FACULDADE DE TECNOLOGIA DE AMERICANA
CURSO SUPERIOR DE TECNOLOGIA EM SEGURANÇA DA INFORMAÇÃO

SABRINA OLIVEIRA DOS SANTOS

ENGENHARIA SOCIAL E POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO NO AMBIENTE CORPORATIVO

Americana, SP
2018

FACULDADE DE TECNOLOGIA DE AMERICANA CURSO SUPERIOR DE TECNOLOGIA EM SEGURANÇA DA INFORMAÇÃO

SABRINA OLIVEIRA DOS SANTOS

ENGENHARIA SOCIAL E POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO NO AMBIENTE CORPORATIVO

Trabalho de graduação apresentado como requisito parcial para a obtenção do grau de Tecnólogo no Curso Superior de Tecnologia em Segurança da Informação, pela Faculdade de Tecnologia de Americana, sob a orientação do Prof. M.e Benedito Luciano Antunes de França.

Americana, SP

2018

SABRINA OLIVEIRA DOS SANTOS

ENGENHARIA SOCIAL E POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO NO AMBIENTE CORPORATIVO

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo no Curso Superior de Tecnologia em Segurança da Informação, pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.

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

S238e SANTOS, Sabrina Oliveira dos

Engenharia social e políticas de segurança da informação no ambiente corporativo. / Sabrina Oliveira dos Santos. – Americana, 2018.

48f.

Monografia (Curso de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Prof. Ms. Benedito Luciano Antunes de França

1 Engenharia Social I. FRANÇA, Benedito Luciano Antunes de II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana

CDU:681.518.5

Sabrina Oliveira dos Santos

ENGENHARIA SOCIAL E POLÍTICAS DE 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, 21 de fevereiro de 2019.

Banca Examinadora:

Benedito Luciano Antunes de França (Presidente)
Mestre
Fatec Americana

Wladimir da Costa (Membro)
Mestre
Fatec Americana

Clerivaldo José Roccia (Membro)
Mestre
Fatec Americana

AGRADECIMENTOS

Agradeço, primeiramente, aos meus pais, que sempre estiveram ao meu lado sendo minha maior fonte de inspiração, que me deram forças nos momentos difíceis, além de amor, incentivo e apoio incondicional.

Agradeço a minha irmã Bianca Oliveira que sempre me inspirou e me apoiou nunca me deixando fraquejar diante das adversidades. Sem você, seria tudo mais difícil.

Agradeço ao meu irmão João Felipe que sempre me passou uma palavra de ânimo.

Agradeço ao Thiago Papani meu grande parceiro e melhor amigo, pela paciência, apoio e motivação.

Agradeço também à FATEC Americana que me deu a oportunidade de cursar Segurança da Informação nesta renomada instituição.

Agradeço imensamente ao meu orientador, M.e Benedito Luciano Antunes de França pela paciência, pelo apoio e pela determinação em me ajudar a produzir este trabalho mesmo quando pensei em desistir.

À PPG Brasil, por acreditar no meu potencial desde o início de minha jornada acadêmica e me fornecer minha primeira oportunidade efetiva de desenvolvimento profissional e pessoal além de todo apoio no meu projeto. Desta forma, gostaria de agradecer em especial a minha equipe, Kenia, Andressa e Rodolfo pelo apoio e amizade.

Quero conceder meu imenso agradecimento a Melina, Tatiane, Raquel pelo suporte na aplicação do meu estudo de caso e por toda disponibilidade durante o processo de validação não posso deixar de agradecer ao Denyson e Fabricio que além do suporte no estudo de caso me ajudam no meu desenvolvimento profissional diariamente e não menos importante quero agradecer ao Vitor, que me ajudou na versão teste do questionário afim de garantir funcionalidade perfeita no envio oficial. ‘

Quero deixar registrado meu agradecimento a todos os funcionários que dispuseram de seu tempo para o responder o questionário. Todos vocês, sem exceção, me inspiraram a me tornar uma profissional melhor a cada dia.

Aos meus amigos, pela força e torcida para que tudo desse certo.

Meu muito obrigado a Deus pelo dom da vida e por seu amor infinito.

"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 de pesquisa tem por objetivo apresentar uma ótica sobre a Segurança da Informação e a engenharia social nas empresas. Atualmente a engenharia social tem encontrado muitos desafios com as políticas de Segurança da Informação dentro das organizações. Os engenheiros sociais possuem a arte de hackear e manipular pessoas para se auto beneficiar, conseguindo a partir de suas vítimas informações que fazem parte do sucesso de seus golpes. Diante deste problema muito atual, o presente trabalho tem como objetivo analisar e estudar as vulnerabilidades da engenharia social e suas ameaças dentro das organizações. Assim sendo será composto por pesquisas, historias fundamentada em autores conceituados em pesquisas desta área, e por fim uma pesquisa de analise através de questionários aplicados em uma empresa. Este último terá o intuito de analisar como os profissionais das organizações, incluindo os profissionais de T.I, protegem as informações do seu ambiente de trabalho e se são capazes de identificar um ataque de engenharia social.

Palavras Chave: Palavras-chave: Engenharia Social; Segurança da Informação; Fator Humano.

ABSTRACT

This research aims to present an optics about information security and social engineering in companies. Today social engineering has encountered many challenges with information security policies within organizations. Social engineers have the art of hacking and manipulating people to benefit from themselves, getting from their victims information that is part of the success of their hits. Faced with this very current problem, the present work aims to analyze and study the vulnerabilities of social engineering and its threats within organizations. Thus, it will be composed of researches, histories based on authors reputed in researches of this area, and finally a research of analysis through questionnaires applied in a company. The latter will attempt to analyze how organizations' professionals, including T.I professionals, protect information from their work environment and are able to identify a social engineering attack.

Keywords: Social Engineering; Security of Information; Human Factor.

LISTA DE ILUSTRAÇÕES: FIGURAS E GRÁFICOS

Figura 1 – Segurança da Informação nas empresas George Dawel.....19
Figura 2 – Ataque via *Pishing*.....21
Figura 3 – Pilares da Segurança da Informação.....24
Figura 4 – Os polos da Segurança da Informação.....26

Gráfico 1 – Alvos de violação de dados.....32
Gráfico 2 – Informações almejadas nas violações.....33
Gráfico 3 – Local de trabalho do grupo de respondentes.....36
Gráfico 4 – Vínculo empregatício direto ou indireto (terceirizado) do grupo de respondentes..... 37
Gráfico 5 – Uso do crachá de identificação funcional.....38
Gráfico 6 – Bloqueio automático bloqueia da máquina (Desktop, Notebook ou Celular corporativo) 39
Gráfico 7 – Acesso a informações confidencias.....40
Gráfico 8 – Treinamento interno relacionado à Segurança da Informação.....41
Gráfico 9 – Relação de vítimas de crimes virtuais.....42
Gráfico 10 – O uso do e-mail corporativo.....43
Gráfico 11 – Conhecimento em “Engenharia Social”.....44

Gráfico 12 – Conhecimento sobre as Políticas de Segurança da Informação.....44

LISTA DE TABELAS

Tabela 1 – Classificação de resultados positivos.....30

SUMÁRIO

LISTA DE ILUSTRAÇÕES: FIGURAS E GRÁFICOS.....11
LISTA DE TABELAS.....11
INTRODUÇÃO.....13
CAPÍTULO I - ENGENHARIA SOCIAL.....16
1.1 ENGENHARIA SOCIAL NAS ORGANIZAÇÕES.....17
1.2 PERFIL DO ENGENHEIRO SOCIAL.....18
1.2.1 HACKERS E CRACKERS.....19
1.3 MEIOS DE ATAQUES.....20
1.4 TÉCNICAS DE ATAQUES.....20
1.4.1 PISHING.....21
1.4.2 SMISHING.....22
1.4.3 VISHING.....22
CAPÍTULO II - SEGURANÇA DA INFORMAÇÃO.....23
2.1 PILARES DA SEGURANÇA DA INFORMAÇÃO.....24
2.2 MÉTODOS DE SEGURANÇA DA INFORMAÇÃO.....26

2.3 POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO.....27
2.4 AMEAÇAS E VULNERABILIDADES CORPORATIVAS.....29
CAPÍTULO III - O FATOR HUMANO NA SEGURANÇA DA INFORMAÇÃO.....31
3.1 O ELO MAIS FRACO DA SEGURANÇA DA INFORMAÇÃO.....34
CAPÍTULO IV - ESTUDO DE CASO.....35
4.1 ANÁLISE DE ESTUDO DE CASO.....45
CONCLUSÃO.....46
REFERÊNCIAS.....47

INTRODUÇÃO

A Engenharia Social descreve pessoas com conhecimento ambíguo em métodos de ataques, visando à fragilidade de sistemas em empresas de diversos setores abusando da inocência de pessoas que são manipuláveis.

Nos dias atuais ela conta com um enorme poder de persuasão e manipulação conseguindo convencer as pessoas a lhe passar informações para seu benefício próprio. O maior poder do engenheiro social é a mente, para Peixoto eles são um tipo de pessoa considerada agradável a nível encantador a fim de conseguir informações de suas vítimas. Visto isso o autor afirma que:

> Engenharia Social é a ciência que estuda como o conhecimento do comportamento humano pode ser utilizado para induzir uma pessoa 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 (PEIXOTO, 2006, p. 4).

Mitnick e Simon (2003) destacam que a Engenharia Social como uma arte, devido a precisão, percepção e atenção que estimulam o interesse nas pessoas as tornando vulneráveis. Engenheiros sociais têm como ambição o intuito de explorar a natureza daquilo que nos cerca, são curiosos, e essa curiosidade leva a busca por conhecimento, alguns adquirem um conhecimento fora do comum para uma pessoa normal, a diferença entre a curiosidade de um engenheiro social e a de uma pessoa considerada “Normal” é que eles não se limitam às restrições impostas que os impedem de explorar, sua necessidade de exploração é livre.

Salienta o autor que a relação entre Engenharia Social e a Segurança da Informação é mostrar o elo fraco da tecnologia, assim como a mesma veio trazendo diversos benefícios à população ela trouxe desvantagens e se tornou o foco principal de grandes golpes realizados por engenheiros sociais. É recomendável e necessário fazer verificações periódicas dos sistemas de Segurança da Informação para identificar ameaças.

O ambiente corporativo é bastante competitivo, além da precaução contra empresas concorrentes, é necessário também precaução contra pessoas de má-fé que pode se aproveitar das vulnerabilidades da empresa. Devido a isso, atenção às ameaças de negócio é imprescindível, pois pode chegar a encerrar a atividade de alguma empresa para sempre (LEAL, 2001).

A segurança tecnológica nas empresas pode contar com as melhores ferramentas de proteção e ainda assim estará vulnerável. A maior vulnerabilidade dentro das empresas são as pessoas, pois por falta de atenção e descuido mesmo que de maneira involuntária pode tornar o funcionário conivente com um crime de roubo de informação, sem saber que foi usado pelo real criminoso (DAWEL, 2005).

Diante da realidade atual em que vivemos, destaca-se a importância do conhecimento da Engenharia Social para proteger as informações corporativas, as políticas de Segurança da Informação devem ser reforçadas nas organizações a fim de evitar fraudes e ataques internamente.

