UNIVERSIDADE FEDERAL DO PARÁ
INSTITUTO DE CIÊNCIAS NATURAIS E EXATAS
FACULDADE DE COMPUTAÇÃO
CURSO DE BACHARELADO EM SISTEMAS DE INFORMAÇÃO

GEDEAN GONÇALVES CARVALHO

ENGENHARIA SOCIAL: ESTUDO EM UMA EMPRESA DE MINERAÇÃO DE BARCARENA

BELÉM/PA
2018

GEDEAN GONÇALVES CARVALHO

ENGENHARIA SOCIAL: ESTUDO EM UMA EMPRESA DE MINERAÇÃO DE BARCARENA

Trabalho de Conclusão de Curso apresentado como um dos requisitos para obtenção do grau de Bacharel em Sistemas de Informação, pela Universidade Federal do Pará.

Orientadora: Dr.ª Marianne Kogut Eliasquevici.

BELÉM/PA
2018

GEDEAN GONÇALVES CARVALHO

ENGENHARIA SOCIAL: ESTUDO EM UMA EMPRESA DE MINERAÇÃO DE BARCARENA

Trabalho de Conclusão de Curso apresentado como um dos requisitos para obtenção do grau de Bacharel em Sistemas de Informação, pela Universidade Federal do Pará.

Orientadora: Dr.ª Marianne Kogut Eliasquevici.

Banca Examinadora

_____

Profª. Marianne Kogut Eliasquevici
Orientadora

_____

Profª. Marcelle Pereira Mota
Examinadora

_____

Profª. Regiane Silva Kawasaki Francês
Examinadora

Aprovado em: _____/_____/ 2018 .

Conceito: _____

BELÉM/PA
2018

Dedico aos meus familiares, pelo amor, carinho, confiança e incentivo durante toda essa jornada.

AGRADECIMENTOS

Agradeço ao meu amado Jesus, por me proporcionar a dádiva de estudar numa Universidade Pública, por sempre me abençoar, por sua graça e infinita misericórdia que me acompanharam durante esses anos de faculdade.

Agradeço a minha mãe e meu pai, Sônia e Geraldo, pelo cuidado, amor incondicional, por todo esforço com o intuito de dar o melhor para os meus irmãos e eu. De nada valeria essa jornada sem vocês ao meu lado. Obrigado por tudo, todas as minhas conquistas são poucas perto daquilo que vocês merecem. Aos meus irmãos e familiares, obrigado pelo apoio e incentivo.

Agradeço a minha melhor amiga, companheira e esposa, Kalyúpe Carvalho. Você esteve presente no dia que eu fui aprovado na UFPA, como amiga, e está presente no dia que eu me formo, como esposa. Seu amor e seus incentivos foram determinantes na minha caminhada acadêmica.

Agradeço as amizades verdadeiras que conquistei na UFPA. Nossos trabalhos em grupo onde um sempre ajudou o outro e todos os desafios que enfrentamos juntos, me fizeram crescer e amadurecer. Valeu a pena.

Agradeço à orientadora, Profª Drª Marianne Kogut Eliasquevici, por toda sua paciência, pelo conhecimento transmitido durante a construção do TCC e pela sua competência. Muito obrigado.

Agradeço também aos docentes do curso de Sistemas de informação pela convivência e troca de conhecimento.

RESUMO

O objetivo principal desse trabalho é avaliar o conhecimento dos colaboradores de uma mineradora de Barcarena quanto aos perigos de um engenheiro social, além de apresentar o perfil do engenheiro e o perfil de possíveis vítimas. Para tal, utilizou-se de uma pesquisa de campo com uma parte dos colaboradores que compõe o quadro de funcionários da mineradora e ilustrou-se os resultados de maneira gráfica e analítica. Fez-se necessário realizar uma pesquisa bibliográfica para entender os métodos de ataques do engenheiro social. Constatou-se então os pontos a serem melhorados na empresa e as estratégias que precisam ser aplicadas para sanar esses pontos.

Palavras-chave: Engenharia Social; Segurança da informação, Sistema de Informação

ABSTRACT

The main objective of this work is to evaluate the inclination of the employees of a Barcarena mining company regarding the dangers of a social engineer, besides presenting the profile of the engineer and the profile of possible victims. For this, a quantitative method was used by means of a field research with a part of the employees that compose the mining company's staff and the results were illustrated graphically and analytically. It was necessary to carry out a bibliographical research to understand the methods of attacks of the social engineer. The points to be improved in the company and the strategies that need to be applied to remedy these points.

Keyword: Social engineering; Information Security, Information System

LISTA DE FIGURAS

Figura 1 - Tríplice PPT..15

LISTA DE GRÁFICOS

Gráfico 1 - Idade dos colaboradores 28
Gráfico 2 - Escolaridade 29
Gráfico 3 - Tempo de serviço e Cargo 30
Gráfico 4 - Senha pessoal 31
Gráfico 5 - Uso de senhas de outros 32
Gráfico 6 - Compartilhamento de senha própria 33
Gráfico 7 - Troca de senha 34
Gráfico 8 - Senha padrão compartilhada 34
Gráfico 9 - Divulgação de informação 35
Gráfico 10 – Informações vitais 36
Gráfico 11 - Política de segurança da informação 37
Gráfico 12 – Informações sobre a mesa 38
Gráfico 13 - Bloqueio dos computadores 39
Gráfico 14 – Importância para o departamento 39
Gráfico 15 – Tipos de informações 40
Gráfico 16 - Grau de conhecimento sobre Engenharia Social 41
Gráfico 17 - Foi vítima? 42
Gráfico 18 - A empresa foi vítima? 43
Gráfico 19 - Recuperação de dados 43

SUMÁRIO

INTRODUÇÃO 10
1 SEGURANÇA DA INFORMAÇÃO E ENGENHARIA SOCIAL 13
1.1 SEGURANÇA DA INFORMAÇÃO 13
1.2 ENGENHARIA SOCIAL 16
1.3 TIPOS DE ENGENHARIA SOCIAL 17
1.3.1 Engenharia social baseada em pessoas 17
1.3.2 Engenharia social baseada em computadores 17
1.4 PRINCIPAIS MÉTODOS DE ATAQUES 18
1.4.1 *Phishing* 18
1.4.2 *Pharming* 19
1.4.3 Análise do lixo 19
1.4.4 Internet e redes sociais 19
2 ENGENHARIA SOCIAL E O FATOR HUMANO 20
2.1 PERFIL DO ENGENHEIRO SOCIAL 20
2.1.1 Engenheiros sociais amadores 21
2.2 HABILIDADES DOS ENGENHEIROS 21
2.2.1 Conhecimento tecnológico 22
2.2.2 Atuação teatral 22
2.2.3 Sagacidade 23
2.2.4 Persuasão 24
3 ESTUDO DE CASO REALIZADO NA MINERADORA 26
3.1 TRABALHOS CORRELATOS 26
3.2 OBJETO DE ESTUDO 26
3.3 ANÁLISE DE DADOS 27
3.3.1 Perfil do colaborador 27
3.3.2 Políticas de senha 30
3.3.3 Estrutura e práticas da empresa 35
3.3.4 Tratamento das informações 37
3.3.5 Instrução sobre engenharia social 40
REFERÊNCIAS 46
APÊNDICE A – INSTRUMENTO PARA COLETA DE DADOS 49

INTRODUÇÃO

A humanidade possui uma característica intrínseca, a necessidade de se comunicar. Com a evolução e transformação no decorrer dos séculos, desenvolveram-se diversos modos para aperfeiçoar essa comunicação que em outras eras foi-se possibilitada por meio de pinturas em cavernas e hoje transformaram-se em letras, palavras e idiomas.

O desenvolvimento tecnológico trouxe aprimoramento nos meios de comunicação, os quais representam os instrumentos designados para difundir a informação entre homens, por exemplo rádio, televisão, jornal, e o mais atual, a internet, a qual está impulsionando a criação de tecnologias para um diálogo mais eficaz.

O avanço humano tem percorrido por diversas transformações tecnológicas e todo esse processo nos fez ser uma sociedade repleta de informações, segundo Luís Manuel Borges Gouveia (2004):

> A sociedade da informação está baseada nas tecnologias de informação e comunicação que envolve a aquisição, o armazenamento, o processamento e a distribuição da informação por meios electrónicos, como a rádio, a televisão, telefone e computadores, entre outros. Estas tecnologias não transformam a sociedade por si só, mas são utilizadas pelas pessoas em seus contextos sociais, económicos e políticos, criando uma nova comunidade local e global: a Sociedade da Informação.

Alguns autores como Gouveia (2004), trazem a ideia de um novo espécime de sociedade, dita como Sociedade da Informação, baseada no atual formato de comunicação que foi estabelecido pelos meios de interação para propagação do conhecimento. Compreendendo que a mudança gera crescimento, aperfeiçoamento e transformação na conjuntura socioeconômica.

O avanço tecnológico potencializou os serviços que as empresas prestam para a sociedade. Pode-se comprar, utilizar serviços bancários e interagir com pessoas, por meio da internet. É inegável a influência e dependência da nossa geração a esses sistemas. À medida que o uso dessas ferramentas abre novos horizontes para a tecnologia, crescem também novas possibilidades de ações contra a segurança da informação.

Nasce então a necessidade de garantir a solidez dessas informações, pois se tornou o ativo mais valioso de uma corporação e o mais visado por pessoas com intenções de esmiuçar e furtar dados sigilosos e confidenciais, trazendo danos às pessoas e empresas.

Diante desse cenário, instituições, entidades e corporações aplicam capital no crescimento e melhoria de seus parques tecnológicos. Investimentos em *firewalls*, antivírus, servidores, *tokens*, biometria, *scanner* e etc., são de suma importância para garantir a integridade da informação, entretanto apenas esse nível de proteção não é suficiente.

A dificuldade de invasão dos sistemas atuais e avançados faz com que os *hackers* direcionem seus esforços em outra direção. Direção essa que não é levada como elemento primordial para a segurança, o ser humano. Lamentavelmente as corporações não cultivam a cultura de treinamento e aperfeiçoamento de seus funcionários, tendo em vista que eles são parte fundamental da segurança da informação. Quanto mais difícil se torna avançar pelas tecnologias, mais exploradas serão as vulnerabilidades do ser humano.

Pereira (2005, p. 3) afirma que: “Não há *patch* contra a burrice humana”. De forma cômica, o autor retrata na frase que não existe um *software* para correção da estupidez humana. Ele traz à tona uma realidade esquecida pelas empresas, que é a de qualificar seus colaboradores. Para *softwares* e *hardwares* existem as atualizações que corrigem erros e falhas, para seres humanos não, é necessário investimento em treinamento e todo arcabouço advindo dele, com intuito de conscientizar sobre os riscos e perigos da negligência com a segurança da informação.

Segundo o laboratório de tecnologia da McAfee LABS:

> Em julho de 2014, mais de 1.000 empresas de energia na América do Norte e Europa foram relatadas por terem sido comprometidas por *cyberattacks*. [...] esses ataques são diferentes em tudo. Contudo, um tema comum entre eles é a **engenharia social.** [...] o modo operante para a maioria dos criminosos é empregar alguma técnica de engenharia social para coagir a vítima à uma ação que facilite a infecção. (MCAFEE LABS, 2014, p. 5, tradução nossa).

O *cyberattack* é uma forma de ataque da Engenharia Social, a mesma possui um conjunto de práticas utilizadas por pessoas maliciosas para enganar e persuadir indivíduos, cujo objetivo é captar informações sigilosas e confidenciais, como o relato exposto pela McAfee.

No livro a Arte de Enganar, os autores Kevin Mitnick e William Simon, desenvolvem pesquisa sobre o elo mais fraco da segurança, afirmando que:

> Uma empresa pode ter adquirido as melhores tecnologias de segurança que o dinheiro pode comprar [...] 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 [...] porque o fator humano é o elo mais fraco da segurança (MITINICK; SIMON, 2003, p. 3).

Com base no livro citado anteriormente, pode-se dizer que o homem é o elo mais fraco na segurança, pois ele repassa todas as informações para o engenheiro social sem analisar a gravidade do que está fazendo. Informações que para ele não são de muita importância, mas nas mãos erradas acabam se tornando uma grande ameaça para as organizações.

O objetivo do trabalho apresentado é teorizar sobre os temas de Segurança da Informação e de Engenharia Social, explorando o Fator Humano e identificando o Perfil dos Funcionários de uma empresa multinacional de mineração, localizada na cidade de Barcarena. A pesquisa realizada na empresa é de cunho quantitativo, prosseguindo através de um questionário sobre a importância que os dados da empresa e dos próprios funcionários são tratados. As informações geradas pela pesquisa, expõe como esses profissionais lidam com os ataques de engenharia social.

Assim, o primeiro capítulo desse trabalho, detalhará a contextualização de Segurança da Informação e Engenharia Social. Será apresentada também a fundamentação teórica sobre ambos assuntos.

No segundo capítulo será abordado o Fator Humano, abordando o perfil do engenheiro social.

O terceiro capítulo refere-se ao estudo de caso na mineradora, que trará a pesquisa utilizada na empresa para demonstrar o conhecimento dos seus colaboradores diante da engenharia social. Salientará, ainda, as áreas que foram analisadas na pesquisa, o método para obtenção dos resultados e gráficos contendo as respostas.

É de suma importância que ocorra a conscientização de nossa sociedade sobre engenharia social. Devemos ter clareza que ninguém está imune a esse tipo risco e que suas causas são imensuráveis, tanto a uma pessoa quanto a uma corporação.

1 SEGURANÇA DA INFORMAÇÃO E ENGENHARIA SOCIAL

A seguir iremos nos ater em contextualizar a segurança da informação e engenhara social, expondo os tipos de engenharia social e os principais tipos de ataques encontrados na internet.

