UNIVERSIDADE FEDERAL DE SANTA CATARINA
CAMPUS ARARANGUÁ
CURSO DE TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO

JEISON ESTEVAM COSTA

ENGENHARIA SOCIAL E SEGURANÇA DA INFORMAÇÃO NO AMBIENTE CORPORATIVO: UM ESTUDO DE CASO EM UMA COOPERATIVA DE CRÉDITO LOCALIZADA NO SUL DE SANTA CATARINA

ARARANGUÁ
2018

JEISON ESTEVAM COSTA

ENGENHARIA SOCIAL E SEGURANÇA DA INFORMAÇÃO NO AMBIENTE CORPORATIVO: UM ESTUDO DE CASO EM UMA COOPERATIVA DE CRÉDITO LOCALIZADA NO SUL DE SANTA CATARINA

Trabalho de Conclusão do Curso de Graduação em Tecnologias da Informação e Comunicação do Campus Araranguá da Universidade Federal de Santa Catarina como requisito para a obtenção do Título de Bacharel em Tecnologias da Informação e Comunicação.
Orientador: Prof. Dr. Paulo César Leite Esteves

ARARANGUÁ

2018

Ficha de identificação da obra elaborada pelo autor,
através do Programa de Geração Automática da Biblioteca Universitária da UFSC.

Costa, Jeison Estevam
ENGENHARIA SOCIAL E SEGURANÇA DA INFORMAÇÃO NO AMBIENTE CORPORATIVO : UM ESTUDO DE CASO EM UMA COOPERATIVA DE CRÉDITO LOCALIZADA NO SUL DE SANTA CATARINA / Jeison Estevam Costa ; orientador, Paulo César Leite Esteves, 2018.
73 p.

Trabalho de Conclusão de Curso (graduação) - Universidade Federal de Santa Catarina, Campus Araranguá, Graduação em Tecnologias da Informação e Comunicação, Araranguá, 2018.

Inclui referências.

1. Tecnologias da Informação e Comunicação. I. Esteves, Paulo César Leite. II. Universidade Federal de Santa Catarina. Graduação em Tecnologias da Informação e Comunicação. III. Título.

Jeison Estevam Costa

ENGENHARIA SOCIAL E SEGURANÇA DA INFORMAÇÃO NO AMBIENTE CORPORATIVO: UM ESTUDO DE CASO EM UMA COOPERATIVA DE CRÉDITO LOCALIZADA NO SUL DE SANTA CATARINA

Este Trabalho de Conclusão de Curso foi julgado adequado para obtenção do Título de "Bacharel em Tecnologias da Informação e Comunicação" e aprovado em sua forma final pelo Curso de Graduação em Tecnologias da Informação e Comunicação.

Araranguá/SC, 15 de junho de 2018.

Prof.ª Patricia Jantsch Fiuza, Drª.
Coordenadora do Curso/Universidade Federal de Santa Catarina

Banca Examinadora:

Prof. Paulo César Leite Esteves, Dr.
Orientador/Universidade Federal de Santa Catarina

Prof.ª Eliane Pozzebon, Drª.
Examinadora/Universidade Federal de Santa Catarina

Profª. Andréa Cristina Trierweiller, Drª.
Examinadora/Universidade Federal de Santa Catarina

Dedico esta pesquisa à Letícia, que me dá apoio e incentivo nas horas necessárias.

AGRADECIMENTOS

Agradeço, primeiramente, a Jesus, por ter permitido trilhar essa jornada com sabedoria e dedicação, me dando forças para superar cada dificuldade.

Aos meus pais, Leonir e Neuci que me concederam o dom da vida.

A Cooperativa, que possibilitou a realização da pesquisa com seus colaboradores.

A todos os profissionais que passaram pela minha formação acadêmica ao longo desses anos, também contribuindo para minha formação pessoal.

E ao professor Paulo César Leite Esteves pela sua dedicação e orientação durante o período de elaboração do trabalho.

“A melhor maneira de ficar em segurança é nunca se sentir seguro."
Benjamin Franklin

RESUMO

A presente pesquisa refere-se a um estudo de Segurança da Informação com ênfase no conceito de Engenharia Social, tendo o objetivo de analisar as atitudes dos colaboradores de uma Cooperativa de Crédito localizada no Sul de Santa Catarina em relação às práticas de Engenharia Social que podem afetar a manutenção da Segurança da Informação da entidade. Quanto à metodologia, a pesquisa caracteriza-se como qualitativa, descritiva, sendo desenvolvida por meio de um estudo de caso. A coleta de dados foi realizada por meio de questionário e do teste de *phishing*. Os resultados obtidos revelaram que grande parte dos colaboradores mantém comportamento adequado para a manutenção da Segurança da Informação e de golpes provenientes de Engenharia Social, entretanto, uma parcela significativa ainda não segue rigorosamente as normas de Segurança da Informação. É fundamental que as organizações conscientizem todos seus colaboradores a respeito das consequências que a divulgação indevida de dados pode acarretar à sua política interna de Segurança de Informação, para a redução dos índices de fraudes e golpes.

Palavras-chave: Segurança da Informação. Engenharia Social. Cooperativa de Crédito.

ABSTRACT

The present research refers to an Information Security study with emphasis on the concept of Social Engineering, with the objective of analyzing the attitudes of the employees of a Credit Cooperative located in the South of Santa Catarina in relation to the Social Engineering practices that can affect the maintenance of the entity's Information Security. Regarding the methodology, the research is characterized as qualitative, descriptive, being developed through a case study. The data collection was performed through a questionnaire and the phishing test. The results showed that most of the employees maintain adequate behavior for the maintenance of Information Security and Scams from Social Engineering, however, a significant portion still does not strictly follow the Information Security norms. It is fundamental that organizations make all their employees aware of the consequences that undue disclosure of data may entail to their internal information security policy, in order to reduce the rates of frauds and blows.

Keywords: Information Security. Social Engineering. Credit Cooperative.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE GRÁFICOS

LISTA DE ABREVIATURAS E SIGLAS

ID – Identificador

TI – Tecnologia da Informação

TIC’s – Tecnologias da Informação e Comunicação

VPN – *Virtual Private Network*

SUMÁRIO

1 INTRODUÇÃO

As tecnologias da informação e comunicação estão presentes no ambiente corporativo como ferramenta imprescindível para o desenvolvimento das organizações em suas mais diversas áreas. Ao mesmo tempo em que novas tecnologias se inserem no mercado, a fim de facilitar a gestão dos negócios, há o aumento da competitividade e, para tanto é fundamental inserir ou adequar os recursos tecnológicos já existentes para se manter em boa posição no mercado.

Na década de 60, foram criados os primeiros sistemas de computadores, que tiveram como função auxiliar na administração de dados corporativos, ocupando o lugar dos procedimentos manuais que existiam até aquele momento (DIAS, 2000).

A partir dessa época, o mundo da informática passou por muitos avanços tecnológicos. Cada vez mais, os computadores aumentam seus recursos de *hardware* e *software*, a *internet* passa a ser mais rápida e acessível. Até mesmo os usuários leigos passam a construir suas próprias aplicações devido ao grande número de ferramentas de *software* disponíveis (DIAS, 2000).

Da mesma forma em que o acesso aos meios digitais se tornou mais fácil, houve o aumento da complexidade para armazenar informações importantes e confidenciais, visto que indivíduos mal intencionados, os quais estão entre a vasta gama de usuários beneficiados com a evolução tecnológica, estudam e criam métodos de manipulação para roubo de informações sigilosas. Estas, por sua vez, caso sejam roubadas ou perdidas, podem ocasionar danos irreversíveis para uma organização.

A preservação da informação é vital para a entidade que a possui, uma vez que é através dela que se tem a possibilidade de gerir os processos existentes no meio corporativo. Deste modo, pode-se dizer que, sem informação, não se obtém resultados.

Por conta da enorme facilidade de atribuir valor a produtos e serviços, as tecnologias propiciam caminhos que resultam na conquista dos objetivos organizacionais. Sendo um ativo de enorme valor, as informações essenciais para o negócio precisam ser protegidas contra as ameaças que podem pôr em risco sua adulteração, divulgação não autorizada e destruição (BEAL, 2008).

São inúmeros os mecanismos para mantê-la sob confidencialidade: antivírus, *firewalls*, *intranet*, sistemas de autenticação, *token*, entre outros. Obviamente, que essas tecnologias têm papel importante para manter os dados em segurança. Contudo, ainda não é o suficiente para garantir a confidencialidade dos dados. Um ponto extremamente relevante e

que não pode ser negligenciado na segurança da informação, é a forma de se proteger de ataques provenientes de engenharia social. Pessoas mal intencionadas e *Hackers*, também conhecidas como engenheiros sociais, trabalham para aplicar seus golpes aproveitando-se da ignorância ou ingenuidade dos usuários, com o propósito de coletar dados confidenciais que podem afetar à segurança da organização (BEAL, 2008).

