pesquisas acerca de emoções, mineração de textos, redes sociais e engenharia social, visando adquirir bom embasamento teórico para dos experimentos realizados. Posteriormente fez-se a escolha das ferramentas que foram utilizadas e optou-se por realizar a implementação de um algoritmo em Java que pudesse realizar as etapas de mineração de textos, bem como realizar os cálculos necessários para identificar as emoções nos textos coletados.

Concluída a implementação do algoritmo, para validação do estudo elaborado, iniciou-se a etapa de testes e experimentos. Neste contexto, foram realizados experimentos combinando os léxicos ANEW-BR e LIWC com o intuito de aperfeiçoar a identificação de emoções em textos publicados no Facebook. Tais associações colaboraram para que o algoritmo implementado obtivesse valores de saída fortemente correlacionados às seis emoções básicas. Também foi realizada uma análise detalhada em diversos perfis da rede social objetivando identificar o nível de exposição dos usuários e como suas publicações seriam fontes de dados tanto para de campanhas publicitárias quanto para usuários mal-intencionados.

Os resultados obtidos no estudo exploratório evidenciaram que usuários do Facebook, muitas vezes disponibilizam dados pessoais (telefone, *e-mail*, ou endereço residencial) desnecessariamente, e tal comportamento os tornam vulneráveis. Também foi possível comprovar que os léxicos ANEW-BR e LIWC quando usados juntamente com o método TF-IDF permite a identificação de emoções em textos postados no Facebook. Bem como, é possível fazer uso dos conceitos de mineração de texto para a criação de um algoritmo que possa identificar emoções de forma automatizada. E tais textos poderiam servir como base inicial para um ataque de engenharia social mais elaborado.

Como contribuição principal desta pesquisa destaca-se: (i) definição da abordagem de reconhecimento de emoção por meio de texto, (ii) definição e confirmação da hipótese de que a identificação de emoções a partir de texto favorece a engenharia social, (iii) comparação de léxicos para a tarefa de identificação de emoções, (iv) resultados de que combinações de léxicos e métodos de representação de texto levam a resultados significativamente superior

comparados a utilização individual dos léxicos.

Por fim, pode-se ressaltar como trabalhos futuros a possibilidade de se utilizar algoritmos de aprendizado de máquina para melhorar a eficiência e precisão de se identificar emoções em textos. Espera-se ter alcançado as expectativas do leitor, bem como ter colaborado de alguma maneira para a disseminação do conhecimento assimilado através dessa pesquisa que resultou na criação da monografia proposta.

REFERÊNCIAS

ABNT, NBRISO/IEC 27002. **Tecnologia da informação — Técnicas de segurança — Código de prática para a gestão da segurança da informação**. 1. ed. Rio de Janeiro: ABNT, 2005. Disponível em:<http://www.fieb.org.br/download/senai/NBR_ISO_27002.pdf>. Acesso em: 29 Ago. 2017.

ALAM, Firoj; STEPANOV, Evgeny A.; RICCARDI, Giuseppe. **Personality Traits Recognition on Social Network - Facebook**. Trento, Italy, 2013.Monografia (Computer Science)-University of Trento, 2013 Disponível em <https://www.aaai.org/ocs/index.php/ICWSM/ICWSM13/paper/download/6167/6307.>. Acesso em: 25 Out 2017.

ALCOFORADO, Acilégna C. D. G.; RIBEIRO, Emerson C.; CUNHA, Jacqueline A. **Condutas do Fator Humano: Alicerce da Segurança da Informação** In: ENCONTRO REGIONAL DE ESTUDANTES DE BIBLIOTECONOMIA, DOCUMENTAÇÃO, CIÊNCIA E GESTÃO DA INFORMAÇÃO, 15. 2012. João Pessoa, 2012. Disponível em <http://portaldeperiodicos.eci.ufmg.br/index.php/moci/article/viewFile/2157/1346>. Acesso em: 16 Mai 2017.

ALLEM, Malcolm. Social Engineering: A Means to Violate a Computer System. **SANS Institute InfoSec Reading Room**. june./dec, 2006. Disponível em <https://www.sans.org/reading-room/whitepapers/engineering/social-engineering-means-violate-computer-system-529>. Acesso em: 12 Set 2017.

ALVES, Cássio Bastos. **Segurança da Informação Vs. Engenharia Social**: Como se proteger para não ser mais uma vítima. Brasília, f. 128, 2010. 128 p. Monografia (Sistemas de Informação)-CENTRO UNIVERSITÁRIO DO DISTRITO FEDERAL, 2010 Disponível em <http://www.administradores.com.br/_assets/modules/academicos/academico_3641.pdf>. Acesso em: 19 Abr 2017.

ARAÚJO, Eduardo Edson De . **A Vulnerabilidade Humana Na Segurança Da Informação**. Uberlândia, f. 95, 2005. TCC (Sistemas De Informação) - União Educacional Minas Gerais S/C Ltda, 2005 Disponível em:<http://docplayer.com.br/514163-A-vulnerabilidade-humana-na-seguranca-da-informacao.html>. Acesso em: 5 Set. 2017.

AVAST, . Crime virtual. **Avast**. 2017. Disponível em <https://www.avast.com/pt-br/c-cybercrime>. Acesso em: 31 Out 2017.

AZEREDO, J. C.. **Gramática Houaiss da Língua Portuguesa**. São Paulo: Publifolha, 2008.

BARBOSA, Alexandre N.. **Descoberta de Conhecimento Aplicado à Base de Dados Textual de Saúde**. São Leopoldo, 2012.TCC (Programa Interdisciplinar de Pós-Graduação em Computação Aplicada)-Universidade do Vale do Rio dos Sinos, 2012 Disponível em <http://www.repositorio.jesuita.org.br/bitstream/handle/UNISINOS/4559/42c.pdf?sequence=1&isAllowed=y>. Acesso em: 23 Ago 2017.

BARBOSA, Fernanda. Necessidades Humanas Básicas na Enfermagem: Maslow e Wanda Horta. **Concursos da Saúde**. Bahia, 2016. Disponível em <http://blog.concursosdasaude.com.br/necessidades-humanas-basicas-na-enfermagem-maslow-e-wanda-horta/>. Acesso em: 04 Set 2017.

BARION, Eliana Cristina Nogueira; LAGO, Decio. Mineração de Textos. **Revista de Ciências Exatas e Tecnologias**. Anhanguera, v. 3, n. 3. 8. dez., 2008.Anhanguera Educacional S.A.. Disponível em <http://pgsskroton.com.br/seer/index.php/rcext/article/viewFile/2372/2276>. Acesso em: 02 Out 2017.

BRADLEY, Margaret M; LANG, Peter J. Affective Norms for English Words (ANEW): Instruction manual and affective ratings. 1999. Disponível em <http://www.uvm.edu/pdodds/files/papers/others/1999/bradley1999a.pdf>. Acesso em: 20 Jun 2017.

BRAGA, Luis Paulo Vieira. **Introdução à Mineração de Dados**. 2. ed. Rio de Janeiro: E-Papers Serviços Editoriais, 2005. 212 p.

BRASIL. Congresso Nacional. Decreto-Lei n. 12.737, 30 de outubro de 2012. Diario Oficial da União. Brasília, 30 de outubro de 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 31 Out 2017.

CAVALCANTE JR., Reinaldo Leopoldino. **Engenharia Social nas Redes Sociais**. Maringá, f. 48, 2011. 48 p. TCC (Especialização em Desenvolvimento de Sistemas para Web)-Universidade Estadual de Maringá, 2011 Disponível em<https://www.docdroid.net/sw4u/social-nas-redes-sociais.pdf#page=2>. Acesso em: 21 Mai 2017.

_____. Código Penal. Decreto-Lei n. 2.848, 07 de dezembro de 1940. Diario Oficial da União. Rio de Janeiro, 07 de dezembro de 1940. Disponível em: <http://www.oas.org/juridico/mla/pt/bra/pt_bra-int-text-cp.pdf>. Acesso em: 31 Out 2017.

CERT.BR, . Cartilha de Segurança para Internet. **cert.br**. 2017. Disponível em<https://cartilha.cert.br/>. Acesso em: 05 Ago 2017.

_____. Incidentes Reportados ao CERT.br -- Janeiro a Dezembro de 2016: Tentativas de Fraudes. **CERT.br**. 2016a. Disponível em: <https://www.cert.br/stats/incidentes/2016-jan-dec/fraude.html>. Acesso em: 17 Out. 2017.
_____. Incidentes Reportados ao CERT.br -- Janeiro a Dezembro de 2016: Top 10 CCS origem dos ataques. **CERT.BR**. 2016b. Disponível em:<https://www.cert.br/stats/incidentes/2016-jan-dec/top-cc.html>. Acesso em: 18 Out. 2017.

CERVI, Cristiano Roberto. **Um Estudo sobre Mineração de Dados em Redes Sociais**. Porto Alegre, f. 39, 2008.Trabalho de Disciplina (PÓS-GRADUAÇÃO EM COMPUTAÇÃO)-UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL, 2008 Disponível em<http://usuarios.upf.br/~cervi/publications/ti_ii_2008.pdf>. Acesso em: 30 Jul 2017.

CIRIBELLI, Marilda Corrêa. **Projeto de Pesquisa**: Um Instrumental da Pesquisa Cientifica. Rio de Janeiro: 7Letras, f. 88, 2000. 86 p. Disponível em<https://pt.scribd.com/document/39690455/CIRIBELLI-Marilda-Correai-Projeto-de-Pesquisa>. Acesso em: 03 Set 2017.

COELHO, Carlos . Como criminosos virtuais lucram com o roubo e a venda de dados. **Gazeta do povo**. 2017. Disponível em:<http://www.gazetadopovo.com.br/economia/nova-economia/como-criminosos-virtuais-lucram-com-o-roubo-e-a-venda-de-dados-6gf3n9qwsmkm5p7c2tk4jgy7u>. Acesso em:15 Nov. 2017.

CORTELA, João José Corrêa. **Engenharia Social No Facebook**. Londrina, 2013.TCC (Ciência da Computação)-UNIVERSIDADE ESTADUAL DE LONDRINA, 2013 Disponível em <http://www.uel.br/cce/dc/wp-content/uploads/TCC-JoaoCortela-BCC-UEL-2013.pdf>.Acesso em: 11 Set 2017.

CRESWELL, John W.. **Projeto de pesquisa**: métodos qualitativo, quantitativo e misto. Tradução Luciana de Oliveira da Rocha. 2. ed. Porto Alegre: Artmed, 2007. 248 p. Tradução de: Research design: qualitative, quantitative, and mixed methods approaches. Disponível em<https://edisciplinas.usp.br/pluginfile.php/696271/mod_resource/content/1/Creswell.pdf>. Acesso em: 29 Ago 2017.

CÔRTEZ, Sérgio da Costa; LIFSCHITZ, Sérgio; PORCARO, Rosa Maria. **Mineração de Dados**: Funcionalidades, Técnicas e Abordagens. Rio de Janeiro, f. 35, 2002.Tese ()-PONTIFÍCIA UNIVERSIDADE CATÓLICA DO RIO DE JANEIRO, 2002 Disponível em<http://www.dbd.puc-rio.br/depto_informatica/02_10_cortes.pdf>. Acesso em: 23 Mai 2017.

DAMÁSIO, Antonio. **Ao Encontro de Espinosa**: As Emoções Sociais e a Neurologia do Sentir. 2. ed. Europa-America, 2003. Disponível

em<https://pt.scribd.com/document/247783797/Antonio-Damasio-Ao-Encontro-de-Espinosa>. Acesso em: 06 Set 2017.

DANHIEUX, Pieter. Ataques de Phishing. **The SANS Institute**. fev., 2013.OUCH!. Disponível em<http://www.ticorporativa.df.gov.br/conscientizacao-em-sic/cartilhas-e-manuais/doc_downloa d/88-ataques-de-phishing-ouch--fevereiro-de-2013.html>. Acesso em: 17 Out 2017.