1.1 SEGURANÇA DA INFORMAÇÃO

"A informação representa a inteligência competitiva dos negócios e é reconhecida como ativo crítico para a continuidade operacional da empresa" (PEIXOTO, 2006, p. 37). Nesse sentido, este autor deixa claro o valor que as informações têm para as empresas e que elas não podem ser irrelevantes para tomadas de decisões. Todo conteúdo que pode ser transferido ou armazenado de alguma maneira, tendo utilidade e propósito ao ser humano, pode ser considerado informação.

De acordo com David Ben Svaiter (2015), especialista e professor de criptografia, atualmente a informação é o produto mais significativo para as empresas, por serem manipuláveis e visualizadas de diversas maneiras, além de possuir um valor de mercado considerado. De acordo com Svaiter (2015), em 2013 o "tráfico de dados" movimentou mais de 1 trilhão de dólares. A informação é gerada em todos os processos, em todos os ambientes e em todos os fluxos, dessa forma ela se torna o vigor da empresa. A informação desloca-se de empresa para empresa, de integrante para integrante, e os dados, procedimentos e outros recursos, se tornam frágeis em vários lugares e a todo o momento os usuários dessas informações sucumbem por não compreender seu real valor e colocam-na em risco.

A Norma Brasileira Regulamentadora ISO/IEC 27002:2007 (FONTE?) afirma que o papel principal da segurança da informação é garantir a preservação da:

A. Confidencialidade: garantia de que as informações não serão dissipadas para lugares onde não deveria e nem sofrerá acesso não autorizado.
B. Integridade: garantia de que as informações não tiveram nenhuma alteração durante o processo, garantindo assim sua exatidão e veracidade.
C. Disponibilidade: garantia de que o canal de acesso a essas informações esteja sempre disponível às pessoas autorizadas.

Porém, sabe-se que é impossível existir um ambiente totalmente livre de ameaças e resta somente maximizar a segurança desses ambientes. O valor investido em tecnologia para tentar sanar os problemas de segurança é cada vez mais elevado, biometria, criptografia, certificado digital, senhas complexas entre outras são consideráveis, entretanto não resolvem a questão de segurança da informação.

Segundo Schneier (2001, p. 12): “Se você acredita que a tecnologia pode resolver seus problemas de segurança, então não conhece os problemas e nem a tecnologia”. Mesmo que toda a segurança tecnológica esteja à disposição, a ausência de políticas de segurança, planos de contingência ou senhas jamais trocadas, acabam por comprometer toda a estrutura de defesa tecnológica.

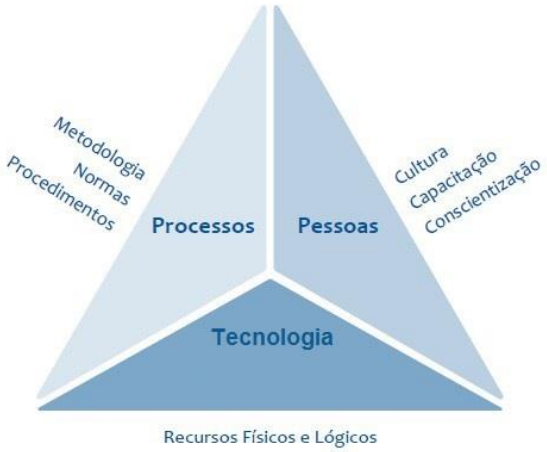
Para além da tecnologia, processos que garantam a segurança da informação devem ser bem elaborados para a criação de um ambiente seguro. Ambos devem estar em conjunto para obtenção de uma esfera com o máximo de segurança possível. Mesmo com o parque tecnológico avançado e falhas processuais sanadas, não há como afirmar que as vulnerabilidades do ambiente foram totalmente extintas.

A falta de conhecimento sobre as melhores práticas de segurança, de como operar as tecnologias e dúvidas a respeito dos processos empresariais ou até mesmo ceder informações importantes, como senhas e credencias à vista, fazem com que o dinheiro gasto com inovação e o esforço para melhorar seus processos fracassem. Erros humanos podem destruir todo o esforço para que um ambiente tenha a segurança, a máxima.

Segundo o artigo de Oliveira (2005“A segurança das informações jamais será alcançada se a tríplice PPT – Pessoas, Processos e Tecnologias – não for aplicada à estratégia de segurança”. Ou seja, para um sistema funcionar com o máximo de segurança, é necessário que três elementos estejam em harmonia: pessoas, processos e tecnologias.

A figura 1 a seguir ilustra a tríplice PPT, Pessoas, Processos e Tecnologias.

Figura 1 - Tríplice PPT



Fonte: elaborado pelo próprio autor.

Kevin Mitnick relata:

> Com frequência, a segurança é apenas uma ilusão, que as vezes fica pior ainda quando entram em jogo a credulidade, a inocência ou a ignorância. O cientista mais respeitado do mundo no século XX, Albert Einstein, disse: "Apenas duas coisas infinitas: o universo e a estupidez humana, e eu não tenho certeza se isso é verdadeiro sobre o primeiro". No final, os ataques da engenharia social podem ter sucesso quando as pessoas são estúpidas ou, em geral, apenas desconhecem as boas práticas de segurança. [...] A medida que os especialistas contribuem para o desenvolvimento contínuo de melhores práticas tecnológicas de segurança, tornando ainda mais difícil a exploração de vulnerabilidades técnicas, os atacantes se voltarão cada vez mais para a exploração do elemento humano. Quebrar a "firewall humana quase sempre é fácil, [...] e envolve um risco mínimo (MITNICK, 2003, p. 3).

Mitnick (2003) ainda aborda que as empresas investem em sistemas e deixam de lado as pessoas e os processos, que são vitais e compõem a base da segurança informacional. Desta forma, compreende-se que os colaboradores de uma empresa necessitam ser bem instruídos e capacitados quanto ao sigilo e zelo das informações, pois são a maior parte de sustentação da segurança e podem causar grandes prejuízos financeiros e comprometimento da imagem da organização, caso não sejam treinados.

1.2 ENGENHARIA SOCIAL

A engenharia social está inserida num cenário em que as pessoas contêm o maior volume de informações e proporcionalmente são menos treinadas. Ela é a arte de se conseguir informações utilizando todas as maneiras possíveis. A engenharia social conta com telefonemas, e-mails, sites e qualquer tipo de meio que transmita dados.

Para Mitnick (2003), a engenharia social usa a influência e a persuasão para enganar as pessoas e convencê-las de que o engenheiro social é alguém de boa índole, como exemplo, cliente de uma empresa, funcionário de outro departamento. Como resultado, o engenheiro social pode aproveitar-se das pessoas para obter as informações como ou sem uso da tecnologia.

Guenther (2001, p.8) define a engenharia social como:

> Engenharia social é o nome dado à categoria de ataque de segurança em que alguém manipula outro a fim de revelar informações que podem ser usadas para roubar dados, acessar sistemas, acessar telefones celulares, dinheiro ou até mesmo a sua identidade. [...] Engenharia social é a aquisição de informações sensíveis ou privilégios de acessos inapropriados por uma pessoa externa, baseada na construção de uma relação de confiança inapropriada com pessoas internas. O alvo da engenharia social é enganar alguém com o intuito dessa prover informações valiosas ou acesso a informações. [...] Engenharia social é ainda o mais efetivo método de burlar os obstáculos da segurança.

O termo engenharia social expressa uma falsa impressão de ser algo benéfico para a sociedade. De modo geral, ela é a arte de manipular psicologicamente os indivíduos para que executem ações ou divulguem informações confidencias de forma involuntária, sem perceber que estão sendo vítimas. Mann (2011, p. 19) fornece uma definição de engenharia social como forma de “manipular pessoas, enganando-as, para que forneçam informações ou executem uma ação”.

Já Lima (2004) afirma que a aplicação da engenharia social ensina quais são as práticas utilizadas para obter acesso às informações importantes ou sigilosas em organizações ou sistemas por meio da enganação ou exploração da confiança dos indivíduos. É possível encontrar diversos conceitos sobre engenharia social, sendo um dos mais utilizados:

> 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 informações) e magistrados (para comprovar se um declarante fala a verdade). Também é utilizada para lograr todo tipo de fraudes, inclusive invasão de sistemas eletrônicos (KONSULTEX, 2004 *apud* PEIXOTO, 2006, p. 4).

1.3 TIPOS DE ENGENHARIA SOCIAL

Existem duas classificações de engenharia social, sendo elas a Engenharia Social baseada em Pessoas e a Engenharia Social baseada em Computadores.

1.3.1 Engenharia social baseada em pessoas

A engenharia social fundamentada em pessoas usufrui do relacionamento humano como forma de ataque para captar os conhecimentos desejados. Guenther (2001, p.20) afirma que: “Engenharia social baseada em pessoas se refere em uma interação de pessoa a pessoa para conseguir a informação desejada”. Com base na manipulação e persuasão, o engenheiro social finge ser um bom empregado, estuda a empresa e pessoas percebendo onde estas não estão realmente capacitadas e que possam lhe fornecer informações importantes causando-lhes danos.

A relação da vítima e do atacante é o mais importante para o sucesso da investida, tendo como exemplo um engenheiro social que busca informações de uma empresa e se torna amigo de um funcionário desta empresa.

1.3.2 Engenharia social baseada em computadores

A internet é um e um meio relativamente fácil para adquirir informações, seja para o bem ou para mal. Ela facilita a invasão dos engenheiros sociais, os *sites* clonados, *e-mails* falsos, *chats*, arquivos com vírus e tantas outras maneiras de alcançar seu objetivo de reter informações restritas.

A engenharia social baseada em computadores é praticada quando não há relacionamento direto entre o engenheiro e a vítima, ou seja, ocorre no âmbito virtual, não impedindo o engenheiro social de persuadir e explorar as vítimas. Ele se beneficia da falta de treinamento dos funcionários que utilizam o computador no seu ambiente de trabalho, geralmente realizando truques nos quais os colaboradores facilmente são ludibriados. Um dos

truques mais comuns é o envio de *e-mail* onde o empregado acredita que seja de um amigo, mas na realidade é uma ferramenta de invasão.

1.4 PRINCIPAIS MÉTODOS DE ATAQUES

Várias técnicas são utilizadas para atacar as vítimas dos engenheiros sociais e, com o avanço tecnológico, as possibilidades de invasão são notadamente maiores e mais difíceis de detecção. Algumas delas estão descritas a seguir.

1.4.1 *Phishing*

Original do inglês *fishing* que quer dizer pesca, é uma forma de fraude eletrônica, caracterizada por tentativas de adquirir dados pessoais de diversos tipos. *Phishing* é considerado pela Norton (2011) como um golpe *on-line* de falsificação. Atualmente é uma espécie de ataque comum, utilizando *sites* enganosos, mensagens maliciosas, *spams* e *e-mails*, que buscam obter, sem o conhecimento da vítima, informações sigilosas, dentre elas os números de contas bancárias e cartões de crédito.

No caso do *site*, geralmente ocorre à cópia do *layout* do site verdadeiro, após digitar as informações necessárias, automaticamente os dados são enviados ao engenheiro social. Outra forma usual é de receber um *e-mail* estranho, de alguém que a vítima não conhece, com um arquivo anexado que consiga aguçar sua curiosidade, para que ela abra e o vírus ou ferramenta de invasão penetrem no computador.

Geralmente esse tipo de *e-mail* também é disfarçado por cartões de visitas, convites e instituições financeiras renomadas como bancos, governos e multinacionais, fazendo com que as vítimas liberem dados confidenciais. Segundo o *site* Kaspersky Lab (2018, p.1), novos truques estão sendo realizados, dentre eles o falso acesso a Bitcoin:

> Outro tópico de spam e phishing em 2017 foi cryptocurrency - como o preço de Bitcoin aumentou drasticamente. [...] De acordo com as descobertas da Kaspersky Lab, os criminosos têm usado truques, como sites disfarçados de trocas de criptografia, serviços falsos que oferecem a mineração em nuvem, ou seja, o uso de centros de dados especializados para alugar. Mas, em todos os casos, os usuários se tornaram vítimas - perdendo dinheiro em vez de ganhar algum. Em esquemas de fraude mais tradicionais, como os ganhos falsos de loteria, os criminosos também começaram a usar o Bitcoin como isca e, além de bancos de dados de endereços direcionados anunciados

> através de spam, bancos de dados com e-mails para usuários de criptografia também foram oferecidos para compra, prometendo ótimas oportunidades.

1.4.2 *Pharming*

O termo vem da junção de *phishing* e *farming*, pois esse ataque pode afetar vários usuários ao mesmo tempo. Ele age na base do funcionamento da internet. Segundo o *site* Kaspersky Lab (2018, p.1) "o pharming é uma forma bastante preocupante de crime virtual, pois, em caso de envenenamento do servidor DNS – Domaine Name System –, o usuário afetado pode ter um computador completamente livre de malware e ainda assim se tornar uma vítima". Ou seja, o usuário que foi vítima tem seu tráfego de internet alterado para sites falsos mesmo que a pessoa tenha digitado o endereço correto.

Como exemplo deste tipo de ataque, a o caso da vítima que tenta acessar o site do bradesco.com.br será direcionada automaticamente para um site falso que é a cópia idêntica do site verdadeiro. Dessa maneira todas as informações digitadas no site falso o criminoso terá acesso.

1.4.3 Análise do lixo

Poucas empresas têm procedimentos para descarte de material tecnológico, entretanto o lixo eletrônico acaba sendo uma rica fonte de informações para pessoas mal-intencionadas. No lixo de empresas é possível encontrar nome de funcionários, telefone, *e-mail*, senhas, contatos de clientes, fornecedores, transações efetuadas, entre outros, ou seja, este é um dos primeiros passos para que se inicie um ataque direcionado à empresa.

1.4.4 Internet e redes sociais

Atualmente é possível encontrar todas as informações de uma pessoa acessando suas redes sociais, como: Facebook e Instagram. Tornou-se comum todas as pessoas postarem tudo relacionado ao seu dia e isso é muito arriscado. O engenheiro social pode usar esse método para conhecer melhor suas vítimas: interesses, preferencias, estilos, costumes, rotinas e etc. Além de adquirir mais informações sobre a empresa através do perfil da vítima.