O escopo deste trabalho visa estudar qual o nível de conhecimento da Engenharia Social nas organizações, e entender se os funcionários realmente têm conhecimento das políticas de Segurança da Informação e se fazem o uso correto dela.

Portanto, o problema de pesquisa do presente Trabalha de Conclusão de Curso propõe o questionamento:

Os colaboradores de uma empresa multinacional estão preparados para manusear, proteger e disponibilizar a informação?

Como justificativa para o tema e para o problema de pesquisa, considera-se o contexto explicado como força motriz, a fim de averiguar os quão preparados estão funcionários de uma multinacional no ramo de tintas e revestimentos, no que diz respeito a lidar com Segurança da Informação relacionada a Engenharia Social e seus malefícios para troca e preservação seguras das informações confidenciais das quais trabalham todos os dias.

Como objetivo geral do trabalho, pretende-se conduzir uma pesquisa de campo, distribuída para funcionários de uma empresa multinacional que abrange funcionários de setores e departamentos diferentes com perguntas variadas acerca do problema de pesquisa.

Já os objetivos específicos da pesquisa se referem ao levantamento bibliográfico sobre Engenharia Social, buscando compreender as práticas mais utilizadas para ataques em seguida conceituar Segurança da Informação com foco organização e os principais métodos de proteção virtual ou física e por meio da pesquisa direta aos funcionários, estabelecer um paralelo entre o fator humano e à Segurança da Informação dentro das organizações visando melhoria de processos e incentivo a treinamentos.

Em termos metodológicos, pretende-se utilizar como instrumento de coleta de dados uma pesquisa anônima realizada com funcionários de uma empresa no ramo de tintas e revestimentos.

O Capítulo I terá como objetivo definir o tema Engenharia Social, perfil do Engenheiro Social, características das vítimas de Engenharia Social, técnicas e meios de ataques, por ser a base conceitual deste trabalho.

O Capítulo II irá discutir a Segurança da Informação e as Políticas de Segurança, pilares, métodos de Segurança da Informação e vulnerabilidades.

O Capítulo III irá abordar o fator humano na Segurança da Informação e como seu comportamento individual e coletivo pode gerar o furto ou o roubo de informações corporativas.

O Capítulo IV irá discorrer sobre o estudo de caso realizado, por meio de questionários divulgados via E-mail interno, via ferramenta Survey Monkey, captando 100 colaboradores atuantes de diversos departamentos dentro de uma multinacional.

E, por último, será apresentada a conclusão do trabalho, verificando o questionamento proposto no problema de pesquisa e estabelecendo um correspondente entre Segurança da Informação e o Fator Humano.

CAPÍTULO I - ENGENHARIA SOCIAL

A Engenharia Social explora a vulnerabilidade do fator humano a fim de aplicar golpes em função de seu benefício próprio. Dentre as habilidades dos engenheiros sociais, destacam-se a influência e persuasão sobre as pessoas, o engenheiro social conquista a confiança da sua vítima, fazendo com que a mesma se sinta confortável e seguro para passar informações das quais irão agregar no golpe de Engenharia Social.

O engenheiro social mostra como somos vulneráveis a ataques, somos aptos a novos tipos de tecnologia, mas não nos atentamos aos danos e riscos que vem junto com o avanço da tecnologia, pois na atualidade nos falta conscientização sobre Segurança da Informação. Portanto, Mitnick e Simon relatam que:

> Nessa era de conscientização sobre a segurança, gastamos somas imensas em tecnologia para proteger nossas redes de computadores e nossos dados. Este livro mostra como é fácil enganar quem trabalha nessas áreas e burlar toda essa proteção tecnológica (MITNICK; SIMON 2003, p. 11).

Mitnick (2011) reforça ainda que um dos pontos mais importantes da Segurança da Informação é mantê-la dentro de seus três pilares, confidencialidade, integridade e disponibilidade, entretanto nem sempre é possível manter sua integridade já que a Engenharia Social explora toda e qualquer vulnerabilidade que possa existir no meio corporativo, pois mesmo que o indivíduo contrate o melhor sistema de segurança e desfrute de uma tecnologia excepcional de segurança em sua organização, a informação ainda continua extremamente vulnerável considerando o fato de que as pessoas são mais fáceis de hackear do que computadores.

De acordo com Rodrigues (2017), em artigo publicado no Portal Micreiros, sob o título “O que é Engenharia Social?”, é possível classifica-la como uma maneira de facilitar as atividades visadas pelos hackers, um dos meios mais utilizados para coletar informações empresariais é verificando e analisando o lixo da empresa, onde pode-se coletar cadastros pessoais de funcionais, senhas anotadas em pedaços de papéis, relatório financeiro e dados sigilosos da empresa.

Outro ambiente favorável para se coletar informações relacionadas a organização, é analisar e invadir as redes sociais dos funcionários o que pode também facilitar no momento em que o engenheiro social estiver planejando seu

golpe. Conforme descrito por Bannwart em artigo publicado no portal Canal Tech, sob o título “Engenharia Social nas Redes Sociais: a inteligência usada para o mal”

> A Engenharia Social continua sendo um fator importante para viabilizar as atividades dos hackers. Eles usam a Engenharia Social para manipular usuários inocentes para obter acesso a informações corporativas sensíveis, como documentos internos, demonstrações financeiras, números de cartão de crédito e credenciais de usuário, ou simplesmente para bloquear serviços com ataques de negação de serviço (DoS). Essa guerra moderna de ameaças e ataques avançados veio para ficar (BANNWART, 2013).

1.1 Engenharia Social nas organizações

A informação é um ativo cada vez mais valorizado nas empresas, pois o desenvolvimento, conceitos e novas descobertas fazem parte do seu ciclo de crescimento. O compartilhamento de informações empresariais internos e externos passou a ser mais utilizados nas empresas para facilitar os processos empresariais. Diante disso, do crescimento tecnológico nas empresas, os primeiros golpes de Engenharia Social foram aplicados, visando mostrar o quão vulnerável é o fator humano das organizações. Sêmola informa que:

> Realizando uma análise análoga ao corpo humano, é possível extrair um valioso aprendizado a fim ratificar o cenário atual vivido pelas empresas diante do aumento exponencial da dependência da informação (SÊMOLA, 2003, p. 5).

Os ataques de Engenharia Social nas organizações se concentram na exploração das falhas humanas ao invés de falhas em sistemas internos. Golpes de Engenharia Social podem ser considerados um ataque à Segurança da Informação nas organizações, mesmo desfrutando de um sistema de segurança automatizado a maior vulnerabilidade não pode ser contida com sistemas automatizados de segurança por se tratar da vulnerabilidade humana. Os engenheiros sociais deixaram de lado as explorações de sistemas de informáticas ou equipamentos automatizados, nos dias atuais é muito mais fácil utilizar pessoas para realizar o trabalho sujo do engenheiro social. Diante disso:

> O fator humano revela não apenas quem está clicando em quê, mas como os agentes de ameaças estão usando Engenharia Social para levar as pessoas a realizar o trabalho de explorações automatizadas.
> Porque, como os dados deixam claro, o elo mais fraco da segurança é todos nós (PROOFPOINT, 2017, p. 1).

O fator humano pode ser considerado a maior vulnerabilidade dentro das organizações afinal como garantir que os funcionários em geral sabem classificar

quando as informações são inofensivas ou valiosas ou como garantir que um funcionário demitido não seja um risco para informação da empresa. (Peixoto, 2006).

O autor explica que além dos meios de segurança automatizados, os funcionários precisam ter conhecimento das boas práticas de Segurança da Informação. Esses cuidados devem ser tomados pelas empresas a fim de evitar ataques voluntários às informações, visto que na atualidade os engenheiros sociais utilizam se da sua arte em trapacear para obter dados sigilosos de uma organização por meio de um funcionário.

Mitnick e Simon informam em seu testemunho que conseguia senhas para acessos e outras informações sigilosas nas empresas simplesmente pedindo para um funcionário após conquistar a confiança da vítima consequentemente “Quebrar o *"firewall humana"* quase sempre são fáceis, não exige nenhum investimento além do custo de uma ligação telefônica e envolve um risco mínimo” (MITNICK; SIMON, 2003, p. 23).

1.2 Perfil do Engenheiro Social

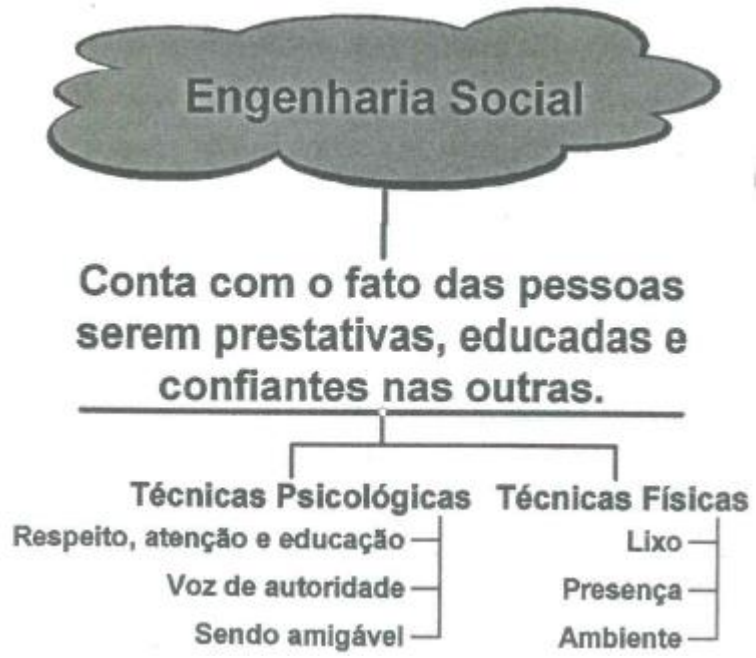
O engenheiro social trabalha com técnicas estratégicas para conseguir informação de suas vítimas, uma técnica comum que caracteriza a Engenharia Social é a abordagem pessoal onde por meio de persuasão e personalidade convincente é possível fazer com que a vítima peça ajuda para seu próprio atacante sem conhecimento de suas intenções subliminares (PEIXOTO, 2006).

O engenheiro social é hábil, e utiliza a arte de enganar e a arte de invadir como metodologia para realizar ataques. Sendo assim o engenheiro social pode ser classificado como:

> (...) Uma pessoa curiosa e extremamente detalhista em suas ações. O mesmo é capaz de estudar sua possível vítima por meses, procurando detalhes mínimos e brechas que podem levar a conseguir a informação necessária. Bibliotecas, livros, notícia de jornal e artigos de revista são inicialmente sua forma de coletar dados. Traçar a trajetória de seu alvo, até conseguir um ponto do qual possa penetrar no mundo social ou empresarial do mesmo, é o objetivo inicial do engenheiro (PEREIRA, 2005, p. 7).

Pereira (2005) ainda reforça que os engenheiros sociais são extremamente astuciosos, pois são calculistas em seus golpes visto que ao realizar um ataque, ele sabe exatamente quais perguntas fazer para sua vítima e como fazer essas perguntas. O engenheiro social primeiramente conquista sua vítima, por meio de perguntas cautelosas visto que perguntas *“*agressivas*”* possa repelir a vítima.

Figura 1 - Segurança da Informação nas empresas George Dawel.