DELLA VALLE, James; ULBRICH, Henrique Cesar. **Universidade Hacker**. 4. ed. São Paulo: Digerati Books, f. 331, 2004. Disponível em<https://tsilvestre.files.wordpress.com/2012/06/universidade-hacker.pdf>. Acesso em: 29 Jun 2017.

DIMANTAS, Hernani. **Linkania**: Uma teoria de redes. São Paulo: Senac, 2010. Disponível em <https://autoriaemrede.files.wordpress.com/2016/01/linkania-uma_teoria_de_redes.pdf>. Acesso em: 28 Ago 2017.

EKMAN, P. et al. Darwin deception and Facial Expression. **Annals of the New York Academy of Sciences**. New York. jun, 2003. 205-221 p. Disponível em<http://www.paulekman.com/downloadablearticles.html;>. Acesso em: 28 Set 2017.

EKMAN, Paul; FRIENSEN, Wallace V.. Facial Action Coding System. **Consulting Psychologists Press**. Palo Alto, n. 6, 1978.

ENEMBRECK, Fabricio et al. Identificando Emoções Em Redes Sociais: Um Estudo de Caso no Facebook. **Revista Eletrônica Científica Inovação e Tecnologia**. Curitiba, v. 2, n. 10, 2014. Disponível em <https://periodicos.utfpr.edu.br/recit/article/download/4308/Williana>. Acesso em: 23 Ago 2017.

ESPERIDIÃO-ANTONIO, V. et al. Neurobiologia das emoções. **Revista de Psiquiatria Clínica**, n. 35. 2008. 55-65 p. Disponível em <http://files.psicologandoja.webnode.com.br/200000059-0b6d60beb0/Neurobiologia%20das%20emoções.pdf>. Acesso em: 18 Set 2017.

FACEBOOK, . Declaração de Direitos e Responsabilidades. **Facebook**. 2017. Disponível em: <https://www.facebook.com/legal/terms>. Acesso em: 14 Dez. 2017.

FERNANDES, Jorge Henrique Cabral; SOUZA, Raul Carvalho de. Um estudo sobre a confiança em segurança da informação focado na prevenção a ataques de engenharia social nas comunicações digitais. **Brazilian Journal of Information Studies**. Brasília, n. 10, 2016. 63-75 p. Research Trends. Disponível

em<https://www.researchgate.net/publication/299451577_UM_ESTUDO_SOBRE_A_CONFIANCA_EM_SEGURANCA_DA_INFORMACAO_FOCADO_NA_PREVENCAO_A_ATAQ UES_DE_ENGENHARIA_SOCIAL_NAS_COMUNICACOES_DIGITAIS>. Acesso em: 28 Ago 2017.

FERRARI, Bruno et al. Ele sabe tudo sobre você. **Revista Epoca**. 25. 01, 2013. Disponível em <http://revistaepoca.globo.com/vida/noticia/2012/02/ele-sabe-tudo-sobre-voce.html>. Acesso em: 09 Out 2017.

FREIRE, Claudia Pontes. **Método de Monitoramento de Redes Sociais**: Epistemologia, técnicas e propostas de mineração de banco de dados para conteúdos gerados por fãs de telenovela em redes sociais. São Paulo, f. 399, 2015. 399 p. Tese (Ciências da Comunicação)-Escola de Comunicações e Artes da Universidade de São Paulo, 2015 Disponível em<www.teses.usp.br/teses/disponiveis/27/27152/tde-24112015.../ClaudiaPontesFreire.pdf>. Acesso em: 03 Mai 2017.

FREITAS-MAGALHÃES, A.. **A Psicologia das emoções**: O fascínio do rosto humano. 3. ed. Porto: Leya Portugal, 2011. Disponível em<http://pdf.leya.com/2013/Sep/a_psicologia_das_emocoes_nea.pdf>. Acesso em: 05 Set 2017.

_____. **O código de Ekman**: O cérebro, a face e a emoção. FEELab Science Books, 2013. Disponível em<https://pt.scribd.com/document/285591719/O-Codigo-de-Ekman-O-Cerebro-a-Face-e-a-Em ocao-pdf>. Acesso em: 20 Set 2017.

HAASE, Vitor Geraldi; LACERDA, Shirley Silva. Neuroplasticidade, variação interindividual e recuperação funcional em neuropsicologia. **Temas em Psicologia**. Ribeirão Preto, v. 12, n. 1. jun, 2004. Disponível em<http://pepsic.bvsalud.org/scielo.php?script=sci_arttext&pid=S1413-389X2004000100004>. Acesso em: 06 Out 2017.

INFOGLOBO, Comunicação e Participações S.A.. O que se sabe até agora sobre o jogo da "Baleia azul". O Globo, ano 2017, 20 Apr 2017. Disponível em <http://oglobo.globo.com/sociedade/o-que-se-sabe-ate-agora-sobre-jogo-da-baleia-azul-21236180#ixzz4fByG3Xjm>. Acesso em: 24 Apr 2017.

JUNIOR, Guilherme. Entendendo o que é Engenharia Social. **Viva o linux**. 2006. Disponível em <https://www.vivaolinux.com.br/artigo/Entendendo-o-que-e-Engenharia-Social>. Acesso em: 26 Out 2017.

KEMP, Simon. DIGITAL IN 2017: GLOBAL OVERVIEW. **We are Social**. 14. jan, 2017. 537 p. Disponível em<https://wearesocial.com/special-reports/digital-in-2017-global-overview>. Acesso em: 06 Jul 2017.

KRISTENSEN, Christian Haag et al. Normas brasileiras para o Affective Norms for English Words. **Trends in Psychiatry and Psychotherapy**. Porto Alegre, v. 33, n. 3. out-dez, 2011. 135-146 p. Associação de Psiquiatria do Rio Grande do Sul. Disponível em <http://www.redalyc.org/pdf/3110/311026370001.pdf>. Acesso em: 18 Set 2017.

LAKATOS, Eva Maria; MARCONE, Marina de Andrade. **Fundamentos da Metodologia Cientifica**. 5. ed. São Paulo: Atlas, f. 310, 2003. 310 p. Disponível em <https://docente.ifrn.edu.br/olivianeta/disciplinas/copy_of_historia-i/historia-ii/china-e-india>. Acesso em: 05 Set 2017.

MACHADO, Felipe Ribeiro. **Segurança da Informação numa perspectiva mais humana. Falhas internas e procedimentos de prevenção e defesa da rede**. Recife, f. 65, 2009. 55 p. Monografia (Ciências da Computação)-Universidade Federal de Pernambuco, 2009 Disponível em <http://www.cin.ufpe.br/~tg/2009-1/frm.pdf>. Acesso em: 14 Fev 2017.
MARCELO, Antonio; PEREIRA, Marcos. **A Arte de Hackear Pessoas**. Rio de Janeiro: Brasport, 2005.

MARCELO, Antonio; PEREIRA, Marcos. **A Arte de Hackear Pessoas**. Rio de Janeiro: Brasport, 2005. Disponível em: <https://books.google.com.br/books?id=yBVNt5Ei6ikC&printsec=frontcover&hl=pt-BR#v=onepage&q&f=false>. Acesso em: 18 Out. 2017.
MARCIANO, João Luiz Pereira. **Segurança da Informação - uma abordagem social**. Brasilia, f. 212, 2006.Tese (Ciência da Informação)-Universidade de Brasília, 2006 Disponível em <http://www.enancib.ppgci.ufba.br/premio/UnB_Marciano.pdf>. Acesso em: 04 Set 2017.

MARTINAZZO, Barbara. **Um método de identificação de emoções em textos curtos para o português do Brasil**. Curitiba, f. 82, 2010. 68 p. Disertação (Mestrado em Informática)-Pontifícia Universidade Católica do Paraná, 2010 Disponível em <https://www.ppgia.pucpr.br/~paraiso/mineracaodeemocoes/recursos/barbara_martinazzo_versaofinal.pdf>. Acesso em: 11 Set 2017.

MITNICK, Kevin; SIMON, William L.. **A arte de enganar: Ataques de Hackers**: Controlando o Fator Humano na Segurança da Informação. Tradução Kátia Aparecida Roque. São Paulo: Pearson Education do Brasil Ltda, f. 286, 2003. 283 p. Tradução de: The art of 17 deception : controlling the human element of security. Disponível em <https://www.docdroid.net/Mq0Edkm/kevin-mitnick-a-arte-de-enganar.pdf.html>. Acesso em: 11 Jan 2017.

NEGRÃO, Celso; CAMARGO, Eleida Pereira de. **Design de Embalagem**: Do Marketing à Produção. São Paulo: Novatec, 2008. Disponível em <https://www.passeidireto.com/arquivo/25089587/design-de-embalagem---celso-negrao-e-eleida-camargo>. Acesso em: 26 Out 2017.

NORTON, . Norton Cyber Security Insights Report 2016: Comparação Global. **Symantec**. 2016. Disponível em:<https://www.symantec.com/content/dam/symantec/br/docs/reports/2016-norton-cyber-security-insights-comparisons-brazil-pt.pdf>. Acesso em: 13 Out. 2017.

_____. Relatório de Crimes Cibernéticos NORTON: O impacto humano. **Symantec**. 2010. Disponível em:<http://www.symantec.com/content/en/us/home_homeoffice/media/pdf/cybercrime_report/Norton_Portuguese-Human%20Impact-A4_Aug18.pdf>. Acesso em: 10 Out. 2017.

PAIM, Aldo Marcelo. **Inferência de personalidade a partir de textos em português brasileiro utilizando léxicos**. Curitiba, f. 184, 2016. 160 p. Disertação (Pós-Graduação em Informática)-Pontifícia Universidade Católica do Paraná, 2016 Disponível em <https://www.ppgia.pucpr.br/pt/arquivos/mestrado/dissertacoes/2016/Aldo_Dissertacao.pdf>. Acesso em: 14 Set 2017.

PEIXOTO, Mário Cesar Pintaudi. **Engenharia Social e Segurança da Informação na Gestão Corporativa**. Rio de Janeiro: Brasport, 2006.

POLONI, Katia Maria; TOMAÉ, Maria Inês. Coleta De Dados Em Plataformas De Redes Sociais: Estudo De Aplicativos In: WORKSHOP DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO, 3. 2014. Londrina, 2014. Disponível em <http://rabci.org/rabci/sites/default/files/222-838-1-PB_0.pdf>. Acesso em: 03 Jul 2017.

POPPER, Marcos Antonio; BRIGNOLI, Juliano Tonizetti. **ENGENHARIA SOCIAL**: Um Perigo Eminente. 2002.TCC (Gestão Empresarial e Estratégias de Informática)-Instituto Catarinense de Pós-Graduação, 2002 Disponível em <http://www.posuniasselvi.com.br/artigos/rev03-05.pdf>. Acesso em: 28 Ago 2017.

PRASS, Fernando Sarturi. **KDD – UMA VISAL GERAL DO PROCESSO**. Florianopolis, 2012.Trabalho de Disciplina ()-Faculdade Estácio de Sá de Santa Catarina, 2012 Disponível em <http://fp2.com.br/blog/wp-content/uploads/2012/07/KDD_Uma_visao_geral_do_processo.p df>. Acesso em: 14 Ago 2017.

RECUERO, Raquel. **Redes sociais na internet**. Porto Alegre: Sulina, 2009. 191 p. (Coleção Cibercultura) Disponível em <http://www.ichca.ufal.br/graduacao/biblioteconomia/v1/wp-content/uploads/redessociaisnai nternetrecuero.pdf>. Acesso em: 28 Ago 2017.