2 ENGENHARIA SOCIAL E O FATOR HUMANO

O elemento de segurança mais fraco é o fator humano (MITINICK; SIMON, 2003), pois os indivíduos são mais fáceis de se enganar ou de servem vítimas dos engenheiros sociais. Neste capítulo será abordado o perfil do engenheiro social e de suas vítimas, para que seja possível compreender as vulnerabilidades humanas.

2.1 PERFIL DO ENGENHEIRO SOCIAL

O engenheiro social é o indivíduo que realiza engenharia social. Parece simples essa definição, porém é preciso estudar com mais vigor esse termo.

De acordo com Freitas (2011, p.13):

> Engenheiro social é qualquer indivíduo que utiliza as facilidades de uma sociedade "ingênua" e orientada por regras para alcançar objetivos pessoais. Ele nos faz acreditar que atua conforme as regras, mas não o faz, o que só percebemos no final do processo, quando já não há mais tempo. Nós substituímos a percepção pela crença.

Para Marcelo (2005, p. 4):

> Esse indivíduo é um tipo de pessoa extremamente inteligente e dotada de um conhecimento da psicologia humana muito grande. O engenheiro social sabe explorar facetas como vaidade, humildade, egocentrismo, utilizando técnicas de galanteio social, a fim de obter informação a respeito de alguém ou de uma instituição.

Ambos retratam e caracterizam o engenheiro social, Freitas a específica como alguém capaz de usar a inocência do outro para atingir sua meta, e Marcelo o descreve como um ser altamente habilidoso e perspicaz, completando a definição do engenheiro social.

Para Antônio Marcelo (2005, p.5) existem duas categorias de engenheiros sociais: amadores e formados.

2.1.1 Engenheiros sociais amadores

A categoria tem esse nome pelo fato de serem pessoas que não receberam treinamentos técnicos ou formais na área, porém possuem habilidades natas para agirem como engenheiros sociais excelentes, como se obtivessem um dom inerente ao indivíduo. Como exemplo, Kevin Mitnick, em seu livro, A arte de enganar, explica que iniciou sua trajetória na engenharia social como amador e hoje é um especialista muito respeitado na área de segurança da informação.

Marcelo (2005, p.05) diz que "normalmente esses indivíduos são frutos de nossa sociedade, com desejos dotados de uma visão de olhar para a situação com vários prismas distintos".

2.1.2 Engenheiros formados

Diferente dos amadores, essa classe é formada por pessoas que buscaram se especializar formalmente, através de cursos, treinamentos e estudos, para assim atuarem no mercado de engenharia social profissionalmente. Como exemplo, pode-se citar os investigadores, detetives e espiões.

2.2 HABILIDADES DOS ENGENHEIROS

Para Mitnick (2003, p.06):

> Na maioria dos casos, os engenheiros sociais bem-sucedidos têm uma habilidade muito boa em lidar com as pessoas. Eles são charmosos, educados e agradam facilmente – os traços sociais necessários para estabelecer a afinidade e confiança. [...] Um engenheiro social experiente pode ter acesso a praticamente qualquer informação-alvo, usando as estratégias e táticas da sua habilidade.

Conforme Santos (2004, p.2), em seu artigo, Engenharia Social: atacando elo mais fraco,

> Para conseguir persuadir as pessoas, o Engenheiro Social utiliza artimanhas com a finalidade de explorar algumas características humanas, tais como Solidariedade, Instinto de Sobrevivência, Ambição, Curiosidade e Confiança, exercendo a influência acima de tudo, enganando muitas vezes,

> misturando pequenas mentiras em grandes verdades. O objetivo do Engenheiro Social é alcançado após conquistar a confiança do usuário.

Os dois autores acima citados concordam com algumas características básicas que um engenheiro social deve ter para obter sucesso: persuasão, influência, engano e confiança. Todavia, ainda existem outras habilidades que são de suma importância para o engenheiro social obter sucesso em suas realizações.

2.2.1 Conhecimento tecnológico

É imprescindível que o engenheiro detenha conhecimento e habilidades técnicas relevantes a área que irá invadir. Se o alvo for uma aplicação web, por exemplo, o engenheiro deve gozar de conhecimentos pertinentes para saber quais informações são adequadas para realizar o ataque.

Entretanto, é correto salientar que o engenheiro social se empenhará a analisar primeiramente as vulnerabilidades humanas. Guenther (2001, p.12) afirma que "Um engenheiro social experto irá tentar explorar essa fraqueza antes de investir tempo e força em métodos para quebrar senhas", retratando que as vulnerabilidades tecnológicas ou processuais, poderão ou não serem usadas em um ataque.

Santos (2004, p.3) reforça:

> O maior objetivo do Engenheiro Social é fazer de seu usuário uma porta de acesso que burle todos os controles tecnológicos de segurança implementados. Passam pelo Firewall, enganam o IPS, não tomam conhecimento do Antivírus e tudo isso porque utilizam acessos válidos. Concedidos gentilmente pelo seu usuário.

Contar com conhecimento tecnológico é importante, porém não é determinante para que o ataque ocorra, tendo em vista que dependendo do tipo de ataque, a tecnologia não será utilizada para obter sucesso. Marcelo (2005, p.4) enfatiza que "existem grandes loucuras usadas na Engenharia Social, temos de concordar que não é coisa para qualquer um, exige em muitos casos, mais 'esperteza' do que conhecimento técnico".

2.2.2 Atuação teatral

Assim como o ator deve saber atuar, de tal modo o engenheiro social também deve. Durante o ataque pode ser necessário o improviso em determinadas situações inesperadas e possuir o “sangue frio” faz com que o engenheiro consiga agir coerentemente em situações de perigo ou de grande exposição.

Mitnick (2003, p.37) intensifica:

> É da natureza humana achar que é improvável que você seja enganado em determinada transação, pelo menos até que tenha algum motivo para acreditar no contrário. Nós ponderamos o risco e, em seguida, na maior parte das vezes, damos às pessoas o benefício da dúvida. Esse é o comportamento natural das pessoas civilizadas... pelo menos as pessoas civilizadas que nunca foram enganadas, manipuladas ou trapaceadas em uma soma grande em dinheiro.

Marcelo (2005, p.42) relata sobre a ação do engenheiro:

> Você deve chamar mais atenção que o golpe, seja o pivô de tudo. Seja convincente ao máximo e acima de tudo mostre “sinceridade”. Ninguém desconfia de uma pessoa segura e sincera, por mais picareta que seja. Represente o papel a ponto de você mesmo acreditar nele! Essa é a chave do sucesso.

Diante do exposto, considera-se a teatralização como algo muito importante, pois é sobre a sua atuação que o engenheiro irá aplicar suas demais habilidades.

2.2.3 Sagacidade

Da mesma maneira que um empreendedor descobre oportunidades onde poucos, ou até mesmo ninguém viu, assim também é o engenheiro social. Ele analisa nas entrelinhas. O engenheiro social sagaz usa primeiramente sua audição para entender o ambiente que o cerca.

Shinder (2004, p.1) define que um bom engenheiro social “não é apenas um bom ator, mas também é bom em “ler” pessoas para determinar que tipo de estratagema funcionará melhor com uma pessoa em particular”. Assim como ser um bom ator, o engenheiro precisa fazer uma boa análise da sua vítima para estabelecer que tipo de estratégia irá funcionar, essa ação é conhecida como Programação Neurolinguística (PNL).

De acordo com o site da Sociedade Brasileira de Programação Neurolinguística (SBPNL) (2004):

> A PNL permite compreender melhor nosso funcionamento interno, identificar nossos modelos mentais, para que possamos questioná-los, refletir sobre os mesmos e se é preciso ressignificá-los. Esse aspecto é que influenciou o surgimento do nome "programação", pois esse conhecimento sugere que a partir das nossas histórias, experiências, valores, somos programados a ter determinadas crenças e modelos mentais que impactam diretamente o nosso comportamento. Da mesma forma, que a partir de técnicas de PNL e ferramentas podemos "reprogramar" a nossa estrutura interna com foco nos resultados que queremos alcançar.

Para Marcelo (2005, p.29), "falar de PNL é falar de uma tática de estudo que permite conhecer maneirismos e através dos mesmos entender como uma pessoa 'funciona', ou melhor, como seus processos mentais funcionam, trazendo à tona as nuances de seu raciocínio". Observar particularidades do ambiente e da vítima são elementos cruciais para o sucesso em um possível ataque. A atenção aos detalhes irá definir quais métodos usar para alcançar seu objetivo.

Mitnick (2005, p.111) afirma que "você precisa ler a sua vítima, entender o seu estado de espírito, enganá-la como se engana um peixe dando um pouco de linha e puxando, mais um pouco de linha e puxando. Até você pegá-lo na rede e jogá-lo no barco! "

2.2.4 Persuasão

O poder de persuasão provavelmente é a característica mais importante que um engenheiro social deve portar, afinal, ela é a chave para que qualquer sistema de segurança seja transgredido.

Com persuasão, o engenheiro conseguirá que a vítima diga qualquer informação que ele jugue como importante, podendo ser login, senha de acesso e até número de cartão bancário. Brenner (2005, p.3) revela que "Em um nível pessoal, existem métodos que são utilizados para fazer que com a pessoa coopere melhor com você. O truque da persuasão pessoal é não forçar a pessoa a fazer o solicitado, mas fazer com que ela faça o que você solicitou voluntariamente."

Guenther (2001, p. 33) também defende que "muitos engenheiros sociais são adeptos do uso da persuasão pessoal para controlar resistências iniciais. O algo é não forçar, mas gerar uma ação voluntária e fazer com que o alvo acredite que eles estão tomando uma decisão conjunta".

O interessante é que os dois autores citam o mesmo entendimento de que a vítima deve acreditar que está decidindo e não sendo forçada a dar informações. A falsa impressão de estar tomando uma decisão em conjunto, vítima e engenheiro, faz com que a vítima tenha

certeza que a escolha dela é a melhor para todos. Praticar um ataque com esse nível de persuasão é a certeza que o objetivo será alcançado.

3 ESTUDO DE CASO REALIZADO NA MINERADORA

Todo conteúdo exemplificado neste trabalho, constata que a sociedade, de modo geral, está indefesa as atividades do engenheiro social. É possível compreender também que não existe nenhum sistema totalmente seguro. Porém, apenas conhecer que nossa sociedade está propícia aos ataques da engenharia social não acrescentam muitos resultados, é preciso entender o nível e onde se encontram essas vulnerabilidades, possibilitando realizar ações com a intenção de minimizar essas falhas.

O estudo foi realizado por meio de um questionário (Apêndice A) contendo 23 perguntas entre os dias 15 e 30 de Maio de 2018. A grande quantidade de informações geradas pela mineradora e a ausência de instrução sobre o tema de Engenharia Social foram determinantes para que a pesquisa fosse feita.

3.1 TRABALHOS CORRELATOS

Não é fácil encontrar estudos em ambientes de trabalho que abordem o tema Engenharia Social. Torna-se ainda mais difícil um estudo em um segmento que movimenta bilhões por ano, que é a mineração.

A partir da identificação desta lacuna, o instrumento deste estudo, foi elaborado tendo como base o “Teste de Conformidade”, apresentado na obra de Sêmola (2003). Ele desenvolveu uma ferramenta com o objetivo de testar a conformidade de uma organização de acordo com a NBR ISO/IEC 17799.

Vieira (2013) utilizou o questionário e aplicou no Centro de Tecnologia da Informação e Comunicação (CTIC), da Universidade Federal do Pará (UFPa), em seu trabalho de conclusão de curso de ciência da computação

De mesmo modo que Vieira (2013), este estudo utilizou parte do questionário de “Teste de Conformidade”, Sêmola (2003), adequado à realidade vivenciada pela mineradora de Barcarena, para que fosse feito um estudo do tema engenharia social e que fosse proposto alternativas para melhorar a segurança da informação.

3.2 OBJETO DE ESTUDO

Com o propósito de aprimorar o estudo sobre engenharia social, foram aplicados questionários junto a profissionais de diversas áreas de uma mineradora situada na cidade de

Barcarena, Estado do Pará. A amostragem foi composta por 70 profissionais da mineradora. Vale ressaltar que estes profissionais não são necessariamente graduados em um curso superior. São de níveis hierárquicos distintos e de diversas classes sociais.

A mineradora é uma multinacional, com sede em Paris/FR, presente em cinco continentes, contabilizando 50 países e com mais de 270 instalações industriais. Tem como missão, produzir minerais de forma competitiva e sustentável, respeitando clientes, colaboradores, comunidade, acionistas e fornecedores.

No Estado do Pará, está em operação desde 1996, em 2010 adquiriu outra empresa, transformando assim na maior mineradora de Caulim do mundo e responsável por 71% da produção brasileira.