Fonte: Dawel, 2005, p. 78

1.2.1 Hackers e Crackers

Hackers são classificados como pessoas em busca de autoconhecimento, são inteligentes e possuem domínio de determinado conteúdo podendo ser relacionados a software ou não. O termo Hackers infelizmente passou a caracterizar boas e más ações realizadas pelos indivíduos que possuem expertise no domínio e com o intuito de não serem generalizados pelos maus hackers, eles caracterizaram pessoas esses tipos de pessoas como Crackers. Hackers podem se destacar pelas três características descritas abaixo:

> Hollinger estudou os crimes informáticos dentro da comunidade universitária e classificou os Hackers, conforme seu nível técnico, em piratas (pirates) navegadores (Browsers) e crackers. Os piratas, menos desenvolvidos tecnicamente, limitam-se a violações de direitos autorais sobre software. Os navegadores, com conhecimentos técnicos médios, possuem habilidades para invadir sistemas, mas não causam danos ás vítimas nem copiam seus programas. Os Crackers, segundo ele, são aqueles de maior conhecimento técnico e responsáveis pelos abusos mais sérios, causando danos ao sistema (VIANNA, 1986, p. 4).

1.3 Meios De Ataques

Peixoto (2006) classifica as principais ferramentas utilizadas pelo engenheiro social sendo elas, telefone onde os praticantes de Engenharia Social podem se passar por alguém que não é em uma chamada telefônica. Dentro de uma organização ele pode ligar tentando se passar por um cliente. Internet sendo o modo mais fácil de conseguir informações das vítimas, visto que as pessoas tendem a expor suas informações pessoais na internet via redes sociais. Além das redes sociais engenheiros sociais se aproveitam também de sites que fornecem Id e Passwords Default, google, registro.br para coleta de informações. Pessoalmente se tratando de um tipo de ataque mais raro, para chegar a uma abordagem pessoal o engenheiro social tem que estar muito confiante em relação as suas habilidades e conhecer a vítima a ponto de saber até que ponto ela irá lhe fornecer informações. Chats que são ataques similares ao ataque telefônico visto que é uma plataforma onde o engenheiro social pode se passar por outra pessoa, enviar fotos *fake* a fim de se tornar mais atrativo para vítima. E por fim, podemos classificar como o método menos utilizado, o envio de cartas e correspondência que apesar de ser obsoleto pode ser utilizado para enviar para vítima uma carta com logomarca solicitando informações confidenciais.

O engenheiro social conta com diversas outras ferramentas que contemplam sua inteligência, intimidação, credibilidade e sedução na hora de desenrolar uma conversa, sendo ela virtual ou pessoal.

1.4 Técnicas De Ataque

As técnicas dos praticantes de Engenharia Social estão em constante evolução, cada golpe praticado despertando ainda mais a curiosidade do engenheiro social em explorar as vulnerabilidades do ser humano. Suas técnicas consistem em perguntas cuidadosamente formuladas, fazer com que as pessoas façam coisas que normalmente não fariam para um estranho e obter informações de suas vítimas via truques com telefonia. “Quando você combina uma inclinação para enganar as pessoas com os talentos da influência e persuasão, você chega ao perfil de um engenheiro social” (MITNICK; SIMON, 2003, p. 16).

Quando se obtém a arte e a proficiência para enganação você se torna um engenheiro social, considerado também como uma artista da trapaça.

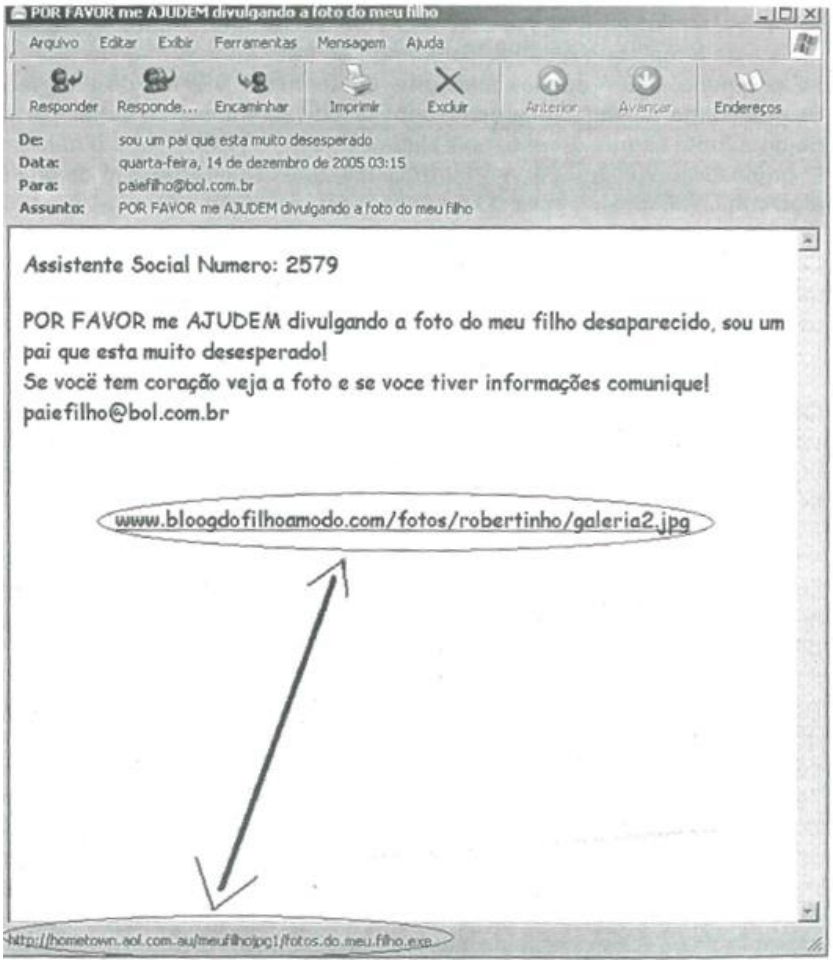
> O hacker convence alguém a entrar no escritório e ligar aquele computador um adversário que quer as suas informações pode obtê-las, em geral, usando uma de várias maneiras. Tudo é uma questão de tempo, paciência, personalidade e persistência. É nesse ponto que entra a arte da fraude (MITNICK; SIMON, 2003, p. 29).

1.4.1 Phishing

Uma das técnicas mais utilizadas pelo engenheiro social é o método *Phishing*, usado para transportar mensagens fraudulentas às vítimas. É o tipo de técnica que engana os usuários com o intuito de conseguir divulgar logins e informações confidenciais involuntariamente. (The Human Factor, 2016). Os engenheiros sociais utilizam como ferramenta para prática de *phishing* uma página de login falso, o link desta página é encaminhado para vítima via e-mail ou Web pages, ao usuário acessar esse link falso, se inicia o ataque.

O Brasil é líder global em ataques de *phishing*, diz Kaspersky, de acordo com a empresa de cybersegurança aproximadamente 28% dos usuários foram vítimas de incidentes envolvendo a técnica de *phishing* (ESTADÃO, 2017).

Figura 2 – Ataque via *Pishing*



Fonte: Peixoto, 2006. p. 13.

1.4.2 Smishing

O *smishing* é considerado uma ferramenta de ataque similar ao *phishing*, mas seu meio de ataque é via mensagens curtas de textos (SMS) ou mensagens de texto enviadas para celulares e smartphones.

Dois processos principais determinam os golpes aplicados via *Smishing*, um envolve uma mensagem de texto recebida de uma fonte desconhecidas, como operadoras e bancos. Outro método é o recebimento de uma mensagem falsa, informando que suas informações (Bancárias normalmente) foram roubadas, em seguida encaminham para vítima um site ou número para validar as informações da conta (CIS JOURNAL, 2009-2014).

1.4.3 Vishing

Vishing é a prática que utiliza mensagens de voz baseadas em IP (Voice over Internet Protocol ou VoIP) para projetar socialmente a vítima a fornecer informações

financeiras, pessoais para fins de recompensa própria do atacante. O *Vishing* é uma combinação de voz que capitaliza a confiança da vítima por serem caracterizadas por um serviço telefônico normalmente utilizado por organizações bancárias, operadoras e outras (CIS JOURNAL , 2009-2014).

CAPÍTULO II - SEGURANÇA DA INFORMAÇÃO

O mundo moderno conta com uma infinidade de dados e informação. Atualmente a informação está em tudo, em função disto Dantas afirma que:

> A boa informação abre verdadeiras oportunidades para quem a possui, o que torna o cenário dos negócios mais dinâmico e acirrado em busca de novos mercados, acordos internacionais, poder e qualidade, dentre outros, o que gera a competitividade e transforma a informação no principal elemento motriz desse ambiente altamente competitivo, que requer, assim, proteção especial (DANTAS, 2011, p.11).

Acrescenta Dantas ainda que determinados conceitos de Segurança da Informação estão ligados a atividades para o negócio, onde cada uma delas se entrelaça com a outra por meio dos componentes da Segurança da Informação, entrada, processamento e saída.

As definições disponíveis quando falamos de informação são diversas, visto que segundo Ferreira (1996, p. 944), o conhecido dicionário da língua portuguesa,

apresenta informação como “ato ou efeito de informar (se); informe; dados a respeito de alguém; conhecimento, participação; instrução.”. Definir informação é um desafio.

As inovações tecnológicas necessitam de uma Segurança da Informação bem estruturada para garantir que durante as transições de dados a informação permaneça íntegra e preservada para utilidade do usuário que a recebe. A transição de dados da informação consiste na entrada da informação, processamento da informação e saída da informação que é quando ela chega ao seu destino ou usuário final (REZENDE; ABREU, 2013).

Companhias em geral, são influenciadas pelas novidades tecnológicas que surgem no mercado de trabalho para melhorar a capacidade e produtividade na empresa. As empresas contam com uma dependência da informação, sejam elas informações compartilhadas, distribuída ou digitalizada.

Dentre as características da informação três delas são fundamentais de acordo com Dantas (2011), sendo elas confidencialidade, integridade e disponibilidade. Essas características garantem a qualquer tipo de usuário uma informação preservada, pois elas compõem os princípios de Segurança da Informação.

A Segurança da Informação protege a informação de ameaças como fraude, quebra de confidencialidade e *malware*, com o intuito de garantir a continuidade do negócio, de modo a garantir a continuidade do negócio, minimizar o risco para o negócio, maximizar o retorno sobre o investimento e as oportunidades de negócio (NBR ISO/IEC 27002:2005).