RIEDER, Bernhard. Studying Facebook via data extraction: the Netvizz application In: PROCEEDINGS OF THE 5TH ANNUAL ACM WEB SCIENCE CONFERENCE, 13. 2013. Paris: WebSci, 2013. 346-355 p. Disponível em <https://dl.acm.org/citation.cfm?doid=2464464.2464475>. Acesso em: 08 Out 2017.

ROSA, Adriano Carlos; SILVA, Bruno Donizete da; SILVA, Pedro Lemes da. Análise de Redes Sociais Aplicada à Engenharia Social In: SIMPÓSIO INTERNACIONAL DE GESTÃO DE PROJETOS, 1. 1. São Paulo, 2012. Disponível em <https://www.researchgate.net/publication/304051118_ANALISE_DE_REDES_SOCIAIS_APLICADA_A_ENGENHARIA_SOCIAL>. Acesso em: 10 Jul 2017.

SANTOS, Denise Cristiane dos. **Coleta Automatizada e Análise de Dados em Fan Pages do Facebook**. Curitiba, 2014.TCC ()-Universidade Federal do Paraná, 2014 Disponível em <http://www.ppgcgti.ufpr.br/publicacoes/download/50_2b41064d59adee16d75d516faa2672a9.html>. Acesso em: 29 Ago 2017.

SANTOS, Luciano Alves Lunguinho. **O impacto da engenharia social na segurança da informação**. Aracaju, f. 83, 2004. 83 p. Monografia (Pós Graduação em Redes de Computadores)-Universidades de Tiradentes, 2004 Disponível em <http://docslide.com.br/download/link/o-impacto-da-engenharia-social-na-seguranca-da-informacao-55c450c92f1cf>. Acesso em: 26 Abr 2017.

SANTOS, Yuri Rafael de Lima. **A Engenharia Social nas Redes Sociais Oline**. Barra dos Bugres, f. 75, 2014. 73 p. TCC (Ciência da Computação)-UNIVERSIDADE DO ESTADO DE MATO GROSSO, 2014 Disponível em <http://www.ebah.com.br/content/ABAAAgzFwAE/a-engenharia-social-nas-redes-sociais-online>. Acesso em: 03 Abr 2017.

SCHNEIER, Bruce. People, Process, and Technology. **Schneier on Security**. 2013. Disponível em <https://www.schneier.com/blog/archives/2013/01/people_process.html>. Acesso em: 02 Ago 2017.

SHIMAKURA, Silvia E.. Interpretação do coeficiente de correlação. **UFPR.BR**. Curitiba, 2006. Disponível em <http://leg.ufpr.br/~silvia/CE003/node74.html>. Acesso em: 27 Out 2017.

SILVA, Antonio Braz de Oliveira. **O cluster da construção em Minas Gerais e as práticas de colaboração e de gestão do conhecimento**: um estudo das empresas da Região Metropolitana de Belo Horizonte (MG). Belo Horizonte, f. 419, 2007. 419 p. Disertação (Programa de Pós-Graduação em Ciência da Informação))-UNIVERSIDADE FEDERAL DE MINAS GERAIS – UFMG ESCOLA DE CIÊNCIA DA INFORMAÇÃO, 2007 Disponível Em <http://www.bibliotecadigital.ufmg.br/dspace/bitstream/handle/1843/EARM-73FNWC/douto rado_antonio_braz_de_oliveira_e_silva.pdf?sequence=1>. Acesso em: 21 Abr 2017.

SILVA, Maicon H.L.F.; COSTA, Veridiana A.SF.. O fator humano como pilar da Segurança da Informação: uma proposta alternativa In: JORNADA DE ENSINO PESQUISA E EXTENSÃO . 9. Recife, 2009. Disponível em

<http://www.eventosufrpe.com.br/jepex2009/cd/resumos/R0052-3.pdf>. Acesso em: 11 Set 2017.

SILVA, Tarcízio; STABILE (ORGS.), Max. **Monitoramento e pesquisa em mídias sociais**: Metodologias, aplicações e inovações. São Paulo: Uva Limão, f. 367, 2016. 364 p. Disponível em <http://www.ibpad.com.br/wp-content/uploads/2016/11/Monitoramento-e-pesquisa-em-midia s-sociais.pdf>. Acesso em: 27 Jun 2017.

STRONGMAN, K. T.. **A psicologia da emoção**. 4. ed. Lisboa: Climepsi Editores, 1998.

TF-IDF. **Tfidf**. 2017. Disponível em <http://www.tfidf.com/>. Acesso em: 12 Out 2017.

TRASK, R. L.. **Dicionário de Linguagem e Linguística**. Tradução Rodolfo Ilari. São Paulo: Contexto, 2004.

WELLMAN, Barry. **FOR A SOCIAL NETWORK ANALYSIS OF COMPUTER NETWORKS**: A Sociological Perspective on Collaborative Work and Virtual Community. Toronto, f. 11, 1996. 11 p. Monografia ()-Universidade de Toronto, 1996 Disponível em <http://courses.ischool.utexas.edu/~i385q/spring2005/readings/Wellman-1996-ForASocial.pdf>. Acesso em: 01 Set 2017.

ANEXO A — Normas brasileiras para o Affective Norms for English Words

Palavra	Valência	DP	Alerta	DP	Palavra	Valência	DP	Alerta	DP
Abalado	2,58	1,81	5,11	2,82	Alvorecer	6,24	2,38	3,09	2,22
Abandonado	1,85	1,7	5,48	2,49	Amabilidade	7,68	2,04	3,5	2,96
Abdução	5	1,85	3,36	2,14	Amado	8,31	1,39	3,49	3
Abelhas	4,58	2,45	4,38	2,83	Amarelo	6,76	2,29	3,11	2,38
Abençoado	8,03	1,84	3,19	3,03	Amável	8,09	1,6	3,4	2,88
Aborto	1,67	1,37	6,42	2,93	Ambição	5	3,08	5,92	3
Abraçar	8,63	1,2	4,3	3,34	Ambulância	2,47	2,28	6,3	3
Abraço	8,77	0,75	3,38	3	Ameaça	1,87	1,68	6,71	2,73
Abrasador	5,43	1,91	3,53	2,49	Amigável	8,25	1,34	3,36	2,93
Abrigado	7,61	1,98	3,21	2,41	Amigo	8,74	0,79	3,68	3,24
Absurdo	2,79	2,12	5,81	2,74	Amor	8,75	0,89	4,39	3,57
Abundância	6,94	2,05	4,19	2,48	Angustiado	2,22	1,9	6,65	2,32
Abuso	2,76	2,65	6,5	2,65	Animação	8,33	1,43	4,64	3,03
Acalmar	7,23	1,81	2,68	2,05	Aniversário	8,39	1,22	4,71	3,34
Acanhado	3,89	2,01	5,03	2,75	Anjo	8,06	1,59	2,45	2,16
Acaso	6,17	2,1	4,28	2,48	Anseio	5,11	2,48	5,18	2,5
Aceitação	7,21	2,16	4,63	2,94	Ansioso	3,5	2,44	7,05	2,44
Acidente	1,67	1,63	6,98	3,02	Aparelho	6	2,29	3,13	2,58
Aconchegante	8,29	1,69	3,76	2,94	Apático	3,21	2,02	4,93	2,69
Aconchego	8,4	1,01	2,68	2,67	Aplauso	8,21	1,17	4,95	3,25
Acordo	6,89	2,01	3,37	2,25	Aprender	7,86	1,81	4,78	3,03
Açúcar	7,04	1,71	3,91	2,58	Ar	8,39	1,24	2,57	2,72
Adaga	4,32	2,3	4,27	2,46	Aranha	3,49	2,26	5,62	2,85
Admirado	7,67	1,53	4,49	2,82	Arma	2,24	2,5	6,97	2,5
Adorável	8,24	1,57	4	3,26	Armamento	2,17	1,65	6,45	2,97
Adulto	6,49	1,99	3,75	2,46	Armário	6,11	1,72	3,21	2,2
Afeição	7,82	1,9	3,84	2,89	Arrependido	3,46	2,46	5,2	2,64
Afinar	5,8	1,54	3,65	2,09	Arrogante	2,05	1,9	6,32	2,77
Afogar	2,53	2,26	6,24	2,61	Arrumado	7,78	1,82	3,24	2,39
Agilidade	7,5	1,58	5,33	2,84	Arte	8,08	1,5	3,68	3,21
Agonia	2,05	1,97	6,61	2,7	Árvore	7,98	1,46	2,27	2,19
Agradável	8,15	1,25	3,18	2,49	Ás	5,71	2	3,84	2,6
Agradecido	8,42	1,52	3,32	2,98	Áspero	3,38	2,34	5,49	2,53
Agressivo	1,89	1,66	6,67	2,99	Assaltante	2,03	2,25	7,24	2,7
Água	8,35	1,4	3	2,9	Assalto	1,47	1,1	7,67	2,25
Agulha	4,04	1,98	4,93	2,54	Assar	6,24	2,73	3,92	2,7
Alcoólico	2,76	2,84	6,34	2,68	Assassino	1,16	0,8	7,51	2,5
Alegre	8,44	1,07	4,04	2,97	Assento	5,87	2,07	3,05	2,2

Palavra	Valência	DP	Alerta	DP	Palavra	Valência	DP	Alerta	DP
Alegria	8,61	1,46	4,87	3,44	Assovio	6,15	2,15	4,48	2,62
Alergia	4,02	3,31	5,2	3	Assustado	2,89	2,17	6	2,54
Alerta	6,08	2,42	5,08	2,94	Astronauta	5,81	1,66	3,84	2,45
Alerto	5,67	2,06	4,95	2,64	Atadura	2,87	2,26	4,5	2,89
Alimento	8,26	1,27	3,61	3,07	Aterrorizado	1,79	1,46	7,32	2,53
Ativar	7,19	1,82	4,19	2,6	Branco	7,18	2,08	2,61	2,47
Atletismo	7,31	2,13	4,27	2,5	Bravo	2,56	2,2	6,31	2,87
Atração	8,22	1,49	4,84	3,43	Brilhante	7,45	1,81	3,21	2,43
Aurora	6,96	2,21	3,02	2,42	Brinquedo	7,54	1,77	3,56	2,45
Autonomia	7,71	1,92	4,29	3,1	Brisa	7,39	2,11	2,76	2,8
Avalanche	2,32	2,1	6,02	2,9	Brutal	1,98	1,84	6,6	2,77
Avenida	5,84	1,84	3,76	2,4	Buquê	7,42	2,41	3,74	3,19
Aventura	8,06	1,53	6,33	2,97	Burro	2,96	1,9	4,7	2,73
Avô	7,18	2,8	4,05	2,9	Cabana	7,21	1,74	3,21	2,68
Azedo	2,87	2,04	4,42	2,13	Cabelo	6,67	2,41	3,78	2,64
Azul	7,42	2,32	3,37	2,78	Cachoeira	8,14	1,65	3,84	3,35
Bacia	4,68	1,84	3,59	2,53	Cachorro	7,98	1,46	3,98	2,8
Bagunçado	3,21	2,28	5,92	2,61	Cadáver	1,7	1,63	6,08	2,95
Bala	6,98	1,99	3,44	2,45	Cadeia	2,02	1,97	5,7	3,2
Bandeira	6,32	1,65	3	2,25	Cadeira	6,3	1,81	2,76	1,72
Banheira	8	1,37	3	2,69	Caderno	5,76	1,85	4,02	2,15
Banheiro	6,82	1,72	3	2,51	Caixão	1,92	1,85	6,08	3,13
Banho	8,29	1,5	2,61	2,74	Calor	6,14	2,68	5,35	2,76
Banqueta	5,84	1,98	2,61	1,76	Cama	8,08	1,36	3,28	2,93
Barata	2,83	1,89	5,23	3,17	Caminhão	4,96	1,76	4,27	2,25
Barra	4,74	1,91	4,37	2,38	Campeão	8,43	1,21	5,03	3,34
Barril	5,85	2,11	4,28	2,58	Campo	7,61	1,78	3,09	2,79
Bastardo	3,42	2,5	4,16	2,66	Canção	8,35	1,53	3,7	3,31
Bebê	8,21	1,41	3,71	2,73	Câncer	1,49	1,19	6,98	2,84
Bebida	6,03	2,79	4,08	3,03	Canhão	2,38	1,99	5,78	2,62
Beco	3,02	2,06	5,8	2,9	Cansado	2,39	1,88	5,39	3,26
Beijo	8,76	0,79	5,24	3,74	Caos	2,05	2	6,51	2,79
Beleza	8,09	1,25	3,91	2,84	Capaz	7,63	1,88	4,89	2,95
Beliscar	3,71	2,37	4,82	2,66	Carcaça	3,75	2,23	4,29	2,72
Belo	7,73	1,77	3,29	2,53	Cárcere	1,89	1,55	5,95	2,84
Benzer	6,5	2,06	2,76	2,68	Carícia	8,78	0,58	4,42	3,51
Berçário	7,6	1,7	3,3	2,33	Cárie	2,27	1,92	5,71	2,91
Berrar	3,63	2,36	6,21	2,73	Carinhoso	8,73	0,8	4,42	3,52
Besta	2,45	1,93	5,3	2,76	Caroço	3,81	1,83	4,49	2,77
Bispo	5,68	2,51	2,71	2,4	Carro	7,95	1,78	4,36	3,19
Blasfêmia	2,63	1,78	5,71	2,6	Carta	7,02	2,05	4,2	2,37
Bobagem	4,84	2,48	4,76	2,78	Casa	8,14	1,58	3,35	2,99