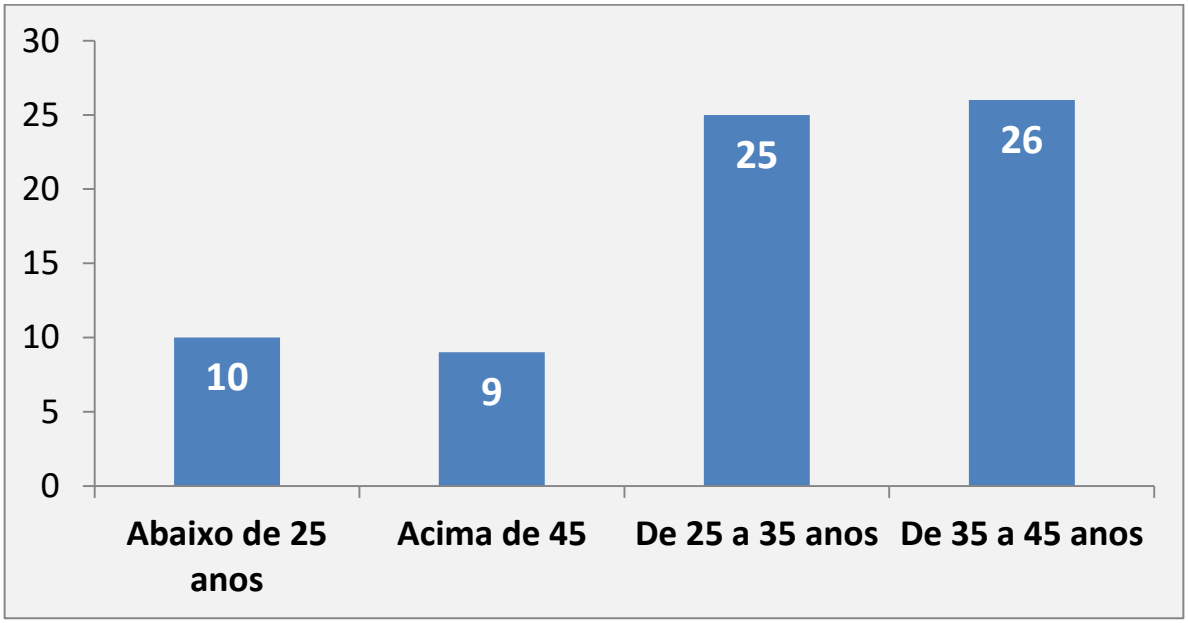
3.3 ANÁLISE DE DADOS

De acordo com o informado previamente, os dados estudados foram coletados com base em um questionário respondido por funcionários dessa mineradora. Todas as questões foram desmembradas por assuntos de acordo com o que se tinha interesse em avaliar. A primeira parte do questionário refere-se ao perfil do colaborador.

3.3.1 Perfil do colaborador

A primeira pergunta teve como objetivo identificar a idade dos colaboradores que participaram da pesquisa. De acordo com o Gráfico 1, a idade varia de 18 a 62 anos, sendo que mais de 72%(51) possuem idade entre 25 e 45 ano.

Gráfico 1 - Idade dos colaboradores



Fonte: Dados da pesquisa (2018).

Referente ao nível de escolaridade dos pesquisados, o Gráfico 2 aponta que menos de 3%(2) obtiveram apenas o 2º grau escolar e que 54%(37) são de pessoas com nível superior e pós-graduação.

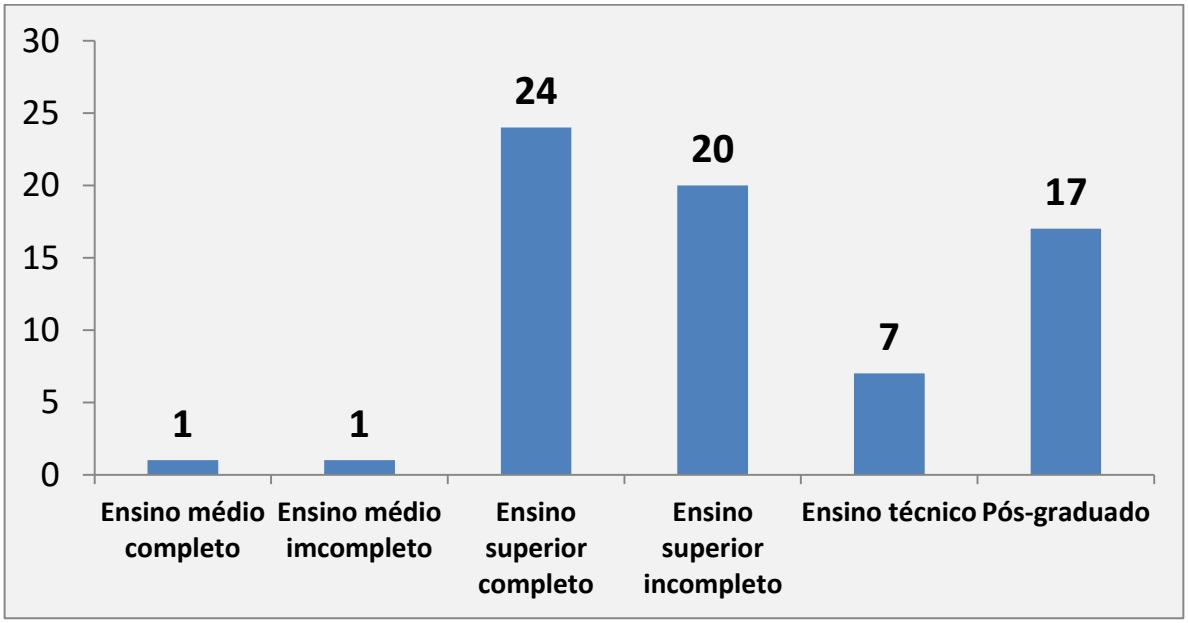
Entende-se que a empresa busca para preencher seu quadro de funcionário, pessoas com maior nível de escolaridade.

O Caged informa:

> Os dados pelo Cadastro Geral de Empregados e Desempregados (Caged), confirmam uma maior vulnerabilidade no mercado de trabalho formal dos brasileiros que estudaram menos. Quanto menor a escolaridade, maior a chance de ficar desempregado, aponta o Caged

O texto acima faz um alerta sobre a escolaridade menos aceita no mercado de trabalho. Ou seja, quando maior a evolução acadêmica, menor são as probabilidades de ficar fora do mercado de trabalho

Gráfico 2 - Escolaridade



Fonte: Dados da pesquisa (2018).

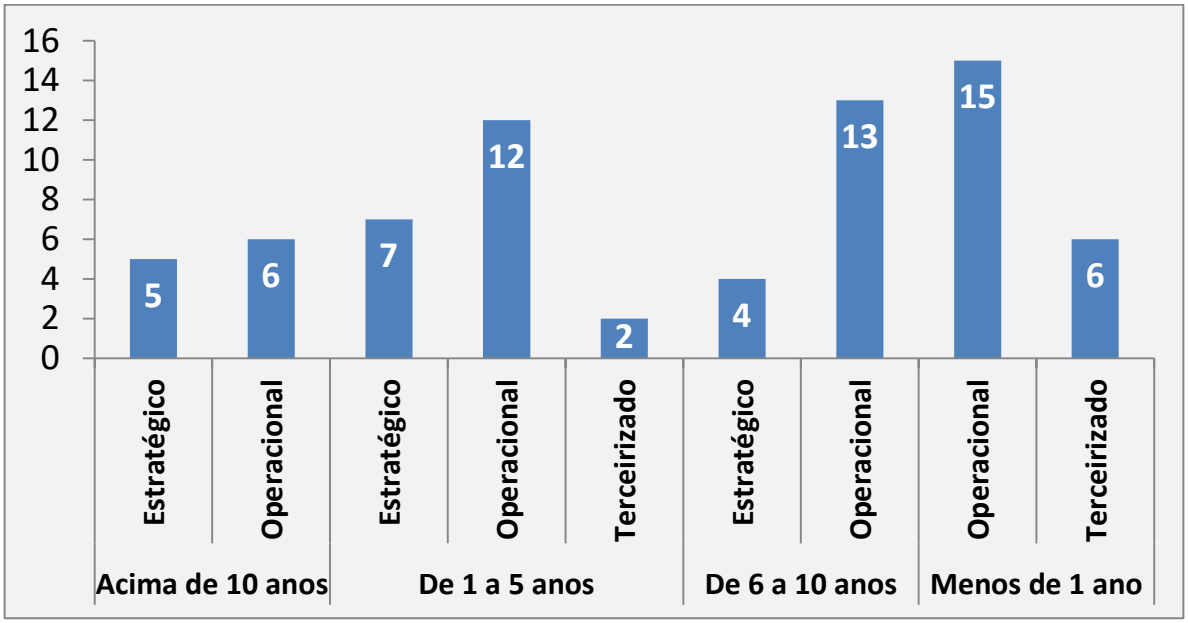
Sobre o tempo serviço que os pesquisados possuem na empresa (Gráfico 3), verificou-se que a maioria (60%; 42) dos colaboradores entrevistados estão trabalhando na empresa por um período inferior a cinco anos, 16%(11) das pessoas trabalham a mais de dez anos, ou seja, são colaboradores mais comprometidos e com maior autoridade sobre os processos. Essa informação demonstra que a empresa busca reter seus colaboradores como uma maneira de permanecer com o conhecimento adquirido. Conclui-se que, a maioria dos entrevistados, são de cargo operacional, analistas, técnicos e auxiliares, e 22%(15) são de cargo estratégico.

De acordo com o site do Estadão (2016):

> O tempo médio de permanência do brasileiro no seu emprego atingiu um patamar recorde de 161,2 semanas (ou pouco mais de três anos) no primeiro trimestre deste ano. Segundo dados do Instituto Brasileiro de Geografia e Estatística (IBGE) compilados pelo 'Estado', este patamar é o mais alto de toda a série histórica, iniciada em 2002".

A realidade vivida pela empresa está de acordo com os dados levantados pelos IBGE e pelo Estadão, em que a maioria dos colaboradores estão a menos de cinco anos.

Gráfico 3 - Tempo de serviço e Cargo



Fonte: Dados da pesquisa (2018).

3.3.2 Políticas de senha

Analisou-se que 7%(5) das pessoas tem suas senhas conhecidas por outros, e todas são de cargo operacional. Todos terceirizados e estratégicos, tem suas senhas confidencias. A indústria da mineração é muito competitiva e todas as empresas buscam maneiras de guardar seus segredos e conhecimentos industriais do melhor modo (Gráfico 4).

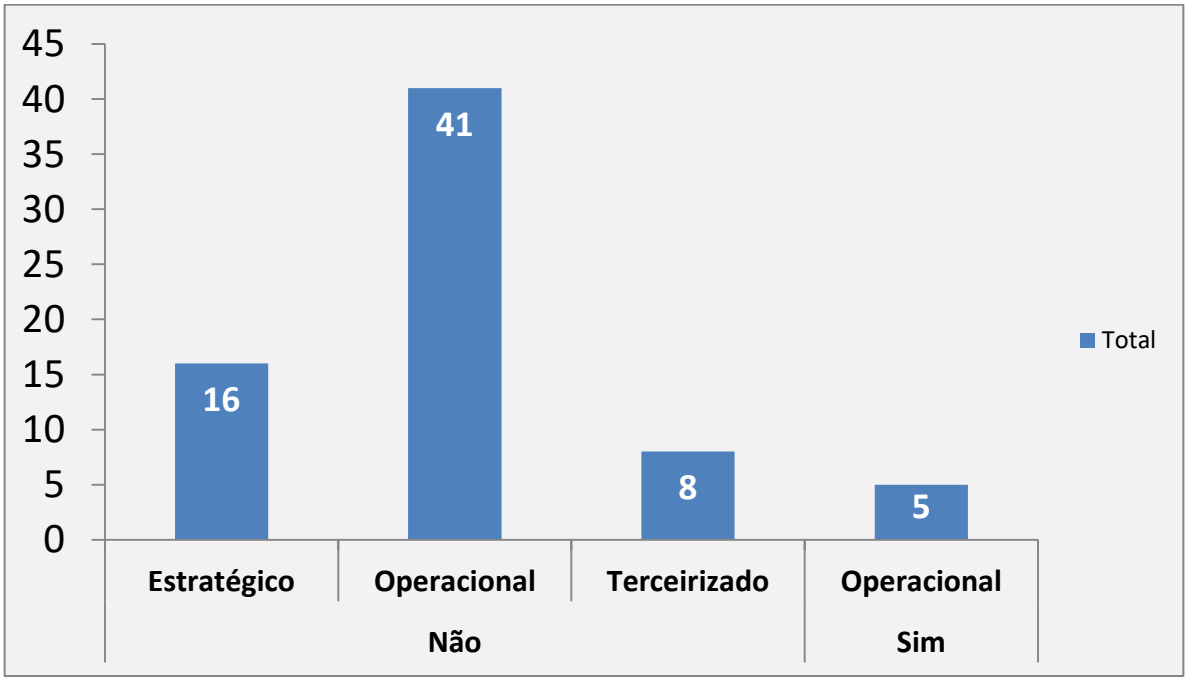
Quando falamos em engenharia social é preocupante saber que algumas senhas são de conhecimento de outras pessoas. Por mais que essas pessoas se conheçam e sejam de confiança, as senhas devem ser secretas.

Para CERT.BR (2018):

> Cuidados a serem tomados ao usar suas contas e senhas: certifique-se de não estar sendo observado ao digitar as suas senhas; não forneça as suas senhas para outra pessoa, em hipótese alguma; procure manter sua privacidade, reduzindo a quantidade de informações que possam ser coletadas sobre você.

O documento cita alguns dos cuidados que devem ser tomados para garantir que as senhas sejam privadas e seguras.

Gráfico 4 - Senha pessoal

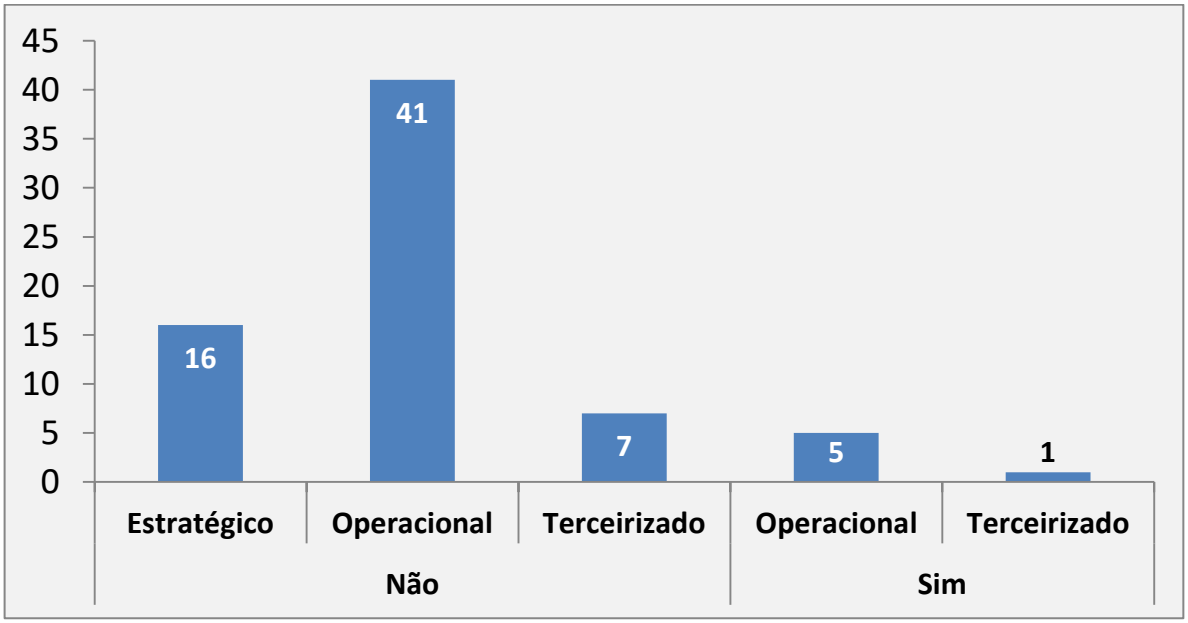


Fonte: Dados da pesquisa (2018)

O gráfico 5 exemplifica que apenas 8%(6) dos entrevistados utilizam senhas de outras pessoas para acessar dados da empresa, e são pessoas que ocupam cargos operacionais e terceirizados.