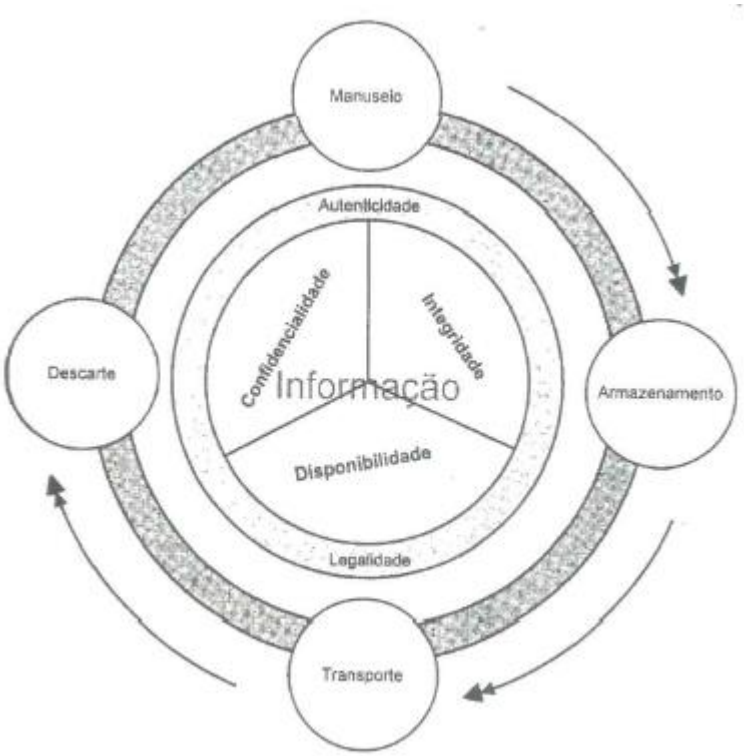
Segundo a NBR ISO/IEC 27002:2005, Segurança da Informação pode ser definido por:

> Preservação da confidencialidade, da integridade e da disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas. (DANTAS, 2011, p.13).

2.1 Pilares Da Segurança da Informação

Nesta seção, desdobraremos a respeito dos três pilares da Segurança da Informação.

Figura 3: Pilares da Segurança da Informação



Fonte: Peixoto, 2006, p. 38.

De acordo com Sêmola (2003), integridade, confidencialidade e disponibilidade trabalham juntas para proteger a informação.

A confidencialidade, por exemplo, se baseia na garantia de que a informação acessada somente por pessoas autorizadas a terem acesso. A quebra de confidencialidade pode acarretar em divulgação indevida da informação, podendo trazer ao usuário perdas financeiras por vazamento de informações. A informação não é mais considerada válida, quando ela é acessada por pessoas não autorizadas.

A respeito da integridade, ela garante que documentos sigilosos não sejam violados. Quando algum documento deve ser enviado, a integridade garante que este documento chegue até a destinatária com exatidão completa e intacta da informação.

No que se refere à disponibilidade, é a garantia de que os usuários autorizados acesso à informação e aos ativos correspondentes sempre que necessário.

Esses conceitos de segurança da informação garantem proteção dos processos organizacionais de Segurança da Informação, pois integram confidencialidade, integridade e disponibilidade possibilitando que as organizações atinjam seus objetivos, garantindo sucesso nos negócios (FONTES, 2006).

Dantas (2006) explica que além de contarmos com o triângulo da Segurança da Informação, há mais oito princípios que as organizações devem adotar para proteger suas informações.

A respeito de legalidade, podemos descrever como a aplicação de conhecimentos e leis para garantir que as informações estejam dentro da legalidade devida nos quais as organizações necessitam estar em conformidade.

A autenticidade identifica a informação, garantindo qualidade das fontes utilizadas para informação, podendo assim identificar com confiança quem está prestando tais informações.

Se tratando de confiabilidade diferente de confidencialidade, é a política que protege a informação e garante que ela não seja uma informação falsa.

Já a conformidade garante que as informações estejam de acordo com os controles, normas e padrões estabelecidos.

Investigação, por exemplo é o mecanismo utilizado para averiguação da informação. Ela deve ser feita por pessoas com conhecimento em T.I, comprometimento e responsabilidade.

Não repúdio é um processo que possibilita a identificação do autor da informação ou mensagem e garante que a informação chegará ao destino correto sem sofrer repúdio.

A respeito da responsabilidade é o que garante que todos os princípios citados acima sejam executados de modo correto.

Esses termos possuem a mesma importância, em certos podemos ver alguns que se destacam, sendo assim Dantas (2006) conclui que:

> Dessa forma, a autenticidade do emissor é a garantia de que quem se apresenta como remetente é realmente quem diz ser. A confiabilidade é a garantia de que a informação está completa e igual à sua forma original quando do envio pelo remetente, e expressa uma verdade. O não repúdio é a garantia de que o emissor ou receptor não tem como alegar que a comunicação não ocorreu, e a responsabilidade diz respeito aos deveres e proibições entre remetente e destinatário (DANTAS, 2006, p. 15).

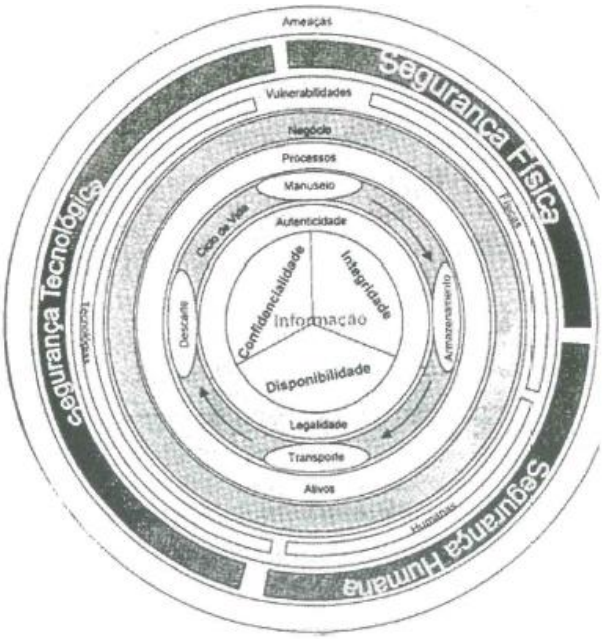
2.2 Métodos de Segurança da Informação

Os métodos de Segurança da Informação conforme mencionado por Fontes (2008) é um conjunto de controles que partem do mesmo princípio de tal informação. Para garantir a segurança é necessário analisar o acesso à informação, como é

classificação a informação, quais tipos de proteções técnicas e recursos de informação, como são desenvolvidos os aplicativos, como garantir a conscientização e treinamento de funcionários, analisar o bom funcionamento do ambiente físico e infraestrutura e analisar os mecanismos de criptografia.

Essas ferramentas de análise, assim como outras, estão relacionadas à proteção de um conjunto de dados para garantir e preservar a informação.

Figura 4: Os polos da Segurança da Informação.



Fonte: Peixoto, 2006, p. 47.

Aplicar os métodos recomendáveis faz parte das boas práticas de Segurança da Informação, pois é um ativo muito importante para qualquer instituição. Garantir que a informação não foi adulterada reflete a responsabilidade das empresas, pessoas de má-fé e concorrentes empresariais podem ir à busca de comprometer informações causando enorme transtorno para Segurança da Informação corporativa, pois caso não seja dado devida importância às medidas de proteção aos dados da informação é possível inviabilizar a continuidade da empresa.

Destaca o autor que uma atenção necessária deve ser dada a Segurança da Informação, cada empresa deve conhecer seus ativos para poder entender o valor de tal ativo e suas vulnerabilidades, o risco de alguém de fora prever uma fraqueza dentro de um ativo da empresa pode causar diversos danos aos negócios. Diante

disto Araújo, Bezerra e Coelho (2014) relatam os problemas mais comuns da Segurança da Informação sendo:

- Destruição de informações e outros recursos.
- Modificação ou deturpação de informações.
- Roubo, remoção ou perda da informação ou de outros recursos.
- Revelação de informações.
- Interrupção de serviços.

As organizações cada vez mais reconhecem o valor e as vulnerabilidades de seus ativos. (ARAÚJO; BEZERRA; COELHO, 2014).

2.3 Políticas de Segurança da Informação

Para evitar a inviabilidade da continuidade da empresa é necessário implantar políticas de Segurança da Informação, uma forma mais culta e padrão de implantar métodos de Segurança da Informação. A aplicação de políticas de S.I deve conter princípios, normas e padrões, sem esses fatores elas não funcionam.

A implementação da política de Segurança da Informação deve ser adaptada para possíveis mudanças, nem sempre uma política é implementada com sucesso, sendo assim ela deve ser reversível, assim caso não seja algo bem-sucedido, ela pode passar por nova elaboração e manutenção para ser reaplicada com a probabilidade de sucesso maior.

Outro ponto a ser relevado é a importância da atualização após ter passado pelas principais etapas, elaboração, aprovação, implementação, divulgação e manutenção. Conforme descrito no livro “Boas Práticas em Segurança da Informação”, publicado pelo Tribunal de Contas da União, em 2012:

> Normalmente, após a consecução das três primeiras etapas (elaboração, aprovação e implementação), as gerências de segurança acreditam terem cumprido o dever e esquecem-se da importância da divulgação e atualização da PSI (TRIBUNAL DE CONTAS DA UNIÃO, 2012, p.12).

As principais fases para aplicação das políticas de Segurança da Informação para se obter bons resultados nas corporações sem risco de sair dos padrões se baseiam na tabela 1.

Tabela 1 – Classificação de resultados positivos

Identificação dos recursos críticos	Aprovação
Classificação das informações	Publicação
Definição, em linhas gerais, dos objetivos de segurança a serem atingidos	Divulgação
Análise das necessidades de segurança (identificação das possíveis ameaças, análise de riscos e impactos)	Treinamento
Elaboração de proposta de política	Implementação
Discussões abertas com os envolvidos	Avaliação e identificação das mudanças necessárias
Apresentação de documento formal à alta administração	Revisão

Fonte: Tribunal de Contas da União, 2012, p. 12-13.

Os princípios são classificados conforme sua importância, a empresas devem dar determinada atenção para que essas políticas de Segurança da Informação não sejam violadas, por isso são determinados métodos que devem ser adotados para evitar violação dos protocolos de políticas de Segurança da Informação, por isso a divulgação é ampla aos diversos usuários para que o processo de Segurança da Informação seja implantado com sucesso, evitando violação da integridade (CARUSO; STEFFEN, 1999)

Quando a política de Segurança da Informação é violada pode haver punições como, advertência verbal ou escrita e em casos mais graves pode chegar a uma ação judicial.

> Conforme citado no livro A Lei n.º 9.983, de 14 de julho de 2000, que altera o Código Penal Brasileiro, já prevê penas para os casos de violação de integridade e quebra de sigilo de sistemas informatizados ou banco de dados da Administração Pública. O novo art. 313-A trata da inserção de dados falsos em sistemas de informação, enquanto o art. 313-B discorre sobre a modificação ou alteração não autorizada desses mesmos sistemas. O 1º do art. 153 do Código 14 Penal foi alterado e, atualmente, define penas quando da divulgação de informações sigilosas ou reservadas, contidas ou não nos bancos de dados da Administração Pública. O fornecimento ou empréstimo de senha que possibilite o acesso de pessoas não autorizadas a sistemas de informações é tratado no inciso I do 1º do art. 325 do Código Penal. (TRIBUNAL DE CONTAS DA UNIÃO, 2012, p.12)

As organizações acreditam que a política de Segurança da Informação não pode ser alterada, e sua alteração pode ser considerada “Crime Virtual”. Porém a mesma pode ser alterada e é até mesmo é recomendada, pois na atualidade a tecnologia avança rapidamente, sendo assim as políticas já implementadas devem ser revisadas de período em período garantindo a reavaliação e visualização do que pode ser alterado sem afetar de maneira negativa a análise de risco original.

2.4 Ameaças e vulnerabilidades corporativas

Profissionais capacitados e um bom sistema de monitoramento fazem grande diferença quando se fala de ameaças à Segurança da Informação pois uma falha técnica ou humana pode trazer grandes problemas as gestões organizacionais.