Palavra	Valência	DP	Alerta	DP	Palavra	Valência	DP	Alerta	DP
Bolinho	7,5	1,54	3,4	2,47	Casal	7,84	1,91	4,09	3,05
Bolo	7,37	2,01	3,26	2,64	Casamento	7,59	2,03	4,57	3,27
Bom	8,19	1,53	3,36	2,65	Cassino	5,21	2,71	4,98	2,71
Bomba	1,53	1,39	6,87	2,56	Cavalo	6,89	1,93	3,24	2,68
Boneca	5,57	2,19	3,05	2,24	Caveira	2,61	1,77	5,07	2,75
Bonito	8,42	1,41	3,45	2,94	Cédula	7,43	2,1	4,76	2,86
Borboleta	7,38	1,82	2,56	1,88	Cefaléia	2,92	1,89	5,47	2,67
Boxeador	4,13	2,5	5,34	2,5	Cego	2,35	1,87	4,68	2,65
Brabeza	2,83	2,15	6,02	2,71	Célula	5,06	2,06	3,02	2,2
Brabo	2,26	1,83	6,05	2,7	Cemitério	2,22	1,9	5,27	3,06
Braço	6,35	2,12	3,64	2,12	Cesta	6,06	1,71	3,33	2,28
Cético	4,89	1,8	3,61	1,96	Continência	4,4	1,91	3,81	2,69
Céu	8,1	1,21	2,76	2,3	Controle	5,75	2,28	5,04	2,65
Chacina	1,43	1,48	6,86	2,78	Cor	7,65	1,63	3,48	2,94
Chaleira	5,19	1,7	3,02	2,16	Coração	7,73	1,93	4,88	3,17
Chamuscar	4,46	2,1	4,24	2,37	Coragem	7,96	1,65	5,19	3,01
Chantagem	1,61	1,44	6,84	2,77	Corda	4,53	1,72	3,96	2,36
Chapéu	6,16	1,85	2,54	1,74	Cordeiro	5,56	2,05	2,58	2,29
Charme	7,63	1,77	5,35	2,75	Coroa	5,58	1,94	3,76	2,37
Chateação	2,3	2,28	6	2,7	Corpo	6,94	2,34	4,67	2,79
Chave	5,46	1,79	3,36	2,4	Corredor	5,3	1,76	4,27	2,54
Chocalho	5,73	1,94	3,12	2,29	Corrupto	1,63	1,18	6,04	3,11
Chocolate	8,08	1,4	4,88	3,03	Corte	3,3	1,81	5,09	2,69
Chute	4,4	2,4	4,27	2,75	Cortesia	8,02	1,42	3,6	2,96
Chuva	5,54	2,51	4,47	2,73	Cortiça	5	1,32	3,68	2,31
Cicatriz	3,23	1,99	3,98	2,6	Cortinas	5,88	1,84	2,42	2,04
Ciclone	2,67	1,99	6,04	2,77	Coruja	5,68	1,86	3,57	2,39
Cidade	6,41	2,12	4,71	2,7	Costa	5,54	1,92	3,5	2,58
Cinema	8,25	1,4	4,75	3,3	Costume	5,42	1,82	3,87	2,45
Circo	6,77	2,08	3,1	2,49	Cotovelo	4,88	1,72	2,4	2,02
Círculo	5,29	1,49	3,71	2,31	Covarde	2,51	1,77	5,45	2,66
Cirurgia	2,85	2,34	5,81	2,8	Cozinheiro	6,79	2	3,4	2,8
Ciúme	2,86	1,84	6,05	2,45	Crepúsculo	5,34	2,06	4,28	2,54
Cobertura	7,33	1,74	3,57	3,08	Criança	7,92	1,83	4,08	3,04
Cobra	2,68	1,86	6,16	2,73	Crime	1,72	1,55	6,45	3
Coelhinho	7,31	1,68	2,83	2,5	Criminoso	1,75	1,63	6,27	2,98
Coelho	6,96	1,7	3,41	2,5	Crise	2,31	1,73	5,97	2,73
Cofre	6,13	1,83	3,63	2,84	Cru	3,58	2,18	3,1	2,69
Cogumelo	5,35	1,64	3,35	2,36	Crucificar	2,36	1,62	5,32	2,97
Colete	4,63	1,92	3	2,33	Cruel	1,67	1,39	5,58	3,1
Colisão	2,4	1,75	6,16	2,66	Culinária	7,03	2,23	4,51	3,05
Coluna	4,65	2,1	3,92	3,03	Culpado	2,27	1,57	5,19	2,84

Palavra	Valência	DP	Alerta	DP	Palavra	Valência	DP	Alerta	DP
Comédia	8,39	1,25	4,4	3,29	Cupim	2,99	1,85	4,56	3,03
Comer	7,42	2,22	4,58	2,94	Curar	7,83	1,74	4,42	3,09
Complacente	4,71	1,5	3,95	2,26	Curioso	6,77	1,82	5,48	2,57
Comprometido	6,33	2,53	4,65	3,08	Dádiva	7,73	1,75	3,31	2,81
Computador	6,62	1,98	4,66	2,62	Dançarino	6,7	2,2	4,33	3,09
Concentrado	6,71	2,14	4,1	2,87	Dano	2,32	1,78	4,72	2,69
Confiança	7,97	2,08	4,67	3,31	Débil	3,13	1,83	3,86	2,55
Confiante	7,42	1,99	4,64	3,09	Débito	2,47	1,82	5,3	2,84
Conforto	8,03	1,53	4,17	3,12	Decepcionar	1,76	1,28	6,09	2,7
Confuso	2,54	1,61	5,83	3	Decompor	3,94	2,06	2,92	2,24
Conhecimento	8,29	1,32	5,08	3,32	Decorar	6,22	2,78	4,72	2,9
Cônjuge	6,02	2,52	4,23	3,18	Dedo	5,75	1,87	2,56	2,31
Consolado	5,36	2,11	3,55	2,44	Defeito	3,15	1,99	5,17	2,54
Constrangido	2,96	1,41	5,15	2,73	Deficiente	3,13	1,91	4,13	2,92
Contentamento	6,72	2,33	4,18	2,84	Deformado	2,43	1,78	4,95	2,89
Conteúdo	7,04	1,87	3,81	2,6	Deleite	5,53	2,14	2,82	2,37
Contexto	5,36	1,56	3,99	2,32	Delicado	6,3	2,11	3,72	2,57
Demônio	2,1	1,67	4,49	3,25	Doente	1,69	1,19	5,29	2,94
Demorado	2,94	2,14	6	2,81	Dólar	5,45	2,44	5,09	2,73
Dentista	5,18	2,51	4,02	2,65	Dominador	3,96	2,15	4,71	2,8
Depressão	1,96	1,55	5,69	3,05	Dor	1,91	1,65	5,97	2,87
Deprimente	1,82	1,29	4,88	3,11	Doutor	4,84	2,22	3,86	2,68
Deprimido	2,2	1,58	5,12	2,73	Duro	4,41	2,13	4,6	2,64
Derrotado	1,69	1,33	5	3,13	Edifício	5,76	1,88	2,49	1,8
Desafiante	4,37	2,93	5,64	2,86	Educação	8,04	1,75	4,92	3,07
Desafio	7,2	1,97	6	2,84	Egoísta	2,04	1,78	5,33	2,89
Desagradado	4,83	2,49	5,68	2,38	Elegante	7,38	1,76	4,62	2,68
Desajeitado	3,67	1,95	3,65	2,4	Elevador	5,37	1,98	3,24	2,39
Desamparado	2,48	1,65	5	2,62	Emprego	7,31	2,18	5,97	2,88
Desanimado	1,84	1,3	4,47	3,04	Encardido	3,08	1,59	4,02	2,53
Desastre	1,84	1,56	5,97	2,93	Encharpe	5,59	1,8	3,64	2,34
Desavença	1,98	1,42	5,44	2,83	Encontro	7,67	2,1	5,67	2,86
Desconforto	2,31	1,76	5,6	2,86	Enfermeira	5,33	2,2	4,39	2,47
Desculpa	5,9	2,67	4,37	2,83	Enferrujado	3,41	1,68	3,25	2,18
Desdenhoso	3,01	1,75	4,86	2,52	Enfurecido	2,67	2,09	6,89	2,17
Desejo	7,78	1,72	5,06	2,9	Enganação	1,76	1,56	6,31	2,91
Desertor	3,72	1,59	4,58	2,19	Enjoativo	2,63	1,5	4,72	2,45
Desesperador	1,92	1,58	6,12	3,11	Enlameado	3,57	1,83	3,65	2,54
Desinteressado	3,46	1,9	5,16	2,65	Entediado	2,44	1,92	5,19	2,83
Desleal	1,63	1,3	5,9	3,17	Enterro	1,65	1,32	5,31	3,31
Desligado	3,31	1,86	5,13	2,64	Entulho	3,61	2,12	3,54	6,56
Despejar	4,08	2,04	3,92	2,81	Entusiasmo	8,02	1,83	4,78	3,11