Conforme Mitnick e Simon (2003) não importa quanto seja feito de investimentos na área de tecnologias da segurança da informação e, treinamentos de pessoal para garantir a confidencialidade de seus dados, bem como, os colaboradores seguirem as melhores recomendações para práticas de segurança e instalação de programas que, ainda assim, a organização estará vulnerável.

Sendo assim, cabe salientar que diversas são as organizações que em algum momento se tornam vítimas de aplicações de golpes elaborados por engenheiros sociais. Dentre elas, as cooperativas de crédito, objeto dessa pesquisa, tendem a ser alvos comuns, em decorrência de sua atividade operacional estar relacionada a grandes movimentações financeiras, chamando a atenção desses indivíduos, os quais analisam e identificam oportunidades para a aplicação de golpes.

Diante deste contexto, tem-se a seguinte questão de pesquisa: Quais atitudes dos colaboradores de uma Cooperativa de Crédito localizada no Sul de Santa Catarina em relação às práticas de engenharia social que podem afetar a manutenção da segurança da informação da entidade?

1.1 OBJETIVOS

Neste tópico serão apresentados os objetivos geral e específicos.

1.1.1 Objetivo geral

O objetivo geral deste estudo é analisar as atitudes dos colaboradores de uma Cooperativa de Crédito localizada no Sul de Santa Catarina em relação às práticas de engenharia social que podem afetar a manutenção da segurança da informação da entidade.

1.1.2 Objetivos específicos

Por meio dos objetivos específicos, será definido o caminho para chegar ao objetivo geral:

- Apresentar os elementos que integram a segurança da informação no ambiente corporativo;
- Expor as características da engenharia social aplicada às organizações;
- Demonstrar a importância de administrar a segurança da informação para redução de fraudes e golpes;
- Identificar os pontos negativos e positivos das atitudes dos colaboradores com relação a proteção da informação e prevenção de golpes de engenharia social.

1.2 JUSTIFICATIVA

No atual cenário global envolvido pelas Tecnologias da Informação e Comunicação (TIC’s), se destaca o aumento da importância que as informações possuem para os negócios. Cada vez mais, as informações são armazenadas em componentes tecnológicos diversos, os quais necessitam que o usuário tenha prudência quanto ao seu manuseio. Por conta disso, é indispensável que sejam elaborados e aplicados métodos para prevenção de fraudes e erros, pois estão diretamente relacionados com a continuidade operacional das organizações.

Muitos indivíduos mal intencionados, visando ganhos monetários, ou somente prejudicar uma instituição, podem desenvolver armadilhas para obtenção de dados sigilosos e posterior aplicação em golpes. Uma organização precisa estar sempre atenta, desenvolvendo métodos e realizando treinamentos de seu pessoal, a fim de alertá-los sobre as consequências de seus atos, que por muitas vezes involuntários, podem trazer prejuízos significativos a ela (MITNICK; SIMON, 2003).

Os engenheiros sociais atacam de diversas formas, sendo mais comuns os métodos virtuais. Em nível global, um estudo do *Norton Cyber Security Insights* no ano de 2016 apontou um crescimento na quantidade de ataques cibernéticos de 10% em relação ao que haviam constatado no ano de 2015. No Brasil, cerca de 42,4 milhões de pessoas foram vítimas, resultando em um prejuízo estimado em 10,3 bilhões de dólares (NORTON CYBER SECURITY INSIGHTS, 2016).

O estudo ainda apontou que as pessoas estão a par dos riscos reais, entretanto, ainda são negligentes quanto a segurança de dados armazenados nos dispositivos, permitindo que invasões de *hackers* por meio de *phishing* sejam realizadas com sucesso e, consequentemente, ocasionando perdas monetárias (NORTON CYBER SECURITY INSIGHTS, 2016).

Diversos setores econômicos estão suscetíveis a ataques, entretanto, o setor de serviços financeiros é um dos maiores alvos. De acordo com a pesquisa da Accenture em parceria com o Ponemon Institute, há um custo elevado para controlar e evitar ataques virtuais, principalmente para o setor financeiro, que fica em primeiro lugar nesse quesito. De 2015 a 2017, o custo do setor obteve um crescimento de 40%, resultando em um valor aproximado de 18,28 milhões de dólares no ano de 2017. Ademais, houve o triplo da quantia de incidentes considerando o período de 2012 para 2017 (40 para 125), quantia significativa quando comparada à média global de 130 ocorrências para todos os setores (PORTAL IPNEWS, 2018).

Ainda conforme a pesquisa, 87% das consequências advindas dos ataques em instituições financeiras são representadas pela suspensão das atividades operacionais e perda de informações de valores inestimáveis e, 13% pela perda de receita (PORTAL IPNEWS, 2018).

Diante do exposto, a presente pesquisa visa a identificação de possíveis falhas humanas e falta de conhecimento dos colaboradores quanto ao manuseio de informações da instituição financeira em estudo, para contribuir com o bom andamento das atividades e evitar perdas relevantes. Também servirá de fonte de consulta para demais pesquisadores ou interessados no tema, destacando sua contribuição empírica. Além disso, poderá ser verificada a aplicabilidade e replicação dessa pesquisa para outras instituições financeiras, contribuindo de um modo geral para a prevenção de golpes e redução dos índices de ataque.

1.3 ESTRUTURA DO ESTUDO

Após a seção introdutória, este estudo está organizado de acordo com as seguintes etapas: fundamentação teórica; procedimentos metodológicos; apresentação e análise dos resultados; e considerações finais. A fundamentação teórica engloba a revisão da literatura com estudos teóricos e empíricos acerca da segurança da informação e da engenharia social. O foco é analisar se as atitudes humanas dos colaboradores de uma Cooperativa de Crédito, em relação às práticas de engenharia social estão prejudicando a manutenção da segurança da

informação. Em seguida, apresenta-se os procedimentos metodológicos com o enquadramento metodológico e procedimentos de coleta e análise de dados. Posteriormente, são discutidos os resultados e, finalmente, são apresentadas as considerações finais, limitações do trabalho e sugestões para pesquisas futuras.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 INFORMAÇÃO

Antes de definir o que é informação, precisa-se compreender uma característica fundamental da mesma: os dados.

Os dados podem ser caracterizados como elementos brutos, os quais, se observados isoladamente, não são capazes de gerar compreensão de determinado fato e, para tanto devem ser estruturados para tornarem-se informação útil (BAZZOTTI; GARCIA, 2006).

Dessa forma, pode-se definir informação como:

> Conjunto de dados utilizados para a transferência de uma mensagem entre indivíduos e/ou máquinas em processos comunicativos (isto é, baseados em troca de mensagens) ou transacionais (isto é, processos em que sejam realizadas operações que envolvam, por exemplo, a transferência de valores monetários) SÊMOLA (2003, p. 45).

No ambiente corporativo, em especial, a informação pode ser compreendida como um ativo de valor, um recurso essencial utilizado para a manutenção das atividades operacionais e alcance da missão das organizações (FONTES, 2006).

A informação é um ativo primordial para os negócios de uma organização e precisa ser devidamente preservada. Por conta do grande aumento da interconectividade, a informação está nos dias de hoje exposta a uma grande variedade de ameaças e vulnerabilidades (ABNT NBR ISO/IEC 17799, 2005).

Filho (2009), cita que a informação é compreendida por qualquer conteúdo possível de ser armazenado ou repassado de alguma maneira, o qual tenha utilidade e possua uma aplicação relevante para os indivíduos, no âmbito pessoal ou organizacional.

Cabe salientar que em diversas situações, os usuários da informação, por não terem o conhecimento adequado sobre o seu valor, podem comprometer uma instituição ou, até mesmo, seu profissionalismo ao se deparar com um engenheiro social (FILHO, 2009).

2.1.1 Ativos da informação

Qualquer componente associado a organização, que possua valor para o negócio, e que obrigatoriamente precise de proteção é considerado um ativo da informação (BEAL, 2008).

Sendo assim, considera-se ativo toda a informação que não pode ser perdida, os meios em que é armazenada, bem como, todos os equipamentos que são utilizados para seu manuseio, transporte e descarte (SÊMOLA, 2003).

2.2 SEGURANÇA DA INFORMAÇÃO NAS ORGANIZAÇÕES

Pode-se definir a Segurança da Informação como sendo um conjunto de práticas voltadas à proteção dos ativos da informação, administrando ameaças internas e externas que possam ocasionar em danos significativos, afetando os princípios da segurança: confidencialidade, integridade e disponibilidade (SÊMOLA, 2003).