De um lado pode-se afirmar que todas as pessoas que ocupam cargos estratégicos utilizam apenas as suas próprias senhas, por outro lado saber que 8% das senhas podem ser utilizadas por mais de uma pessoa preocupa, pois, em um eventual vazamento de informações por essas senhas compartilhadas, ficará difícil identificar o culpado.

Gráfico 5 - Uso de senhas de outros



Fonte: Dados da pesquisa (2018).

O gráfico 6 demonstra um dado ainda mais preocupante, pois constatou-se que 30%(21) dos entrevistados fornecem a sua senha para que outros utilizem. É de extrema importância salientar que 7%(5) das pessoas que ocupam cargos estratégicos compartilham sua senha, talvez com pessoas de sua equipe para que sejam executados serviços do cotidiano.

Entretanto deve-se entender que o nível de acesso de um cargo estratégico é completamente diferente de um cargo operacional e o compartilhamento de senhas estratégicas colocam em risco as informações vitais para a empresa.

De acordo com a CERT.BR (2018):

> Uma senha, ou password, serve para autenticar uma conta, ou seja, é usada no processo de verificação da sua identidade, assegurando que você é realmente quem diz ser e que possui o direito de acessar o recurso em questão. É um dos principais mecanismos de autenticação usados na Internet devido, principalmente, a simplicidade que possui.

A quantidade de possibilidades de acessos a dados com uma senha é diversas e por isso necessita-se de uma atenção especial as senhas.

Gráfico 6 - Compartilhamento de senha própria

Fonte: Dados da pesquisa (2018)

Quanto a política de mudança de senha, o gráfico 7 demonstra que 93%(65) dos entrevistados alteram as suas senhas somente quando o sistema solicita, a cada três meses. A troca de senhas a cada 90 dias é uma política de segurança amplamente difundida, porém, completamente equivocada.

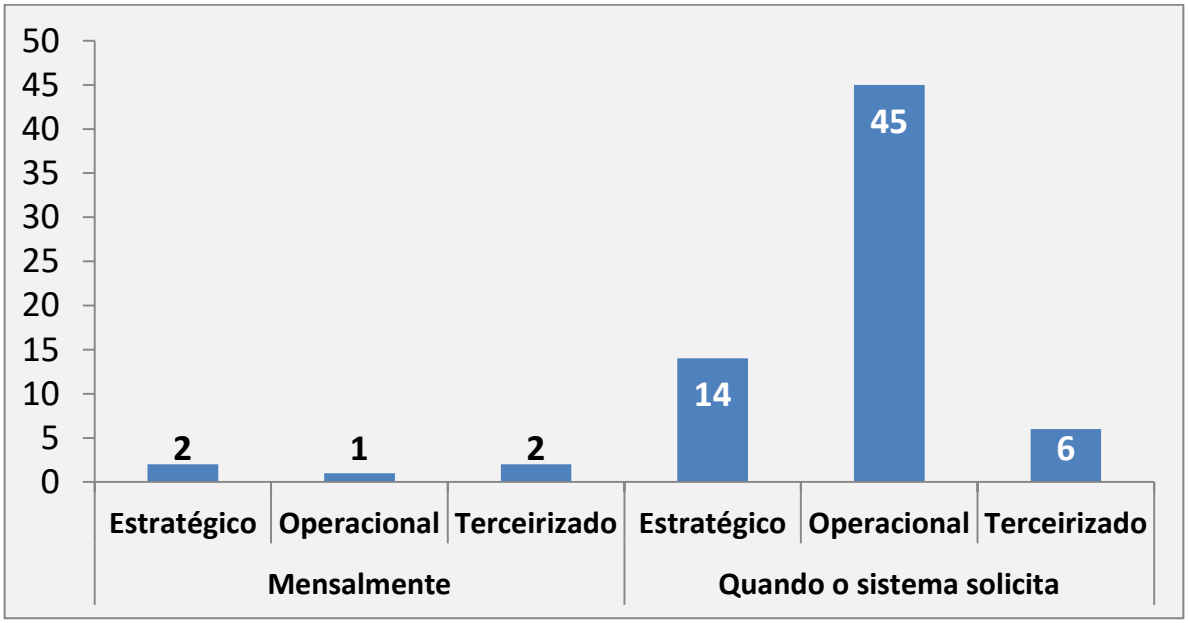
Um estudo realizado pela FCC, Comissão Federal de comércio dos EUA, demonstra que essas mudanças facilitam ainda mais os trabalhos dos hackers.

De acordo com a publicação de Rohr (2016, p.1) diz:

> A troca da senha é ineficaz. Quando o atacante pode comprometer a nova senha com o mesmo método usado para comprometer a antiga (como um ladrão de senhas presente no computador de usuário) ou quando um atacante tem um meio de manter o acesso ao alvo sem a senha, como pela instalação de um 'backdoor' [programa de controle remoto] no alvo. A expiração de senhas também é frequentemente uma fonte de frustração para os usuários, que precisam criar e lembrar-se de novas senhas a cada um ou dois meses para dezenas de contas.

Mesmo que seja uma prática comum, as trocas de senhas facilitam a sua descoberta por pessoas mal intencionadas.

Gráfico 7 - Troca de senha

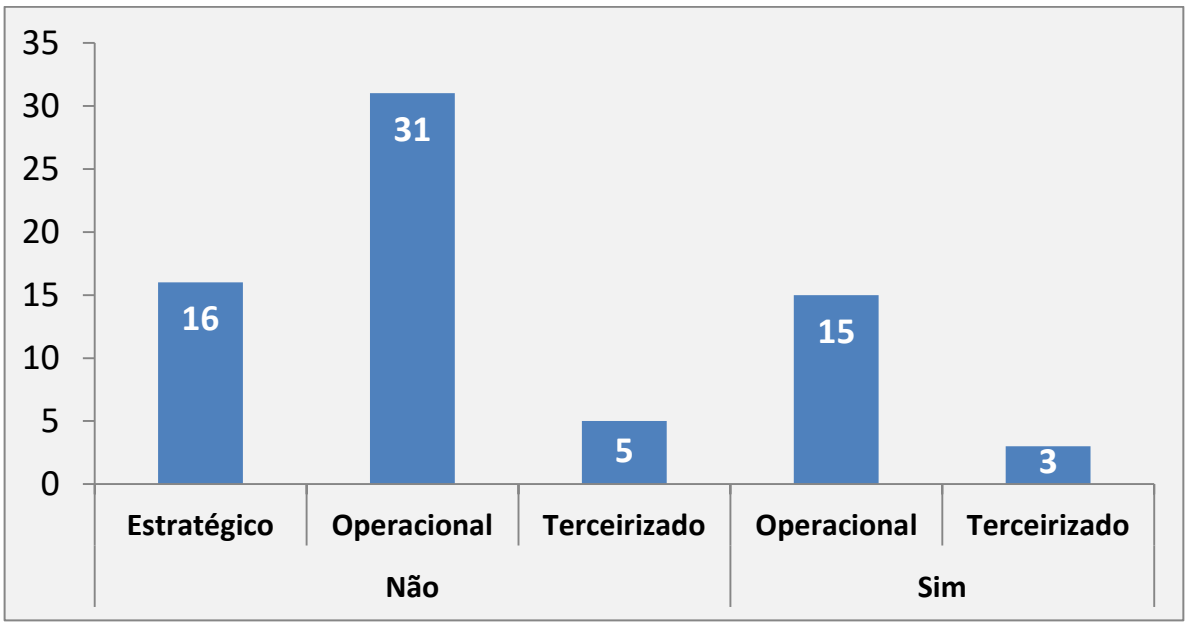


Fonte: Dados da pesquisa (2018).

Se imaginarmos que uma informação foi roubada de uma determinada empresa através de um usuário que é compartilhado com diversas pessoas. Torna-se improvável saber foi o responsável por aquela vulnerabilidade.

De acordo com o gráfico 8, aproximadamente 25%(18) dos entrevistados estão propensos a esse tipo de risco, afinal, eles utilizam senhas compartilhadas por várias pessoas.

Gráfico 8 - Senha padrão compartilhada



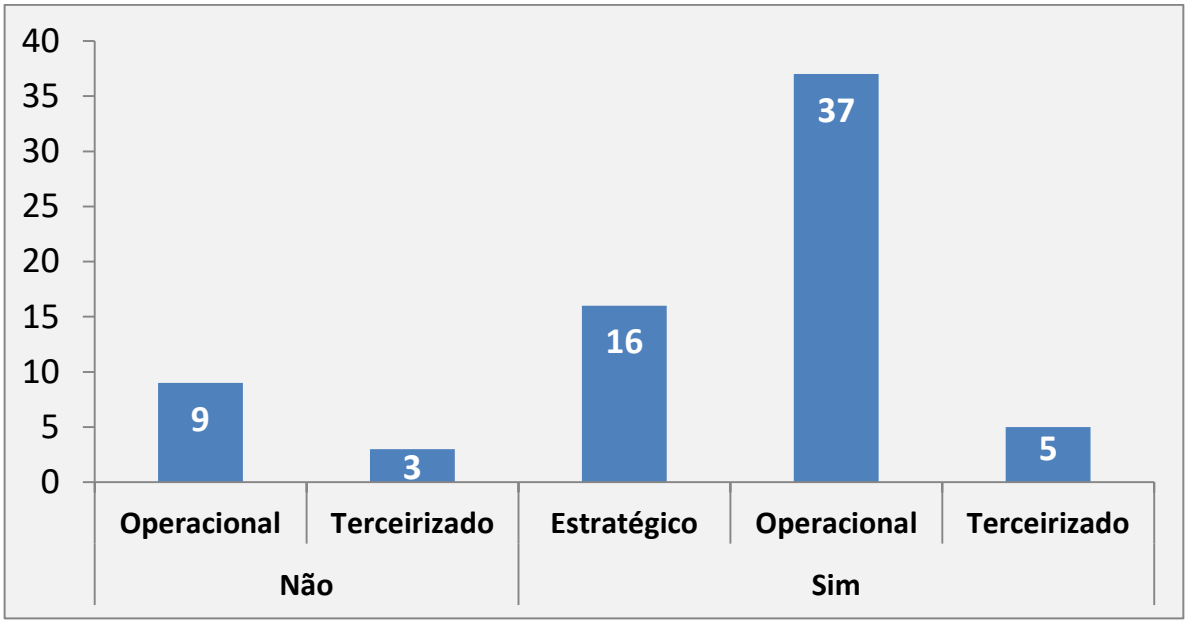
Fonte: Dados da pesquisa (2018).

3.3.3 Estrutura e práticas da empresa

O gráfico 9 demonstra que 17%(12) dos entrevistados afirmam que não existe nenhum tipo de divulgação sobre os cuidados que devem mantidos com as informações empresariais.

Ter a orientação correta de como utilizar essas informações se faz necessário, caso queira que as ações de um engenheiro social sejam minimizadas.

Gráfico 9 - Divulgação de informação

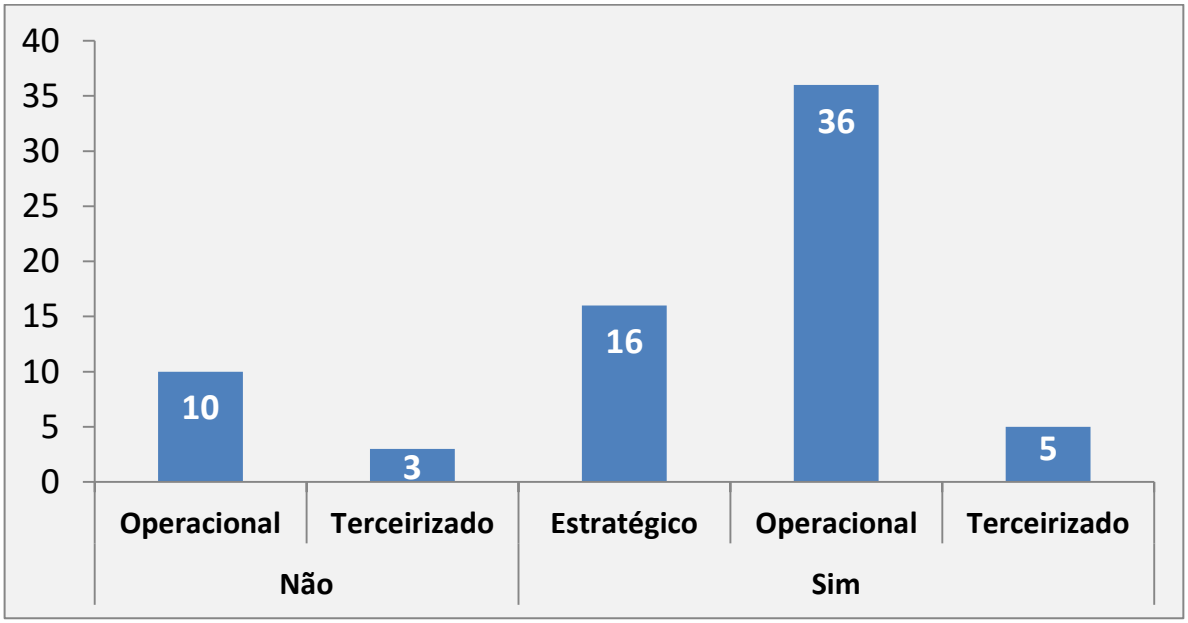


Fonte: Dados da pesquisa (2018).