Palavra	Valência	DP	Alerta	DP	Palavra	Valência	DP	Alerta	DP
Desperdício	3,45	1,89	4,99	2,5	Envergonhado	3,29	1,95	5,33	2,42
Despreocupado	5,33	2,7	3,35	2,45	Erótico	7,31	2,03	4,8	3,21
Desprezar	2,08	1,67	5,91	2,87	Erro	2,43	1,91	6,4	2,57
Desprezo	1,71	1,32	4,96	3,18	Erudito	5,47	1,97	2,86	2,31
Destacado	6,82	1,81	4,53	2,57	Esbanjamento	3,47	2,29	5,25	2,64
Destroçar	2,53	1,79	4,39	3	Escaldante	4,2	1,89	3,86	2,76
Destruição	2,13	1,93	5,88	2,81	Escândalo	3,31	2,22	5,51	2,73
Destruir	2	1,68	5,35	3,17	Esconder	4,08	1,91	4,51	2,78
Detalhe	6,36	1,8	4,4	2,67	Escorbuto	3,77	1,94	4,03	2,55
Detestar	2,29	1,71	4,39	3,08	Escorpião	3,53	2,11	4,61	2,91
Deus	8,11	1,54	3,8	3,15	Escravo	2,36	2,21	5,82	2,93
Devotado	5,8	2,01	2,82	2,37	Escritor	7,02	1,92	2,57	1,81
Diabo	2,67	2,2	4,63	2,86	Escritório	5,7	2,18	4,41	2,39
Diamante	7,22	2,09	4,1	2,88	Escuro	4,49	2,26	3,67	2,86
Digno	7,69	1,67	4,01	2,75	Esfera	5,43	1,65	3,53	2,43
Dinheiro	7,2	2,52	5,39	3,03	Esfomeado	3,61	2,66	5,22	2,89
Diploma	8,33	1,39	6,03	3,05	Esmagado	2,54	1,85	5,46	2,69
Diversão	8,31	1,76	5,16	3,2	Esnobe	1,96	1,41	5,22	3,03
Divertido	8,57	1,26	5,12	3,42	Espaço	6,88	2,13	4,39	2,79
Divertimento	8,27	1,56	4,88	3,24	Espantado	4,47	1,93	4,8	2,87
Divórcio	2,97	2,06	5,29	2,96	Esperança	8,29	1,37	5,04	3,11
Doce	7,88	1,75	4,46	3,2	Esperançoso	7,55	1,87	4,08	2,76
Doença	1,77	1,57	5,81	3,2	Espingarda	2,82	2,28	5,66	2,85
Espinho	2,98	1,7	4,45	2,89	Fedor	5,58	3,61	5,43	3,43
Espírito	6,87	2,04	4,27	2,7	Feito	3,17	2,25	4,15	2,64
Esposa	5,8	2,34	3,71	2,72	Feliz	8,69	1	4,13	3,44
Espuma	6,77	1,95	3,71	2,75	Feno	4,65	1,62	3,24	2,29
Esquina	4,67	1,45	3,27	2,48	Feriado	4,99	3,49	4,55	3,23
Estagnado	3,54	1,97	4,86	2,31	Férias	8,62	1,5	5,87	3,6
Estátua	4,88	2,06	2,53	2,22	Feridas	4,29	2,52	4,65	2,51
Esterco	3,26	1,93	3,76	2,6	Ferimento	2,54	1,84	5,08	2,59
Estômago	5,14	2,15	3,71	2,45	Ferramenta	7,07	2,11	4,78	2,79
Estrangeiro	6	1,91	4,22	2,48	Ferro	4,91	1,72	3,84	2,06
Estranho	4,58	1,73	5,16	1,93	Festa	8,22	1,63	4,49	3,31
Estrela	7,75	2,01	3,57	3,07	Festivo	8,09	1,76	5,54	3,31
Estresse	2,22	1,77	6,51	2,77	Filhote	6,88	2,03	3,96	2,38
Estupendo	3,88	3,47	6,67	3,03	Firmamento	6,66	2,19	4	2,93
Estúpido	2,21	1,98	6,18	2,71	Firme	6,97	2,04	3,94	2,46
Estupro	4,94	3,29	5,1	2,9	Flácido	2,43	1,97	4,77	2,9
Evento	7,03	2,4	4,51	2,93	Flexível	7,25	2,29	4,06	2,74
Exame	4,22	2,13	3,93	11,52	Flor	8,11	1,67	3,17	2,95
Excelência	6,24	2,13	4,35	2,41	Florescer	6,38	2,49	3,31	2,49

Palavra	Valência	DP	Alerta	DP	Palavra	Valência	DP	Alerta	DP
Excitação	7,73	1,75	6,26	3,01	Fofoca	2,44	2,29	5,65	3,11
Excursão	7,82	2,04	4,85	3,15	Fogão	4,71	2,75	4,76	3,02
Execução	3,92	2,92	4,79	2,75	Fogo	4,55	2,68	5,35	2,68
Exercício	6,68	2,36	4,7	2,82	Força	4,62	2,46	4,76	2,77
Exército	4,67	2,3	4,76	2,58	Forte	7,66	1,66	4,66	3,01
Êxtase	7,34	1,92	5,44	2,77	Fortuito	6,61	2,07	3,91	2,6
Exultante	5,97	2,1	4,29	2,71	Fotografia	7,71	1,96	4,61	3,15
Faca	3,9	1,96	5,21	2,45	Fragrância	5,98	2,51	3,8	2,45
Fácil	7,31	2,16	3,49	2,91	Fraude	1,6	1,47	6	2,82
Faixa	4,67	1,14	4,24	1,64	Freira	4,89	2,49	3,91	2,62
Falcão	5,82	2,04	3,97	2,52	Frígida	2,43	2,07	4,79	2,78
Falha	2,03	1,46	6,93	2,18	Frio	4,45	2,71	4,85	2,7
Falido	2	1,73	5,4	3,06	Frustrado	1,84	1,57	5,84	2,84
FALSO	5,45	3,59	5,03	3,27	Fuga	3,63	2,39	5,26	2,82
Fama	6,73	2,04	5,38	2,76	Funeral	1,52	1,39	4,89	3,34
Família	7,07	2,22	4,09	3,05	Fungo	3,84	1,99	4,65	2,56
Faminto	2,94	2,54	5,7	2,89	Furacão	2,72	2,35	6,08	2,84
Famoso	5,76	2,08	4,24	2,23	Gabinete	5,35	1,87	3,88	2,38
Fantasia	7,06	2,08	5,18	2,9	Gangrena	2,64	2,05	4,81	2,81
Farol	6,75	1,99	5	2,7	Garfo	6,12	2,03	3,83	2,47
Farolete	5,2	1,81	3,4	2,26	Garotos	6,94	2,28	4,77	2,97
Fascinar	5,37	2,65	4,39	2,51	Garrafa	6,49	2,35	4,19	2,77
Fase	5,44	2,24	4,33	2,65	Gatinho	7,06	2,72	3,95	3,13
Fatigado	5,1	2,97	4,72	3,06	Gato	5,75	2,76	4,04	2,72
Favela	1,64	1,25	5,63	2,96	Gato	3,47	2,6	5,24	2,76
Favor	7,62	1,78	3,75	2,71	Geladeira	6,86	1,72	3,33	2,61
Favorito	7,27	2,07	5,12	2,84	Geléia	5,84	1,96	3,7	2,22
Fazenda	4,32	3,12	4,43	3,08	Geleira	4,33	2,37	3,59	2,31
Febre	2,2	1,65	4,9	2,91	Gênero	4,33	2,09	4,56	2,1
Gentil	8,23	1,53	3,38	2,95	Igreja	4,22	2,75	4,7	2,72
Germes	4,69	2,93	5,46	2,77	Imaginar	8,02	1,69	5,06	3,25
Ginasta	6,4	1,93	4,12	2,7	Imaturo	2,85	1,88	5,7	2,66
Glamour	5,26	2,04	4,13	2,28	Imoral	2,03	1,56	5	3
Glória	8,16	1,58	4,72	3,45	Implicar	4,69	2,8	5,47	2,63
Golfista	4	2,09	4,66	2,54	Impotente	2,08	1,54	5,34	3
Golpe	2,2	2,03	5,32	2,95	Impressionado	6,97	2,42	4,09	2,82
Gordo	4,78	3,02	4,82	2,92	Imundície	1,86	1,74	5,18	2,88
Gosto	7,57	1,67	4,31	2,74	Incentivo	4,76	3,25	5,4	2,67
Gracinha	7,15	2,02	3,73	2,82	Incomodado	2,45	1,9	5,66	2,64
Graduado	8,17	1,69	5,3	3,37	Incomodar	2,97	2,22	5,86	2,79
Grama	5,75	1,95	3,21	2,12	Incumbência	5,02	2,1	4,29	2,3
Gramado	7,75	1,85	3,9	3,18	Indiferente	4,37	2,37	4,59	2,24

Palavra	Valência	DP	Alerta	DP	Palavra	Valência	DP	Alerta	DP
Grampos	6,54	2,37	3,42	2,49	Indústria	5,63	2,55	4,5	2,5
Granada	2	2,05	6,03	3,16	Infante	2,99	2,11	5,24	2,84
Grito	4,42	2,44	6,19	2,31	Infecção	1,77	1,54	5,61	2,96
Grosso	2,71	1,98	5,88	2,63	Infeliz	1,54	1,37	6,2	3,01
Guerra	1,61	1,62	6,79	2,97	Inferior	2,49	1,86	4,5	2,73
Guilhotina	5,56	3,09	4,27	2,92	Inferno	3,81	2,85	4,88	3,13
Gula	3,88	2,54	4,94	2,67	Infiel	2,08	1,97	6,34	3,15
Habilidade	6,91	1,91	4,27	2,36	Inocente	3,74	2,53	5,45	2,68
Habitante	5,55	1,74	3,34	2,06	Insano	3,11	1,96	4,61	2,52
Hábito	4,13	2,48	4,95	2,39	Inseguro	2,26	1,48	6,02	2,55
Hemodiálise	3,78	2,42	4,9	2,94	Inseto	3,54	2,42	5,44	2,68
Heroína	5,35	3,23	4,89	3,18	Insolente	5,67	3,03	4,9	3
Hidrante	6,45	2,08	3,75	2,47	Insosso	3,55	1,92	4,21	2,6
Hidrofobia	3,48	2,16	3,67	2,74	Inspirado	4,72	3,51	5,48	3,24
História	3,54	3,08	5,48	3,23	Inspirar	7,31	2,15	4,03	3,1
Homem	6,85	2,78	4,47	3,16	Insulto	5,28	3,52	4,72	3,32
Homicida	5,13	3,44	5,54	3,09	Intelecto	6,8	2,37	4,33	2,49
Honesto	8,6	1,2	3,32	5,38	Inteligente	7,81	2,28	4,75	3,26
Honra	4,75	3,43	5,09	3,04	Intercurso	5,02	1,36	2,33	6,42
Horrível	1,98	1,78	5,55	2,84	Interesse	4,74	3,21	5,68	2,9
Horror	2,54	2,11	5,83	2,9	Íntimo	7,27	1,88	4,8	2,84
Hospital	2,75	2,55	5,39	3,18	Intrometer	2,4	1,81	5,73	2,67
Hostil	5,6	2,97	4,58	2,72	Intrometido	2,52	2	5,94	2,56
Hotel	7,11	2,02	3,79	2,84	Intruso	2,29	1,65	5,99	2,56
Humanitário	4,58	3,69	5,31	3,34	Inundação	1,88	1,68	6,02	2,8
Humbúrguer	6,91	2,47	4,19	2,8	Inútil	4,81	2,97	5,63	2,82
Humilde	7,66	1,88	3,6	2,69	Invasor	2,2	2,14	6,61	2,7
Humilhar	4,36	3,34	5,8	3,11	Investir	4,35	3,14	6,16	2,69
Humor	7,97	2,15	5,26	3,5	Irmão	7,78	2,15	5,11	3
Iate	6,73	1,98	3,97	2,37	Irritar	4,45	3,02	4,99	3,15
Idéia	8,14	1,6	5,31	3,32	Item	5,08	1,33	3,13	2,06
Identidade	7,35	1,92	4,5	2,9	Janela	7,29	2,13	3,32	2,71
Idiota	2,28	2	5,28	2,9	Janta	7,47	2,02	4,61	2,94
Ídolo	5,99	2,52	3,73	2,36	Jardim	5,85	2,8	4,52	3,03
Ignorância	2,11	1,83	5,57	2,99	Jarra	5,72	1,95	3,66	2,57
Jibóia	4,96	2,58	4,39	2,86	Malária	2,12	1,6	5	3,16
Jogo	6,34	2,35	4,89	2,66	Malcheiroso	1,8	1,34	4,89	3,04
Jóia	7,76	1,82	4,19	2,94	Malícia	4,47	2,59	4,43	2,89
Justiça	6,52	2,95	5,61	2,73	Maluco	4,31	2,66	5,46	2,57
Juventude	4,51	3,55	5,7	3,2	Malvado	2,09	1,78	5,77	2,91
Ketchup	5,31	2,54	3,92	2,54	Mamilo	5,51	1,37	4,18	2,58
Ladrão	2,9	2,19	5,4	3,08	Maneira	5,85	1,74	3,62	2,26