De acordo com Caruso e Steffen (1999, p. 24) a "segurança, mais que estrutura hierárquica, homens e equipamentos, envolve uma postura gerencial, o que ultrapassa a tradicional abordagem da maioria das empresas".

Sêmola (2003), afirma que o termo Segurança da Informação pode gerar interpretações ambíguas. Primeiramente, pode ser interpretada como um conjunto de métodos e aplicações adotados para estabelecer um ambiente seguro e garantir a sequência dos negócios nos eventuais incidentes que possam ocorrer. Em segunda interpretação, pode ser considerada como um resultado dos procedimentos aplicados, um objetivo que planeja-se alcançar.

É imprescindível que ao utilizar essa expressão se tenha a percepção deste duplo sentido, com o propósito de identificar qual o conceito mais aplicável, sendo eles, de acordo com Sêmola (2003, p. 44):

> **Segurança como "meio"** – A segurança da informação visa garantir a confidencialidade, integridade e disponibilidade da informação, a impossibilidade de que agentes participantes em transações ou na comunicação repudiem a autoria de suas mensagens, a conformidade com a legislação vigente e a continuidade dos negócios.
> **Segurança como "fim"** – A segurança da informação é alcançada por meio de práticas e políticas voltadas a uma adequada padronização operacional e gerencial dos ativos, e processos que manipulam e executem informação.

O termo Segurança da Informação também pode ser utilizado para fazer referência às medidas de proteção das informações mantidas em elementos tecnológicos contra as ameaças a que estas se expõem (BEAL, 2008).

2.2.1 Princípios básicos da segurança da informação

Visando a preservação dos ativos de informação, tem-se três princípios básicos da Segurança da Informação: confidencialidade, integridade e disponibilidade (SÊMOLA, 2003).

O primeiro princípio é o da confidencialidade, o qual estabelece que o acesso à informação seja limitado apenas a quem se destine (SÊMOLA, 2003; BEAL, 2008).

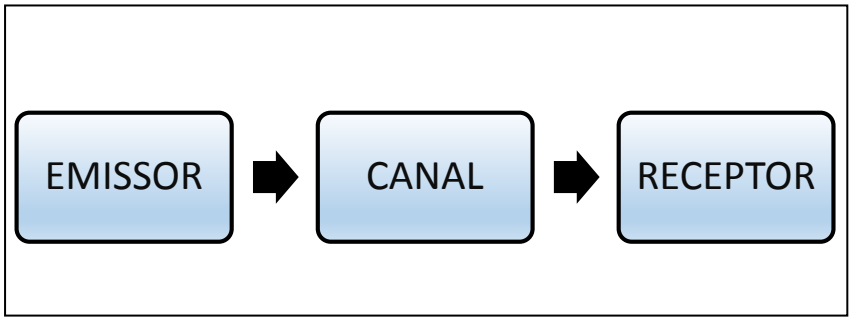
O segundo princípio é o da integridade, que tem como finalidade garantir que a informação possa ser mantida de forma legítima, sem inconsistências, prevenindo-a contra possíveis modificações não autorizadas (criação, alteração e destruição) (BEAL, 2008).

O terceiro e último princípio é o da disponibilidade, que tem como propósito definir que toda informação deve estar acessível aos usuários legais, de maneira tempestiva (SÊMOLA, 2003).

Além destes princípios básicos de segurança da informação, é necessário adotar alguns cuidados adicionais a respeito da segurança, quando esta precisa ser transmitida por meio do processo de comunicação (BEAL, 2008).

O processo de comunicação pode ser observado na Figura 1.

Figura 1 - Processo de transmissão da informação



Fonte: Beal (2008, p. 2)

Como é possível analisar através da Figura 1, a comunicação é transmitida quando um emissor encaminha uma mensagem (incluindo uma ou várias informações) a um receptor, se utilizando de um canal que funciona como uma conexão e proporciona a transmissão da referida mensagem (BEAL, 2008).

Beal (2008) em sua obra, também destacou que o processo de proteger a segurança da comunicação deve possuir alguns objetivos, conforme descritos no Quadro 1.

Quadro 1 - Preservação da Segurança da Comunicação

Integridade do conteúdo	A mensagem que foi enviada pelo emissor, tem a garantia de que o receptor irá recebê-la de maneira completa.
Irretratabilidade da comunicação	Não há como o emissor e receptor alegar que uma comunicação de êxito não tenha ocorrido.
Autenticidade do emissor e receptor	Assegurar de que quem se mostre como remetente ou destinatário da informação, seja realmente quem deva ser.
Confidencialidade do conteúdo	A disponibilidade quanto ao conteúdo da mensagem somente pode ser concedida ao seu(s) destinatário(s).
Capacidade de recuperação do conteúdo pelo receptor	Certificar que o conteúdo transmitido na comunicação pode ser recuperado na forma original pelo destinatário.

Fonte: Adaptado de Beal (2008).

De acordo com o disposto no Quadro 1 e, em conformidade com Dantas (2011), ressalta-se que existem muitos aspectos da segurança. A confidencialidade é a raiz do controle de segurança do sistema de informação. A disponibilidade e integridade de seus dados, bem como, suas funcionalidades, estão envolvidas para fortalecer a segurança de um sistema. Em vista disso, a organização deve definir documentos em níveis adequados e, onde os dados devem ser armazenados, quem pode acessar os dados e, como ele pode ser protegido. Com essas informações, é possível ter uma visão precisa das suas exposições e então aproveitar esse conhecimento para criar um ambiente mais seguro.

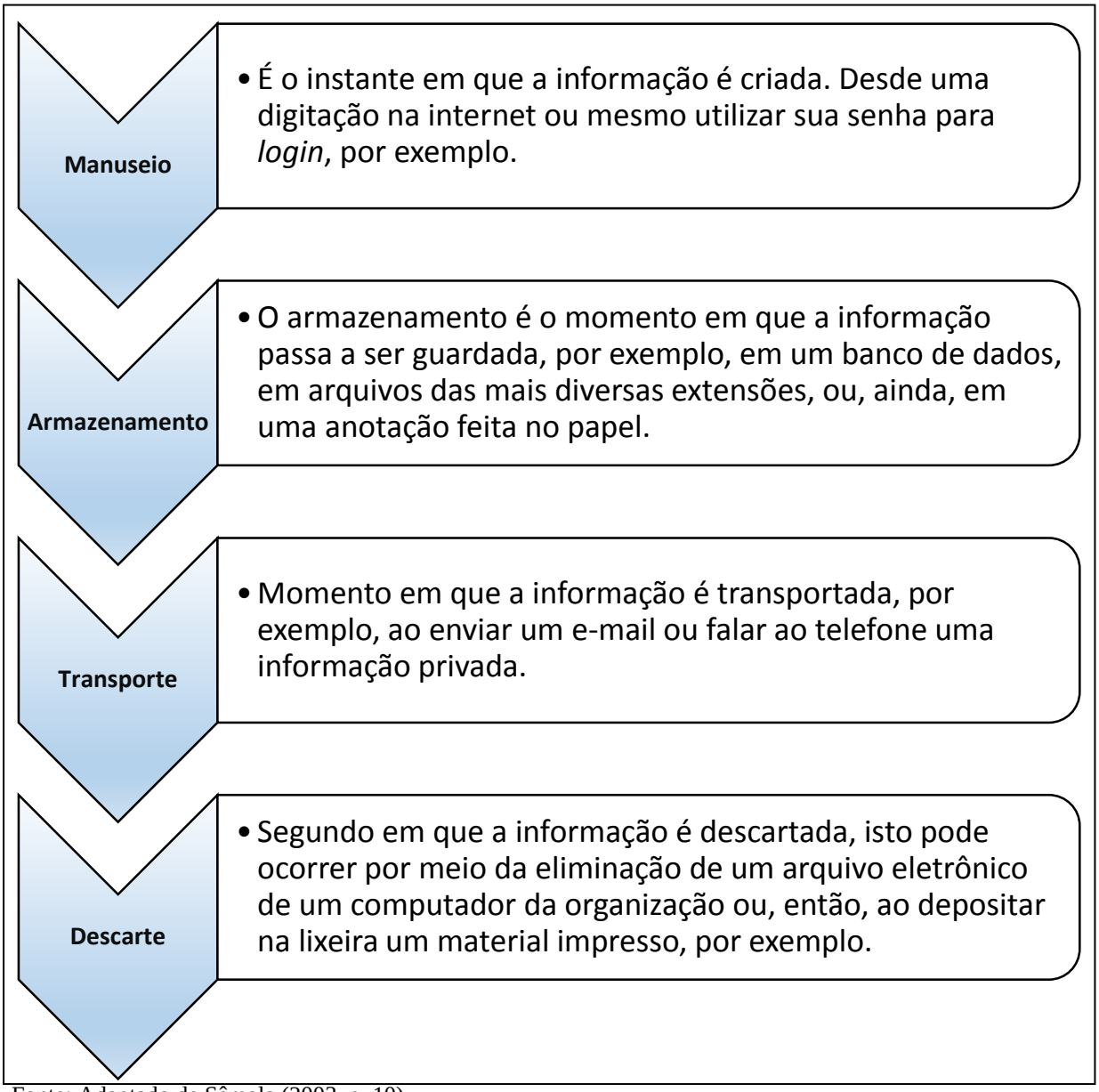
2.2.2 Ciclo de vida da informação

Constituem e identificam o ciclo de vida da informação, todos os momentos vividos por ela que a colocam em risco. Os ativos físicos, tecnológicos e humanos utilizam dos recursos de informação, mantendo assim, processos que sustentam a operação da organização (SÊMOLA, 2003).