Os tipos de ameaças e vulnerabilidades variam conforme o ambiente externo e interno da organização e de acordo com o tipo de proteção que as áreas de T.I e infraestrutura oferecem.

Quando se fala de negócios é possível identificar constantes vulnerabilidades e ameaças que podem influenciar na quebra de Segurança da Informação. Com base em Freitas (2009, p. 32) identificar os riscos importa em identificar as ameaças e as vulnerabilidades que podem ser aproveitadas por estas aos sistemas de informação envolvidos e o impacto que as perdas de confidencialidade, integridade e disponibilidade podem causar aos ativos.

Desta maneira Peixoto (2006, p.43) identifica os tipos de ameaças, sendo:

- Ameaças naturais: fenômenos da natureza, como enchentes, tempestades, furacões, etc.
- Ameaças involuntárias: ameaças inconscientes, decorrentes de desconhecimento ou acidentes.
- Ameaças voluntárias: ameaças propositais, causadas por agentes humanos mal-intencionados.

Com base em Freitas (2009) não existe ambiente seguro, com a evolução da tecnologia da informação os níveis de ameaça e fragilidade dos sistemas tende a expandir. As vulnerabilidades são os pontos principais em que o sistema e a infraestrutura se tornam predispostos a ataque.

Desta forma, Peixoto (2006) indica que as vulnerabilidades físicas, naturais, de hardware, software, mídias, comunicação e humanas podem comprometer um

ambiente corporativo. Principalmente a vulnerabilidade humana por meio da qual por falta de treinamento e/ou conscientização, ausência de Políticas de Segurança, dentre outros ataques relacionados a Engenharia Social podem ser facilitados.

CAPÍTULO III - O FATOR HUMANO NA SEGURANÇA DA INFORMAÇÃO

De acordo com os estudos de Mitnick e Simon (2003), a maior vulnerabilidade se origina da natureza humana. Transpassar segurança e confiança pode fazer com que o atacante de Engenharia Social obtenha sucesso ao coletar informações corporativas de funcionários não preparados para proteger a informação.

> Como observou o consultor de segurança Bruce Schneier, "a segurança não é um produto, ela é um processo". Além disso, a segurança não é um problema para a tecnologia — ela é um problema para as pessoas e a

> direção. A medida que os especialistas contribuem para o desenvolvimento contínuo de melhores tecnologias 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, não exige nenhum investimento além do custo de uma ligação telefônica e envolve um risco mínimo (MITNICK; SIMON, 2003, p. 23)

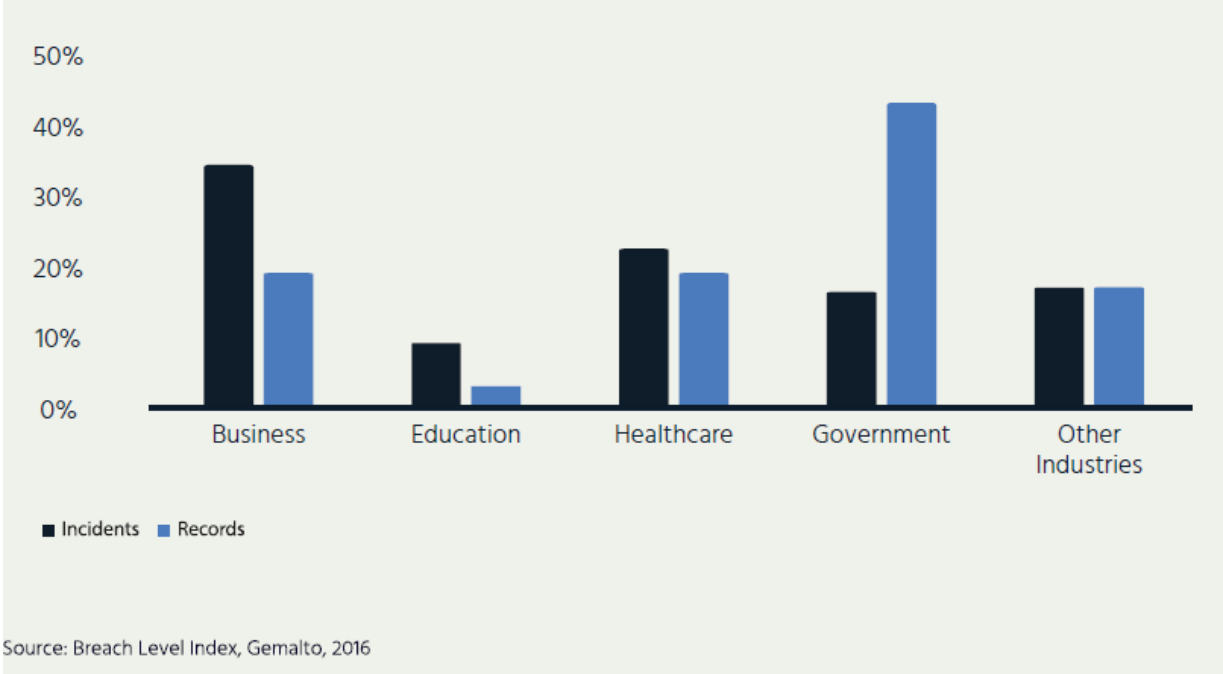
Considerando o contexto corporativo as informações podem ser consideradas um dos principais patrimônios de uma organização tornando a empresa vulnerável visto que a perda ou roubo de informações podem comprometer a sobrevivência da empresa.

O artigo *The Human Factor Report* (2017) e a organização *Internet Society* (2016) concordam que o método mais acessível de se obter acesso a informação é por meio da Engenharia Social.

> Não podemos tomar a Internet como garantia. O caminho para futuro digital está em nossas mãos. Podemos começar hoje adotando ações que preservarão os valores subjacentes da Internet e manterão o caminho para que permaneçam abertos, conectados globalmente e seguros (INTERNET SOCIETY, 2016).

Considerando cenário de negócios, é possível visualizar nos histogramas abaixo pelo gráfico 1 quais foram os alvos de ataques em relação a furto de informações, e no gráfico 2 é possível identificar quais os tipos de informações foram almejados para furto.

Gráfico 1 – Alvos de violação de dados



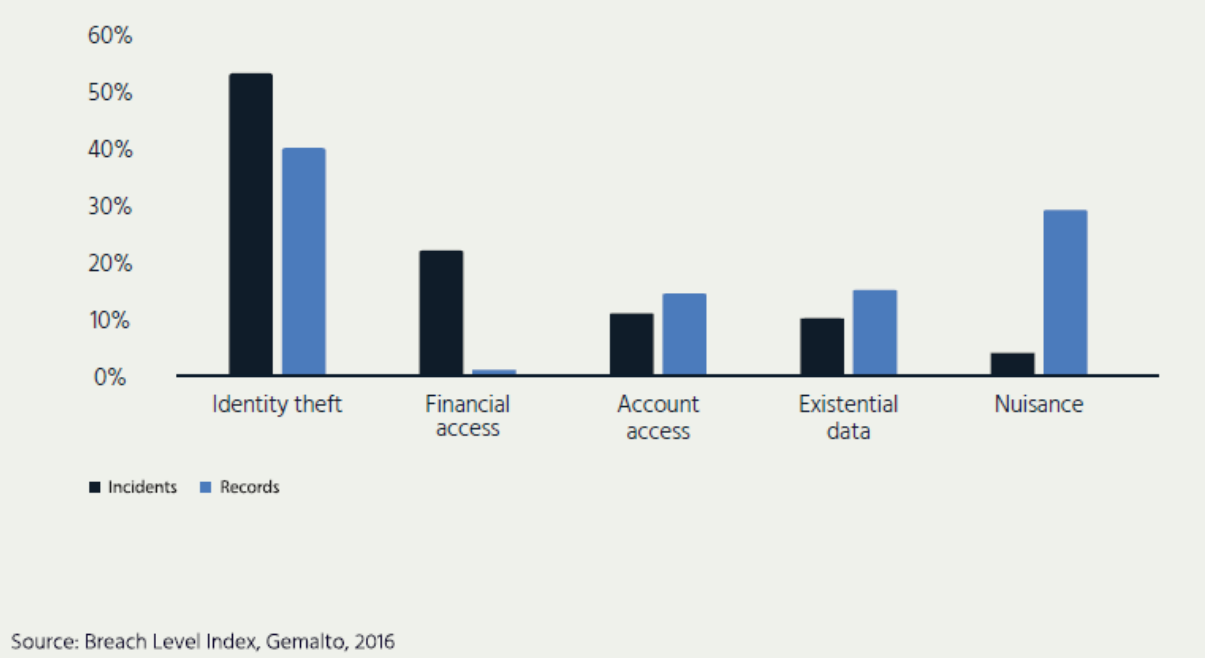
Fonte: Imagem de Breach Level Index; Gemalto, 2016 *Apud* Internet Society, 2016, p. 41

Dentre as informações de áreas atingidas, é possível identificar pelo Gráfico 1 que as áreas de negócio (Bussiness) comprometem de 20% a 40% das eventualidades cibernéticas. As demais áreas que abrange relacionadas mais a fundo no relatório mostra que 13% do setor de varejo identificaram violações em relação a informação e 6% dessas violações foram reportadas. Consecutivamente o setor financeiro sofreu 15% das violações das quais apenas 0,1% de registros. Por outro lado, a tecnologia trouxe 6% das violações dentre 12% de registros (INTERNET SOCIETY, 2016, p. 40).

É possível identificar com base nas informações estatísticas é possível verificar que as empresas costumam negligenciar as violações sofridas internamente afins de não denegrir a imagem da empresa.

Em uma pesquisa mais antiga Mitnick e Simon (2003, p. 5-6) reportam uma preocupação crescente com base em uma pesquisa sobre os crimes de computadores, a pesquisa relata que 85% das organizações entrevistadas detectaram quebras na segurança dos computadores no decorrer dos 12 meses do ano.

Gráfico 2 – Informações almejadas nas violações



Fonte: Imagem adaptada de Breach Level Index; Gemalto, 2016 *Apud* Internet Society, 2016, p. 42

Dentre os tipos de informações furtadas é possível observar através do Gráfico 2 que o furto de identificações (Indentity Theft) se destaca em aproximadamente 53% de incidentes e aproximadamente 40% dos incidentes foram classificados como reportáveis comparando as demais eventualidades cibernéticas. Considerando o acesso financeiro classificado pelo relatório como cartões de créditos e contas bancarias a taxa de incidente é considerada alta levanto em conta que foram identificadas um total de 20% de incidentes e em média 1% apenas, reportado. Referindo se a contas online, serviços de internet que requerem login as estatísticas apontam uma média de 10% de incidentes em conjunto com mais de 12% dos incidentes reportáveis. Nos dados existências que classificam os relatórios de segurança e essências para a sobrevivência do negócio é possível identificar 10% de incidentes em conjunto com uma porcentagem relativamente maior de incidentes reportáveis. E por fim, podemos classificar transtornos virtuais, como mensagem de “Clique aqui”, spam e outras infinidades como *Nuisance*, ou seja, “Dados de perturbação” que relato um baixo número de incidentes, porém um alto número de registros.

3.1 O elo mais fraco da Segurança da Informação

De acordo com o relatório emitido pelo *The human Factor Report* (2018) os engenheiros sociais continuam aumentando seus recursos de ataque com base na interação humana que a cada dia pode se tornar mais explorável, considerando a falta de preparo e treinamento para proteger a informação.

