CENTRO PAULA SOUZA

FACULDADE DE TECNOLOGIA DE AMERICANA

Segurança da Informação

Jessika Tais Coelho Lobo

ENGENHARIA SOCIAL E A SEGURANÇA DA INFORMAÇÃO NO AMBIENTE CORPORATIVO

AMERICANA, SP

2016

CENTRO PAULA SOUZA

FACULDADE DE TECNOLOGIA DE AMERICANA

Segurança da Informação

Jessika Tais Coelho Lobo

ENGENHARIA SOCIAL E A SEGURANÇA DA INFORMAÇÃO NO AMBIENTE CORPORATIVO

Trabalho de conclusão de curso do curso Tecnologia em Segurança da Informação na entidade Fatec Americana, realizado sob a orientação do professor Benedito Cruz.

AMERICANA, SP

2016

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte

Lobo, Jessika Tais Coelho
L783e Engenharia social e a segurança da informação no ambiente corporativo. / Jessika Tais Coelho Lobo. – Americana: 2016.
51f.

Monografia (Graduação em Tecnologia em Segurança da Informação). - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza.
Orientador: Prof. Benedito Aparecido Cruz

1.Segurança em sistemas de informação I. Cruz, Benedito Aparecido II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana.

CDU:681.518.5

Jessika Tais Coelho Lobo

Engenharia social e a segurança da informação no ambiente corporativo

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – Fatec/ Americana.
Área de concentração: Segurança da Informação.

Americana, 20 de junho de 2016.

Banca Examinadora:

Benedito Aparecido Cruz (Presidente)
Mestre
Fatec Americana

Pedro Domingos Antoniolli (Membro)
Doutor
Fatec Americana

Samuel Tanaami (Membro)
Mestre
Fatec Americana

Jessika Tais Coelho Lobo

ENGENHARIA SOCIAL E A SEGURANÇA DA INFORMAÇÃO NO AMBIENTE CORPORATIVO

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.
Área de concentração: Segurança da Informação

Americana, 06 de Junho de 2016

DEDICATÓRIA

Dedico este trabalho a todos os meus familiares e professores do curso, que foram tão importantes na minha vida acadêmica e no desenvolvimento deste trabalho. E a cima de todos, agradeço a Deus, que nada seria de mim sem a fé que eu tenho nEle.

"Há um ditado popular que diz que um computador seguro é aquele que está desligado. Isso é inteligente, mas é falso: O hacker convencerá alguém a entrar no escritório e ligar aquele computador. Tudo é uma questão de tempo, paciência, personalidade e persistência."

Kevin David Mitnick

RESUMO

Este trabalho tem como objetivo elucidar e informar que, por mais poderosos e bem configurados *firewalls*, passaportes biométricos e toda gama de tecnologia, tudo se mostra ineficaz a um ataque de engenharia social bem feito. A tecnologia também é um elemento básico para que a evolução aconteça e o desenvolvimento humano se realize de forma completa. A informação é o elemento essencial para todos os processos de negócio da organização, sendo, portanto, um bem ou ativo de grande valor, podendo ser alvo de uma série de ameaças com a finalidade de explorar as vulnerabilidades e causar prejuízos consideráveis. As empresas vêm investindo na modernização de seus parques tecnológicos e estão negligenciando o fator humano, e é essa vulnerabilidade que é explorada pelos engenheiros sociais.

Palavras chave: engenharia social, tecnologia da informação, vulnerabilidade.

ABSTRACT

The purpose of this work is to elucidate and inform that despite the most powerful and well-configured firewalls, biometric passports and the whole range of technology, it has proven ineffective to an efficient social engineering attack. Technology is a key element in evolution and also helps human development to fully happen. Information is the key element for every business processes, thereby considered an asset of great value hence a target to threats in order to exploit the vulnerability and cause considerable damage. Companies are now more focused on improving its technological parks and are neglecting the human factor, and this is the vulnerability that is exploited by social engineering.

Keywords: social engineering, information technology, vulnerability.

SUMÁRIO

1 INTRODUÇÃO

Atualmente, a informação se constitui em um bem de suma importância para as organizações dos mais variados segmentos. A *internet*, popularizada ao longo dos anos 90, permitiu a troca e disponibilidade de informações por meio da *World Wide Web* (WWW). Outros mecanismos de comunicação e troca de informações como *e-mails* também têm proporcionado benefícios no uso profissional e pessoal. Nota-se que a informação compreende qualquer conteúdo que possa ser armazenada ou transferido de algum modo, servindo a determinado propósito e sendo de utilidade ao ser humano, inclusive sendo um ativo de grande importância dentro de uma empresa. Na grande maioria das situações, usuários de informações desconhecem seu valor e podem colocar a si ou uma instituição numa condição vulnerável, principalmente, quando diante de um engenheiro social.

Engenharia social é uma determinada artimanha ou manipulação por meio de palavras, para se utilizar da ingenuidade do ser humano em benefício próprio. Esses especialistas que têm o conhecimento amplo em técnicas para analisar o perfil de suas vítimas, são conhecidos como engenheiros sociais. Eles criam e traçam uma estratégia para atingirem os seus objetivos através da ingenuidade de suas futuras vítimas. Isso ocorre o tempo todo através da rede mundial. As vítimas geralmente são pessoas que não têm a ciência, não compreendem ou não valorizam suas informações, a ponto de resguardá-las dessas pessoas mal-intencionadas.

Caruso (1999) afirma que tradicionalmente, as empresas dedicam grande atenção à proteção de seus ativos físicos e financeiros, mas pouca ou até mesmo nenhuma atenção aos ativos de informação que possuem.

Segundo Mitnick (2003), a prioridade de todos que trabalham é fazer o trabalho. Sob essa pressão, as práticas de segurança em geral ficam em segundo plano e são desprezadas ou ignoradas. Os engenheiros sociais usam isso ao praticarem sua arte.

2 ENGENHARIA SOCIAL

Peixoto (2006) define a palavra “engenharia” em si, como a arte de aplicar conhecimento científicos e empíricos e certas habilitações especificas à criação de estruturas, dispositivos e processos que se utilizam para converter recursos naturais em formas adequadas ao atendimento das necessidades humanas, e define a engenharia social como a ciência que estuda como o conhecimento do comportamento humano pode ser utilizado para induzir uma pessoa a atuar segundo seu desejo. Não trata-se 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). Também é utilizada para lograr todo o tipo de fraudes, inclusive invasão de sistemas eletrônicos.

O termo engenharia social ficou conhecido no ano de 1990, através do famoso *hacker* Kevin Mitnick. Alguns consideram essa prática uma arte. Geralmente quem faz o ataque se aproveita de dados ou informações da vítima e a mesma, sem perceber, acaba passando ao atacante tais dados e/ou informações. O ser humano sempre vai tentar ser útil, e de alguma forma tentar ajudar, e com essa “fraqueza” é possível obter todas as informações necessárias para que o atacante consiga atingir o seu objetivo.

Mitnick (2003) afirma que 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.

Oliveira (2003) afirma que nenhuma área da informática é tão vasta e apreciada como a segurança da informação: o ponto principal da segurança leva a um outro ponto principal, o ser humano. Todo o processo de segurança se inicia e tem o seu término em um ser humano. Nada adianta serem gastos fortunas em equipamentos e sistemas de segurança se não saber quem utilizará os sistemas, e quem pode ter

acesso a eles, mesmo sem autorização. No ciberespaço, a percepção do que é ser herói ou bandido dissipa-se nos interesses pessoais, opções políticas, ideologias e vínculos ao poder, e a ação puramente sintática da criptografia encontra enormes obstáculos para realizar o papel principal que pode exercer no processo da segurança de redes fechadas.

No ponto de vista de Peixoto (2006), mesmo existindo inúmeros engenheiros sociais espalhados pelo mundo exercendo propositalmente esta arte para o bem ou para o mal, assim como pessoas que mesmo sem o conhecimento prévio desta designação já cometerem o ato de engenharia social de alguma forma ocasionalmente em suas rotinas diários, dois personagens merecem destaques relevantes no contexto da engenharia social: Frank Abagnale W. Jr e Kevin D. Mitnick.

Frank Abagnale ficou famoso por tornar-se o maior fraudador da história nos EUA. Além de roubar milhões de dólares através dos seus cheques falsificados, ele também conseguiu passar-se por professor do ensino médio, piloto de avião e advogado, tudo isso antes de completar 19 anos de idade. Após ser preso, foi recrutado pelo FBI (*Federal Bureau of Investigation*), americano e, posteriormente, tornou-se um dos melhores e mais bem pagos consultores de segurança contra fraudes, tonando-se um "*hacker* do bem".

Já Kevin D. Mitnick foi considerado uns dos *hackers* mais famosos do mundo, e após várias prisões, em 2000, quando saiu em liberdade condicional, foi proibido de tocar em qualquer computador com ligação à *internet*, *modem*, pacote de *software* ou até mesmo um telefone sem alguém por perto. Atualmente, Mitnick estabeleceu-se como um dos maiores especialistas em segurança de computadores mais requisitados de todo o mundo. Ele testemunhou no comitê do senado para assuntos governamentais sobre a necessidade da legislação que garanta a segurança dos sistemas de informações do governo.

2.1 FIGURAS DA ENGENHARIA SOCIAL

Através da engenharia social, informações valiosas poderão ser obtidas, tais como descobrir informações pessoais sobre o administrador da rede, informações sobre fornecedores de suprimentos e manutenção, descobrir quem tem acesso privilegiado a qualquer servidor ou estação, avaliar o grau de conhecimento desta

pessoa, descobrir números de telefone importantes, tentar também obter uma lista de endereços de correio eletrônico importantes, e até mesmo ter acesso ao seu lixo, afinal, como diz Mitnick (2003), uma das maiores fontes de informações sobre a vítima, será o seu lixo. Segundo ele, o engenheiro social cria o problema e, em seguida, o resolve num passe de mágica, enganando a vítima para que ela forneça o acesso aos segredos mais bem guardados da empresa.

Pontiroli (2013) afirma que a maioria dos cibercriminosos não gastam muito tempo em provar tecnologias complexas para seus ataques, quando eles sabem que é muito mais fácil usar a engenharia social para os seus fins. Além disso, existem até mesmo *sites* com informações valiosas para aprender sobre esses tipos de técnicas e por que elas são tão bem-sucedidas quando usadas para enganar as pessoas, uma vez que usa a linguagem falada diariamente para influenciar uns aos outros, mesmo sem o próximo estar ciente de tal ação. Desde o ponto de vista da engenharia social, a linguagem tem algumas desvantagens já que está ligada à experiência subjetiva de um fato que pode distorcer as coisas ou realizar generalizações

Em seu livro, Mitnick (2005) aponta que, na maioria dos ataques de engenharia social, o atacante assume certos acessórios do “papel” que está representando para fazer com que o alvo infira outras características e aja de acordo com o esperado. Esse papel pode ser o de um técnico de TI, o de cliente, o de um novo contratado ou de qualquer um que requeira o cumprimento de uma solicitação. Táticas comumente usadas são mencionar o nome do chefe do alvo ou de outros funcionários, usar terminologia ou jargão da empresa ou do setor. Para ataques 'físicos', os atacantes podem escolher roupas, joias (um alfinete da empresa, um relógio de atleta, uma caneta cara, um anel de formatura) ou modos de se arrumar (por exemplo, o estilo do penteado), também acessórios que podem conferir credibilidade ao papel desempenhado pelo atacante. A força desse método deve-se ao fato de que, ao aceitar-se alguém (como um executivo, cliente ou funcionário), faz-se inferências e atribui-se à outras características a essa pessoa (um executivo é rico e poderoso; um desenvolvedor de software têm conhecimentos técnicos, mas pode ser socialmente inibido; um funcionário é digno de confiança).