O ciclo de vida da informação começa pelo seu manuseio, em seguida o armazenamento, transporte e por fim o descarte. O valor e os riscos com relação aos ativos, podem oscilar durante o período de vida da informação. Como por exemplo, caso uma informação privada seja exposta de maneira não autorizada, no que diz respeito ao seu valor, não será tão grande como era anteriormente (ABNT NBR ISO/IEC 27002, 2013).

Com o intuito de detalhar as situações em que a informação é exposta às ameaças que atingem suas particularidades comprometendo a sua segurança, Sêmola (2003) apresenta as 4 etapas do ciclo de vida da informação, ilustrada na Figura 2.

Figura 2 - Ciclo de Vida da Informação



Fonte: Adaptado de Sêmola (2003, p. 10).

2.2.3 Ameaças e vulnerabilidades no ambiente corporativo

Muitas vezes os indivíduos podem se sentir ameaçados, entretanto, isso não significa, necessariamente, que estão vulneráveis. Já em uma situação oposta, quando um indivíduo se sente vulnerável, certamente, também está se sentindo sob ameaça (PEIXOTO, 2006).

Na perspectiva de Peixoto (2006), todas as ameaças são consequência das vulnerabilidades existentes, provando assim, que houve a perda dos princípios de confidencialidade, integridade e disponibilidade que são necessários para existir a segurança da informação. Há três formas de classificação dessas ameaças: naturais, que englobam acontecimentos da natureza, como enchentes, terremotos e tempestades; involuntárias, que são ameaças ocasionadas, muitas vezes, por conta da falta de conhecimento e, geralmente, causadas por erros, acidentes ou falta de energia; e voluntárias, que abrangem as ameaças propositais que tendem a estar associadas com a Engenharia Social, sendo provocadas por agentes humanos, *hackers,* ladrões, entre outros.

Não importa quais medidas de segurança a empresa adote para a proteção da informação, as ameaças perduram no ambiente interno e externo, fazendo-se necessário compreendê-las para que seja possível criar medidas de segurança tendo como objetivo eliminar a causa do problema (GABBAY, 2003).

As vulnerabilidades, nada mais são do que ameaças propagadas e que ganharam força, comprometendo a segurança das informações (PEIXOTO, 2006).

Para Sêmola (2003), apenas as vulnerabilidades não causam incidentes, devido ao fato de serem elementos passivos, o que necessita para tal, de um pretexto ou situação favorável, que são as ameaças.

Na ótica de Peixoto (2006), as vulnerabilidades estão exemplificadas da seguinte maneira no meio corporativo:

- **Físicas:** Mal planejamento quanto a salas de CPD, não cumprimento dos padrões com relação a estrutura de segurança;
- **Naturais:** Os computadores são propensos a sofrerem danos naturais, como incêndios, poeira e falta de energia;
- ***Hardware*:** Com o decorrer do tempo, o *hardware* pode vir a apresentar falhas em virtude do seu desgaste ou má utilização;
- ***Software*:** Vazamento de informações e má instalação ou configuração;

- **Mídias:** Mídias de armazenamento como fitas, discos e DVDs, podem sofrer danos ou simplesmente, acabarem-se perdidas;
- **Comunicação:** Ausência de comunicação ou acessos não autorizados;
- **Humanas:** Refere-se principalmente, no caso de ataques provenientes de Engenharia Social, as vulnerabilidades tendem a aumentar por exemplo, pelo não cumprimento da política de segurança e falta de treinamento.

Em geral, pode-se dizer que é por meio da exploração das vulnerabilidades que indivíduos mal intencionados preparam armadilhas e se beneficiam. Concomitantemente ao que afirmam Avizienis et al. (2004), os quais defendem que fatores como a dificuldade de interações entre máquinas e pessoas, agravam o desafio de se manter a segurança da informação, visto que, o lado obscuro da natureza humana pode se manifestar, provocando e antecipando comportamentos maliciosos, os quais resultam em diversas espécies de falhas propositais e, para tanto exigem que novas formas de defesa sejam desenvolvidas.

2.2.4 Segurança do ambiente físico

As medidas de prevenção para a proteção de equipamentos, documentações e informações contra acessos não autorizados, fazem parte dos controles de segurança do ambiente físico. Assim, estes controles formam uma barreira complementar de segurança que, consequentemente, contribuem para a gestão e segurança do acesso lógico (ABNT NBR ISO/IEC 27002, 2013).

Em concordância com a ABNT NBR ISO/IEC 27002 (2013), há duas categorias em que os controles da segurança física estão divididos: os controles administrativos que têm o propósito de identificar visitantes e funcionários, controlar a entrada e saída de terceiros, entre outros, e; os controles explícitos formados por intermédio de câmeras, alarmes, fechaduras e guardas de segurança.

Diante das inúmeras formas de proteger a informação, a segurança física é um fator que possui muitos mecanismos de controle de segurança. Considerando apenas o seu conceito, pode-se aplicá-los nas organizações, de tal modo que a decisão de qual controle utilizar, vai depender da criticidade da informação para os negócios da empresa (ALEXANDRIA, 2009).

2.2.5 Segurança do ambiente lógico

Em todos os casos nos quais um indivíduo deseja acessar um objeto intangível, o indivíduo geralmente é um usuário ou processo, e o objeto neste cenário, pode ser um software ou arquivo. Logo, encontram-se como controles de acesso ao ambiente lógico de uma organização, ações e procedimentos cuja finalidade é a proteção dos dados, programas e sistemas diante de tentativas de acesso não autorizadas, estas, provenientes de outros usuários ou outros programas (DIAS, 2000).

Para melhor compreender os problemas relacionados com a segurança lógica e criar mecanismos de proteção ideais, deve-se entender os conceitos das principais áreas: autenticação e autorização, *Virtual Private Network* (VPN), *firewall* e antivírus.

2.2.5.1 Autenticação e autorização

As formas de autenticação são fundamentais para atender às necessidades de identificação de pessoas, equipamentos e sistemas (SÊMOLA, 2003).

A autenticação, de acordo com Whitman e Mattord (2012), é o processo de validação da provável identidade de um indivíduo e, para tal, utiliza-se de três fatores para a sua realização: o que a pessoa sabe, o que a pessoa tem e o que a pessoa é.

Neste sentido, o primeiro fator depende de algo que o indivíduo conheça e possa se recordar, como por exemplo, uma senha ou código de identificação único. O segundo, refere-se ao que a pessoa tem e pode apresentar, como um cartão magnético. O terceiro fator de autenticação diz respeito às características físicas individuais, como impressões digitais, reconhecimento facial e de voz (WHITMAN; MATTORD, 2012).

A autorização é a correspondência de uma entidade autenticada, que por sua vez, individualmente possui seu privilégio de acesso dentro das políticas e regras do sistema (WHITMAN; MATTORD, 2012).

Em geral, a autorização pode ser reconhecida por três maneiras: primeiramente, para cada usuário autenticado, há uma autorização na qual o sistema executa um processo de validação para analisar cada usuário e, por conseguinte, concede acesso aos recursos que estão disponíveis para cada um; a segunda maneira é a autorização para membros de um grupo, onde o sistema combina usuários autenticados à uma lista de membros de um grupo e, em seguida, concede acesso aos recursos que estão disponíveis para aquele grupo e; por fim, o conceito de autorização em vários sistemas, em que um sistema central de autenticação e

autorização verifica a identidade de cada usuário e atribui um conjunto de credenciais. (WHITMAN; MATTORD, 2012).