> Eles encontraram novas maneiras de explorar “O fator humano” - os instintos de curiosidade e confiança que levam à bem-intencionada pessoas para clicar, baixar, instalar, mover fundos e mais a cada dia (PROOFPOINT, 2018, p. 17).

É improvável identificar algo que possa erradicar os ataques de Engenharia Social considerando que o fator humano é o elo mais fraco da Segurança da Informação (MITNICK; SIMON, 2003).

As maiores ameaças se concentram nas pessoas e em seus papeis dentro da organização. O engenheiro social gosta de analisar o perfil da vítima antes de aplicar o golpe, considerando principalmente os tipos de informações confidenciais que as vítimas têm acesso. Os ataques relatados pelo *The human Factor Report* (2018) consiste em:

- *Pishing*, considerando os domínios de grandes empresas registrados de maneira suspeita.
- Atualizações falsas de navegador e plug-in atingindo de 95% dos ataques observados via WEB envolvendo kits de exploração, Engenharia Social incorporada para induzir os usuários a instalar *malwares*.
- Cerca de 55% dos ataques nas redes sociais representavam contas de suporte ao cliente - uma tendência conhecida como “phishing de pescador” - clientes-alvo de empresas de serviços financeiros.
- Cerca de 35% dos golpes de mídia social que usaram links e “Clique aqui” que levaram os usuários ao streaming de vídeo e sites de download de filmes. Mineração de moeda no navegador, na qual atacantes sequestram computadores das vítimas para gerar criptomoedas.

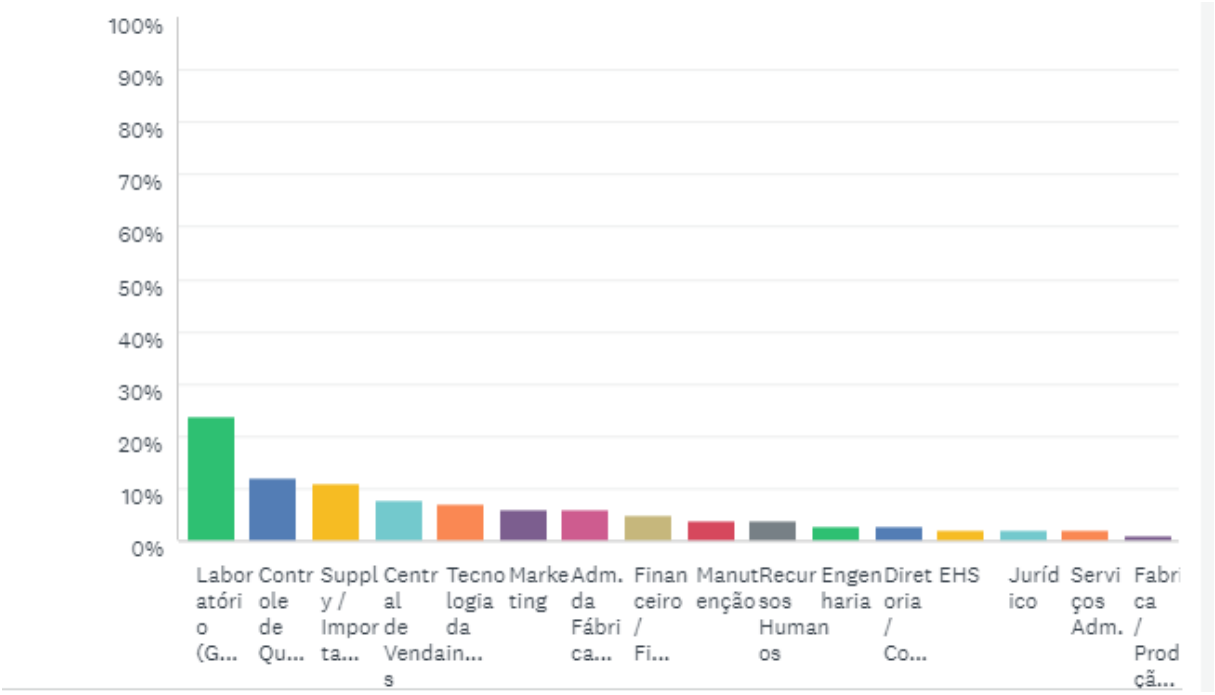
CAPÍTULO IV – ESTUDO DE CASO

No presente capítulo, deve-se analisar acerca do nível de ciência, esperado e desejado, dos funcionários de uma empresa multinacional focada no ramo de pinturas e revestimentos sobre Segurança da Informação e Engenharia Social. A análise que será apresentada foi amparada por uma pesquisa realizada por meio de uma ferramenta online chamada Survey Monkey. A pesquisa buscou coletar dados que serão tratados de forma quantitativa e qualitativa, foi realizada entre os meses de outubro de 2018, e contou com 100 (CEM) respondentes. A pesquisa foi conduzida de forma anônima, de modo a preservar a identidade dos respondentes, sob o intuito de não comprometer de maneira alguma a empresa na qual os respondentes-colaboradores atuam. Foram elaboradas dez perguntas das quais duas destinavam-se para a coleta de respostas abertas (questões 1 e 10):

Abaixo, por razões metodológicas, explicitam-se os conteúdos delas:

1) *Em qual setor/departamento você trabalha?*
2) *Você é funcionário terceirizado? (Temporário, estagiário, menor aprendiz, e etc.)*
3) *Você tem o hábito de usar o crachá de identificação funcional?*
4) *Você **sempre** bloqueia sua máquina (Desktop, Notebook ou Celular corporativo) ao sair da estação de trabalho?*
5) *Você tem acesso a informações confidenciais ou sigilosas (documentos internos; tabelas de custos ou financeiras; fórmulas químicas dos produtos internos; contratos de prestação de serviços; informações técnicas gerais; dados da avaliação técnica de controle de qualidade)? Você pode selecionar mais de uma opção.*
6) *Você já realizou algum treinamento direcionado à questão de Segurança da Informação, no intuito de preservar informações confidenciais e/ou sigilosas?*
7) *Você já foi vítima de crimes virtuais?*
8) *A respeito do uso de e-mail corporativo/institucional, você envia informações:*
9) *Você sabe o que significa a expressão "Engenharia Social"?*
10) *Você conhece as Políticas de Segurança da Informação desta empresa?*

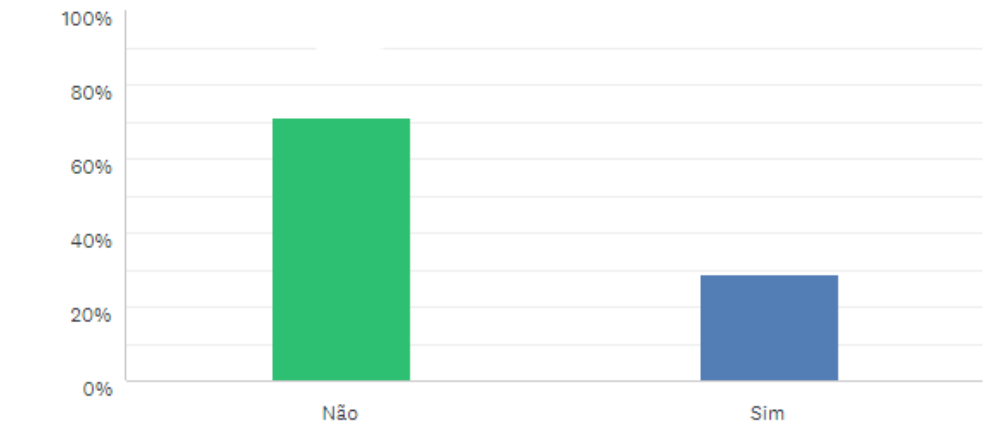
Gráfico 3 – Local de trabalho do grupo de respondentes



Fonte: Autoria própria (2018): Dados da pesquisa

De acordo com o Gráfico 1, cuja questão indagava o local de trabalho dos 100 (cem) respondentes, das 16 possibilidades indicadas por esta pesquisadora, o “Laboratório (Geral) ” ocupou quase ¼ das respostas apresentadas. Os departamentos vinculados ao “Controle de Qualidade (Qualidade) ” e “Supply”, o qual agrega a Importação, Logística, Recebimento e Separação, aparecem na segunda e terceira posições, respectivamente, com 12% e 11% do quadro de servidores respondentes. Quantitativamente, os menores números de respostas obtidas são, respectivamente, dos Setores “Jurídico”, “EHS” e “Serviços Administrativos”, cada qual com 2 respostas, e, por último, o setor vinculado à “Fábrica” (Produção Geral).

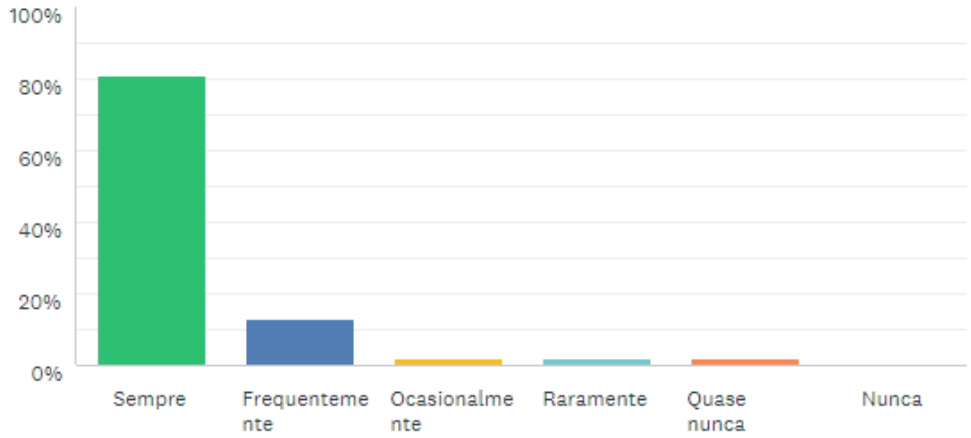
Gráfico 4 – Vínculo empregatício direto ou indireto (terceirizado) do grupo de respondentes



Fonte: Autoria própria (2018): Dados da pesquisa

Conforme os dados estatísticos ilustrados no Gráfico 2, quase ¾ dos colaboradores desta pesquisa são servidores com vínculo empregatício direto com a empresa, ao passo que menos de 30% são funcionários terceirizados, portanto, cujos contratos são indiretos, mediados por agências de emprego atuantes no setor terciário da economia brasileira.