Palavra	Valência	DP	Alerta	DP	Palavra	Valência	DP	Alerta	DP
Lago	7,38	2,2	3,82	2,99	Maníaco	1,95	1,74	6,24	3,03
Lama	2,58	2,17	5,36	2,99	Manso	6,73	2,02	2,96	2,25
Lâmpada	6,51	2,41	3,82	2,65	Manteiga	5,68	2,11	3,25	2,3
Lanterna	5,95	1,56	3,06	2,21	Mão	6,88	2,07	2,95	2,42
Lápis	6,24	1,62	3,42	2,12	Máquina	5,61	1,77	3,96	2,5
Lar	8,23	1,73	3,43	2,88	Maravilha	6,8	2,37	3,72	2,83
Larva	3,07	1,89	4,27	2,75	Mareado	4,78	1,48	3,35	2,22
Leal	8,27	1,47	3,21	2,7	Maricas	4,23	1,87	3,26	2,26
Leão	5,89	2,16	5,51	2,54	Martelo	5,04	1,55	3,3	2,24
Leite	6,68	2,1	3,01	2,35	Massa	7,13	2,18	2,99	2,46
Lenda	6,36	1,69	3,69	2,36	Massacre	1,31	0,92	5,94	3,26
Lento	3,77	2,07	4,66	2,98	Mastigar	6,62	2,01	3,35	2,5
Lepra	1,87	1,46	4,83	2,99	Masturbar	5,6	2,28	5,21	2,87
Lésbica	4,01	1,9	3,65	2,72	Matador	1,49	1,11	6,69	3,21
Letárgico	3,93	1,77	3,31	2,31	Material	6,07	1,85	3,37	2,06
Letra	6,5	2	3,4	2,57	Medo	2,13	1,77	6,36	3,05
Liberdade	8,8	0,57	5,27	3,73	Mel	7,28	2,15	3,48	2,7
Líder	6,92	1,96	4,27	2,89	Melhorar	8,21	1,55	4,58	3,02
Liga	5,88	1,47	3,59	2,14	Melodia	7,73	1,66	4,51	3,22
Lindo	8,17	1,43	3,9	3,31	Memória	6,36	2,33	4,43	2,75
Livrar	6,26	2,16	4,31	2,38	Memórias	6,96	2,43	5,14	2,98
Livre	8,37	1,48	3,95	3,29	Menina	7,1	1,77	3,26	2,54
Livro	7,18	1,97	4,14	2,75	Menino	7,36	1,81	4,77	2,75
Lixo	2,48	2,14	5,14	3	Menosprezado	2,03	1,89	6,05	3,15
Lodo	2,91	2,17	4,41	2,64	Mensageiro	6,05	1,58	3,97	2,21
Loiro	5,97	1,95	3,37	2,48	Mente	7,03	2,01	3,91	2,85
Loteria	7,03	2,15	5,11	2,98	Mentira	1,35	0,97	6,28	3,07
Louco	3,87	2,33	4,9	2,79	Mercado	6,59	2,2	4,12	2,7
Lucro	7,64	1,86	5,48	3,07	Meretriz	3,82	1,91	3,52	2,41
Lustre	5,65	1,8	2,58	1,92	Mergulhador	5,71	2,04	3,79	2,75
Luta	5,66	2,81	5,51	2,53	Mês	6,11	1,9	3,9	2,51
Luto	1,7	1,39	5,32	3,15	Mesa	6,18	1,5	2,75	2
Luxo	6,82	1,9	4,65	2,72	Metal	5,15	1,32	3,17	2,04
Luxúria	4,15	2,48	4,71	2,92	Método	6,06	2,13	3,83	2,59
Luz	7,96	1,64	4,25	3,02	Milagre	7,95	1,71	4,99	3,26
Machucado	2,38	1,75	5,65	2,9	Milionário	6,55	2,23	4,19	2,83
Macio	7,74	1,79	4,08	3,09	Miséria	1,21	1,07	5,89	3,22
Mãe	8,75	1,14	3,31	3,2	Místico	6,6	2,33	3,44	2,63
Mágico	7,38	1,83	4,54	2,91	Mobilidade	6,17	1,75	4,06	2,59
Magoar	1,88	1,55	5,94	3,2	Modesto	6,79	1,92	3,08	2,23
Mal	1,58	1,2	6,1	3,04	Moeda	6,76	2,07	4,1	2,79
Mofo	2,48	1,98	4,64	2,89	Obsceno	3,89	1,98	4,09	2,77

Palavra	Valência	DP	Alerta	DP	Palavra	Valência	DP	Alerta	DP
Moinho	5,45	1,16	3,44	2,18	Obsessão	3	2,07	5,19	2,86
Molde	5,21	1,79	3,48	2,32	Obstruir	2,64	1,78	5,29	3
Momento	7,09	1,9	4,57	2,84	Oceano	7,77	1,81	3,58	2,93
Montanha	7,13	2,03	3,72	2,78	Ódio	2,86	2,16	4,76	3,05
Moral	6,72	2,07	3,45	2,43	Ofender	1,78	1,48	6,23	3,14
Mórbido	2,07	1,69	5,24	2,99	Ofuscar	4,51	2,04	4,14	2,47
Morte	1,4	1,04	6,18	3,14	Ônibus	4,18	2,39	4,58	2,91
Morto	2,01	1,82	5,11	3,22	Onipotente	5,8	2,63	4,76	2,81
Mosquito	2,09	1,71	5,6	3,1	Opção	6,27	1,85	5,18	2,86
Motim	3,77	2,25	4,4	2,88	Opinião	6,78	2,09	5,21	2,6
Motor	5,09	1,82	3,96	2,35	Orgasmo	7,92	1,65	4,37	3,39
Muco	5,43	2,35	3,35	1,98	Orgulho	6,38	2,45	4,55	2,88
Muleta	2,81	1,94	4,75	2,77	Orgulhoso	5,63	2,94	4,85	2,9
Mulher	6,57	1,9	3,89	2,6	Orquestra	7,13	1,92	4,77	2,88
Mundo	6,17	2,65	5,01	2,92	Otimismo	8,41	1,26	4,13	3,01
Muscular	6,99	2,55	4,54	3,27	Ouro	6,99	2,15	4,25	2,91
Museu	6,01	2,01	3	2,13	Ousado	6,57	1,93	4,38	2,59
Música	5,18	3,7	5,73	3,31	Outono	5,95	2,33	4,35	2,65
Mutação	4,53	2,26	4,4	2,75	Ovo	6,12	1,8	2,78	2,19
Mutilar	4,66	3,57	5,46	3,33	Paciente	5,96	2,64	4,06	2,77
Nadador	6,38	2,16	3,49	2,82	Padre	5,29	2,21	2,7	2,33
Namorada	7,59	2,09	4,89	3,28	Pai	8,08	2,28	5,55	3,29
Narcótico	2,77	2,02	4,94	2,94	País	5,8	2,56	4,53	2,76
Nascimento	8,31	1,23	4,29	3,3	Paixão	6,34	2,71	5,27	3,3
Natal	8,06	1,98	3,69	3,11	Palácio	6,28	2,05	3,6	2,45
Natural	4,97	3,36	4,76	3,16	Panfleto	6,28	2,3	3,45	2,62
Natureza	8,58	1,09	3,25	3,03	Pânico	2,14	1,85	6,7	3,06
Náusea	3,95	2,72	4,78	2,77	Panqueca	6,88	1,97	4,03	2,75
Navalha	2,64	1,81	5	3,24	Pântano	4,15	2,03	4,33	2,7
Navio	6,55	2,16	3,68	2,72	Papel	7,29	2,08	3,85	2,93
Necrotério	2,1	2,07	5,75	3,15	Paquerar	7,99	1,51	4,45	3,06
Néctar	4,66	3,08	5,41	3,25	Paraíso	7,07	2,1	4,79	3,23
Negligência	2,4	1,8	5,78	2,85	Paralisia	1,86	1,69	5,77	3,24
Nervoso	4,21	3,04	5,33	3,05	Parte	6,43	2,17	3,32	2,44
Neurótico	2,49	1,65	6,1	2,98	Passagem	5	2,52	4,01	2,77
Neve	6,93	2,27	5,19	2,91	Pássaro	7,11	2,06	4,06	2,76
Nó	3,9	1,79	4,76	2,77	Patente	4,77	1,91	3,23	2,41
Noiva	6,84	1,9	5,31	2,78	Patriota	6,21	1,97	3,7	2,7
Nome	7,5	1,98	3,53	2,79	Paz	8,64	1,14	3,71	3,5
Notícia	6,49	1,77	4,93	2,62	Pazinha	4,41	1,73	3,76	2,47
Novo	7,96	1,31	4,94	2,94	Pé	5,99	2,4	2,91	2,48
Nu	7,14	1,65	4,49	2,88	Pecado	3,29	2,14	4,23	2,82

Palavra	Valência	DP	Alerta	DP	Palavra	Valência	DP	Alerta	DP
Nublado	3,91	2,06	3,73	2,53	Pecaminoso	3,43	2,09	4,72	2,74
Nutrir	6,42	2,36	4,9	2,72	Peçonha	4,67	2,28	4,33	2,56
Nuvem	6,67	2,07	2,7	2,16	Pedinte	3,23	2,11	4,85	2,58
Obedecer	4,55	2,46	4,2	2,62	Peito	6,22	1,75	4,91	2,61
Obesidade	2,14	1,99	5,55	3,3	Peixe	6,45	2,32	3,14	2,33
Pelado	4,72	2,35	4,73	2,69	Prazer	8,65	1,05	5,29	3,63
Pêlo	4,29	1,8	3,65	2,3	Preguiçoso	3,66	2,31	4,14	2,65
Penalidade	5,43	2,61	4,86	2,87	Prejudicado	2,13	1,52	5,59	2,73
Penhasco	3,43	2,22	5,21	3,08	Prejudicar	1,68	1,22	6,04	2,95
Pênis	6,85	1,78	5,03	2,89	Presente	8,33	1,31	4,81	3,22
Penitente	4,06	1,88	4,01	2,55	Pressão	3,16	2,09	5,9	2,83
Pensamento	4,88	3,09	5	2,82	Prestígio	7,75	2,01	4,3	3,03
Pensativo	5,99	2,23	4,36	2,75	Preto	5,26	2,19	3,85	2,35
Perdedor	4,22	3,02	5,54	2,97	Primavera	8,33	1,18	3,76	3,3
Perdido	2,93	1,67	5,17	2,55	Primo	6,63	2,29	3,62	2,51
Perfeição	6,85	2,3	4,87	2,84	Prisão	1,68	1,39	5,79	3
Perfume	8,2	1,24	4,33	3,31	Privação	2,86	2,16	5,53	2,66
Perigo	2,56	2,06	6,74	2,47	Privacidade	7,99	1,54	3,73	2,97
Perseguir	3,46	2,26	5,5	2,63	Problema	2,17	1,74	6,14	2,75
Perturbado	2,49	1,57	6,01	2,71	Processo	4,31	2,27	4,97	2,54
Perturbar	2,32	1,58	5,35	2,96	Proeminente	5,43	1,58	4,1	2,21
Pervertido	3,35	2,32	5,09	2,72	Professor	6,74	1,95	4,54	2,51
Pesadelo	2,11	1,88	5,92	3,11	Progresso	7,9	1,89	4,76	3,09
Pesar	3,41	2,4	4,78	2,6	Promoção	7,89	1,88	4,9	3,07
Pessoa	7,85	1,61	4,46	2,98	Próspero	7,78	1,92	4,44	3,11
Peste	2,17	1,67	5,43	2,84	Prostituta	2,58	2,03	4,55	2,98
Piada	8,14	1,3	4,45	3,07	Protegido	7,26	2,21	3,45	2,7
Picada	2,58	1,53	5,12	2,53	Prova	4,21	2,43	6,85	2,33
Piedade	5,82	2,21	4,08	2,53	Pulga	2,68	2,01	4,3	3,11
Pintar	7,26	1,88	3,68	2,8	Pulverizador	4,72	1,82	3,88	2,3
Piolho	2,08	1,52	5,08	3,17	Punição	2,89	2,17	5,44	2,88
Piscar	6,38	1,86	3,26	2,38	Pus	2,74	1,85	4,77	2,73
Pistola	2,18	1,82	5,83	3,03	Pútrido	3,25	2,07	4,16	2,59
Pizza	8,35	1,18	4,16	3,3	Quadrado	5,18	1,95	2,95	1,97
Planície	6,24	1,95	3,17	2,43	Quadro	5,87	1,85	3,8	2,22
Plano	7,11	1,91	4,96	2,75	Qualidade	8,29	1,43	4,61	3,2
Planta	7,83	1,53	3,22	2,74	Quebrado	2,57	1,78	5,23	2,64
Pobreza	1,41	1,18	5,83	2,79	Queda	2,6	2	5,84	2,59
Poder	5,53	2,58	5,39	2,63	Queimadura	1,94	1,58	5,54	3,05
Poderoso	6,09	2,17	4,88	2,64	Queixo	5,79	1,56	2,97	2,02
Podre	1,81	1,58	5,1	3,05	Querido	8,36	1,2	4,01	3,16
Poente	6,75	2,08	3,23	2,37	Querosene	4,04	1,87	3,78	2,53