Guilherme Junior (2006) ensina que são várias as figuras encontradas em um ataque de engenharia social, algumas utilizadas apenas na fase de coleta de informações, outras utilizadas apenas na fase de ataque direto e por fim, algumas que

são utilizadas durante todo o processo de realização do ataque, dentre elas pode-se destacar:

- *Phishing*: o *phishing* pode ser traduzido como “pescaria” ou “*e-mail* falso”, que são *e-mails* manipulados e enviados à organizações e pessoas com o intuito de aguçar algum sentimento que faça com que o usuário aceite o *e-mail* e realize as operações solicitadas. Os casos mais comuns de *phishing* são *e-mails* recebidos de supostos bancos, nos quais afirmam que a conta está irregular, ou que existe um novo *software* de segurança do banco que precisa ser instalado senão irá bloquear o acesso. Outro exemplo de *phishing* pode ser da Receita Federal informando que o CPF da pessoa está irregular ou que o imposto de renda apresentou erros e para regularizar consta um *link*, até as situações mais absurdas que muitas pessoas ainda acreditam por falta de conhecimento. A maioria dos *phishings* possuem algum anexo ou *links* dentro do *e-mail* que direcionam para a situação que o *cracker* – mais conhecido como o *hacker* do mal - deseja.
- Disfarces: nessa tática, o atacante deixa de ser a pessoa que é se torna a pessoa que a vítima passa a acreditar. É parte fundamental de qualquer ataque de engenharia social essa capacidade do atacante de esconder a sua identidade e de assumir a identidade de alguém que possui acesso a informação que o ataque tem como alvo.
- Informações descartadas incorretamente: o descarte de informação na forma impressa ou o ato de esvaziar a lixeira de um *desktop* não são seguros o suficiente quando se trata de dados sigilosos, já que basta uma inspeção mais cautelosa para que um atacante chegue até eles. Deve-se sempre garantir o descarte seguro da informação, usando meio adequados para isso - a queima no caso da informação física, como o papel, ou o uso de *softwares* seguros para apagar dados sigilosos do *hard disk*. São poucas as empresas que se preocupam com o destino do lixo que é gerado em seu ambiente, tornando-o assim uma fonte potencial de informações para os engenheiros sociais, pois nele podem ser encontrados relatórios, anotações de senhas, entre outras informações.
- Redes de contato e funcionários descontentes: por via das vezes essa é uma das formas mais fáceis de obter informações dentro de uma empresa. Funcionários insatisfeitos na maioria das vezes acabam por fornecer informações importantes, as quais podem prejudicar seus superiores ou toda a organização, além de possuírem

uma rede de contatos dentro e fora (fornecedores) da organização, o que se torna válido pois estes podem fornecer informações sobre outras pessoas e sobre caminhos para chegar a mais dados. Amigos e conhecidos são uma fonte de informação valiosa, se bem explorada. Por isso, um engenheiro social experiente se aproximará destas pessoas a fim de extrair informações e conseguir favores.

- Apelo sentimental: muitas vezes é realizado no mundo virtual (*chats*), pois o atacante pode, por exemplo, transforma-se em homem ou mulher, usando a tática de disfarce citada a cima, para atrair e conquistar a confiança da pessoa atacada, subtraindo assim informações importantes. Emoções são a maneira mais fácil de se manipular alguém. Uma história convincente que leve a vítima a achar que está fazendo o bem, ou que ganhará algo no final pode ser determinante para o sucesso de um ataque de engenharia social.
- Programação neuro-linguística: umas das técnicas mais utilizadas nesta fase chama-se acompanha-acompanha-acompanha-acompanha, seu objetivo é confundir a vítima. Neste método, o atacante imita os trajetos de seu interlocutor por um determinado tempo até que forma-se um elo de intimidade e a vítima imagina estar no comando, baixando a guarda. Deste modo em diante, o atacante comanda a conversa sem que a vítima perceba, obtendo assim todas as informações que ela detém. Consiste no uso de jargões e maneirismos artificiais por parte do engenheiro social para que a vítima acredite na sua história e no seu disfarce, sendo assim uma peça central de um ataque de engenharia social.

> "A programação neuro-linguística ou PNL, embora inventado para fins terapêuticos, é considerada hoje em dia como uma forma evoluída de hipnose usada por muitos engenheiros sociais como uma ferramenta para influenciar e manipular suas vítimas, a fim de levá-las a fazer as ações necessárias para um ataque bem-sucedido. Com esta técnica, os cibercriminosos podem compreender quaisquer dados pessoal ou informações confidenciais para atingir seu objetivo." (PONTIROLI, 2013)

- Pesquisas na *internet*: vários atacantes formulam *sites* afim de obter dados pessoais e noções sobre o comportamento de suas vítimas. Para isso, oferecem para a realização do cadastro brindes, participação em promoções, etc. Desta forma, conseguem obter, por exemplo, números de CPF, RG e cartões de crédito. Qualquer concurso público feito por uma pessoa, seu CPF, a faculdade que cursou, a escola na qual se formou, entre outros dados, podem ser facilmente encontrados com uma busca na *internet*. Além disso, redes sociais permitem que um indivíduo mal-intencionado descubra diversas informações pessoais sobre seus usuários. Pode-se

afirmar que as informações na *internet* são uma das maiores armas do engenheiro social.

2.2 CARACTERÍSTICAS DAS VÍTIMAS

Uma segunda rota de invasão para o sistema é o erro humano. Define-se por erro humano todo comportamento inseguro, seja ele um ato contínuo ou fruto de um momento de distração, que pode ser usado por um atacante para que este consiga comprometer um sistema. O grande problema com o erro humano é que ele não pode ser completamente corrigido, apenas mitigado, afinal nenhuma pessoa é perfeita e, mesmo quando aplicados inúmeras vezes dentro do ambiente coorporativo, nenhum treinamento pode mudar isso.

Mitnick (2003) aponta que a maioria das pessoas supõe que nunca será enganada, com base na crença de que a probabilidade de ser enganada é muito baixa; o atacante, entendendo isso como uma crença comum, faz a sua solicitação soar tão razoável que não levanta suspeita quanto explora a confiança da vítima. Aponta também que a vítima é levada a acreditar que o atacante é um colega ou alguma outra pessoa que está autorizada a acessar as informações confidenciais ou que está autorizada a dar à vítima instruções que envolvam a tomada de ações com um computador ou com equipamento relacionado com o computador.

Algumas características das vítimas, apontadas por Torres (2012):

- Vaidade pessoal e/ou profissional: o ser humano costuma ser mais receptivo à avaliação positiva e favorável dos seus objetivos, aceitando basicamente argumentos favoráveis à sua avaliação pessoal ou profissional ligada diretamente ao benefício próprio ou coletivo, de forma demonstrativa.
- Autoconfiança: o ser humano busca transmitir em diálogos individuais ou coletivos o ato de fazer algo bem, coletivamente ou individualmente, buscando transmitir segurança, conhecimento, saber e eficiência, buscando criar uma estrutura base para o início de uma comunicação ou ação favorável a uma organização ou indivíduo.
- Formação profissional: o ser humano busca valorizar uma formação e suas habilidades adquiridas desta faculdade, buscando o controle em uma comunicação,

execução ou apresentação, seja ela profissional ou pessoal, buscando o reconhecimento pessoal inconscientemente em primeiro plano.

- Vontade de ser útil: o ser humano, comumente, procura agir com cortesia, bem como ajudar outros quando necessário.
- Busca por novas amizades: o ser humano costuma se agradar e sentir-se bem quando elogiado, ficando mais vulnerável e aberto a dar informações
- Propagação de responsabilidade: trata-se da situação na qual o ser humano considera que ele não é o único responsável por um conjunto de atividades
- Persuasão: compreende quase uma arte a capacidade de persuadir pessoas, onde se busca obter respostas especificas. Isto é possível porque as pessoas possuem características comportamentais que as tornam vulneráveis a manipulação.

2.3 TIPO DE *HACKERS*

A diferença entre *hacker* e *cracker*, embora muitas pessoas não saibam, é muito grande. Enquanto o primeiro está mais focado no aprendizado e na boa fé, o segundo segue tendências criminosas. Entretanto, como com passar do tempo a figura do *hacker* acabou se misturando com a do *cracker*, defender a especificação às vezes soa como preciosismo, já que as empresas que topam com *hackers* automaticamente os ligam a atividades obscuras.

Por trabalharem no anonimato no passado, os *hackers* ainda são muito associados a pessoas que roubam informações e aplicam golpes na *internet*. No entanto, o *hacker* é um profissional que utiliza seu conhecimento para indicar as possíveis falhas no sistema segurança da informação das empresas. Porém, por conta do crescimento de ataques virtuais, suas habilidades são cada vez mais requisitadas e o preconceito em relação a suas atividades tem diminuído.

2.3.1 *HACKER (WHITE HATS)*

Segundo Marques Filho (2010), *hackers* ou *white hats* são os *hackers* do “bem”. É a categoria que os *hackers* “de verdade” se enquadram. São aqueles especializados em explorar os sistemas de segurança, em busca de falhas ou possíveis problemas, a fim de solucioná-los e não de buscar proveitos próprios. Eles procuram detectar os

erros, atuando dentro da lei. Os *white hats* utilizam seus conhecimentos sobre invasão de sistemas com o propósito de ajudar empresas, governos ou qualquer outro tipo de órgão para o qual eles trabalhem, com a intenção de evitar possíveis problemas relacionados às invasões. Ou seja, ele é apenas um profissional de segurança, que, vale salientar, estudou por muitos anos e que se dedica a proteger sistemas. Normalmente, das ações dos *white hats*, ao encontrar problemas no sistema de segurança do órgão para o qual trabalham, a primeira atitude dos mesmos é entrar em contato com os donos ou responsáveis pelo sistema e avisá-los dos problemas, a fim de que medidas sejam providenciadas. A maioria dos *white hats* trabalha junto a auditorias de sistemas, redes e banco de dados. Encontram-se também *white hats* na função de pesquisadores acadêmicos dentro das universidades e nas escolas ministrando palestras sobre segurança na *internet* e computação em geral. Devido ao sentido negativo com que a imprensa costuma estigmatizar os *hackers*, julgando-os de *crackers*, os *white hats* normalmente são classificados pela mídia como especialistas em tecnologia de informações, analistas de sistemas ou qualquer outra função na área da informática. Porém, o que eles são na verdade, é simplesmente *hackers*, no sentido mais original da terminologia.

2.3.2 *CRACKER (BLACK HATS)*

Segundo Marques Filho (2010), os *black hats*, são os *hackers* do lado negro, compõem exatamente os tipos de indivíduos que é comum se associar quando o termo *hacker* é utilizado pela população em geral. Tal termo é erroneamente associado, especialmente pela mídia, aos criminosos virtuais. Na verdade, a maioria das ações que prejudicam sistemas e usuários da *internet* e é atribuído aos "*hackers*", são ações promovidas pelos *black hats*, ou seja, os *crackers*. São pessoas com um bom nível de conhecimento sobre programação, sistemas operacionais e redes de computadores. Eles costumam investigar as falhas dos sistemas operacionais, das redes ou banco de dados para, através dessas deficiências, invadi-los e desenvolver ações ilícitas, em busca de benefício próprio. São capazes de desenvolver seus próprios *softwares* a fim de encontrar vulnerabilidades para, posteriormente, modificar valores de um banco de dados, furtar informações, assim como derrubar servidores e sistemas e descobrir informações sigilosas e importantes em busca de ganho próprio.