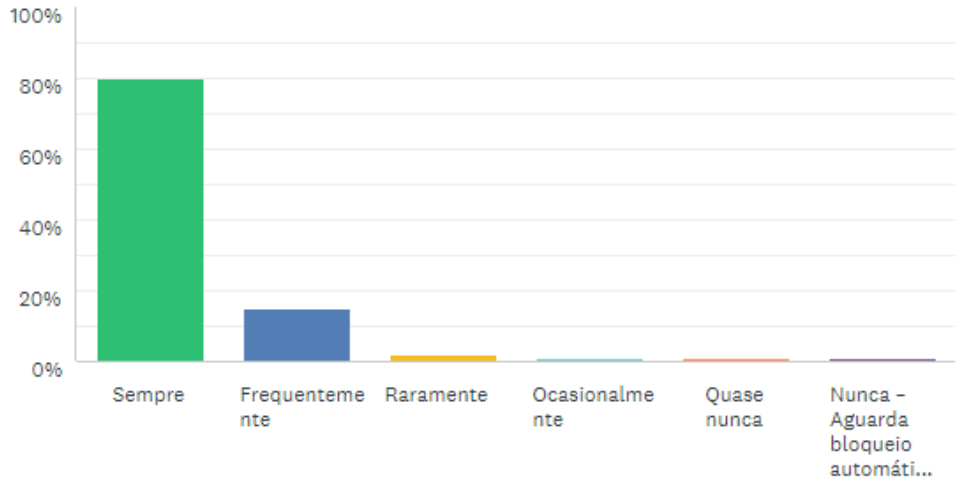
Gráfico 5 – Uso do crachá de identificação funcional



Fonte: Autoria própria (2018): Dados da pesquisa

Os dados colhidos pela pesquisa, elucidados no Gráfico 3, no tocante ao uso do crachá de identificação funcional, revelam que uma expressiva maioria de funcionários o usa sempre (81%). Não obstante, três grupos de respostas, cada qual com 2 (dois) respondentes, nos chamam a atenção, pois relatam que ocasional ou raramente ou quase nunca usam a aludida documentação funcional.

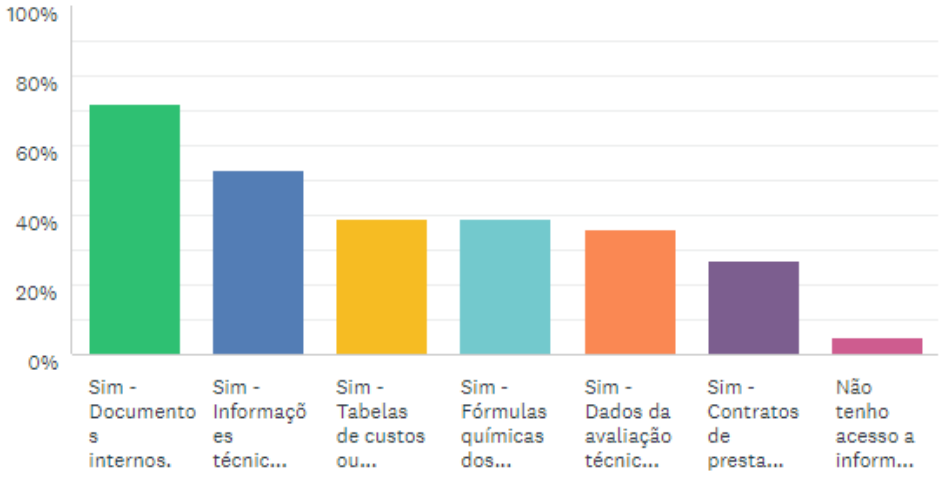
Gráfico 6 – Bloqueio automático bloqueia da máquina (Desktop, Notebook ou Celular corporativo)



Fonte: Autoria própria (2018): Dados da pesquisa

Em consonância as informações apresentadas no gráfico 4 observa que a maior parte dos respondentes, 80% da amostragem, tem o habito de bloquear a máquina (Desktop, Notebook ou Celular corporativo) ao sair da estação de trabalho no entanto cinco grupos de respostas não fazem o bloqueio automático ao sair da estação de trabalho totalizando 20%, sendo 15% bloqueia a estação de trabalho com frequência, 2% raramente bloqueia a estação de trabalho, 1% bloqueia a estação de trabalho ocasionalmente, 1% bloqueia a estação de trabalho quase nunca e por fim 1% nunca bloqueia a estação de trabalho aguardando assim o bloqueio automático.

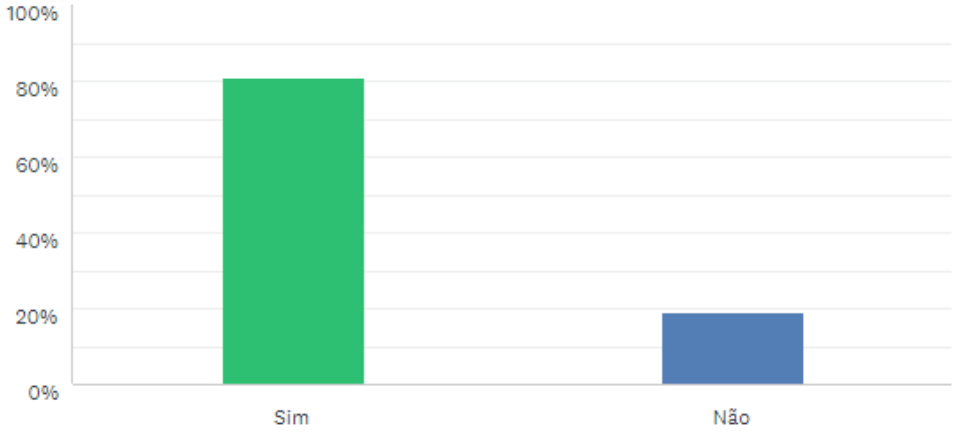
Gráfico 7 – Acesso a informações confidencias



Fonte: Autoria própria (2018): Dados da pesquisa

Conforme os dados estatísticos ilustrados no gráfico 7 apenas 5% não lidam com informações confidenciais da empresa, nos revelando que uma maioria de expressiva de funcionários 95% tem acesso a informações confidenciais da empresa. Seguindo essa linha de raciocínio as próximas perguntas nos direcionam o quão seguro é o ambiente de trabalho.

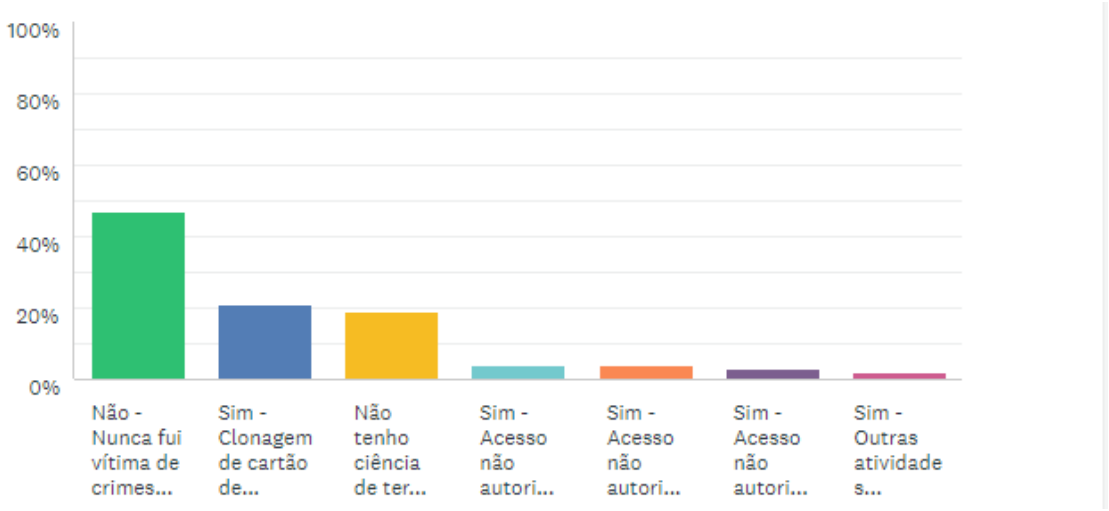
Gráfico 8 – Treinamento interno relacionado à Segurança da Informação



Fonte: Autoria própria (2018): Dados da pesquisa

De acordo com o Gráfico 8, cuja questão indagava o treinamento sobre Segurança da Informação a maioria dos respondentes, 81% indicou já ter realizado treinamento direcionado à Segurança da Informação. Não obstante, temos uma quantidade de 20% dos respondentes que não realizaram nenhum tipo de treinamento voltado a Segurança da Informação os tornando não inaptos na proteção da informação.

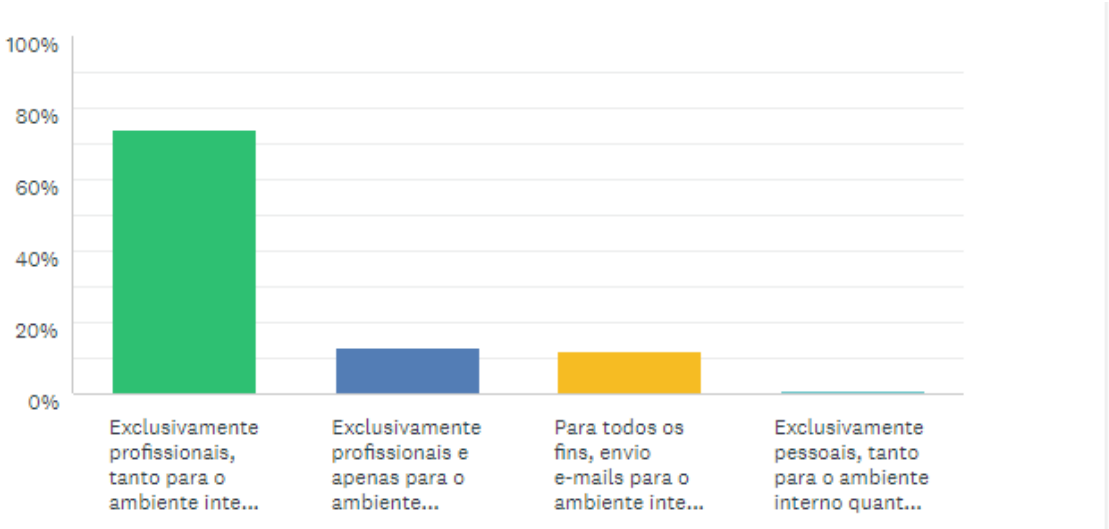
Gráfico 9 – Relação de vítimas de crimes virtuais



Fonte: Autoria própria (2018): Dados da pesquisa

De maneira positiva é possível observar com base no Gráfico 9, que 47% dos respondentes nunca sofreram ataques virtuais. No entanto nos chama atenção que um total de 20% já passou por clonagem de cartão de crédito nos deixando a brecha de que de alguma maneira a informação foi inserida de forma insegura no ambiente virtual. Outro ponto preocupante é que 19% não tiveram a certeza suficiente para selecionar a opção “Não, nunca fui vítima de crimes virtuais”, o que revela que as potenciais vítimas não têm absoluta certeza se sofreram ou não ataques virtuais.