Palavra	Valência	DP	Alerta	DP	Palavra	Valência	DP	Alerta	DP
Poesia	7,66	1,74	3,13	2,76	Quieto	5,23	2,02	3,21	2,15
Poluir	1,51	1,14	6,05	2,91	Quimioterapia	1,97	1,91	5,61	3,18
Pomba	6,04	2,37	2,97	2,25	Rã	4,01	2,05	4,11	2,87
Porão	3,86	1,91	4,22	2,6	Radiador	4,75	1,95	3,63	2,31
Porco	4,29	1,94	3,6	2,45	Radiante	8,08	1,61	4,7	3,28
Porta	5,92	1,95	3,97	2,49	Rádio	7,84	1,7	4,12	3,13
Pôster	6,05	2,12	3,51	2,34	Rainha	6,27	1,95	3,99	2,52
Povo	6,22	2,27	4,87	2,46	Raiva	1,97	1,72	7,13	2,49
Pradaria	5,77	1,98	3,51	2,43	Ralé	2,94	1,81	3,96	2,36
Praia	8,29	1,43	4,64	3,58	Rançoso	2,49	1,82	5,16	2,57
Pranto	2,52	2,01	5,49	2,71	Rápido	6,32	2,23	5,37	2,64
Rato	3,19	2,09	5,18	2,87	Salvar	8,1	1,36	4,56	3,16
Razão	6,49	2,25	4,56	2,4	Sangrento	2,29	1,96	5,42	3,01
Realização	8,51	1,07	5,23	3,47	Santo	6,65	2,01	3,44	2,59
Receoso	3,89	1,86	4,51	2,37	Sarampo	2,49	1,61	4,46	2,74
Recompensa	7,59	2,16	4,96	3,05	Satisfeito	8,09	1,58	3,99	3,04
Recreio	7,65	1,86	4,1	2,96	Saudar	8	1,32	3,64	2,84
Refém	1,84	1,55	6,55	2,61	Saúde	8,39	1,25	4,1	3,16
Refresco	7,86	1,64	3,38	2,91	Secador	5,61	1,92	3,96	2,46
Rei	5,73	2,22	3,71	2,46	Seda	6,38	1,94	2,79	2,34
Rejeitado	1,61	1,24	5,85	2,73	Seguro	7,06	2,46	3,7	2,69
Relâmpago	3,77	2,31	5,85	2,72	Sentimento	7,41	2,02	4,85	2,85
Relaxado	6,36	3,18	3,76	3,01	Sério	5,39	2,16	4,01	2,17
Relógio	5,73	2,17	4,42	2,35	Severo	3,29	2,19	5,12	2,54
Remédio	3,93	2,58	4,24	2,54	Sexo	7,93	1,86	5,28	3,4
Réptil	4,47	2,18	4,34	2,59	Sexy	7,66	1,7	5,26	2,99
Repugnado	2,67	1,8	4,56	2,31	Sífilis	1,93	1,74	5,37	3,22
Repulsivo	3,1	2,15	5,15	2,35	Sobrecarregado	2,58	1,95	6,49	2,54
Reservado	5,75	1,78	3,76	2,26	Sobressalto	4,76	2,28	4,84	2,5
Respeito	8,43	1,06	3,9	3,12	Social	6,74	2,03	4,09	2,5
Respeitoso	7,52	1,71	3,41	2,63	Sociedade	5,53	2,46	5,25	2,29
Resposta	6,96	1,81	4,47	2,73	Sofrimento	1,68	1,65	6,14	2,9
Ressentido	2,83	1,87	4,8	2,24	Sol	8,28	1,68	4,27	3,38
Restaurante	7,7	1,56	3,96	2,77	Solene	5,29	1,99	4	2,08
Reunião	5,06	2,26	4,88	2,76	Solidão	1,58	1,28	5,37	2,82
Reverente	5,41	1,86	3,75	2,08	Solitário	2,47	2,09	5,28	2,95
Revista	6,9	1,8	3,51	2,54	Sombra	6,19	2,15	3,49	2,38
Revolta	2,44	2,09	6,47	2,52	Sombrinha	5,09	2,09	3,78	2,32
Revólver	1,94	1,78	6,24	3,05	Sonho	7,59	1,93	4,36	3,03
Rico	6,49	1,89	4,21	2,71	Sono	6,1	2,63	3,22	2,74
Ridículo	2,61	1,9	4,87	2,7	Sórdido	2,9	2,1	4,55	2,57
Rifle	2,36	2,11	5,68	2,91	Sorriso	8,5	1,33	4,15	3,49

Palavra	Valência	DP	Alerta	DP	Palavra	Valência	DP	Alerta	DP
Rígido	4,56	1,89	4,77	2,14	Sortudo	7,46	2,01	4,51	2,96
Rio	6,94	2,09	3,92	2,67	Sozinho	2,47	2,04	4,96	3,03
Riquezas	6,75	2,06	4,24	2,59	Suave	7,79	1,59	3,23	2,84
Risada	8,59	0,92	4,63	3,54	Subjugado	2,95	1,99	5,36	2,69
Rocha	5,49	1,85	3,52	2,11	Sucesso	8,25	1,51	5,31	3,18
Rodovia	5,46	1,95	4,65	2,34	Sufocar	2,05	1,85	6,61	2,59
Romântico	8,34	1,35	4,16	3,33	Suicídio	1,35	1,44	5,13	3,38
Rosto	7,53	1,71	3,95	2,8	Sujeira	1,9	1,83	5,86	2,82
Roupa	7,41	2	4,57	3,2	Sujo	2,43	1,99	5,49	2,75
Rua	6,19	1,56	4,42	2,38	Surpreso	6,6	2,15	5,36	2,49
Rude	2,96	1,82	5,2	2,34	Surra	1,94	1,95	5,55	3,12
Ruidoso	3,97	1,92	4,8	2,37	Suspeito	3,14	2,08	5,64	2,49
Sábio	7,92	1,38	3,96	2,83	Tabaco	2,04	1,86	5,35	3,18
Saboroso	8,24	1,42	4,05	3,17	Talento	8,31	1,2	5,04	3,29
Safira	6	1,93	3,4	2,37	Tanque	4,64	2,27	3,74	2,31
Salada	6,88	2,26	3,67	2,86	Tapa	2,22	1,91	6,19	2,59
Salvador	7,67	1,77	3,57	2,61	Táxi	5,1	2,08	3,71	2,39
Tecido	5,97	1,91	3,37	1,88	Ultraje	3,71	1,78	4,22	2,39
Tédio	2,69	2,01	5,32	2,6	Unidade	5,76	2,26	2,94	2,48
Televisão	6,69	2,21	4,21	2,76	Untensílio	6,63	1,6	3,01	2,32
Temido	4,23	2,02	4,72	2,23	Urina	5,38	2,21	3,14	2,61
Temível	2,95	2,13	5,72	2,44	Útil	8,02	1,41	3,71	2,89
Temperamental	4,37	1,89	4,94	2,16	Vaca	6,29	2,12	2,61	2,17
Tempestade	3,49	2,44	5,53	2,84	Vagão	4,97	1,72	3,81	2,55
Tempo	5,66	2,2	5,25	2,43	Vagina	6,8	2,02	4,06	3,08
Tênis	6,49	1,86	2,83	2,13	Vaidade	6,18	2,13	4,55	2,42
Tenso	2,52	1,61	6,63	2,3	Vampiro	3,55	2,06	4,38	2,92
Teoria	5,65	1,93	3,45	2,28	Vândalo	1,76	1,32	6,28	2,89
Termômetro	4,49	1,72	3,33	2,04	Vantagem	5,71	4,08	4,45	2,62
Terra	7,76	1,93	4,09	2,92	Vara	3,24	1,27	3,66	2,5
Terrível	2,12	1,68	6,41	2,48	Varíola	1,95	1,36	4,95	3,05
Terrorista	1,45	1,15	6,35	2,88	Veículo	7,41	1,73	4,45	2,61
Tesoura	4,62	1,72	3,25	2,34	Veleiro	6,57	1,99	3,39	2,81
Tesouro	7,6	1,92	4,61	3,16	Veloz	6,23	2,06	5,18	2,66
Tímido	4,12	2,3	4,78	2,66	Vencer	8,55	1,35	5,46	3,4
Tinta	6,18	1,68	2,78	2,36	Veneno	1,54	1,01	6,77	2,59
Tio	6,9	2,21	2,82	2,37	Ventilador	6,73	1,98	2,76	2,32
Tobogã	4,88	3,03	5,59	2,93	Verdade	8,56	1,3	3,46	3,08
Tolo	2,71	1,62	4,38	2,61	Verde	7,39	2	3,26	2,9
Tornado	2,41	1,73	5,89	2,8	Vermelho	5,84	2,63	4,94	2,85
Tornozelo	5,49	1,75	2,84	2,35	Vespa	3,63	2,18	4,5	3,08
Torre	5,51	1,96	3,82	2,56	Vestibular	4,93	2,94	6,65	2,44