Conforme é mostrado no gráfico 10, 80%(57) dos entrevistados sabem quais são as informações vitais do seu departamento. Entretanto é preocupante que aproximadamente 20%(13) não saibam quais as informações vitais da sua área, uma vez que eles podem trabalhar com esses dados de extrema importância e não são capazes de dar a atenção necessária para a informação.

O desconhecimento de quais delas são cruciais para o negócio da empresa, podem torna-las bastante indefesas e negativas para a corporação.

Gráfico 10 – Informações vitais



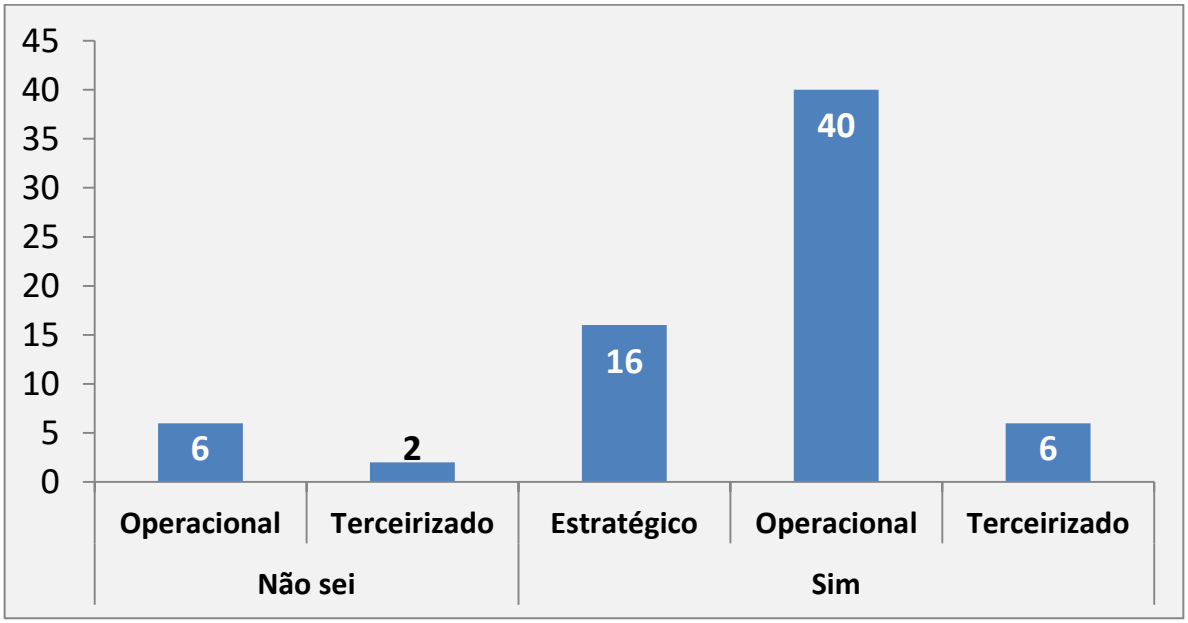
Fonte: Dados da pesquisa (2018).

O gráfico 11 ilustra que 12%(8) das pessoas não sabem se existe uma política de segurança da informação e, de acordo com as entrevistas pessoais, poucas pessoas sabem onde se encontra essa política.

Porém, 100%(70) das pessoas sabem que há um departamento de TI disponível para sanar dúvidas sobre segurança da informação.

A falta de conhecimento da política empregada pela empresa fragiliza a segurança da informação, aja vista que as pessoas não sabem como proceder em algumas situações estabelecidas pelas políticas de segurança.

Gráfico 11 - Política de segurança da informação



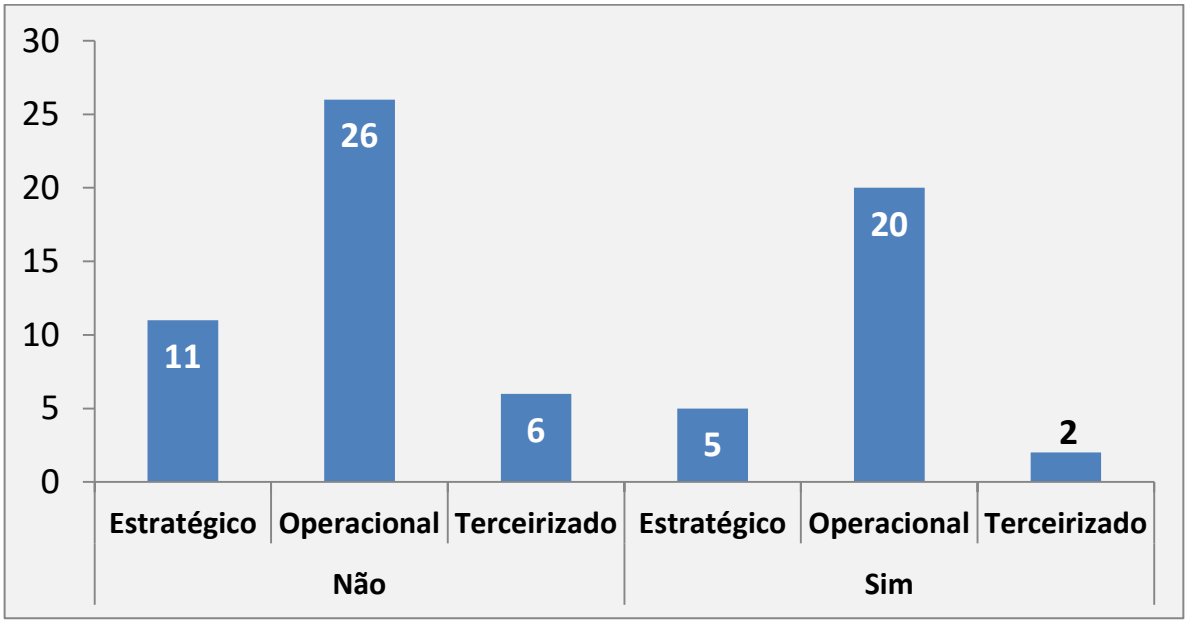
Fonte: Dados da pesquisa (2018).

3.3.4 Tratamento das informações

Na engenharia social entendemos que, ações simples e aparentemente sem perigo, podem tornar-se uma grande adversidade. Diante disso, é grave concluir que mais de 38%(27) dos entrevistados (Gráfico 12) permitem que papeis fiquem amostra, contendo informações que poderão ser usadas por uma pessoa mal-intencionada, como por exemplo, informações de salários, relatórios confidenciais, dentre outras notícias deixadas em mesas e escaninhos.

O hábito de anotar senhas em algum lugar propício de roubo, como por exemplo, perto do computador e na agenda, não condiz com uma postura de profissionais que trabalham em uma multinacional que contém inúmeras informações sigilosas.

Gráfico 12 – Informações sobre a mesa



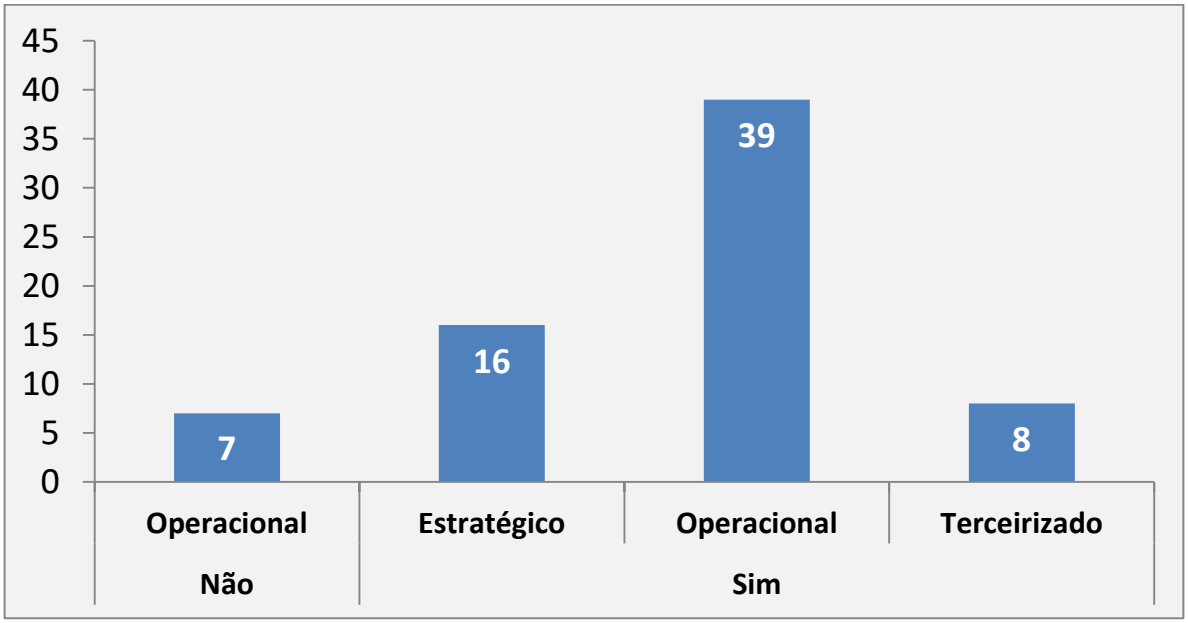
Fonte: Dados da pesquisa (2018).

Na empresa onde a pesquisa foi realizada todas as contas são vinculadas ao usuário de *login*, que é único e pessoal, ou seja, cada colaborador possui o restritamente o seu e-*mail*, ERP (*Enterprise Resource Planning*) e o servidor são acessados somente através do usuário do computador.

Mesmo que 90%(63) das pessoas ajam de maneira correta, bloqueando seus acessos ao ficarem ausentes, 10%(7) das pessoas insistem em não se preocupar com sua segurança e privacidade.

No ano de 2017, na empresa estudada, ocorreu uma campanha informando os riscos que as pessoas corriam ao não bloquear as suas contas.

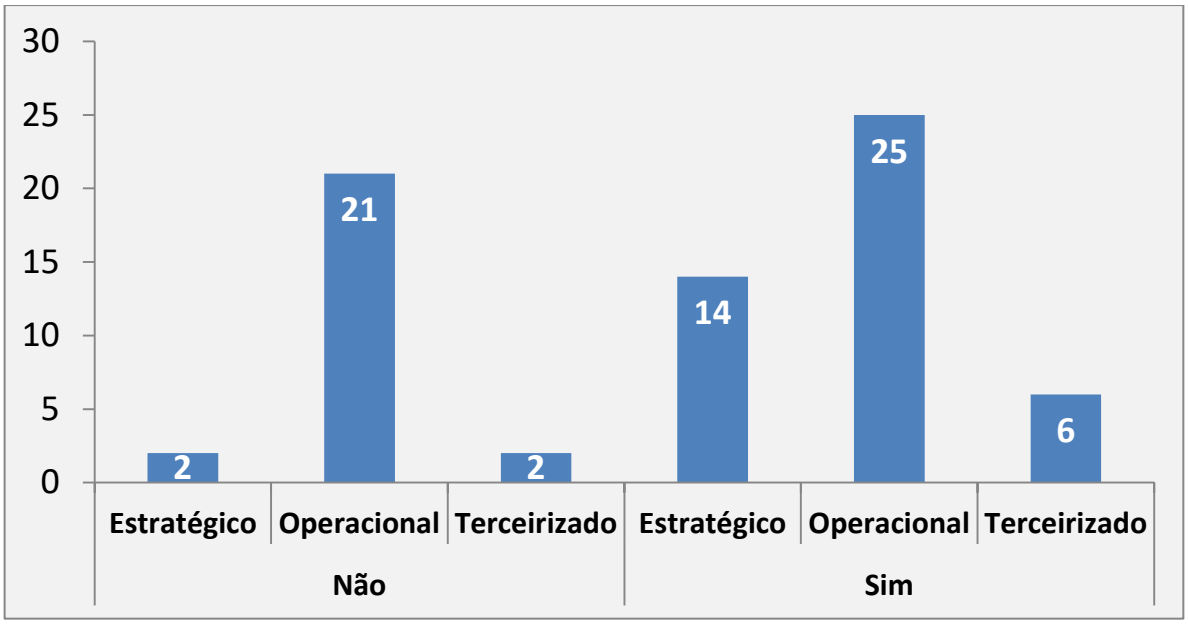
Gráfico 13 - Bloqueio dos computadores



Fonte: Dados da pesquisa (2018).

O gráfico 14 expõe a opinião pessoal dos entrevistados acerca do conhecimento que seus colegas de trabalho possuem sobre a importância das informações da empresa. 36%(25) das pessoas responderam que acreditam que seus colegas não conhecem quais são as informações importantes para o seu departamento.