A metodologia de trabalho desse grupo normalmente é feita de forma individual, cada *black hats* trabalhando sozinho em busca de informações. Porém, também existe uma parcela que costuma participar de comunidades restritas com a intenção de trocar informações técnicas sobre invasões, criação de programas, entre outros. É através do controle de programas e aplicativos que espalham códigos maliciosos, ou seja, dos vírus, que esses *crackers*, normalmente, agem, provocando os mais diversos danos aos usuários.

É importante perceber que os *white hats* e os *black hats* formam uma espécie de dois separadores entre as categorias *hackers/crackers*. Indivíduos com grande conhecimento podem fazer parte tanto de um grupo quanto do outro, variando apenas de acordo com suas atitudes.

2.3.3 *GRAY HATS*

De acordo com Marques Filho (2010), essa categoria é a junção dos *white hats* com os *black hats*. Por isso são conhecidos como os "*hackers*" de chapéu cinza. Eles se tornam muito perigosos pelo fato de não ser possível discernir se esses indivíduos estão atuando de maneira positiva ou de maneira negativa. Eles podem tanto ser do "bem" quanto do "mal". Esse *status* vai variar de acordo com o tipo de serviço que lhes é encomendado. Eles normalmente exigem retribuição financeira para compensar a missão que lhes é dada. São conhecidos por serem mercenários e tem como objetivo primordial a obtenção de lucro financeiro através de seus conhecimentos, mesmo que para isso tenha que realizar alguma tarefa ilícita. De acordo com sua ética, dizem ser aceitável que se invada algum sistema, com acessos não prejudiciais, sem que seja cometido algum furto, configurando-se, segundo eles, com ações que não envolvem propriamente vandalismo ou destruição. Em contrapartida, confiar num *hacker* que não tem sua ética bem definida, que hora pode agir para o mal, hora para o bem, é arriscado. Por mais que afirmem que irão adentrar num sistema e não prejudicar nada, o fato de invadir uma "propriedade" por si só, já se torna uma atitude, de certa maneira, antiética.

2.3.4 *SCRIPT KIDDIE*

Marques Filho (2010) ensina que o *script kiddie* é o nome dado aos indivíduos que não tem um grande poder de conhecimento e de domínio sobre programação. Alguns consideram que são uma espécie de *crackers* inexperientes, normalmente adolescentes, e outros afirmam que nem isso são, configurando-se apenas como pessoas que tentam se passar por *crackers,* a fim de conseguir fama e outras formas de lucros pessoais, provocando a ira e a repulsa dos *hackers*.

A grande maioria dos ataques virtuais são feitas por *script kiddies*, através da utilização de programas para auferir seus objetivos. Esse grupo procura por alvos fáceis, tendo como objetivo principal obter acesso à conta do administrador de uma máquina, seja lá qual ela for. Não existe a procura por informações ou companhias específicas. Sendo assim, suas ações consistem em buscar um pequeno número de falhas pela *internet* inteira, até que se consiga achar uma máquina que tenha uma boa vulnerabilidade. Mesmo que cada *script kiddie* possua o conhecimento diferente um do outro, quando entram em ação, todos seguem basicamente o mesmo raciocínio ou plano de estratégia; procurar, de forma alternada, por falhas específicas, para que, mais a frente, elas possam vir a ser exploradas. Ou seja, sua metodologia consiste em realizar um rastreamento pela *internet* em busca de uma falha específica. Quando encontrada, começam a explorá-la através de ferramentas, muitas delas automáticas, requerendo uma intervenção mínima do *script kiddie*. Pode-se ainda executar tal ferramenta e retornar até alguns dias depois para observar o resultado. Por procurarem falhas comuns, é de praxe que eles busquem invasões mais simplificadas. Sendo assim, tendo o conhecimento de que os *script kiddie* podem atacar qualquer sistema, independentemente de sua importância, a melhor forma de se proteger é entender a maneira como eles atacam, como os sistemas funcionam, assim como suas falhas e vulnerabilidades.

2.3.5 *PHREAKER*

Segundo Moraz (2006), o objetivo do *phreaker* atual é, na maioria das vezes, a quebra de sistemas de segurança envolvendo a telefonia móvel. Sua intenção é a de utilizar serviços de telefonia fixa, publica e celular sem gastar um único centavo. As técnicas geralmente não envolvem ataques excessivamente agressivos a servidores

ou às redes das operadoras, e sim um enorme esforço na identificação de falhas de segurança, permitindo a utilização de programas especiais nos aparelhos e uso de números ilegítimos para a efetuação de ligações (clonagem).

Já Marques Filho (2010) afirma que os intitulados *phreakers* são alucinados por telefonia. Por terem um imenso conhecimento sobre telefonia (móvel e fixa), através de programas e equipamentos, eles são capazes de invadir centrais telefônicas e realizar ligações internacionais sem pagar nenhuma taxa – a partir de ataques a servidores que estão localizados em outros países – por exemplo. Normalmente, os *phreakers* são ex-funcionários de companhias e, que por "n" motivos, tentam prejudicar tais empresas através de seus conhecimentos.

Segundo Marques Filho (2010), o primeiro *phreaker* foi o americano John Draper, mais conhecido como Capitão Crunch. Ele foi o responsável por descobrir que um pequeno apito de plástico que era encontrado nas caixas de um cereal – contendo uma mascote chamado Cap'n Crunch (daí advém seu apelido) –, emitia fielmente a mesma frequência de 2600hz dos orelhões da AT&T, permitindo que o usuário pudesse realizar ligações gratuitas. No ano de 1972, John Draper foi preso por fraude e condenado a cinco anos de estágio. No início da década de 70, ele havia ensinado algumas técnicas das suas habilidades com o *phreaking* a Steve Jobs e a Steve Wosniak. No Brasil, existem alguns *phreakers* que conseguem ter acesso direto à algumas centrais de telefonia. Dessa forma, eles podem tanto ligar quanto desligar telefones, além de ter o poder de apagar contas.

Existem também outros tipos de *crackers*, como o *lammer*, que é aquele indivíduo que se autopromove tentando ser um *hacker*, porém não tem o conhecimento técnico em TI. Os mesmos não criam o seu próprio programa e muitas vezes não têm conhecimento em linguagens de programação, utilizando assim, *softwares* prontos de outras pessoas. Há também o *newbie*, que é aquele iniciante no mundo da tecnologia, mais conhecido como um "*hacker* em estudo". Já o *cracker* intitulado *defacer,* são os *crackers* especializados em *websites*, porém nem sempre um especialista, podendo fazer uso daqueles aplicativos pré-fabricados. O Brasil já é conhecido no mundo inteiro por ter a maior porcentagem de páginas modificadas pelos *defacers*. Essa medição é feita através de *sites* que servem para contabilizar

esses ataques, como uma espécie de *ranking.* O grande objetivo dos *defacers*, ao contrário do que muitos possam imaginar, não é simplesmente se divertir, roubar dados, colher informações ou furtar dinheiro dos *sites*, já que, através das invasões, os *defacers* têm acesso a números de contas e cartões de crédito. Para eles, o grande motivador desse "jogo" é a fama, quanto mais famoso e reconhecido for o *site*, maior prestígio determinado grupo invasor irá obter. Moraz (2006) vê os *defacers* como os pichadores digitais, a versão contemporânea dos pichadores de muros tradicionais. Os considerados "sérios" normalmente apresentam mensagens de protesto sobre páginas de instituições consideradas danosas ao público ou que tenham praticado qualquer ação vista como repugnante ao bem-estar geral de uma comunidade.

Dentre estes apontados acima, existem vários outros termos para esses atacantes, cada um com seu respectivo objetivo na rede mundial. Basicamente a maioria deles tem o mesmo conhecimento, mas a forma que o usam é diferente. *Hacker* ainda assim é um termo muito usado erroneamente para definir os ladrões virtuais, e acabam manchando a imagem de alguns deles.

2.4 TIPOS DE ATAQUES

Em seu livro, Mitnick (2003) afirma que o engenheiro social habilidoso quase sempre visa o pessoal de nível mais baixo da hierarquia organizacional. Pode ser fácil manipular essas pessoas para que elas revelem informações aparentemente inofensivas que o atacante usa para chegar mais próximo da obtenção das informações mais confidenciais da empresa. O autor também afirma que o atacante visa os empregados do nível iniciante porque geralmente eles não têm consciência do valor das informações específicas da empresa, ou dos possíveis resultados de determinadas ações. Da mesma forma, eles tendem a ser facilmente influenciados por algumas das abordagens mais comuns da engenharia social — um interlocutor que invoca a autoridade; uma pessoa que parece amistosa e agradável; uma pessoa que parece conhecer pessoas da empresa que são conhecidas da vítima; uma solicitação que o atacante diz ser urgente ou a sugestão de que a vítima obterá algum tipo de favor ou reconhecimento.

- Ataque indireto: este é tipo de ataque mais intrusivo e usado não só pelos engenheiros social, mas também pelos *crackers* em geral, aplicando técnicas de invasão como vírus e *sites* com códigos maliciosos ou cartas, *e-mails* e *sites* falsos imitando os mais famosos. Os usuários que têm seus dados coletados nestes ataques nem sempre são o alvo principal, servindo apenas de ponte de acesso aos dados da empresa.
- Ataque direto: alguns engenheiros ousam em atacar pessoalmente, mas a maioria ainda é feita por telefone, exigindo muito planejamento prévio de cada fase do ataque. Usando seus dons artísticos e persuasivos, o engenheiro precisa ter muito senso de improviso e um raciocínio muito rápido, caso algo não saia como esperado, para não ser desmascarado.

2.5 MEIOS DE ATAQUE

Peixoto (2006) lista alguns meios pelos quais os ataques são realizados pelos engenheiros sociais:

- Telefone ou VoIP (voz sobre IP): passar-se por alguém que não é, seria um dos típicos ataques de engenharia social, como na personificação (*help desk*);

Internet (coleta de informações): como, por exemplo, *sites* que fornecem ID e *passwords*, *sites* clonados ou via FTP, Facebook, registro.br, Google, dentre outros;

Intranet (acesso remoto): algo extremamente possível de acontecer. Como por exemplo, por acesso remoto, capturando-se o micro de determinado usuário da rede e se passando por alguém que na verdade não é. Como dito anteriormente, um funcionário insatisfeito é uma das maiores ameaças existentes.

- *E-mail* falso*: fakemaisl* nada mais são do que os *e-mails* falsos, o famoso *phishing scam;*
- Pessoalmente: poder de persuasão, habilidades em saber conversar, o tipo de ataque mais raro. O engenheiro social faz-se passar por alguém que na verdade ele não é, adotando toda uma encenação. E como um verdadeiro artista busca manipular a vítima de forma a ser muito convincente no que diz. Esse tipo de ataque ganha mais força quando o atacante já conhece literalmente o território no qual vai pisar, mas, sobretudo, já tem consigo informações que lhe conferem subsídios para persuadir a vítima, valendo-se às vezes até mesmo de informação tidas como confidenciais.

Alguns recursos a favor do engenheiro social seriam: a sedução, a intimidação, a dramaticidade e a credibilidade.