Palavra	Valência	DP	Alerta	DP	Palavra	Valência	DP	Alerta	DP
Torta	7,71	1,76	3,92	2,98	Vestido	6,69	2,05	3,63	2,68
Tortura	1,32	0,9	7,35	2,37	Vestuário	6,8	1,84	3,91	2,7
Tóxico	1,8	1,68	5,53	2,85	Viagem	8,55	1,22	5,26	3,39
Tragédia	1,38	0,98	7,09	2,36	Vibração	6,96	1,95	5,76	2,86
Traidor	1,29	1,09	7,16	2,69	Viciado	1,46	1,23	5,73	2,99
Trair	1,4	1,12	7,24	2,59	Vício	2,16	1,72	5,82	2,93
Tranquilamente	7,89	1,88	2,49	2,66	Vida	8,63	1,01	5,45	3,53
Tranqüilo	8,07	1,75	2,22	2,26	Vidro	4,96	1,37	3,49	2,13
Tratar	6,55	2,06	3,31	2,31	Vigiar	4,13	2,07	4,91	2,83
Trauma	1,86	1,4	6,43	2,61	Vigoroso	6,85	1,83	4,03	2,36
Travesseiro	8,19	1,56	2,58	2,8	Vila	4,94	2,2	3,89	2,5
Travessura	6,56	1,87	4,84	2,52	Vinho	7,19	2	4,09	2,94
Trevas	1,74	1,46	5,46	2,99	Violento	1,46	1,1	6,49	2,95
Triste	1,73	1,29	5,28	2,8	Violino	6,42	2,34	3,14	2,82
Triunfante	8,14	1,42	4,99	3,24	Virgem	5,84	1,99	3,09	2,52
Triunfo	7,93	1,52	4,63	3,01	Virtude	8,02	1,63	3,65	2,85
Troféu	8,04	1,65	4,71	3,4	Visão	7,33	2,32	3,89	2,87
Trompete	5,84	2,04	3,54	2,49	Vítima	2,26	1,6	6,08	2,69
Tronco	5,44	1,77	2,93	2,16	Vitória	8,74	0,67	5,36	3,45
Tubarão	3,4	2,19	6,21	2,64	Vívido	7,02	1,91	3,92	2,7
Tumor	1,44	1,23	6,29	3,1	Vivo	8,34	1,5	4,7	3,21
Túmulo	2,06	1,84	5,39	2,87	Vômito	2,31	1,5	4,47	2,48
Úlcera	1,54	1,04	6	3,06	Vulcão	3,74	2,45	5,5	2,72

Kristensen et al. (2011)

ANEXO B— Lista de Palavras Referentes à Emoção "Alegria" (MARTINAZZO, 2010, p.58)

abundante
acalmar
aceitável
aclamar
aconchego
adesão
admirar
adorar
afável
afeição
afeto
afortunado
agradar
ajeitar
alívio
amabilidade
amado
amar
amável
amenizar
ameno
amigável
amistoso
amizade
amor
animação
ânimo
anseio
ânsia
ansioso
apaixonado
apaziguar
aplausos
apoiar
aprazer
apreciar
aprovação
aproveitar
ardor
admirar
arrumar
atração
atraente
atrair
avidamente
avidez
ávido
belo
bem-estar
beneficência
beneficiador
benefício
benéfico
benevolência
benignamente
benigno
bom
bondade
bondoso
bonito
brilhante
brincadeira
calma
calor
caridade
caridoso
carinho
cativar
charme
cherry
clamar
confortar
coleguismo
comédia
cômico
comover
compaixão
companheirismo
compatibilidade
compatível
complacência
completar
compreensão
conclusão
concretização
condescendência
confiança
confortante
congratulação
conquistar
consentir
consideração
consolação
contentamento
coragem
cordial
considerar
consolo
contente
cuidadoso
cumplicidade
dedicação
deleitado
delicadamente
delicadeza
delicado
desejar
despreocupação
devoção
devoto
diversão
divertido
encantar
elogiado
emoção
emocionante
emotivo
empatia
empático
empolgação
enamorar
encantado
encorajado
enfeitar
engraçado
entendimento
entusiasmadamente
entusiástico
esperança
esplendor
estima
estimar
estimulante
euforia
eufórico
euforizante
exaltar
excelente
excitar
expansivo
extasiar
exuberante
exultar
fã
facilitar
familiaridade
fascinação
fascínio
favor
favorecer
favorito
felicidade
feliz
festa
festejar
festivo
fidelidade
fiel
filantropia
filantrópico
fraterno
ganhar
generosidade
generoso
gentil
glória
glorificar
gostar
gostoso
gozar
gratificante
grato
hilariante
honra
humor
impressionar
incentivar
incentivo
inclinação
incrível
inspirar
interessar
interesse
irmandade
jovial
jubilante
júbilo
lealdade
legítimo
leveza
louvar
louvável
louvavelmente
lucrativo
lucro
maravilhoso

melhor
obter
obteve
ode
orgulho
paixão
parabenizar
paz
piedoso
positivo
prazenteiro
prazer
predileção
preencher
preferência
preferido
promissor
prosperidade
proteção
proteger
protetor
proveito
privilégio
querer
radiante
realizar
recomendável
reconhecer
recompensa
recrear
recreativo
recreação
regozijar
respeitar
ressuscitar
revigorar
risada
risonho
romântico
romantismo
saciar
saciável
satisfação
satisfatoriamente
satisfatório
satisfazer
satisfeito
sedução
seduzir
sereno
simpaticamente
simpático
sobrevivência
sobreviver
sorte
sortudo
sucesso
surpreender
tenro
ternura
torcer
tranquilo
tranquilo
triunfo
triunfal
triunfante
vantagem
vantajoso
vencedor
veneração
ventura
vida
vigor
virtude
virtuoso
vitória
vitorioso
viver
vivo
zelo
zeloso

ANEXO C—Lista de Palavras Referentes à Emoção "Desgosto" (MARTINAZZO, 2010, p.61)

abominável
adoentado
amargamente
antipatia
antipático
asco
asqueroso
aversão
chateação
chatear
desagradável
desagrado
desprezível
detestável
doença
doente
enfermidade
enjoativo
enjoo
feio
fétido
golfar
grave
gravidade
grosseiro
grosso
horrível
ignóbil
ilegal
incômodo
incomodar
indecente
indisposição
indisposto
inescrupuloso
maldade
maldoso
malvado
mau
náusea
nauseabundo
nauseante
nausear
nauseoso
nojento
nojo
obsceno
obstrução
obstruir
ofensivo
patético
perigoso
repelente
repelir
repugnante
repulsa
repulsão
repulsivo
rude
sujeira
sujo
terrível
terrivelmente
torpe
travesso
travessura
ultrajante
vil
vomitar
vômito

ANEXO D — Lista de Palavras Referentes à Emoção "Medo" (MARTINAZZO, 2010, p.62)

abominável
afugentar
alarmar
alerta
ameaça
amedrontar
angustia
angústia
angustiadamente
ansiedade
ansioso
apavorar
apreender
apreensão
apreensivo
arrepio
assombrado
assombro
assustado
assustadoramente
atemorizar
aterrorizante
brutal
calafrio
chocado
chocante
consternado
covarde
cruel
crueldade
cruelmente
cuidado
cuidadosamente
cuidadoso
defender
defensor
defesa
derrotar
desconfiado
desconfiança
desencorajar
desespero
deter
envergonhado
escandalizado
escuridão
espantoso
estremecedor
estremecer
expulsar
feio
friamente
fugir
hesitar
horrendo
horripilante
horrível
horrivelmente
horror
horrorizar
impaciência
impaciente
impiedade
impiedoso
indecisão
inquieto
insegurança
inseguro
intimidar
medonho
medroso
monstruosamente
mortalha
nervoso
pânico
pavor
premonição
preocupar
presságio
pressentimento
recear
receativamente
receio
receoso
ruim
suspeita
suspense
susto
temeroso
temor
tensão
tenso
terrificar
terrível
terrivelmente
terror
timidamente
timidez
tímido
tremor
vigiar
vigilante

ANEXO E— Lista de Palavras Referentes à Emoção "Raiva" (MARTINAZZO, 2010, p.64)

abominação
aborrecer
agredido
agredir
agressão
agressivo
amaldiçoado
amargor
amargura
amolar
angústia
animosidade
antipatia
antipático
asco
assassinar
assassinato
assediar
assédio
atormentar
avarento
avareza
aversão
beligerante
bravejar
chateação
chato
cobiçoso
cólera
colérico
complicar
contrariedade
contrariar
corrupção
corrupto
crucificar
demoníaco
demônio
descaso
descontente
descontrole
desenganar
desgostar
desgraça
desprazer
desprezar
destruição
destruir
detestar
diabo
diabólico
doido
encolerizar
energicamente
enfurecido
enfuriante
enlouquecer
enraivecer
escandalizar
escândalo
escoriar
exasperar
execração
ferir
frustração
frustrar
fúria
furioso
furor
ganância
ganancioso
guerra
guerreador
guerrilha
hostil
humilhar
implicância
implicar
importunar
incomodar
incômodo
indignar
infernizar
inimigo
inimizade
injúria
injuriado
injustiça
insulto
inveja
ira
irado
irascibilidade
irascível
irritar
louco
loucura
magoar
mal
maldade
maldição
maldito
maldizer
maldoso
maleficência
maléfico
malevolência
malévolo
malícia
malicioso
malignidade
maligno
maltratar
maluco
malvadeza
malvado
matar
mesquinho
misantropia
misantrópico
molestar
moléstia
mortal
morte
mortífero
mortificar
nervoso
odiar
odiável
ódio
odioso
ofendido
ofensa
opressão
opressivo
oprimir
perseguição
perseguir
perturbar
perverso
provocar
rabugento
raivoso
rancor
reclamar
repressão
reprimir
repulsa
repulsivo
resmungar
ressentido
revolta
ridículo
tempestuoso
tirano
tormento
torturar
ultraje
ultrajar
vexatório
vigoroso
vingança
vingar
vingativo
violência
violento
zangar

ANEXO F— Lista de Palavras Referentes à Emoção "Surpresa" (MARTINAZZO, 2010, p.66)

admirar
afeição
apavorante
assombro
chocado
chocante
desconcertar
deslumbrar
embasbacar
emudecer
encantamento
enorme
espanto
estupefante
estupefato
estupefazer
expectativa
fantasticamente
fantástico
horripilante
imaginário
imenso
impressionado
incrível
maravilha
milagre
mistério
misterioso
ótimo
pasmo
perplexo
prodígio
sensacional
surpreendente
surpreender
suspense
susto
temor
tremendo

ANEXO G— Lista de Palavras Referentes à Emoção "Tristeza" (MARTINAZZO, 2010, p.67)

abandonar
abatido
abominável
aborrecer
abortar
aflição
afligir
aflito
agoniar
amargo
amargor
amargura
ansiedade
arrepender
arrependidamente
atrito
azar
cabisbaixo
chorão
choro
choroso
coitado
compassivo
compunção
contrição
contristador
contrito
culpa
defeituoso
degradante
deplorável
deposição
depravado
depressão
depressivo
deprimente
deprimir
derrota
derrubar
desalentar
desamparo
desanimar
desânimo
desapontar
desconsol
descontente
desculpas
desencorjar
desespero
desgaste
desgosto
desgraça
desistência
desistir
deslocado
desmoralizar
desolar
desonra
despojado
desprazer
desprezo
desumano
discriminar
disforia
disfórico
dissuadir
dó
doloroso
dor
enfadado
enlutar
entediado
entristecedor
entristecer
envergonhar
errante
erro
errôneo
escurecer
escuridão
escuro
esquecido
estragado
execrável
extirpar
falso
falsidade
falta
fraco
fraqueza
fricção
frieza
frio
fúnebre
funesto
grave
horror
humilhar
inconsolável
indefeso
infelicidade
infeliz
infortúnio
isolar
lacrimejante
lacrimoso
lágrima
lamentar
lástima
lastimoso
lúgubre
luto
lutuoso
mágoa
magoar
martírio
martirizar
mau
melancolia
melancólico
menosprezar
miseravelmente
miséria
mistério
misterioso
morre
morte
mortificante
negligentemente
nocivo
obscuro
opressão
opressivo
oprimir
pena
penalizar
penitente
penoso
penumbra
perder
perturbado
perverso
perverter
pesaroso
pessimamente
piedade
pobre
porcamente
prejudicado
prejudicial
prejuízo
pressão
pressionar
quebrar
queda
queixoso
rechaçar
remorso
repressão
repressivo
reprimir
ruim
secreto
servil
só
sobrecarga
sobrecarregado
sofrer
sofrimento
solidão
sombrio
soturno
sujo
suplicar
suplício
tédio
timidez
tímido
torturar
trevas
triste
tristemente
vazio