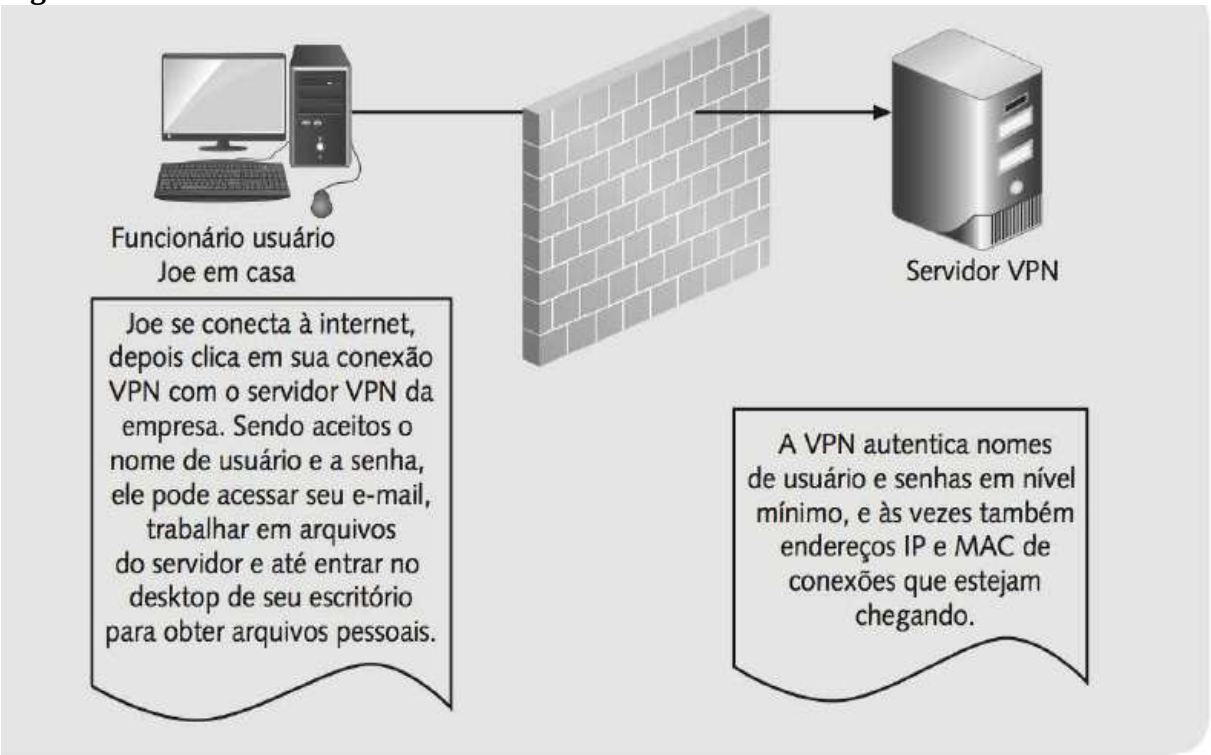
Soluções combinadas de autenticação e autorização possibilitam atender situações específicas, em que um método apenas não é necessário o suficiente para cumprir as exigências mínimas de segurança. Em vista disso, tem-se utilizado essas combinações principalmente, no setor financeiro, no qual o cliente para realizar uma operação deve possuir um cartão magnético, combiná-lo com uma senha e ainda apresentar informações acerca da comprovação da sua identidade (SÊMOLA, 2003).

2.2.5.2 Virtual private network (VPN)

A conexão de rede privada e segura entre sistemas que utilizam a infraestrutura de telecomunicações públicas, mantendo a privacidade através do uso de um protocolo que funciona como túnel para que haja garantia de que os dados sejam enviados para seu destinatário, sem que terceiros consigam acessá-los, é chamada de *Virtual Private Network* (WHITMAN; MATTORD, 2012).

Uma *Virtual Private Network* (*VPN*) proporciona que funcionários de uma organização possam acessar remotamente à rede interna da empresa mediante a utilização da *internet* como transmissora, desconsiderando o acesso discado ou *links Wide Area Network* (*WAN)* dedicados (BASTA; BASTA; BROWN, 2014). A Figura 3 ilustra um modelo *VPN*.

Figura 3 - Modelo *Virtual Private Network*



Fonte: Basta; Basta; Brown (2014, p. 173).

Basicamente, conforme ilustrado na Figura 3, a conexão *VPN* possibilita que um funcionário de uma organização consiga acessar o conteúdo do servidor da empresa, sem interferências e, de maneira segura.

2.2.5.3 Firewall

Uma conciliação entre *hardware* e *software* que tem como finalidade isolar a rede corporativa da internet pública, permitindo a passagem de alguns pacotes e bloqueando a passagem de outros, é considerado um *firewall* (KUROSE; ROSS, 2013).

Para Beal (2008), quando se fala em segurança de redes, o *firewall* é o equipamento mais mencionado. Sobretudo, um *firewall* forma uma barreira de segurança entre um computador ou, para proteger uma rede privada da sua área externa.

Quando uma informação não se adequa às exigências de segurança impostas pelo *firewall*, "o tráfego de informações entre esse computador ou rede e o mundo exterior é examinado e bloqueado (...)" (BEAL, 2008, p. 94).

Os objetivos de um *firewall* estão definidos, conforme a concepção de Kurose e Ross (2013), em três conceitos: i) passa pelo *firewall* o tráfego que vem de fora da rede e, o tráfego que sai de dentro da rede; ii) somente o conteúdo que foi previamente definido pela política de segurança da organização poderá passar pelo *firewall*; iii) por ser uma ferramenta conectada à rede, o *firewall* deve ser instalado de maneira correta, a fim de ser imune às invasões.

2.2.5.4 Antivírus

Os programas que se instalam nas máquinas sem autorização do usuário e executam ações aleatórias, sem autorização prévia, são conhecidos como vírus (FONTES, 2006). Portanto, é necessário que haja o desenvolvimento de sistemas apropriados para combatê-los, os chamados antivírus, os quais se tornam recursos essenciais para a proteção de dispositivos conectados à internet (BEAL, 2008).

Com o intuito de evitar ataques de códigos nocivos, um *software* antivírus faz uma varredura periódica nos arquivos para buscar eventuais modificações nos formatos dos mesmos, em anexos de *e-mail* com origens duvidosas e outros possíveis sinais de alerta, sendo assim uma importante ferramenta para a segurança dos dados corporativos (BEAL, 2008).

2.2.6 Fator humano no processo de segurança da informação

O fator humano no processo de segurança da informação é formado pelos recursos humanos que estão inseridos na organização, especialmente, os que lidam com recursos de Tecnologia da Informação (TI), formando assim, a ligação mais fraca no fluxo da segurança. A ótica em torno da camada humana, passa a ser um procedimento complexo de se analisar os riscos e administrar a segurança, uma vez que deve levar em consideração o fator humano, psicológico com suas particularidades, culturais e emocionais, variando de indivíduo para indivíduo (NETTO; SILVEIRA, 2007; ADACHI, 2004; SCHNEIER, 2001).

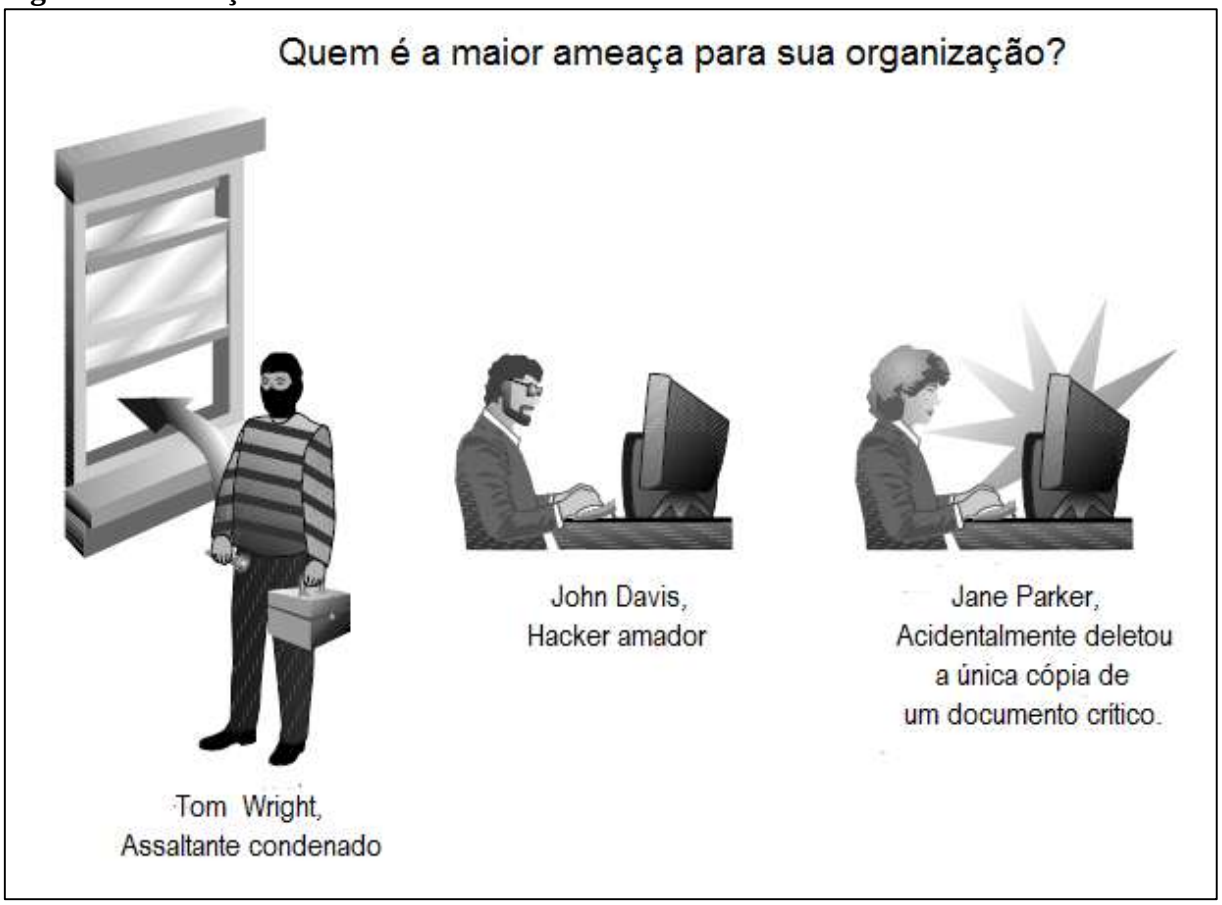
Os elementos relevantes da camada de segurança humana começam pela questão de como as pessoas lidam com os incidentes de segurança que acontecem. Essa importância é baseada levando em conta se o usuário é apto ou ignorante para utilizar os recursos de TI, como eles enfrentam a ameaça dos intrusos maliciosos e, por fim, a engenharia social, na qual