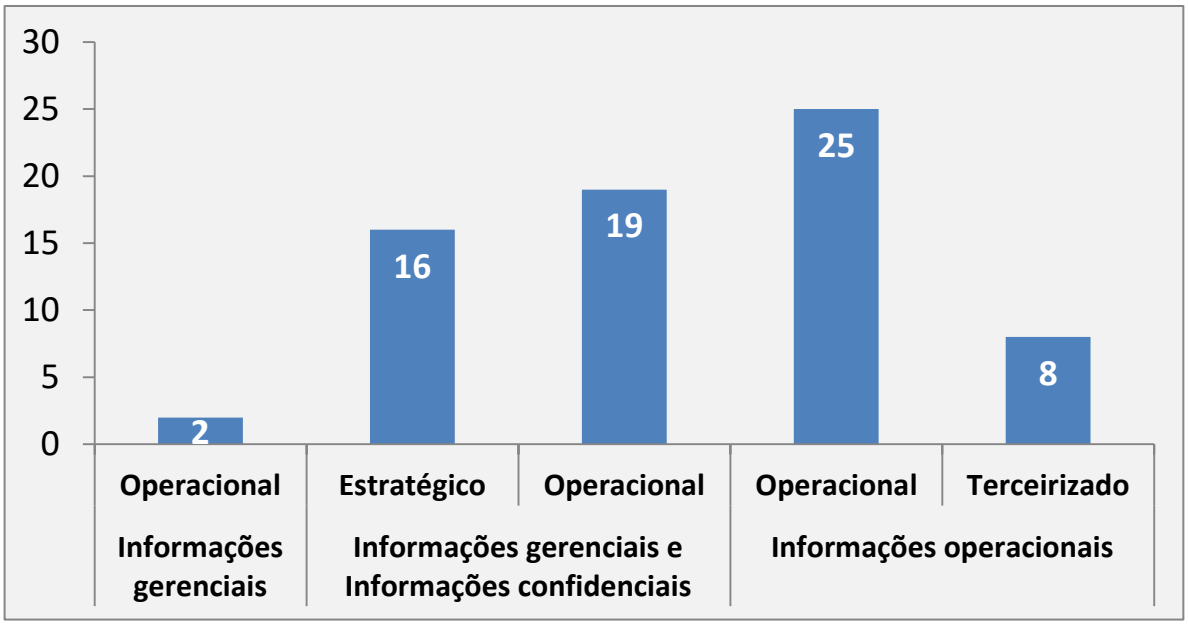
Gráfico 14 – Importância para o departamento



Fonte: Dados da pesquisa (2018).

Considerando que 22%(16) dos entrevistados são de cargos estratégicos, conclui-se que o gráfico 15 demonstra que as informações gerenciais e confidencias, que são vitais para os negócios, estão ao acesso de pessoas que são de cargos operacionais. Essas informações difundidas podem cair em mão erradas, afinal, várias pessoas têm acesso a elas.

Gráfico 15 – Tipos de informações

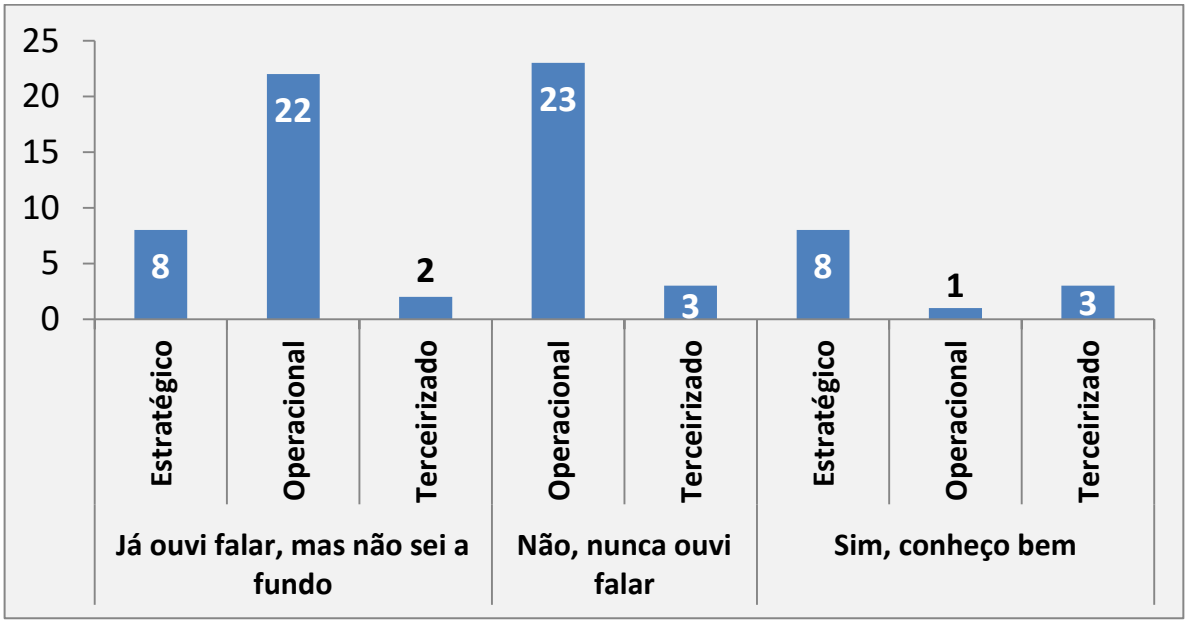


Fonte: Dados da pesquisa (2018).

3.3.5 Instrução sobre engenharia social

O gráfico 16 demonstra um dado alarmante, mais de 80%(58) dos entrevistados não detém conhecimento adequado sobre engenharia social, o que é um risco para empresa. Roubo de informação, fraude, espionagem industrial, são alguns dos tipos de danos causados quando não se retém o conhecimento apropriado.

Gráfico 16 - Grau de conhecimento sobre Engenharia Social



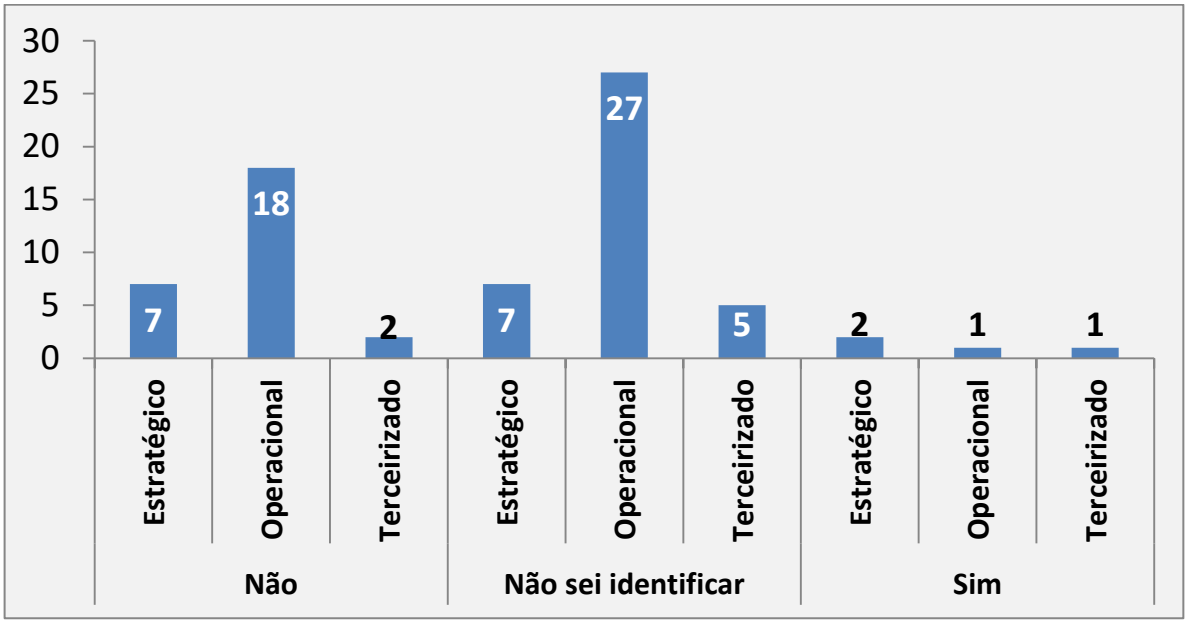
Fonte: Dados da pesquisa (2018).

O gráfico 17 ilustra que aproximadamente 62%(43) dos entrevistados foram vítimas ou não sabem identificar, se levarmos em consideração o gráfico 17 no qual demonstra que 80% não conhecem adequadamente a engenharia social, conclui-se que esse tema é de difícil entendimento, pois alguns indivíduos que declararam não conhecer a engenharia social, dizem já ter sido vítimas dela.

Dos 100% de entrevistados somente 38%(27) afirmam não terem sido vítimas de engenharia social, acreditam que se nenhum dado foi roubado, os mesmos não foram vítimas.

A CERT.BR (2018) relata que, somente em 2017, houveram mais de 800.000 reportes de incidentes ou ataques aos sistemas de informação, onde mais de 7% são fraudes, métodos de má fé com intuito de lesar alguém.

Gráfico 17 - Foi vítima?

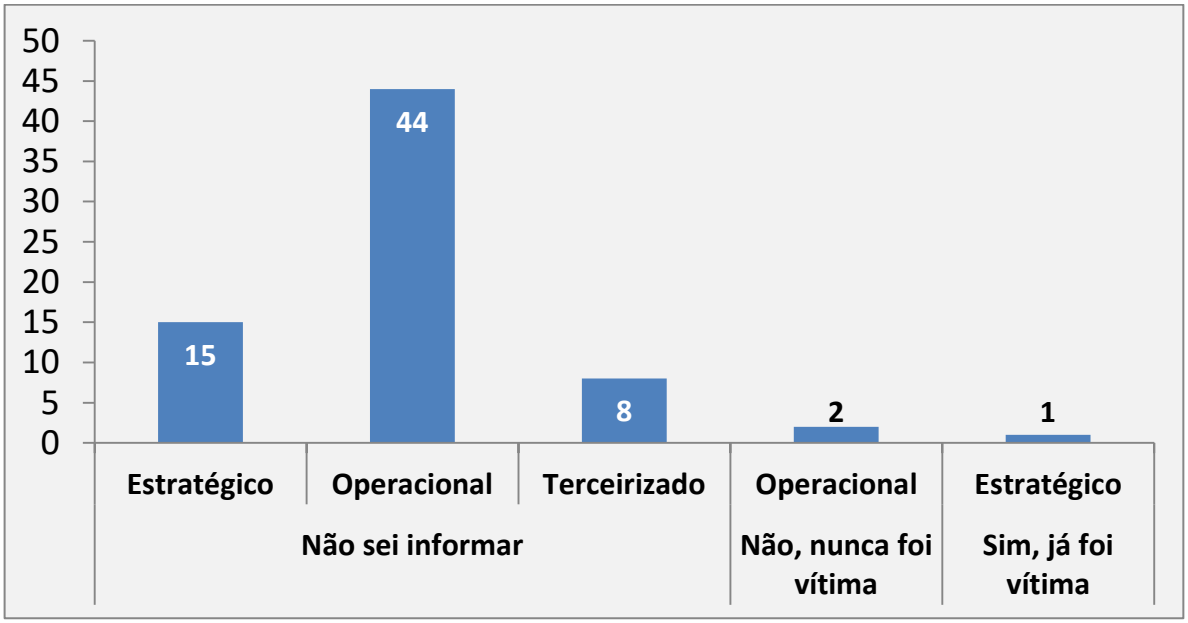


Fonte: Dados da pesquisa (2018).

Ao analisar o gráfico 18, entende-se que apenas uma pessoa afirma que a empresa foi vítima de engenharia social. Essa informação demonstra que esse assunto não é difundido na empresa, o que é ruim para que todos tenham ciência do ocorrido.

O gerente de TI, relatou que em 2015 ocorreu um ataque de engenharia social, onde um ex-colaborador usou a confiança que seus ex-colegas de trabalho tinham nele e dessa maneira modificou alguns dados na hora de carregar o navio de exportação, gerando 01 dia de prejuízo para empresa.

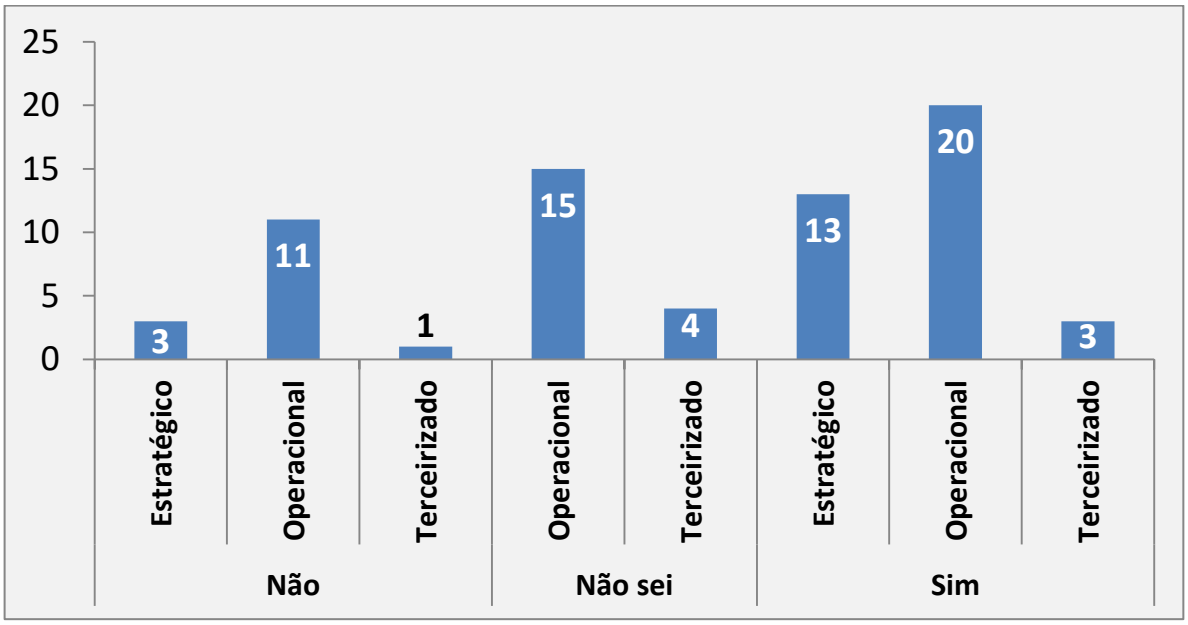
Gráfico 18 - A empresa foi vítima?



Fonte: Dados da pesquisa (2018).

O gráfico 19 demonstra que mais de 50%(34) dos entrevistados desconhecem o plano de recuperação de dados. É importante para o usuário ter conhecimento de qual maneira seus dados poderão ser recuperados em casos extremos, como perda, rouba, catástrofes e etc.