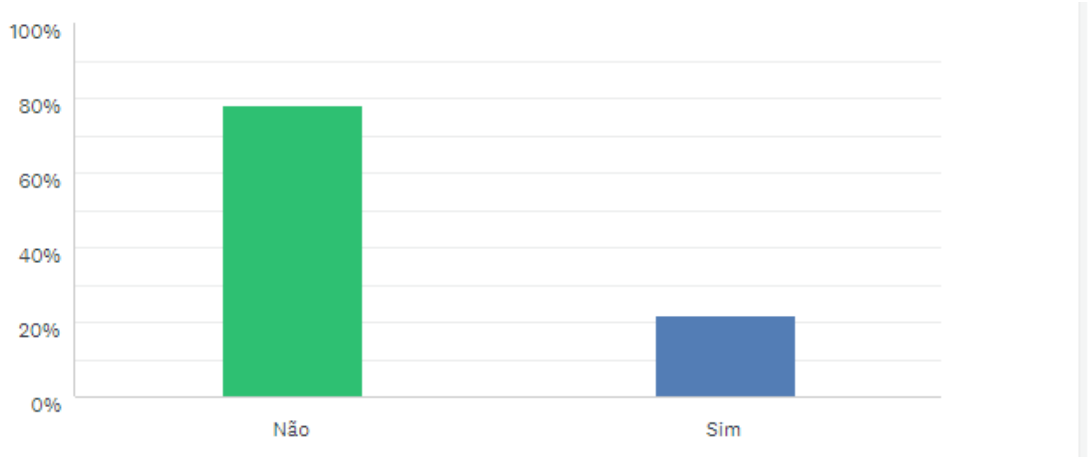
Gráfico 10 – O uso do *e-mail* corporativo



Fonte: Autoria própria (2018): Dados da pesquisa

No Gráfico 10, um total de, aproximadamente, ¾ (74%) dos respondentes informaram que utilizam o *e-mail* corporativo apenas para fins profissionais considerando o ambiente interno e externo, enquanto um total de 13% confirma que a utilização do *e-mail* é somente direcionado ao ambiente interno, para fins profissionais. Em seguida temos o relato de 12% dos respondentes que utilizam o *e-mail* corporativo para fins profissionais, pessoais tanto para o ambiente externo quanto para ao ambiente externo, e, por fim, o que nos chama a atenção é que 1% dos respondentes informa que utiliza o *e-mail* corporativo apenas para fins pessoais, tanto nos ambientes externos e internos.

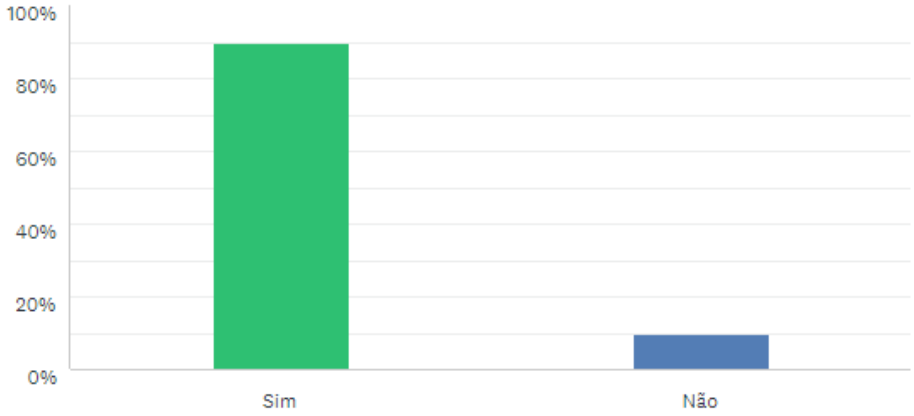
Gráfico 11 – Conhecimento em “Engenharia Social”



Fonte: Autoria própria (2018): Dados da pesquisa

Em consonância as informações apresentadas no Gráfico 11, 78% dos entrevistados indicaram não ter conhecimento sobre o tema aludido, enquanto apenas 22% dos colaboradores conhecem sobre Engenharia Social.

Gráfico 12 – Conhecimento sobre as Políticas de Segurança da Informação



Fonte: Autoria própria (2018): Dados da pesquisa

Diferentemente dos dados obtidos anteriormente, podemos ver, por meio do Gráfico 12, que 90% dos colaboradores afirmaram ter conhecimento das políticas de Segurança da Informação da empresa. No entanto nos chama a atenção que 10% dos respondentes afirmaram desconhecer as políticas de Segurança da Informação da empresa.

4.1 Análises do Estudo de Caso

Com base nos dados apresentados, é possível constatar que o manuseio de informações confidenciais e informações individuais fazem parte da rotina dos colaboradores de uma empresa multinacional considerando de de 100%, apenas 5% não tem acesso a nenhum tipo de informação confidencial.

O maior grupo de respondentes atua dentro dos laboratórios da multinacional de tintas e revestimentos. Vale ressaltar que são funcionários com acessos as formulas, custos, matérias primas, procedimentos de qualidade e outras informações o vazamento de alguma dessas informações pode gerar prejuízo a empresa, se considerarmos o fato de que eles não estejam totalmente preparados e treinados para proteger a informação.

Outro ponto preocupante durante a análise é que dois funcionários informar “Raramente” utilizar o crachá de identificação e dois funcionários “Quase Nunca” utilizar o crachá de identificação. O crachá de identificação da empresa multinacional do acesso físico a própria empresa, a prédios administrativos, a fábrica, aos diversos laboratórios sejam eles de formulação de tinta e até mesmo laboratórios de qualidade. São basicamente quatro pessoas, que por descuido do funcionário podem invadir a empresa colocando em risco os negócios.

Outro aspecto importante para endossar o presente raciocínio é que 78% dos funcionários não conhecem a expressão “Engenharia Social”? O que nos preocupa considerando que de 100% por exemplo, 19% nunca realizou algum treinamento direcionado as questões de Segurança da Informação, 10% não tem conhecimento das políticas de Segurança da Informação, 20% não bloqueia sempre sua máquina (Desktop, Notebook ou Celular corporativo) ao sair da estação de trabalho.

Em relação à pesquisa como um todo, podemos considera-la positiva visto que 80% sempre utiliza o crachá de identificação, 80% sempre bloqueia o desktop ou aparelho celular corporativo, 81% já realizou treinamento direcionado a Segurança da Informação e 90% tem conhecimento das políticas de segurança da informação da empresa, no entanto são os pequenos números que nos preocupam e qual seria o impacto negativo sobre a empresa que esse possível despreparo do funcionário pode causar.

CONCLUSÃO

De acordo com as considerações deste trabalho, é nítido observar que a mentalização a respeito de Segurança da Informação e integridade de dados é um tema que vem ganhando importância entre usuários da rede. As corporações possuem a consciência de que não existe um sistema de Segurança da Informação infalível, mas com treinamento e conscientização é possível erradicar as falhas e vulnerabilidades o máximo possível.

Em uma corporação onde a maioria dos funcionários faz o manuseio de informações confidenciais é necessário educa-los e conscientiza-los sobre o valor da informação e qual seria o impacto caso fosse furtada ou violada. Com um treinamento elaborado e uma segurança da informação eficaz é possível diminuir os impactos negativos causados pela engenharia social e eliminar consideravelmente a brecha em relação a segurança da informação, o Fator Humano.

É importante, também, sempre educar e conscientizar os funcionários, visto que muitos desconhecem o valor da informação que manuseiam todos os dias. Com uma metodologia de segurança eficaz, elaborada para atender às necessidades específicas de cada setor do negócio, acessível a todos e constantemente revisada e informada, o Fator Humano é capaz de diminuir consideravelmente a brecha ainda aberta na Segurança da Informação.

Por conta das limitações desta atual contribuição e a profundidade e complexibilidade da temática, bem como a limitada amostra de colaboradores espera se que novas abordagens sejam investigadas em futuras pesquisas relacionadas a análise de como as empresas e universidades brasileiras se portam quando se trata do assunto, Segurança da Informação, por se tratar de um assunto altamente pertinente ao cenário atual.

REFERÊNCIAS

ABREU, Aline França de; REZENDE, Denis Alcides. **Tecnologia da Informação:** aplicada a Sistemas de Informação empresariais. São Paulo: Atlas, 2013

ARAÚJO, L. G. S; BEZERRA, E. K; COELHO, F. E. S. **Gestão da Segurança da Informação**. Rio de Janeiro: RNP/ESR, 2014. p. 19-24

BANNWART, Claudio. **Engenharia Social nas Redes Sociais:** a inteligência usada para o mal, 2013. Disponível em: <https://canaltech.com.br/seguranca/Engenharia-Social-nas-Redes-Sociais/ >. Acesso em: 15 nov. 2018, às 15h31min

TRIBUNAL DE CONTAS DA UNIÃO**. Boas Práticas em Segurança da Informação**, 2012. Disponível em: <http://www4.planalto.gov.br/cgd/assuntos /publicacoes/2511466.pdf>. Acesso em: 10 nov. 2018, às 17h31min

FREITAS, Eduardo Antônio Mello. **Gestão de Riscos Aplicada a Sistemas de Informação:** Segurança Estratégica da Informação. Brasília: Biblioteca Digital Câmara, 2009. p. 32-33

CARUSO, Carlos A. A.; STEFFEN, Flavio Deny. **Segurança em Informática e de Informações.** São Paulo: Senac, 1999. p. 49-50; 57-58

DAWEL, George. **A segurança da informação nas empresas:** ampliando horizontes além da tecnologia. Rio de Janeiro: Ciência Moderna, 2005.

ESTADÃO, 2017. Brasil é líder global em ataques de phishing, diz Kaspersky. *In.:* **Exame**, 2017. Disponível em: <https://exame.abril.com.br/tecnologia/brasil-e-lider-global-em-ataques-de-phishing-diz-kaspersky/>. Acesso em: 12 nov. 2018, às 13h31min.

FERREIRA, Aurélio Buarque de Holanda. **Novo Aurélio Século XXI**: o dicionário da língua portuguesa, 3. ed. (CD-ROM). Petrópolis: Nova Fronteira, 1999

FONTES, Edison. **Segurança Da Informação:** o usuário faz a diferença. São Paulo: Saraiva, 2006, p. 11-12

_____. **Praticando a Segurança da Informação:** Orientações e Práticas alinhadas com as normas. Rio de Janeiro: Brasport, 2008. p. 45-48

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: 10 nov. 2018, às 21h15min.

LEAL, Marcos Dantas. **Segurança da Informação:** uma abordagem focada em gestão de riscos. Olinda: Livro Rápido, 2011, p. 11–20

MARCELO, Antonio; PEREIRA Marcos. **A Arte de hackear pessoas**. Rio de Janeiro: Brasport Livros e Multimídia LTDA, 2005. p. 7. Disponível em: <https://books.google.com.br/books?hl=ptBR&lr=&id=yBVNt5Ei6ikC&oi=fnd&pg=PA1&dq=perfil+do+engenheiro+social+Seguran%C3%A7a+da+informa%C3%A7%C3%A3o&ots=Lw6dNMfZF&sig=jwgS0JNuh9CDe9nxymeb1hx7CuQ#v=onepage&q&f=false>.

MITNICK, K. SIMON, W. **A Arte de Enganar:** Ataques de Hackers Controlando o Fator Humano na Segurança da Informação. São Paulo: Pearson Brasil. 2003. p.3-24; p.85; p.195-205

PEIXOTO, M. **Engenharia social e segurança da informação na gestão corporativa.** Rio de Janeiro: Brasport, Brasil. 2006. p.3-49

PROFPOINT The Human Factor Report, 2017: How today's threats prey on the human report factor. Disponível em: <https://www.proofpoint.com/sites/default/files/Pfpt-en-uk-human-factor-report-2017.pdf>.

RODRIGUES, Heber. **O que é engenharia social?** *In.:* **Micreiros**, 2017. Disponível em: <http://micreiros.com/o-que-e-engenharia-social/>. Acesso em: 10 nov. 2018, às 13h26min.

VIANNA, Túlio Lima. **Hackers:** Um estudo criminológico da subcultura c*yberpunk*. BuscaLegis, 1986. Disponível em: <http://www.egov.ufsc.br/portal/sites/default/files/anexos/29401-29419-1-PB.pdf>. Acesso em: 10 nov.2018, às 14h02min.