- *Chats* (bate papo): fazer-se passar por alguém que na verdade não é fica mais fácil pelos canais de bate papo. Além de tudo, mandar fotos fica bem mais atrativo e seduz com mais facilidade a conseguir informações que deseja;
- Fax: primeiramente, obter o número do fax da pessoa física ou jurídica para que se possa começar o ataque. Seguindo praticamente os mesmos princípios do *e-mail*, enviando, por exemplo, pedidos de requisição, formulário de preenchimento, dentre outros, para posterior retorno do que se deseja obter;
- Cartas/correspondências: não é o mais moderno, mas é um recurso poderoso que faz como uma das maiores vítimas, as pessoas mais velhas e aquelas que têm certa resistência à tecnologia. É muito fácil hoje elaborar uma carta, documentos com logomarcas e tudo mais, dando-se a impressão de que trata-se realmente daquela origem;
- *Spyware: software* espião usado para monitorar de modo oculto as atividades do computador de um alvo;

Mergulho no lixo: várias coisas que são descartadas para o lixo muitas vezes contêm informações essenciais ao suposto engenheiro social, se não descartado de forma correta;

- Surfar sobre os ombros: é o ato de observar uma pessoa digitando no teclado do computador para descobrir e roubar suas senhas ou outras informações de usuário;

2.6 TÉCNICAS DE ATAQUES

Para Peixoto (2006), as artimanhas usadas por um engenheiro social estão em constante evolução. Procuram sempre buscar algo inovador, diferente do tradicional para conseguir atingir os seus objetivos, porém mesmo perante tais transformações e mudanças no segmento da arte de enganar, modificando ou incrementando seus ataques, o engenheiro social utiliza-se sempre de alguns aspectos clássicos de ataque.

Para Oliveira (2003), uma invasão é a entrada num *site*, servidor, computador ou serviço por alguém não autorizado. Mas, antes da invasão propriamente dita, o invasor pode fazer um teste de invasão, que é uma tentativa de exploração de

vulnerabilidade em partes, onde o objeto é avaliar a segurança de uma rede e identificar os seus pontos vulneráveis. O autor afirma que não existe invasão sem um invasor, que pode ser conhecido, na maioria das vezes, como *hacker* ou *cracker.* Ambos usam os conhecimentos para se dedicarem a testar os limites, ou para estudo e procura de conhecimento ou até mesmo por curiosidade, ou ainda, por simples prazer.

Existem muitas ferramentas para facilitar uma invasão e a cada dia aparecem novidades a respeito. O autor lista algumas:

- *Spoofing*: é onde o invasor convence alguém de que ele é algo ou alguém que não é, sem ter permissão para isso, conseguindo autenticação para acessar o que não deveria ter acesso, falsificando o seu endereço de origem. É uma técnica de ataque contra a autenticidade, onde um utilizador externo se faz passar por um utilizador interno.
- *Snnifers*: é um programa de computador que monitora passivamente o tráfego de rede. Pode ser utilizado legitimamente pelo administrador do sistema para verificar problemas de rede, ou pode ser usado ilegitimamente por um intruso, para roubar nomes de utilizadores e senhas. Este tipo de programa explica o fato dos pacotes das aplicações de TCP/IP não serem criptografados. Para utilizar o *snnifer*, é necessário que ele esteja instalado na rede onde passe tráfegos de pacotes de interesse para o invasor ou administrador.
- DoS (*denial of service*): é um ataque de recusa de serviço. Estes ataques são capazes de anular um *site*, indisponibilizando os seus serviços. É baseado na sobrecarga de capacidade ou em uma falha não esperada. Um dos motivos para existirem este tipo de falhas nos sistemas deve-se a um erro básico de programadores, em que no momento de testar um sistema, muitas vezes não testam o que acontece se o sistema for forçado a dar um erro, se receber muitos pacotes em pouco tempo ou se receber pacotes com erros. Normalmente, apenas é testado se o sistema faz o que deveria fazer e alguns erros básicos. O invasor parte deste princípio e faz diversos tipos de testes de falhas, até acontecer um erro e o sistema parar. Este tipo de ataque não causa perda ou roubo de informações, mas é um ataque preocupante, pois os serviços do sistema atacado ficarão indisponíveis por um tempo determinado. Dependendo da equipe existente na empresa para disponibilizar

novamente o sistema e dependendo do negócio da empresa, este tempo de indisponibilidade pode trazer muitos prejuízos financeiros.

- DDoS (*distributed* DoS): são ataques semelhantes aos DoS, tendo como origem diversos e até milhares de pontos disparando ataques DoS para um ou mais *sites* determinados. Para isto, o invasor coloca agentes para dispararem o ataque numa ou mais vítimas. As vítimas são máquinas escolhidas pelo invasor por possuírem alguma vulnerabilidade. Estes agentes, ao serem executados, transformam-se num ataque DoS de grande escala.
- DNS *Spoofing*: o objeto principal do DNS *Spoofing* é o de destruir o servidor de nomes e com isto permitir que máquinas não confiáveis, que podem ser as do invasor, sejam consideradas confiáveis, pois passarão pelas confiáveis. Para realizar este ataque, o invasor precisa ter o controle sobre a máquina servidor de DNS, onde constam todos os nomes das máquinas confiáveis e os endereços destas máquinas, que são os números IP. Além disso, o invasor precisara saber o nome de umas destas máquinas confiáveis. Na posse destes dados, o invasor altera o registro do DNS que mapeia o endereço IP da máquina confiável escolhida, modificando para que contenha o endereço da máquina do invasor. A partir desta alteração, o invasor terá livre acesso a serviços que necessitam da autenticação deste servidor de nomes. A maioria dos novos sistemas possui métodos contra o DNS *Spoofing*, utilizando uma técnica chamada *cross-check*. Nesta técnica, o nome retornado pela consulta é testado novamente pelo DNS. Se o endereço utilizado para a conexão é diferente do retornado pelo *cross-check*, a conexão é bloqueada e é gerado um alerta. Esta técnica pode ser implementada no servidor de DNS ou nos servidores do serviço com autenticação baseada no DNS. Mas, existem variantes do DNS *spoofing,* onde o invasor tenta enganar o *cross-check*, esgotando o servidor de DNS com pedidos.
- Quebra de *passwords*: para acessar algo, é necessária uma senha de acesso. Muitos invasores tentar descobrir estas senhas através de técnicas de quebra de senhas, como tentativas de nome de conjugue ou, datas etc. Para facilitar a descoberta da senha, existem diversos programas, como dicionários de senhas e programas que tentam todas as combinações possíveis de caracteres para descobri-las.
- Vírus: o vírus de computadores é outro exemplo de programas, utilizados maliciosamente ou não, que se reproduzem introduzindo-se em outros programas. Quando estes programas são executados, o vírus é ativado e pode se espalhar ainda

mais, geralmente danificando sistemas e registro dos computadores onde ele se encontra.

Oliveira (2003) conclui que o invasor pode utilizar-se da evasão, que é a arte de não deixar pistas de quem invadiu, e como isto aconteceu. Quando isto é feito com êxito, dificulta ainda mais a descoberta desta vulnerabilidade e, assim, da correção da mesma, para proteção de novos ataques.

2.7 CRIMES DIGITAIS

> "Poderíamos dizer que os "crimes" digitais seriam todos aqueles relacionados as informações arquivadas ou em trânsito por computadores, sendo esses dados, acessados ilicitamente, usados para ameaçar ou fraudar; para tal prática é indispensável a utilização de um meio eletrônico. Toda sociedade dependente da informação acaba sendo vítima de simples ameaças e até do terrorismo e do vandalismo eletrônicos" (CORRÊA, 2000, p. 43).

Do mesmo jeito que há vários tipos de atacantes, há também vários tipos de crimes digitais, cada um com seu perfil e objetivo. Esses crimes geralmente têm a finalidade de roubar dados das vítimas, como senhas de cartão de crédito ou débito, ou senhas de contas como *e-mail* e rede social.

Sêmola (2014) define ameaças como agentes ou condições que causam incidentes que comprometem as informações e seus ativos por meio da exploração de vulnerabilidades, provocando perdas de confidencialidade, integridade e disponibilidade, e, consequentemente, causando impactos aos negócios de uma organização. O autor classifica as ameaças quanto a sua intencionalidade, podendo ser divididas nos seguintes grupos:

- Naturais: ameaças decorrentes de fenômenos da natureza, como incêndios naturais, enchentes, terremotos, tempestades eletromagnéticas, maremotos, aquecimento, poluição etc.
- Involuntárias: ameaças inconscientes, quase sempre causadas pelo desconhecimento. Podem ser causadas por acidentes, erros, falta de energia etc.
- Voluntárias: ameaças propositais causadas por agentes humanos como *hackers*, invasores, espiões, ladrões, criadores e disseminadores de vírus de computador, incendiários.

2.8 VULNERABILIDADES

Em sua obra, Sêmola (2014) define vulnerabilidades como fragilidades presentes ou associadas à ativos que manipulam e/ou processam informações que, ao serem exploradas por ameaças, permitem a ocorrência de um incidente de segurança, afetando negativamente um ou mais princípios da segurança da informação: confidencialidade, integridade e disponibilidade.

O autor explica também que as vulnerabilidades por si só, não provocam incidentes, pois são elementos passivos, necessitando de um agente causador ou condição favorável, que são as ameaças. E também lista alguns exemplos:

- Físicas: Instalações prediais que não atendem as boas práticas ou as normas e regulamentações vigentes; falta de extintores, detectores de fumaça e de outros recursos para combate a incêndio em ambientes com ativos ou informações estratégicas; controle de acesso deficiente em locais contendo informações confidenciais ou sensíveis etc.
- Naturais: Ambientes com equipamentos eletrônicos próximos a locais suscetíveis a desastres naturais, suscetíveis à incêndios, enchentes, terremotos, tempestades e outros, como falta de energia, acúmulo de poeira, aumento de umidade e de temperatura etc.
- *Hardware:* Computadores são suscetíveis a poeira, umidade, sujeira e acesso indevido a recursos inadequadamente protegidos, podendo ainda sofrer com componentes deficientes ou mal configurados, com falhas ou flutuações no suprimento energético, ou aumento excessivo na temperatura ambiente.
- *Software*: Erros na codificação, instalação ou configuração de sistemas e aplicativos podem acarretar acessos indevidos, vazamento de informações, perda de dados e de trilhas de auditoria ou indisponibilidade do recurso quando necessário.
- Mídias: Discos, fitas, relatórios e impressos podem ser perdidos ou danificados; falhas de energia podem causar panes em equipamentos, podendo danificar trilhas lógicas de dados; discos rígidos usualmente têm vida útil; a radiação eletromagnética pode afetar diversos tipos de mídias magnéticas.

- Comunicação: A comunicação telefônica é vulnerável a escutas (acesso indevido) ou a problemas na infraestrutura física ou lógica que a impeçam de ser estabelecida.
- Humanas: Falta de treinamento ou de conscientização das pessoas, falta de avaliação psicológica adequada ou de verificação de antecedentes (*background check*) que identifique objetivos escusos ou problemas anteriores, ou mesmo má-fé ou o descontentamento de um funcionário, entre outros, podem levar ao compartilhamento indevido de informações confidenciais, à não execução de rotinas de segurança ou a erros, omissões etc. que ponham em risco as informações.

3 SEGURANÇA DA INFORMAÇÃO

> "Um ditado popular diz que nenhuma corrente é mais forte que seu elo mais fraco; da mesma forma, nenhuma parede é mais forte que sua porta ou janela mais fraca, de modo que você precisa colocar as trancas o mais resistente possível nas portas e janelas. De forma similar, quando você implementa segurança em um ambiente de informações, o que na realizada você está procurando fazer é eliminar o máximo possível de pontos fracos ou garantir o máximo de segurança possível para os mesmos". (CARUSO, 1999, p. 21)

Sêmola (2014) define segurança da informação como uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade.