Gráfico 19 - Recuperação de dados



Fonte: Dados da pesquisa (2018).

CONSIDERAÇÕES FINAIS

Os sistemas de informação não podem ser vistos como unidades isoladas dos ambientes que as cercam. Algumas características dos usuários possuem grande influência na segurança desses sistemas. Diante disso, é importante que as atenções à segurança desses processos sejam concentradas nas pessoas e usuários, e não somente nas tecnologias.

No trabalho exposto foi citado alguns métodos de ataques e algumas competências dos engenheiros sociais, entretanto, a tendência é que surjam novos métodos e que novas habilidades sejam adquiridas.

Diante dessa realidade, pode-se afirmar que não existe segurança total e cada empresa precisa descobrir uma estratégia para controlar a segurança da informação. É impossível operar com ameaça zero, por isso sempre haverá riscos e eles devem ser ajustados de acordo com cada corporação, pois esse tipo de incidente geralmente está ligado ao erro humano.

Buscou-se também expor os dados e traçar o perfil dos colaboradores entrevistados. De acordo com os dados obtidos o perfil do colaborador é:

- Faixa etária de 35 a 45 anos.
- Ensino superior incompleto.
- Cargo operacional.
- De 1 a 5 anos de casa.
- Trabalha com informações gerenciais e confidencias.
- Que já ouviu falar, mas não conhece a fundo a engenharia social.
- Já foi vítima ou não sabe identificar.
- Reconhece que tem como recuperar dados.

Nesse sentido, com base nos resultados obtidos durante o desenvolvimento da dissertação, é possível sugerir algumas melhorias futuras:

- Desenvolver uma estrutura para gerenciar a segurança da informação: é necessário estabelecer um bloco de metas contra engenharia social e treinar um grupo de colaboradores responsáveis pelo cumprimento dessas metas.

- Avaliar os riscos independentes: os métodos de ataques, ainda que semelhantes, apresentam níveis de riscos distintos de acordo com cada empresa. É preciso examinar cada um dos riscos e avaliar os perigos que podem apresentar a empresa.
- Programar defesas em sua diretiva de segurança: formar um conjunto de procedimentos que incentivem como os colaboradores devem lidar com situações que possam ser algum ataque de engenharia social.

REFERÊNCIAS

BRENNER, Susan. 2003. **The Psychology of Social Engineering**. Disponível em: <http://empereurpalpatine.free.fr/Media/The%20Psychology%20Of%20Social%20Engineering.pdf>. Acesso em: 30/04/2018.

CERT. 2018. **Cartilha de segurança para internet**. Disponível em: <https://cartilha.cert.br/senhas/>. Acesso em: 17/05/2018.

CERT. 2018. **Incidentes reportados ao CERT.br**. Disponível em: <https://www.cert.br/stats/incidentes/2017-jan-dec/tipos-ataque.html>. Acesso em: 17/05/2018.

CRANOR, Lorrie. **Frequent password changes are the enemy of security**. 2016. Disponível em: <https://arstechnica.com/information-technology/2016/08/frequent-password-changes-are-the-enemy-of-security-ftc-technologist-says/>. Acesso em: 04/05/2018.

FREITAS, Andrey R., **Investigando Vazamento de Informações e de Propriedade Intelectual**. 2013. Disponível em: <http://dfir.com.br/wp-content/uploads/2013/10/Evidencia_Digital_05.pdf>. Acesso em: 05/04/2018.

DOS SANTOS, Rafael Cardoso. **Engenharia social:** atacando o elo mais fraco. Disponível em: <http://mauriciolyra.pro.br/site/wp-content/uploads/2015/12/09-Artigo-Engenharia-social.pdf>. Acesso em: 16/04/2018.

DUARTE, Jane Cristina dos Santos. **Identidade Cultural do Brasileiro:** Razão, Emoção, Ação e Aplicação. 2014. Disponível em: http://publicacoes.unigranrio.com.br/index.php/reihm/article/download/467/458. Acesso em: 30/05/2018.

GOUVEIA, Luís Manuel Borges. **Notas de contribuição para uma definição operacional**. 2004. Disponível em: <http://homepage.ufp.pt/lmbg/reserva/lbg_socinformacao04.pdf>. Acesso em: 16/03/2018.

GUENTHER, Melissa. **Social Engineering**. 2001. Disponível em: <http://www.iwar.org.uk/comsec/resources/security-awareness/social-engineering-generic.pdf>. Acesso em: 04/04/2018.

HOLANDO, Sergio Buarque de. 1995. **Raízes do Brasil**. Disponível em: < http://www.tecnologia.ufpr.br/portal/lahurb/wp-content/uploads/sites/31/2017/09/HOLANDA-S%C3%A9rgio-Buarque-Ra%C3%ADzes-do-Brasil.pdf>. Acesso em: 12/05/2018

KASPERSKY. **Phishing for cryptocurrencies:** How bitcoins are stolen. Acesso em: 12/04/2018. Disponível em: <https://www.kaspersky.com/blog/crypto-phishing/20765/>

LIMA, Luiz Eduardo. **Malefícios da Engenharia Social**. Acesso em: 07/04/2018. Disponível em: <http://web.mit.edu/Saltzer/www/publications/protection/index.html.>

MANN, Ian. **Engenharia Social**. São Paulo. Blucher. 2011.

MARCELO, Antonio; PEREIRA, Marcos. **A Arte de Hackear Pessoas**. Rio de Janeiro: Brasport. 2005.

McAfee LABS. 2014. **Hacking the Human Operating System**. European Cybercrime Centre. Acesso em: 03/03/2018. Disponível em: <https://community.mcafee.com/nysyc36988/attachments/nysyc36988/security-awareness-documents/1068/1/rp-hacking-human-os.pdf>

MISAGHI, Mehran. Segurança de Redes. **A Necessidade de Segurança**. Acesso em: 20/04/2018. Disponível em: <http://ist.sociesc.com.br/mehran/ensino/seg05.ppt>

MITNICK, K. D.; SIMON, W. L. **A arte de enganar**. São Paulo, Pearson Education, 2003.

MÓDULO Security Solutions S.A. **9ª Pesquisa Nacional de Segurança da Informação**. Rio de Janeiro, 2003. Acesso em: 15/01/2018. Disponível em: <http://www.modulo.com.br/temp/9aPesquisaNacional_Modulo.zip>.

NBR ISO/IEC 27002. Norma ABNT NBR ISO/IEC 27002:2007 – **Código de Prática para a Gestão de Segurança da Informação**. Associação Brasileira de Normas Técnicas (ABNT). Rio de Janeiro, 2007. Acesso em: 27/04/2018. Disponível em: <http://www.iso27001security.com/ html/27002.html.>

NEUROLIGÍSTICA, Sociedade Brasileira de programação. **Entenda o que é a Programação Neurolinguística**. Acesso em: 08/02/2018. Disponível em: <https://www.pnl.com.br/programacao-neurolinguistica/o-que-e-pnl-/entenda-o-que-e-a-programacao-neurolinguistica>

OLIVEIRA, Salomão. 2015. **As Tríplices da Segurança da Informação**. Acesso em: 26/02/2018. Disponível em: <https://pt.linkedin.com/pulse/tr%C3%ADplices-da-seguran%C3%A7a-informa%C3%A7%C3%A3o-salom%C3%A3o-de-oliveira>

PAULO, Estadão de S. 2014. **Brasileiro fica mais tempo no emprego**. Acesso em: 28/05/2018. Disponível em: <https://economia.estadao.com.br/noticias/geral,brasileiro-fica-mais-tempo-no-emprego>

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

ROHR, Altieres. 2016. **Troca frequente de senha não melhora a segurança**. Acesso em: 22/05/2018. Disponível em: <http://g1.globo.com/tecnologia/blog/seguranca-digital/post/troca-frequente-de-senha-nao-melhora-seguranca-diz-especialista.html>

SCHNEIER, Bruce. **Segurança.Com. Segredos e Mentiras Sobre a Proteção na Vida Digital**. Rio de Janeiro: Campus, 2001.

SCS, **Informativo**. 2017. Disponível em: <http://www.mdic.gov.br/images/REPOSITORIO/scs/decos/Informativo_2017/128_Informativo_da_Secretaria_de_Com%C3%A9rcio_e_Servi%C3%A7o_2017.pdf> . Acesso em: 08/05/2018.

SECURITY, Norton. **Como Eles Atacam**. Disponível em: <http://br.norton.com/security_response/phishing.jsp>. Acesso em: 24/04/2018.

SHINDER, Debra Littlejohn. **How to Defend your Network Against Social Engineers**. Disponível em: <http://techgenix.com/social_engineers/>. Acesso em: 12/03/2018.

SVAITER, David. 2015. **Qual o valor da Informação?**. Disponível em: <https://www.linkedin.com/pulse/qual-o-valor-da-informa%C3%A7%C3%A3o-david-ben-svaiter?trk=portfolio_article-card_title>. Acesso em: 20/02/2018

TYLOR, Edward B. 1920. **Primitive Culture**. Disponível em: < https://archive.org/stream/primitiveculture01tylouoft#page/n17/mode/2up>. Acesso em: 03/05/2018

APÊNDICE A – INSTRUMENTO PARA COLETA DE DADOS

UNIVERSIDADE FEDERAL DO PARÁ
INSTITUTO DE CIÊNCIAS EXATAS E NATURAIS
FACULDADE DE COMPUTAÇÃO
CURSO DE BACHARELADO EM SISTEMAS DE INFORMAÇÃO

Prezado (a),

Você está sendo convidado (a) para participar, como voluntário, em uma pesquisa acadêmica que está sendo concluída para o curso de sistemas de informação da UFPA – Universidade Federal do Pará intitulada "**ENGENHARIA SOCIAL: ESTUDO EM UMA EMPRESA DE MINERAÇÃO DE BARCARENA**".

O objetivo principal desta pesquisa é avaliar a sensibilidade dos colaboradores da empresa, quanto as consequência de ataques de engenharia social em ambiente corporativo.

Engenharia Social são técnicas utilizadas para obter informações importantes e sensíveis de uma corporação ou de um indivíduo por meio da enganação, realizada de forma pessoal (face-to-face) ou por meio de recursos de tecnológicos.

Não será pedido para você se identificar. A sua identidade será mantida em absoluto sigilo. Os dados obtidos serão gravados e poderão ser transcritos, mas a sua identidade permanecerá no anonimato.

Pesquisador responsável: **Gedean Gonçalves Carvalho**.
Telefone para contato: (91) 3754-7741.
E-mail: Gedean.carvalho@hotmail.com

Desde já agradeço a sua colaboração e me coloco à disposição para qualquer dúvida ou esclarecimento.

Atenciosamente.

QUESTIONÁRIO

1. Qual a sua faixa etária?
   - Abaixo de 25 anos.
   - De 25 a 35 anos.
   - De 35 a 45 anos.
   - Acima de 45
2. Qual seu sexo?
   - Masculino.
   - Feminino.
3. Qual o seu nível de escolaridade?
   - Ensino médio incompleto.
   - Ensino médio completo.
   - Ensino superior incompleto.
   - Ensino superior completo.
   - Ensino técnico.
   - Pós-Graduado.
4. Qual o seu cargo?
   - Estratégico. (Ex: Diretor, Gerente, Coordenador).
   - Operacional. (Ex: Analista, Técnico, auxiliar).
   - Terceirizado. (Ex: Bolsista, Prestador de serviço).
5. Há quanto tempo você trabalha?
   - Menos de 1 ano.
   - De 1 a 5 anos.
   - De 6 a 10 anos.
   - Acima de 10 anos.
6. Além de você, mais alguém conhece a(s) sua(s) senha(s) utilizada(s)?
   - Sim.
   - Não.
7. Você utiliza senha(s) de outro(s) colaborador (es)?
   - Sim.
   - Não.
8. Você permite que algum colaborador utilize sua senha para algum tipo de trabalho rápido?
   - Sim.
   - Não.
9. Você altera suas senhas com que frequência?
   - Mensalmente.
   - Semestralmente.
   - Quando o sistema solicita.
   - Sempre utilizo a mesma senha.
10. Você possui alguma senha padrão para algum serviço, compartilhada com todos do seu departamento?

- Sim.
- Não.

11. A empresa disponibiliza orientação sobre a divulgação de informações?
    - Sim.
    - Não.
12. Em seu setor, você sabe quais são as informações que são vitais para a empresa?
    - Sim.
    - Não.
13. A empresa possui uma política de segurança da informação?
    - Sim.
    - Não.
    - Não sei.
14. A empresa possui um departamento de TI especializado?
    - Sim.
    - Não.
    - Não sei.
15. Neste exato momento, existe algum papel sobre a sua mesa com informações sobre a empresa?
    - Sim.
    - Não.
16. Ao sair de perto do computador, você costuma bloqueá-lo?
    - Sim.
    - Não.
17. O setor que você trabalha possui informações consideradas confidenciais?
    - Sim.
    - Não.
    - Não sei.
18. Em sua opinião, todos os colaboradores do seu setor sabem a importância das informações da empresa?
    - Sim.
    - Não.
19. Quais tipos de informações você possui acesso? (Pode marcar mais de uma)
    - Informações operacionais.
    - Informações gerenciais.
    - Informações confidenciais da empresa.
    - Não possuo acesso a nenhum tipo de informação importante.
20. Você possui conhecimento sobre “Engenharia Social”?
    - Sim, conheço bem.
    - Não, nunca ouvi falar.
    - Já ouvi falar, mas não sei a fundo
21. Você já foi vítima de um engenheiro social?
    - Sim.

- Não.
- Não sei identificar.

22. É do seu conhecimento que a empresa tenha sido vítima de “Engenharia Social”?
    - Sim, já foi vítima.
    - Não, nunca foi vítima.
    - Não sei informar.
23. Em caso de perda, roubo ou desastre, você é capaz de recuperar seus arquivos e documentos?
    - Sim.
    - Não.
    - Não sei.