os *hackers* adquirem informação de maneira ilícita (NETTO; SILVEIRA, 2007; ADACHI, 2004; SCHNEIER, 2001).

Em razão de manusearem os dados em suas atividades diárias, os funcionários de uma organização constituem os agentes de ameaça mais próximos dos dados organizacionais, pois utilizam dos mesmos para conduzir o negócio da empresa. Então, os erros causados por esses agentes, acarretam uma séria ameaça à confidencialidade, integridade e disponibilidade das informações (WHITMAN; MATTORD, 2012).

Como ilustra a Figura 4, pode-se dizer que as falhas de funcionários estão em um patamar prejudicial ainda maior, inclusive, do que as ameaças de pessoas externas à organização.

Figura 4 - Ameaças Humanas



Fonte: Adaptado de Withman; Matttord (2012, p. 94).

Por meio da concepção de Whitman e Mattord (2012), se pode interpretar que os erros de funcionários resultam nos seguintes riscos: revelação de dados confidenciais, gravação de informações inadequadas, exclusão acidental ou modificação de dados

importantes, armazenamento de dados em áreas desprotegidas e, falha na proteção das informações.

Ao pensar no capital humano como um elo indispensável para a diminuição dos riscos, Sêmola (2003, p. 136) propõe:

> O nível de segurança de uma corrente é equivalente à resistência oferecida pelo elo mais fraco. O *peopleware* representa justamente esse elo; por isso, deve ser alvo de um programa contínuo e dinâmico, capaz de manter os recursos humanos motivados a contribuir, conscientes de suas responsabilidades e preparados para agir diante de antigas e novas situações de risco.

Do mesmo modo que um funcionário atual da empresa pode ser fator de risco, um ex-funcionário significa um risco ainda maior com relação às informações confidenciais. Funcionários descontentes ou irritados por conta de uma demissão, precisam ser pontos de questionamentos em ocorrências, muitas vezes inconcebíveis, de perdas de documentos, informações que apenas tal setor deveria saber, além de diversos outros impasses que comprometem o sigilo das informações corporativas (PEIXOTO, 2006).

Em relação aos cuidados que precisam ser adotados com ex-funcionários, Peixoto (2006), frisa a necessidade de haver uma política de encerramento instantânea do acesso do empregado com a estação de trabalho, devendo ser feita antes do colaborador deixar o prédio. Um método para resgatar todas as chaves e demais dispositivos de acesso digital, bem como, o crachá de identificação do empregado. Também, impor medidas que requerem o trabalho dos responsáveis pela segurança, identificarem o ID com foto e autorizarem o acesso a somente o pessoal credenciado nas dependências da organização e a verificação do nome em uma lista com a finalidade de descobrir se o funcionário ainda faz parte da empresa.

2.2.7 Ações para os problemas

Uma empresa sempre está suscetível aos problemas e acidentes que podem vir a ocorrer e, dessa forma comprometer a segurança da informação. Seria ingenuidade acreditar que tais adversidades não atinjam à estrutura organizacional visto que, nem todas podem ser previstas e solucionadas antes de ocorrerem. Em vista disso, é essencial que a organização se mantenha atenta e preparada para a resolução de problemas inesperados (FONTES, 2006).

Sendo assim, Fontes (2006) elenca três categorias de ações que devem ser adotadas nesses casos:

- **Ações preventivas:** Tem como intuito evitar que o acidente aconteça. Tendem a ser as mais comuns e baratas de se aplicar. As ações preventivas podem ser simples, de acordo com Fontes (2006, p. 53) “[...] não traga comida para junto do computador, pois as migalhas podem cair no teclado e estragar esse dispositivo [...]”, e podem ser ações mais sofisticadas, como a verificação diária dos sistemas de câmeras para averiguar se elas estão gravando as filmagens no disco;
- **Ações detectivas:** As ações detectivas visam identificar uma situação ou agente causador de ameaça, seja ela no mundo físico ou virtual. Para um exemplo do mundo físico, podem ser citados os sensores de detecção de incêndio e, no mundo virtual, a medida de bloqueio de acesso, aplicada quando há três tentativas erradas de digitação de senha;
- **Ações corretivas:** Geralmente, as ações corretivas destinam-se a minimizar um problema presente na organização e que possibilite a empresa continuar as suas atividades com os recursos reduzidos. Na hipótese de incêndio, o combate manual pela brigada de incêndio passa a ser uma ação corretiva e; também, a recuperação de uma informação por meio de cópias de segurança.

Os problemas da organização devem ser ajustados de maneira responsável, fazendo uso dos procedimentos das ações de detecção, prevenção e correção. Apesar de custar um tempo considerável para ajustar esses métodos, é preciso compreender que para o negócio da organização, eles são fundamentais para sustentar não somente a empresa, como também a vida profissional (FONTES, 2006).

2.2.8 Política de segurança da informação

A fim de reforçar que os métodos de segurança de informação sejam seguidos, cria-se então, a política de segurança da informação, formada por um conjunto de diretrizes internas que determinam as regras para a melhor proteção dos dados de acordo com a área de negócio e requisitos contratuais, regulamentares e normativos inseridos a toda estrutura da organização (ABNT NBR ISO/IEC 27001, 2013). Por meio dela, definem-se as responsabilidades e, os objetivos que precisarão ser implantados para assegurar a proteção da segurança da informação. Assim sendo, obrigatoriamente, a política de segurança precisa

estar atualizada e, evidentemente, definida para que seja divulgada e apoiada pelos responsáveis da organização (ABNT NBR ISO/IEC 27001, 2013).

Em consequência dos riscos que a informação pode se sujeitar, e por conta disso, a organização perceba a real necessidade em prover maneiras de minimizar esses riscos, um guia deve ser criado, apresentando as práticas essenciais para sustentar as informações fundamentais para o negócio. Geralmente, este documento é denominado como a sua política de segurança, sendo a base para a conscientização dos colaboradores da empresa (ADACHI, 2004).

A política de segurança tem como papel fornecer orientações acerca da conduta do funcionário e constitui-se em um elemento relevante para o desenvolvimento de controles apropriados para combater às diversas ameaças que possam vir a trazer riscos para a organização. Ademais, é fundamental para a prevenção e detecção de ataques advindos da Engenharia Social (FONSECA, 2009).

Mesmo que a política de segurança seja elaborada com os melhores procedimentos e, seguida rigorosamente, por todos os colaboradores, ainda assim, não é possível afirmar que a organização está imune aos golpes de engenheiros sociais. Portanto, um dos principais propósitos da execução de uma política de segurança, é minimizar os riscos até a obtenção de um nível considerado aceitável (FONSECA, 2009).

2.2.9 Plano de continuidade dos negócios

Atualmente, as organizações demonstram uma dependência dos recursos tecnológicos, que são vitais para a continuidade do negócio. Deste modo, se houver perda de equipamentos ou informações elas podem trazer consequências significativas para a atividade operacional, acarretando em prejuízos financeiros e, dependendo de gravidade, resultar em insucessos irreversíveis (ABNT NBR ISO/IEC 27002, 2013).