Para Rezende (2003), a informação é todo o dado trabalhado, útil, tratado com valor significativo atribuído ou agregado à ele e com um sentido natural e logico para quem usa essa informação. O dado é entendido como um elemento da informação, um conjunto de letras, números ou dígitos, que, tomado isoladamente, não transmite nenhum conhecimento, ou seja, não contem um significado claro. Afirma também que a informação tem um valor altamente significativo e pode representar grande poder para quem a possui, seja pessoa ou seja instituição. Ela possui seu valor, pois está

presente em todas as atividades que envolvem pessoas, processos, sistema, recursos financeiros, tecnologias etc.

O conceito de segurança da informação, segundo a norma ABNT NBR ISO/IEC 17799:2005 (2005) é: “A segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade de negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio”. Esta norma rege também que a segurança da informação é caracterizada por três fundamentos essências, o famoso CID: confidencialidade, integridade e disponibilidade.

Resumindo o termo, informação é o resultado do processamento, manipulação e organização de dados numa forma que se some ao conhecimento da pessoa que o recebe.

3.1 O VALOR DA INFORMAÇÃO

Caruso (1999, p. 21) afirma que, acima de tudo, o bem mais valioso de uma empresa pode não ser o gerado pela linha de produção ou o serviço prestado, mas as informações relacionadas com esse bem de consumo ou serviço. É importante que os executivos em geral se conscientizem de que todas as informações têm algum tipo de valor para alguém e/ou para algo; o que ocorre é que ainda não se descobriu para quem ou para quê. Acrescenta também que ao longo da história, o ser humano sempre buscou o controle sobre as informações que lhe eram importantes de alguma forma. Isso é verdadeiro mesmo nas mais remota antiguidade, e o que mudou desde então foram as formas de registro e armazenamento das informações. Se na pré-história e até mesmo nos primeiros milênios da idade antiga o principal meio de armazenamento e registro de informações era a memória humana, com o advento dos primeiros alfabetos isso começou a mudar, mas foi somente nos últimos dois séculos que as informações passaram a ter importância crucial para as organizações humanas.

3.2 OS PILARES DA SEGURANÇA DA INFORMAÇÃO

Sêmola (2014), em sua obra, lista os três princípios básicos da segurança da informação. São elas:

- Confidencialidade: toda informação deve ser protegida de acordo com o grau de sigilo de seu conteúdo, visando a limitação de seu acesso e uso apenas às pessoas a quem é destinada.

Já Dantas (2011) define confidencialidade como a garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso. Comenta também que ocorre a quebra da confidencialidade da informação ao se permitir que pessoas não autorizadas tenham acesso ao seu conteúdo. A perda da confidencialidade é a perda do segredo da informação e garanti-la é assegurar o valor da informação e evitar a divulgação indevida.

- Integridade: toda informação deve ser mantida na mesma condição em que foi disponibilizada pelo seu proprietário, visando protegê-la contra alterações indevidas, intencionais ou acidentais.

Dantas (2011) assegura que a integridade é a garantia da exatidão e completeza da informação e dos métodos de processamento. Garantir a integridade é permitir que a informação não seja modificada, alterada ou destruída sem autorização, que ela seja legítima e permaneça consistente. Ocorre a quebra da integridade quando a informação é corrompida, falsificada, roubada ou destruída. Garantir a integridade é manter a informação na sua condição original. Contribuem para a perda da integridade: as inserções, substituições ou exclusões de parte do conteúdo da informação; as alterações nos seus elementos de suporte, que podem ocorrer quando são realizadas alterações na estrutura física e lógica onde ela está armazenada, ou quando as configurações de um sistema são alteradas para se ter acesso a informações restritas, bem como são superadas as barreiras de segurança de uma rede de computadores.

- Disponibilidade: toda informação gerada ou adquirida por um indivíduo ou instituição deve estar disponível aos seus usuários no momento em que eles necessitem delas para qualquer finalidade.

No ponto de vista de Dantas (2011), a disponibilidade é a garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário. Ocorre a quebra da disponibilidade quando a informação não está disponível para ser utilizada, ou seja, ao alcance de seus usuários e destinatários, não podendo ser acessada no momento em que for necessário utilizá-la. Garantir a disponibilidade é assegurar o êxito da leitura, do trânsito e do armazenamento da informação.

Esses são as três características fundamentais que devem ser preservadas, pois são tidas como princípios da segurança da informação.

Dantas (2011) aponta também outros quatro fundamentos importantes, são eles:

- Autenticidade: é a garantia de que a informação é oriunda da fonte que lhe é atribuída e elaborada por quem tem autoridade para tal.
- Confiabilidade: é a garantia de que a informação é confiável, oriunda de uma fonte autêntica e que expressa uma mensagem verdadeira. A autenticidade e confiabilidade estão interligadas. A primeira diz respeito à idoneidade da fonte, isto é, digna de fé e confiança, e a segunda ao seu conteúdo. A avaliação da fonte para a sua autenticidade pode ser feita com relação à sua idoneidade, como, por exemplo: completamente idônea, regularmente idônea, inidônea e cuja idoneidade não se pode avaliar. E a avaliação da confiabilidade pode ser feita com relação ao seu conteúdo, como, por exemplo: confirmação por outras fontes, por ser verdadeira, duvidosa ou improvável.
- Não repúdio: é a garantida de que a informação chegará ao destino certo e não será repudiada.
- Responsabilidade: é a coparticipação de responsabilidades por todos os que produzem, manuseiam, transportam e descartam a informação, seus sistemas e redes de trabalho.

4 COLETA E ANÁLISE DE DADOS

4.1 PROBLEMA E JUSTIFICATIVA

4.1.1 PROBLEMA

No cenário atual, em que as empresas dependem cada vez mais da tecnologia e da informação, é vital garantir a segurança adequada deste ativo, considerado estratégico em sua missão de prestar serviços de qualidade. A empresas precisam investir mais em treinamento de manuseio de seus dados pelos seus funcionários.

4.1.2 JUSTIFICATIVA

A solução mais adequada é o estabelecimento de um conjunto de normas e regras que regulem a utilização dos sistemas das empresas, assim como o acesso à redes sociais e *e-mails* pessoais. Todo processo de segurança começa no recrutamento e é importante lembrar que os trabalhadores devem estar cientes do manuseio das informações.

4.2 OBJETIVOS

4.2.1 OBJETIVO GERAL

O objetivo desta pesquisa se caracteriza por investigar como os funcionários e empresas de vários segmentos procedem para garantir a segurança da informação e verificar se o compartilhamento de conhecimento é o principal meio pelo qual os indivíduos tentam garantir a segurança da informação.

4.2.2 OBJETIVO ESPECÍFICO

Também são objetivos desta pesquisa, investigar o conhecimento que os indivíduos associados à estas empresas têm sobre normas e melhores práticas de segurança da informação, além dos meios tecnológicos utilizados por eles. Para atingir os objetivos, foram escolhidos funcionários de diversas áreas e de empresas de diversos segmentos, nas quais serão realizados questionários.

Como futuros estudos, seria adequado dirigir o estudo à uma empresa especializada em Gestão e Auditoria em TI, para que adotassem os novos métodos e

que estes durante o passar do tempo fossem observados. E por fim, refazer um novo questionário ou entrevista com os indivíduos para avaliar os pontos que tiveram progresso e concluir se realmente a nova abordagem é vantajosa aos propósitos da empresa.

4.3 METODOLOGIA

Segundo Queiroz (2006) a pesquisa quantitativa e a pesquisa qualitativa, considera-se que existe de fato uma diferença entre as duas abordagens, mas que elas não são excludentes e sim complementares.

Em relação ao método de estudo o presente trabalho é uma pesquisa descritiva. São inúmeros os estudos que podem ser classificados sob este título e uma de suas características mais significativas está na utilização de técnicas padronizadas de coleta de dados, tais como o questionário e a observação sistemática.

4.3.1 INSTRUMENTO DE COLETA

O instrumento de coleta foi em forma de questionário com perguntas fechadas para o proprietário, funcionário, diretor, gerente ou coordenador de empresas. As empresas de diversos setores foram escolhidas devido à existência de diversos riscos inerentes à prestação de serviços de tecnologia da informação e da ausência de pesquisas empíricas sobre segurança da informação neste setor, causando assim, o desconhecimento por parte do empregador e do empregando.

O questionário foi aplicado *online* e é uma ferramenta que, ao ser utilizada, demonstra o nível de ciência que os funcionários da empresa têm em relação à importância da segurança da informação e se eles foram preparados para tal, considerando diversos aspectos e, especialmente, a segurança dos dados.

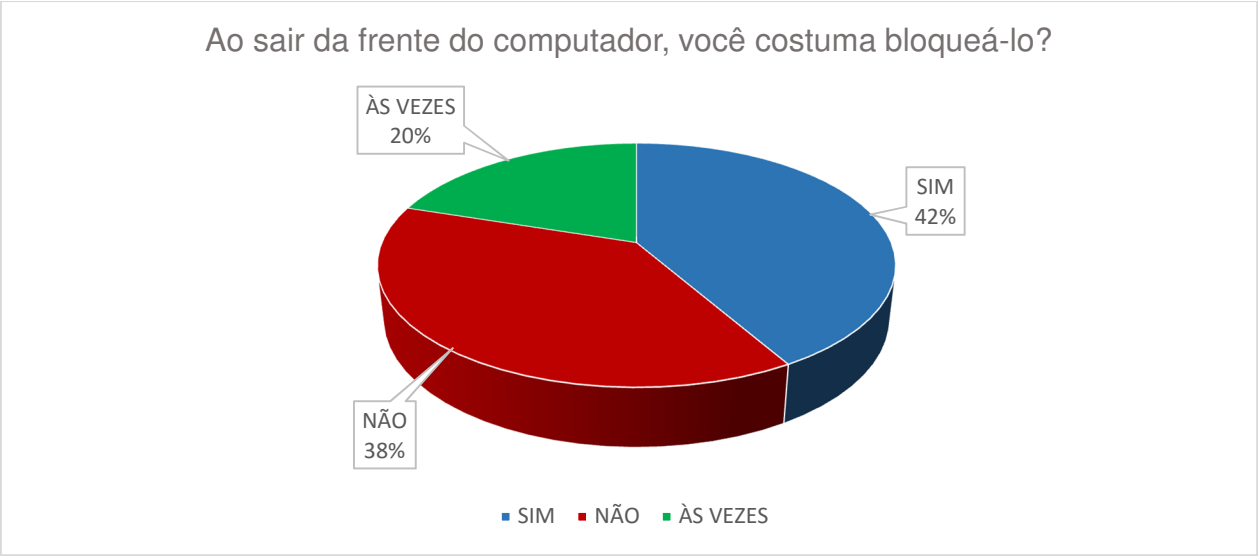
4.4 RESULTADOS

Foram elaboradas e aplicadas 10 questões e as mesmas foram respondidas por 60 pessoas de diversas empresas. Abaixo, serão expostos os resultados de algumas delas, para futura análise.

QUESTÃO 1: Ao sair da frente do computador, você costuma bloqueá-lo?