Dessa forma, é imprescindível que haja a compreensão sobre a relevância da recuperação de desastres e, um plano de continuidade dos negócios, os quais são fundamentais e utilizados como estratégia para alcançar os objetivos organizacionais (ABNT NBR ISO/IEC 27002, 2013).

Um plano de continuidade de negócio deve ter como objetivo prover soluções para incidentes relacionados à segurança que não possam ser, previamente, impedidos de ocorrer, de tal modo que assegure a continuação dos trabalhos dentro de um curto período de tempo, visando reduzir os impactos ocasionados pelo incidente (SÊMOLA, 2003).

Especialmente, nas instituições financeiras há uma maior preocupação para desenvolver planos de continuidade devido ao fato de pertencerem a uma área de negócio na qual a confiabilidade das informações está diretamente relacionada com a credibilidade da instituição, favorecendo sua sobrevivência no mercado. Vale ressaltar que estes procedimentos de contingência precisam ser elaborados antes dos acidentes, pois, se algum desastre acontecer e nenhuma solução tiver sido criada, a resolução do problema ficará comprometida (DIAS, 2000).

2.3 ENGENHARIA SOCIAL NAS ORGANIZAÇÕES

A Engenharia Social é um conjunto de técnicas e habilidades utilizadas para induzir as pessoas a revelarem dados confidenciais, que se tornam informações úteis para o fraudador (WHITMAN; MATTORD, 2012).

O processo de exploração da fraqueza humana com a finalidade de extrair informações de um funcionário que a princípio precisa mantê-las de maneira privada é conhecido como Engenharia Social (ENGEBRETSON, 2011).

A engenharia social pode ser definida segundo Hadnagy (2011), a partir do significado de dois termos: engenharia e social. Entende-se “engenharia” como uma ciência que visa aplicar conhecimentos técnicos às questões cotidianas; e “social” inclui a capacidade de relacionamento dos indivíduos dentro de um grupo. Logo, um indivíduo que executa a técnica de engenharia social aproveita-se das informações que já possui, aplica seus conhecimentos técnicos na qual, com antecedência, prevê como as pessoas irão se comportar diante de tal situação, fazendo então, com que chegue ao seu objetivo final: obter dados para o seu privilégio.

Para Mitnick e Simon (2003) o termo Engenharia Social refere-se ao uso da influência e persuasão como meio para iludir as pessoas e fazê-las repassar informações sigilosas, seja por meio de tecnologias ou não.

Na ótica de Basta, Basta e Brown (2014) a Engenharia Social “(...) envolve um ato de fraude por parte de quem ataca, com o objetivo de enganar indivíduos de boa-fé para que forneçam o acesso a informações ou sistemas não autorizados”.

Ainda para esses autores as práticas de Engenharia Social partem da exploração da ingenuidade humana e do pressuposto da confiança, ou seja, geralmente um engenheiro social se passa por um usuário genuíno de um determinado sistema e, com isso, consegue extrair da vítima as informações desejadas com facilidade.

Ao se deparar com um indivíduo que se apresente como um especialista em tecnologias, por exemplo, os usuários tendem a agir com negligência e repassar para o fraudador informações altamente confidenciais, que finge necessitar para realização de testes, verificação de segurança ou restauração de sistemas (BASTA; BASTA; BROWN, 2014).

2.3.1 Características do engenheiro social

O engenheiro social não possui, necessariamente, uma formação específica para a realização da sua atividade profissional, podendo estar inserido em qualquer ramo de atuação no mercado de trabalho. Para aplicar os golpes, as empresas de médio e grande porte, passam a ser mais cobiçadas. Os engenheiros sociais utilizam como as principais técnicas para os golpes, a simpatia e uma boa conversa, exploração do ambiente e de suas possíveis vítimas, distinguindo seus pontos vulneráveis e, além disso, os pontos fracos do local pretendido (SILVA; ARAÚJO; AZEVEDO, 2013).

Na maioria das vezes, o engenheiro social transmite ser uma pessoa educada e carismática. No entanto, acima de tudo, a criatividade faz com o engenheiro social tenha uma conversa bastante atrativa, sendo bem articulados e astutos, os engenheiros sociais são peritos no quesito de distrair as pessoas para que então, elas cooperem em prol do seu objetivo (PEIXOTO, 2006).

Os talentos de persuasão e influência quando combinados para confundir uma pessoa, levam ao perfil de um engenheiro social. No conhecimento de Mitnick e Simon (2003) compreende-se que a arte de trapacear é dividida em duas particularidades específicas: o indivíduo que engana as pessoas com o propósito de obter seu dinheiro que fazem parte da especialidade denominada de *grifter*. Por outro lado, alguém que utiliza das fraudes, persuasão e domínio contra as empresas na maior parte dos casos, tendo em vista suas informações, que pertencem a especialidade de engenheiro social.

Em tese, o engenheiro social aproveita-se de assuntos que são capazes de abalar o emocional de seus alvos, a fim de confundi-los e manipulá-los para que concedam informações de acordo com o seu interesse. Audacioso, o engenheiro social simula amizades para servirem de isca, podendo então, assumir várias personalidades em seu benefício para concluir determinado objetivo. Uma alta capacidade de persuasão e talento em comunicar-se, são características perceptíveis do engenheiro social (ABS JUNIOR; BARCAROLI, 2016).

2.3.2 Vulnerabilidades humanas exploradas pelos engenheiros sociais

É de conhecimento do engenheiro social que mesmo no maior ambiente de segurança que possa existir, há um componente delicado que pode vir a se romper facilmente: o ser humano (MITNICK, SIMON, 2003).

Na maioria das vezes, os engenheiros sociais usam uma situação de mentira ou persuasão pessoal, na qual tem como objetivo, aumentar a chance de que seu pedido venha a ser bem sucedido. O sucesso de tais ataques pode ser ampliado criando-se um cenário em que determinadas respostas psicológicas são despertadas dentro da vítima, considerando que alguns indivíduos podem ter uma pré-disposição para expor com maior facilidade as informações. Sendo assim, a vulnerabilidade das pessoas está diretamente associada com a eficácia dos engenheiros sociais em estimular respostas e, aos aspectos relacionados à personalidade dos indivíduos (PARSONS et al., 2010).

A fragilidade humana no ponto de vista de Workman (2008) está amplamente relacionada com a simpatia e confiança das pessoas, e eventualmente os indivíduos mais confiantes têm maior probabilidade de submeter-se aos ataques de engenharia social. Mitnick e Simon (2003) esclarecem que faz parte da natureza humana depositar confiança nas pessoas, em especial quando os pedidos não induzem a suspeitas e quando aparentam ser razoáveis. Normalmente, o desejo de ser prestativo está presente nas pessoas e por isso, muitas vezes elas não possuem uma condição emocional adequada para discernir uma ameaça real. Logo, os engenheiros sociais tendem a usufruir desse conhecimento para explorar indivíduos e em alguns casos, construir uma relação de amizade, sabendo que será mais fácil para o agressor se as vítimas simpatizarem ou confiarem nele.

A criação de um afeto aumenta o estado emocional das vítimas, tornando-as propensas a apresentarem certas informações, as quais, em ocasiões normais seriam recusadas. À medida que as emoções de raiva, surpresa, pânico ou medo são estimuladas, é provável que o indivíduo seja facilmente distraído, não sendo capaz de avaliar e questionar de maneira lógica o relato do agressor (GRAGG, 2002).

Com o enfoque de exemplificar tais vulnerabilidades humanas, Aiello (2008) em sua obra menciona que o invasor pode criar uma situação planejada em que o trabalho da vítima é ameaçado por conta do uso indevido dos recursos da empresa. Neste caso, o engenheiro social pode propor a solução do problema e solicitar a senha da vítima para finalizar essa atividade. Nessa situação, com medo de perder seu trabalho e o pânico

provocado por conta disso, a pessoa, pode se disponibilizar a atender o pedido com o propósito de resolver o problema.

Solicitações que aparentam ser inofensivas são na maior parte das vezes confiáveis. Caso um engenheiro social requisite uma informação que ao que tudo indica não seja prejudicial a sua exposição, as pessoas normalmente tendem a querer ser úteis e, então, possivelmente acatarão. Muitas vezes, os engenheiros sociais conseguem coletar pequenas informações de diversas fontes, e as várias vítimas do ataque não se dão conta que revelaram informações úteis em favor do golpe. A título de exemplo, revelar a versão de um *software* específico ou o nome de um gerente pode aparentar como não sendo uma informação relevante, entretanto, uma informação como essa seria capaz de ser usada para ajudar o engenheiro social a atacar outro funcionário (PARSONS et al., 2010).

De natureza igual, os sentimentos de culpa também tendem a diminuir consideravelmente a capacidade de um indivíduo interpretar logicamente uma solicitação. Assim, os engenheiros sociais visam proporcionar situações pré-definidas para gerar empatia, influenciando a vítima acatar ao pedido para ajudar a reduzir o problema do solicitante (AIELLO, 2008).