RESULTADO:

Figura 1: Dados da questão 1



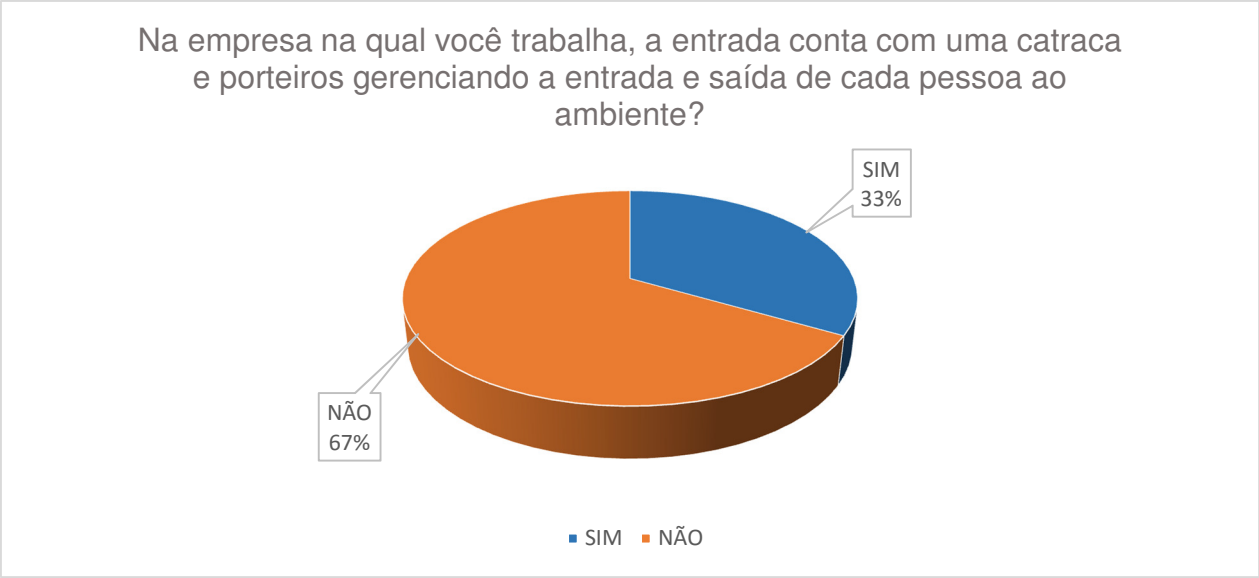
Fonte: Elaborado pela autora

ANÁLISE: Vê-se que quase metade dos empregados não costumam bloquear o computador ao se ausentar de sua mesa, o que não é aconselhável, tendo em vista que outra pessoa pode se aproveitar da ausência do dono do computador, e desfrutar de acessos privilegiados daquele determinado usuário, sem ao menos necessitar das senhas de seus acessos.

QUESTÃO 2: Na empresa na qual você trabalha, a entrada conta com uma catraca e porteiros gerenciando a entrada e saída de cada pessoa ao ambiente?

RESULTADO:

Figura 2: Dados da questão 2

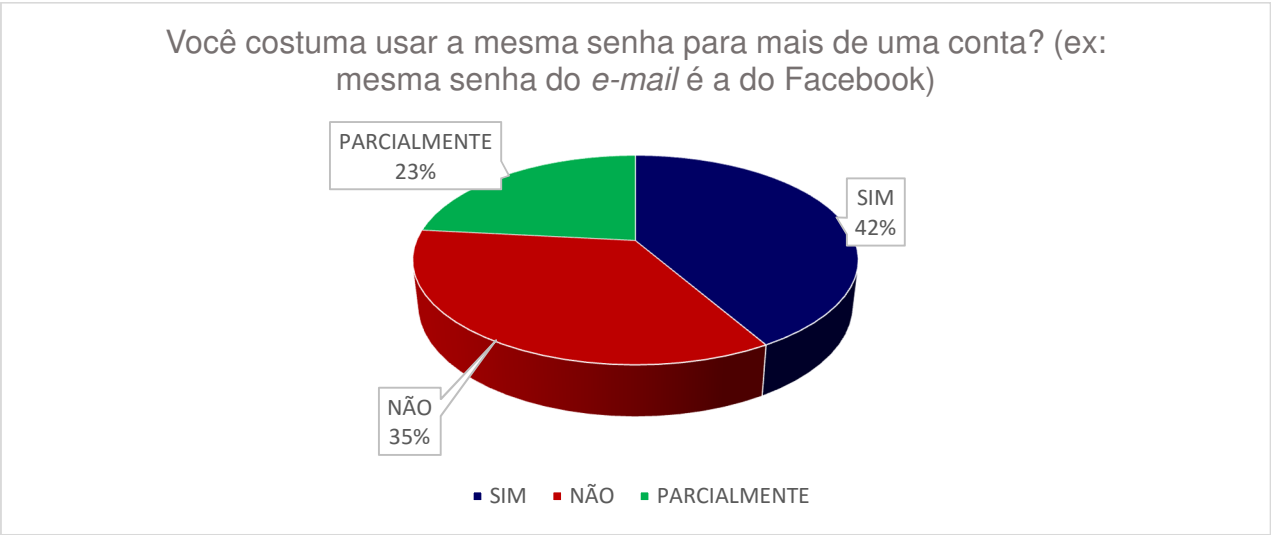


Fonte: Elaborado pela autora

ANÁLISE: Nesta questão, nota-se que mais da metade dos entrevistados trabalham em empresa cuja segurança física não é levada em consideração, ou seja, qualquer intruso pode ter acesso físico ao ambiente de trabalho e, posteriormente, acessos autorizados onde somente funcionários credenciados deveriam ter.

QUESTÃO 3: Você costuma usar a mesma senha para mais de uma conta? (Ex: mesma senha do *e-mail* é a do Facebook)

Figura 3: Dados da questão 3



Fonte: Elaborado pela autora

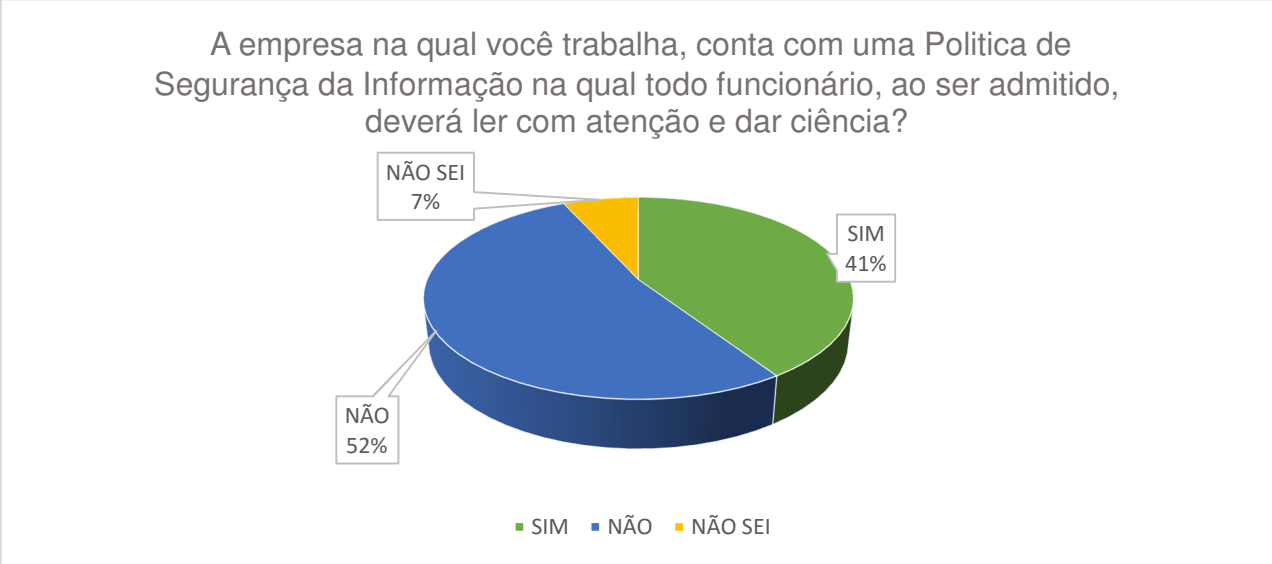
ANÁLISE: Na questão acima, pode-se verificar uma grande falha humana. A maioria dos entrevistados garante que usa a mesma senha para mais de uma

aplicação, facilitando para aquele que já conta com uma senha roubada ou até mesmo retirada do próprio dono, deixando-o apenas com a parte do “teste e sucesso”.

QUESTÃO 4: A empresa na qual você trabalha, conta com uma Política de Segurança da Informação na qual todo funcionário, ao ser admitido, deverá ler com atenção e dar ciência?

RESULTADO:

Figura 4: Dados da questão 4



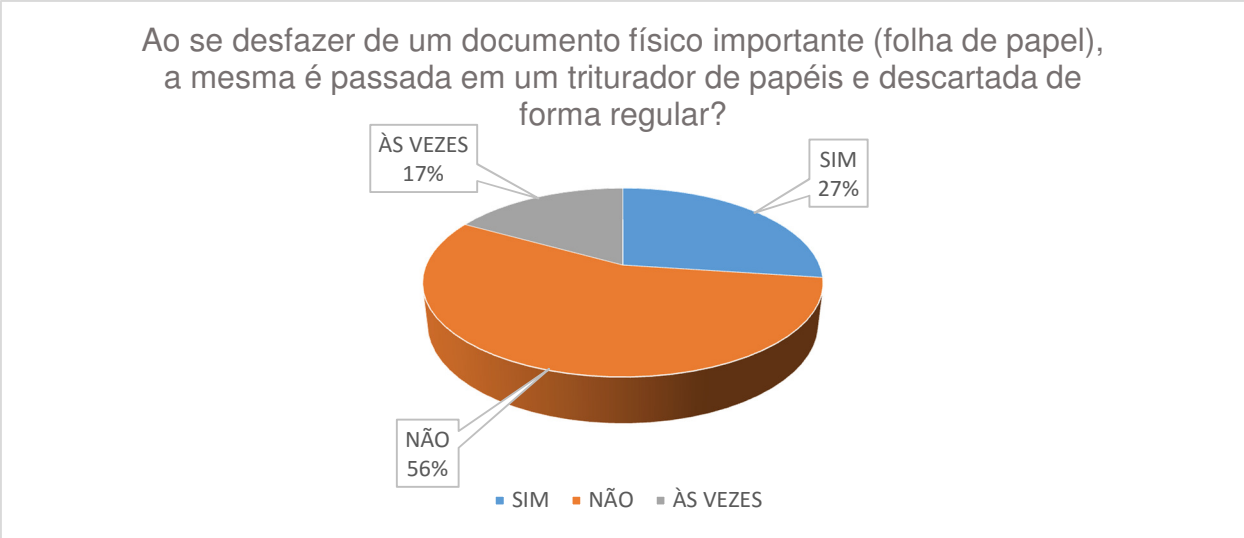
Fonte: Elaborado pela autora

ANÁLISE: Mais da metade dos entrevistados garante que não há uma Política de Segurança da Informação na empresa na qual trabalha, impossibilitando assim o seu funcionário de ficar ciente das medidas a serem tomadas quanto à segurança dos dados dentro da corporação. A mesma precisa ser adotada pelas organizações para situações em que a tecnologia não consegue atender, visto que muitos incidentes estão relacionados aos comportamentos humanos, ou seja, falhas humanas. Este item será melhor abordado no capitulo 5.

QUESTÃO 5: Ao se desfazer de um documento físico importante (folha de papel), a mesma é passada em um triturador de papéis e descartada de forma regular?

RESULTADO:

Figura 5: Dados da questão 5



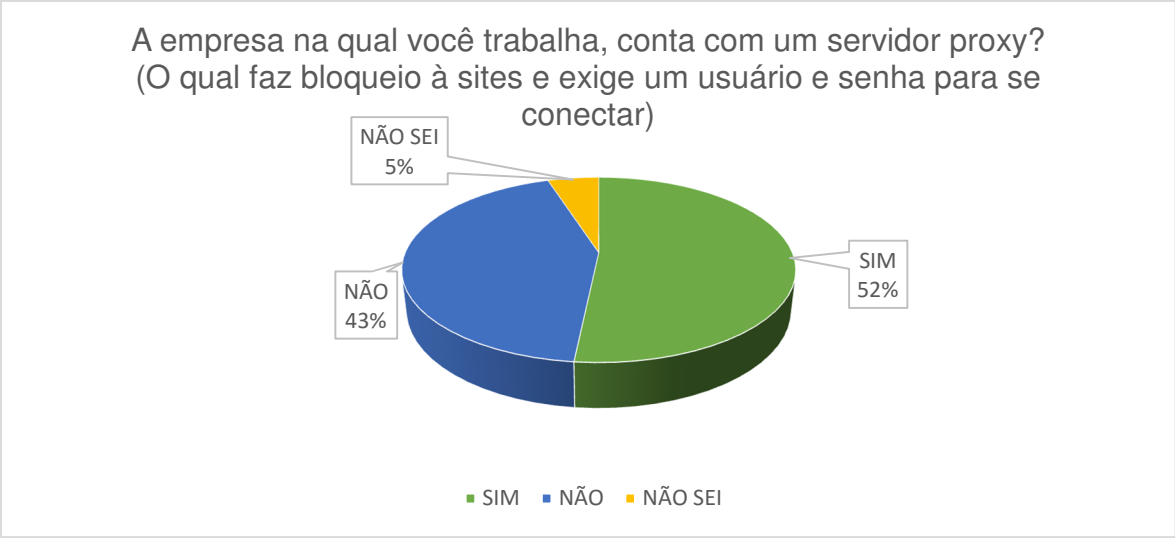
Fonte: Elaborado pela autora

ANÁLISE: Nesta questão, nota-se que que mais da metade dos entrevistados garantem que não se desfazem dos documentos importantes de maneira correta, podendo ser alvo dos engenheiros sociais “mergulhadores de lixo”. Muitas das informações não descartadas adequadamente podem parar em mãos erradas. Este poderia ser um item abordado na Política de Segurança de uma empresa, porem os mesmos afirmaram que desconhecem tal documento na admissão.

QUESTÃO 6: A empresa na qual você trabalha, conta com um servidor proxy? (O qual faz bloqueio à *site*s e exige um usuário e senha para se conectar)

RESULTADO:

Figura 6: Dados da questão 6



Fonte: Elaborado pela autora

ANÁLISE: Nesta ultima questão a ser análisada, pode-se ver que metade das empresas não contam nem com servidor *proxy*, permitindo os seus funcionarios a terem acesso total à *internet*. Isso pode ser um problema caso o funcionário não seja treinado de forma adequada a fazer o uso da rede, podendo assim entrar em *sites* infectados ou fazer o *download* de um vírus.

5 PREVENÇÃO

Segundo Mitnick (2003), as empresas que realizam testes de penetração de segurança relatam que suas tentativas de invadir os sistemas de computadores de uma empresa cliente com métodos da engenharia social têm um índice de sucesso de quase 100%. As tecnologias de segurança podem dificultar esses tipos de ataques retirando as pessoas do processo de tomada de decisão. Entretanto, o único meio verdadeiramente efetivo de amenizar a ameaça da engenharia social é usar a conscientização para a segurança combinada das políticas de segurança da que definem as principais regras para o comportamento do empregado, junto com sua educação e treinamento. Ressalta também que algumas autoridades recomendam que 40% do orçamento geral seja direcionado para a segurança da empresa seja aplicado no treinamento da conscientização.

5.1 DESCARTE DE LIXO

Peixoto (2006), em sua obra, lista 8 “segredos” para tratar o lixo com mais sabedoria, são eles:

1. Classificar todas as informações confidencias com base no grau de confiabilidade;
2. Estabelecer procedimentos em toda a empresa para descartar as informações confidenciais;
3. Insistir para que todas informações confidenciais descartadas passem primeiro pela máquina cortadora de papel e fornecer um modo seguro de se livrar das informações importantes em pedaços de papel que são pequenos demais e passam pela máquina. As máquinas não devem ser muito baratas, as quais resultam em tiras de papel que podem ser montadas novamente por um atacante determinado e com paciência. Elas devem ser do tipo que faz cortes cruzados ou do tipo que transforma a saída em polpa inútil;
4. Fornecer um modo de inutilizar ou apagar completamente as mídias de computador (disquetes CDs, DVDs, HDs) usadas para armazenar arquivos. Devendo lembrar-se de que os arquivos apagados não são realmente removidos, eles ainda podem ser recuperados;

5. Manter um nível de controle apropriado sobre a seleção das pessoas da equipe de limpeza da organização, usando a verificação de antecedentes, se for apropriado;
6. Garantir com que os empregados pensem periodicamente na natureza do material que estão jogando no lixo;
7. Trancar os contêineres de lixo;
8. Usar contêineres separados para material confidencial e fazer com que os materiais dispensados sejam manuseados por uma empresa especializada neste trabalho.

5.2 EDUCAÇÃO E TREINAMENTO

É importante conscientizar as pessoas sobre o valor da informação que elas dispõem e manipulam, seja ela de uso pessoal ou institucional. Também informar aos usuários sobre como age um engenheiro social.

Marques Filho (2010) aponta alguns fatores a serem cuidados para que as informações continuem protegidas e podem ser usadas como tópicos em treinamento de usuários, são eles:

- *Logout*, sair ou equivalente: ao se ter acesso ao e-*mail* na *web*, a conta em um *site* de comércio eletrônico, um *home banking* ou qualquer outro serviço que exige que seja fornecido um nome de usuário e uma senha, sempre, ao final da sessão. Aconselha-se que o *click* em um botão/*link* de nome *logout, logoff*, sair, desconectar ou equivalente para sair do *site*. Muita gente simplesmente sai do *site* fechando a janela do navegador de *internet* ou entrando em outro endereço. Isso é arriscado, pois o *site* não recebeu a instrução de encerrar seu acesso naquele momento e alguém mal-intencionado pode abrir o navegador de *internet* e acessar as informações da conta, caso essa realmente não tenha sido fechada devidamente.
- Senhas difíceis de serem descobertas: não utilizar senhas fáceis de serem descobertas, como nome de parentes, data de aniversário. Dar preferência a sequências que misturam letras e números. Não usar como senha uma combinação que tenha menos que 6 caracteres. Não guardar senhas em arquivos do *Word* ou de qualquer outro programa. Se necessário, pode ser anotado em um caderno, mas

apenas em casos extremos, destruindo assim que a sequência for decorada. Evitar usar a mesma senha para vários serviços, mudando-a periodicamente.

- *Downloads*: Ao usar programas de compartilhamento de arquivos, ou ao obter arquivos de *sites* especializados em *downloads*, deve-se ficar atento ao que baixar. Ao término do *download*, verificar se o arquivo não possui alguma irregularidade, como mais de uma extensão, pois muitos vírus e outras pragas se passam por arquivos de áudio, vídeo e outros para enganar o usuário. Além disso, vale examinar o arquivo baixado com um antivírus. Também deve-se ter cuidado com *sites* que pedem para instalar programas para continuar a navegar, ou para usufruir de algum serviço.
- Programas de mensagens instantâneas: é comum encontrar vírus que exploram serviços de mensagens instantâneas. Esses vírus são capazes de, durante uma conversa com um contato, emitir mensagens automáticas que contém *links* para vírus ou outros programas maliciosos. Nessa situação, é natural que a parte que recebeu a mensagem pense que seu contato é que a enviou, e clica no *link*;
- *E-mails* falsos: mais conhecidos como *phishing scam*, ou seja, um *e-mail* falso. Se uma mensagem recebida contiver textos com erros ortográficos e gramaticais, fizer ofertas tentadoras ou tem um *link* diferente do indicado, deve-se desconfiar imediatamente. Muitos *e-mails* são enviados com propostas de sorteios ou se passando por agências de banco, persuadindo a pessoa a *clickar* no *link* fornecido, redirecionando para o vírus;
- *Site* de conteúdo duvidoso: muitos *sites* contêm, em suas páginas, *scripts* capazes de explorar falhas do navegador de *internet*;
- Anexos de *e-mail*: Essa é uma das instruções mais antigas, mesmo assim, o *e-mail* ainda é uma das principais formas de disseminação de vírus. Deve-se tomar cuidado ao receber mensagens que pedem para abrir o arquivo anexo, principalmente se o *e-mail* veio de alguém desconhecido;
- Antivírus e *antispyware* atualizados: É necessário atualizá-los regularmente, do contrário, o antivírus não saberá da existência de novos vírus e praticamente todos os antivírus disponíveis permitem configurar uma atualização automática. Além disso, usar um *antispyware* com frequência para tirar arquivos e programas maliciosos de seu computador é uma boa opção;

- Compras na *internet* e *sites* de bancos: é sempre bom fazer uma pesquisa na *internet* para descobrir se existe reclamações contra a empresa antes de realizar a compra no *site* da mesma. Também deve-se ter cuidado ao ter acesso à conta bancária através da *internet*, principalmente em computadores públicos. Deve-se verificar também se o endereço do *link* é mesmo o do serviço bancário;
- Informações importantes: Em serviços de bate-papo, deve-se evitar dar detalhes do cotidiano pessoal. Evitar também disponibilizar dados ou fotos que forneçam qualquer detalhe relevante sobre a rotina ou informações de onde estará nas próximas horas ou lugares frequentados regularmente, pois toda e qualquer informação relevante sobre o pessoal pode ser usada indevidamente por pessoas mal-intencionadas, inclusive para localização;
- Cadastros: Muitos *sites* exigem um cadastro para usufruir de seus serviços, mas isso pode ser um meio de roubo de informações. Se um *site* pede o número do cartão de crédito sem ao menos ser uma página de vendas, as chances de ser um golpe são grandes. Além disso, as informações podem ser entregues a empresas que vendem assinaturas de revistas ou produtos por telefone para ser inserido em listas de *spams*.

4.3 SEGURANÇA FÍSICA

Dentro do ambiente corporativo, é importante permitir o acesso às dependências de uma organização apenas às pessoas devidamente autorizadas, bem como dispor de funcionários de segurança, como porteiros, com treinamentos adequados e um controle reforçado de acessos internos e externos, a fim de monitorar entrada e saída da organização.

Cada funcionário munir-se de um crachá com acesso às determinadas áreas também faz com que a segurança dentro do ambiente se torne melhor, evitando de que pessoas não autorizadas tenham acesso à determinado setor ou sala.

5.3 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Por mais criteriosas que sejam as políticas de segurança de um sistema de computador, ele ainda pode ser comprometido por fruto de um deslize do seu

operador. Funcionários não treinados e não conscientes tendem a não tratar os dados da forma correta, prejudicando, mesmo que sem intenção, a segurança da empresa. A PSI (Política de Segurança da Informação) é um documento onde constam algumas boas práticas a serem seguidas dentro da corporação em relação à TI.

Para Caruso (1999), a política de segurança deve conter diretrizes claras a respeito, pelo menos, dos seguintes aspectos:

- Objetivo da segurança: deve explicar de forma rápida e sucinta a finalidade da política de segurança. A política deve definir claramente qual é seu proposito e qual o seu objetivo de proteção.
- A quem se destina: deve definir claramente quais as estruturas organizacionais às quais a mesma aplica-se. Neste ponto da política de segurança deve-se definir claramente os ativos da empresa sobre os quais a mesma versará, ou o que ela deverá abranger. Pode-se também, a esta altura, definir o que se espera como proteção para cada tipo de ativo envolvido, ao menos em nível geral.
- Propriedade dos recursos: deve definir de forma clara as regras que regerão os diversos aspectos relacionados com as propriedades de ativos de informações. Nesta seção da política de segurança, devem-se definir claramente os responsáveis pelos ativos envolvidos, ou pelo menos as regras para se definir os responsáveis. Não deve-se confundir a propriedade dos ativos com responsabilidade sobre ativos: enquanto o primeiro conceito envolve a fonte da autoridade sobre determinado ativo, a responsabilidade sobre ativos define a pessoa que está exercendo a posse sobre o mesmo, ainda que em nome de outra pessoa. Também deve ser deixada clara a diferença entre a propriedade de ativos, exercida pelo seu proprietário, e a responsabilidade pela segurança do mesmo, que está intimamente associada à sua integridade. Normalmente, a integridade de um ativo é de responsabilidade do seu ator, que exerce a posse em nome do proprietário.
- Responsabilidades: deve definir de forma clara quais os tipos de responsabilidades envolvidas com o manuseio dos ativos de informações, a quem as mesmas devem ser atribuídas, e os mecanismos de transferência. Nesta parte da política, determina-se quem é o responsável e qual o grau de responsabilidade envolvido na política de segunda para cada uma das funções que tenham ativos a serem regulados no âmbito da política de segurança. Não se deve confundir responsabilidade sobre ativos com responsabilização: este último conceito envolve a

identificação clara das pessoas que acessam ativos e o nível de acesso que estão tendo sobre os mesmos. Não é preciso ser responsável por um ativo para se ter o direito de acesso a ele. Muitas políticas determinam de maneira especifica o que é esperado de cada área funcional em termos de responsabilidade, apoio e execução da política. Cada usuário de ativos da organização deve entender que ele tem um papel a cumprir, no esquema de segurança, e deve aprender e aceitar claramente qual é esse papel.

- Requisitos de acesso: deve indicar de forma clara quais os requisitos a serem atendidos para o acesso à ativos de informações. Nesta etapa devem-se definir claramente os critérios segundo os quais cada ocupante de função dentro da organização pode acessar ativos, o nível de acesso permitido e as operações permitidas. Também é nesta seção que deve aparecer de forma bem nítida o conceito de permissão de acesso à ativos, decorrente apenas de necessidade funcional. Deve também ser definida nesta seção, de forma clara, a diretriz de separação de funções. Se já houver algum tipo de definição a respeito, é nesta seção também que devem constar as diretrizes que regerão o trabalho dos administradores de segurança.
- Responsabilização: devem indicar as medicas a serem tomadas nos casos de infringência às normas da mesma. Os ativos informacionais de uma organização são de propriedade da mesma, tanto quanto qualquer outro tipo de ativo, e são franqueados aos seus funcionários como parte da função que exercem na organização. Cada ocupante de posição que faça uso de ativos da organização, deve ser claramente identificado. O uso desses ativos deve ser controlado e o ocupante deve ser responsabilizado por esse uso, isto é, prestar contas. Isso deve ficar claramente definido na política de segurança, devendo até mesmo constar do contrato do trabalho, sempre que possível.

5.4 CONTROLE DE ACESSO LÓGICO

Os mecanismos de controle de acesso têm o objetivo de implementar privilégios mínimos a usuários a fim de que estes possam realizar suas atividades a que foram destinadas.

Para Caruso (1999) o controle de acesso está relacionado diretamente ao acesso concedido. A função desse controle é garantir que o acesso seja feito somente dentro dos limites estabelecidos. Abaixo, algumas sugestões listadas pelo autor:

- Senhas: constituem o mecanismo de controle de acesso mais antigo usado pelo homem para impedir acessos não autorizados. No passado, eram usadas para identificação de pessoas que não se conheciam, ou como forma de impedir a participação de não-membros em reuniões de sociedades secretas. Elas foram e ainda são muito usadas como forma de se controlar o acesso aos recursos de informações; entretanto, o risco de revelação de uma senha de acesso aumenta na proporção direta da quantidade de pessoas que a conhecem. Os métodos de controles de acesso mais recentes tendem a usar senhas mais como mecanismo de autenticação de identidade de usuários pela atribuição de uma senha exclusiva para cada chave de acesso ou identificação de usuários individuais. Essa senha é pessoal e não pode ser revelada.
- Chave de acesso ou identificações: São códigos de acesso atribuídos a usuários. Cada um recebe uma chave de acesso única que pode ser de conhecimento geral, seu próprio nome, por exemplo. A cada chave de acesso é associada uma senha destinada a autenticar a identidade do usuário que possui essa chave. O mecanismo de chave de acesso permite que ela seja associada a cada recurso que seu possuidor tenha o direito de acessar, possibilitando, dessa forma, a responsabilização individual de cada usuário.
- Lista de acesso: mecanismo usado para controle o acesso de usuários a recursos. Constitui uma espécie de tabela onde constam o tipo e o nome do recurso, ao qual são associadas as identificações de usuários com os tipos de operações permitidas aos mesmos. As tabelas de lista de acesso também podem ser organizadas em função das chaves de acesso, as quais se associam os tipos de nomes de recursos que cada chave pode acessar com os tipos de operações permitidas às mesmas.
- Operações: determinam o que cada usuário pode fazer em relação a determinado recurso. Normalmente, consistem no seguinte:

  Leitura: o usuário pode somente consultar informações;

  Gravação: o usuário pode incluir informações;

  Alteração: o usuário pode alterar informações existentes;

  Exclusão: o usuário pode excluir informações existentes.

- Execução: aplica-se somente à ambientes informatizados, para arquivos que contenham programas ou comandos. Permite que o usuário execute comandos ou programas existentes nos mesmos.
- Privilégios: dento do controle de acesso, determinados usuários têm privilégios de acesso relacionados com as funções exercidas; normalmente, quanto maiores os privilégios de acesso, maior o grau hierárquico de seu detentor.
- Ferramentas de segurança: ferramenta usada para controlar o acesso de usuários aos acervos de informações. Em informática, constituem um sistema de programas que executa o controle de acesso dentro de determinado ambiente de informações. Entretanto, há diversos outros mecanismos de segurança que, mesmo não sendo específicos para informática, podem ser usados com essa finalidade. Dentre eles destaca-se os cartões magnéticos, os *smart cards,* a identificação de padrão de voz, de impressões digitais e de formato de rosto, a identificação do padrão de vascularização da retina e muitos outros.
- Categoria: é o mecanismo que permite classificar usuários, propiciando a segregação dos mesmos a partes do ambiente, normalmente, com estruturas de nível hierárquico semelhante, a exemplo das Forças Armadas.

A prevenção é necessária pois os *hackers* sabem como encontrar as brechas de proteção, sendo elas físicas ou lógicas. Eles costumam estudar o elo mais fraco da segurança e atacar assim que sentir-se confiante.

6 CONCLUSÃO

Neste trabalho, conclui-se que o fator humano em segurança da informação tem um valor muito grande, porém as corporações não investem em treinamentos de funcionários, sendo o orçamento total para o uso de máquinas poderosas para garantir a segurança do ambiente. A engenharia social é uma área muito nova, porém já explorada por seus atacantes, os mesmos têm experiência com fator humano e têm êxito em grande parte dos seus ataques, tornando-se então cada vez mais simples conquistar, persuadir e atacar suas vítimas.

Apesar de parecer algo que apenas afeta o usuário leigo, o engenheiro social é uma das maiores ameaças à segurança da informação, e a sua aparente simplicidade esconde uma forma de invadir até os sistemas mais complexos e seguros. Sendo o elemento chave da engenharia social, o fator humano jamais será removido dos sistemas computacionais, tendo em vista que a máquina pode ser inteligente, mas exige alguém para controlá-la. Este fato jamais deve ser ignorado por todos que prezam pela segurança da informação, uma vez que a engenharia social se torna ainda mais perigosa quando a vítima a descarta como uma ameaça séria.

Através da pesquisa realizada, pode-se perceber que grande parte das empresas ainda não estão cientes de como o roubo de dados pode acontecer, muitas vezes passando despercebido, e acabam não aplicando os devidos treinamentos aos usuários, onde os mesmos não lidam com as informações de maneira correta, acabando sendo vítimas de pessoas mal intencionadas como os engenheiros sociais que agem de má fé em busca de se aproveitar da ingenuidade alheia.

REFERÊNCIAS BIBLIOGRÁFICAS

- ABNT. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 17799:2005** – Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da Informação. Rio de Janeiro: ABNT, 2005.

- CARUSO, A. A. Carlos. STEDDEN, Flávio Denny. **Segurança em informática e de informações.** 2ª ed. rev. e ampl. Editora Senac: São Paulo, 1999.

- CORRÊA, Gustavo Testa. **Aspectos jurídicos da internet**. Saraiva: São Paulo, 2000.

- DANTAS, Marcus Leal. **Segurança da informação**: uma abordagem focada em gestão de riscos. Livro Rápido. Olinda, 2011.

- GUILHERME JUNIOR. **Entendendo o que é engenharia social**. 2006. Disponível em: <http://www.vivaolinux.com.br/artigo/Entendendo-o-que-e-Engenharia-Social?pagina=1> Acesso em 08 nov. 2015.

- MARQUES FILHO, Glenio Leitão. **Hackers e crackers na internet:** as duas faces da moeda. Revista eletrônica temática. 2010. Disponível em
- < http://www.insite.pro.br/>

- MITNICK, Kevin. SIMON, William L. **A arte de enganar**. Makron Books: São Paulo, 2003

- MITNICK, Kevin. SIMON, William L. **A arte de invadir**. Editora Pearson Education do Brasil: São Paulo, 2005.

- MORAZ, Eduardo. **Treinamento profissional anti-hacker**. Digerati Books: São Paulo, 2006.

- OLIVEIRA, Wilson. **Técnicas para hackers,** soluções e segurança. Editora Centro Atlântico: Portugal, 2003.

- PEIXOTO, Mário César Pintaudi. **Engenharia social & segurança da informação na gestão corporativa**. Brasport: Rio de Janeiro, 2006.

- PONTIROLI, Santiago. **A engenharia para enganar pessoas**. 2013. Disponível em: <https://blog.kaspersky.com.br/engenharia-social-hackeando-humanos/1845/> Acesso em 08 nov. 2015.

- QUEIROZ, Luis Ricardo Silva. **Pesquisa quantitativa e pesquisa qualitativa: Perspectivas para o campo da etnomusicologia**. 2006. Disponível em: <http://www.biblionline.ufpb.br/ojs/index.php/claves/article/view/2719> Acesso em 06 mai. 2016.

- REZENDE, D. A.; ABREU, A. F. **Tecnologia da informação aplicada a sistemas de informação empresariais**. 3ª ed. rev. e ampl. São Paulo: Atlas, 2003.

- SÊMOLA, Marcos. **Gestão da segurança da informação**: uma visão executiva. 2. ed. Elsevier: Rio de Janeiro, 2014.

- TORRES, Plinio. **Engenharia social**. 2012. Disponível em: <http://www.dgti.ufla.br/site/?p=631> Acesso em 08 nov. 2015.