O afeto que se desenvolve entre a vítima e o engenheiro social começa a partir do início da interação. O agressor faz uma declaração que acarreta em emoções fortes, que não se limitam somente ao medo ou pânico, podendo também ser o sentimento de alegria gerado pela promessa de um valioso prêmio. Esta onda de emoções atua como fator contundente para a distração da vítima, interferindo assim, na capacidade de avaliar e pensar logicamente, ou criar uma medida de defesa contra o pretexto em questão (PARSONS et al., 2010).

Há uma regra conhecida no inter-relacionar-se com as pessoas que funciona da seguinte forma: quando alguém fornece ou promete algo, deve-se retribuir o favor. Isso é relativamente verdadeiro, independente se o presente original não foi solicitado, ou então, o retorno possui um valor superior com relação ao originalmente fornecido. Esta verdade é conhecida como reciprocidade (GRAGG, 2002). Atrelado a isso, Mitnick e Simon (2003) ilustram que no ambiente corporativo, dificilmente as pessoas analisam uma solicitação de maneira minuciosa, levando-as a um atalho mental que funciona como um pensamento inferido de que se alguém estiver ajudando a resolver um problema, consequentemente, sua índole não será contestada.

Mitnick e Simon (2003, p. 99) ainda reforçam:

> A verdade é que ninguém está imune contra ser enganado por um bom engenheiro social. Devido ao ritmo da vida normal, nem sempre pensamos com cuidado antes de tomarmos as decisões, mesmo em questões que são importantes para nós. As situações complicadas, a falta de tempo, o estado emocional ou a fadiga mental podem facilmente nos distrair. Assim sendo, tomamos um atalho mental e resolvemos sem analisar cuidadosamente as informações, um processo mental conhecido como resposta automática. Isso é válido até para os agentes da lei dos governos federal, estadual e municipal. Somos humanos.

Em consonância ao que citam Mitnick e Simon (2003), Gragg (2002) expõe que os casos em que o engenheiro social cria um cenário problemático e ao mesmo tempo propõe soluções eficientes, pode ser enquadrado como engenharia social reversa.

Nessa forma de atuação, o fraudador cria a situação adversa e, em seguida, aparece como sendo um herói pronto e destinado a corrigir o problema da vítima. Então, antes que o problema tenha sido solucionado, o alvo sente-se em dívida com o *hacker,* formando assim, um cenário favorável para o engenheiro social usufruir dos dados (GRAGG, 2002).

Outro aspecto de exploração da vulnerabilidade é o de autoridade. As pessoas tendem a seguir uma solicitação quando ela é proveniente de uma pessoa com autoridade. O atacante pode alegar que faz parte do departamento de Tecnologia da Informação (TI) ou que é uma pessoa que trabalha para um diretor da empresa e, com isso, a vítima na maior parte das vezes não questionará a solicitação (MITNICK; SIMON, 2003).

2.3.3 Métodos e ferramentas utilizadas para os ataques

Os engenheiros sociais geralmente fixam sua estratégia de ataque baseando-se em cinco pilares: o tempo de resposta, o tempo de preparação, as circunstâncias, o nível de consciência dos responsáveis pelo gerenciamento de dados e a fragilidade da informação. Para efetivar sua estratégia geram uma combinação de métodos, incluindo as vulnerabilidades identificadas nas vítimas, a utilização de dados públicos, prévio conhecimento de processos internos e uso de quaisquer recursos para obter colaboração das vítimas (AIELLO, 2008).

Os meios mais utilizados para realização do ataque de engenharia social são o telefone, *e-mail*, *internet* e muitas vezes, pessoalmente. Habitualmente, são realizadas várias abordagens aos alvos, de formas distintas, com pequenas solicitações aparentemente inofensivas, mas que, ao final são unidas em um conjunto de informações sigilosas, chegando assim, ao objetivo, previamente, estabelecido. Depois de coletar todos os dados necessários, o

engenheiro social efetua novos ataques ou interrupções de sistemas, com o propósito de causar danos à organização (AIELLO, 2008).

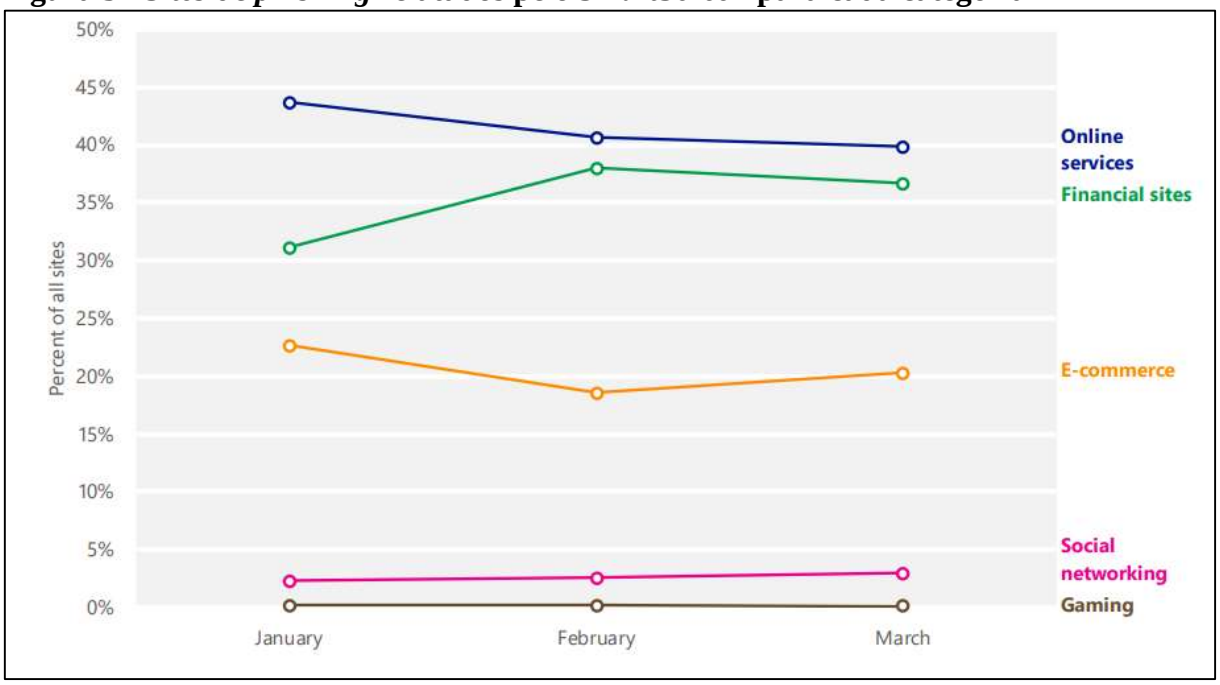
Outra ferramenta utilizada é a falsa identidade. Os engenheiros, por exemplo, podem se passar por funcionários ou colegas de outras filiais ou departamentos e por responsáveis pela manutenção de sistemas diversos. Também podem se infiltrar nas instalações da empresa por meio da conversação com recepcionistas ou secretárias, fingindo fazer parte do pessoal credenciado para realização de serviços específicos de manutenção (AIELLO, 2008).

Dentre as várias ferramentas existentes no campo da engenharia social, o que mais vem obtendo destaque são os chamados *phishing.* O termo *phishing* pode ser entendido como toda e qualquer atividade de enviar *e-mails* com conteúdo atrativo para o destinatário. Muitas vezes essas mensagens contêm *links* ou arquivos anexados que possuem natureza maliciosa. São as mais simples formas para raptar dados de grandes organizações ou órgãos governamentais, pois está diretamente relacionada com o preparo dos colaboradores (HADNAGY, 2011).

Rowe e Custy (2008) tratam o termo *phishing* como um tipo de *e-mail* fraudulento (*spam*) que extrai informações confidenciais dos destinatários direcionando-os para *sites* adulterados, geralmente utilizados com a finalidade de obter dados financeiros. Silva (2012) afirma que a maioria desses *spams* se intitulam originados de instituições financeiras, cujo foco é fazer com que as vítimas repassem dados privados de acesso, como por exemplo número de cartões, número de documentos e senhas.

A Central de Proteção e Segurança da Microsoft desenvolve relatórios estatísticos sobre ataques de *phishing* detectados por meio do filtro *SmartScreen* presente no navegador *internet explorer,* o qual foi desenvolvido para auxiliar na proteção de usuários acerca de páginas com conteúdo malicioso. A Figura 5 ilustra dados com relação às categorias de sites que mais são alvos de *phishing*.

Figura 5 - *Sites* de *phishing* relatados pelo *SmartScreen* para cada categoria

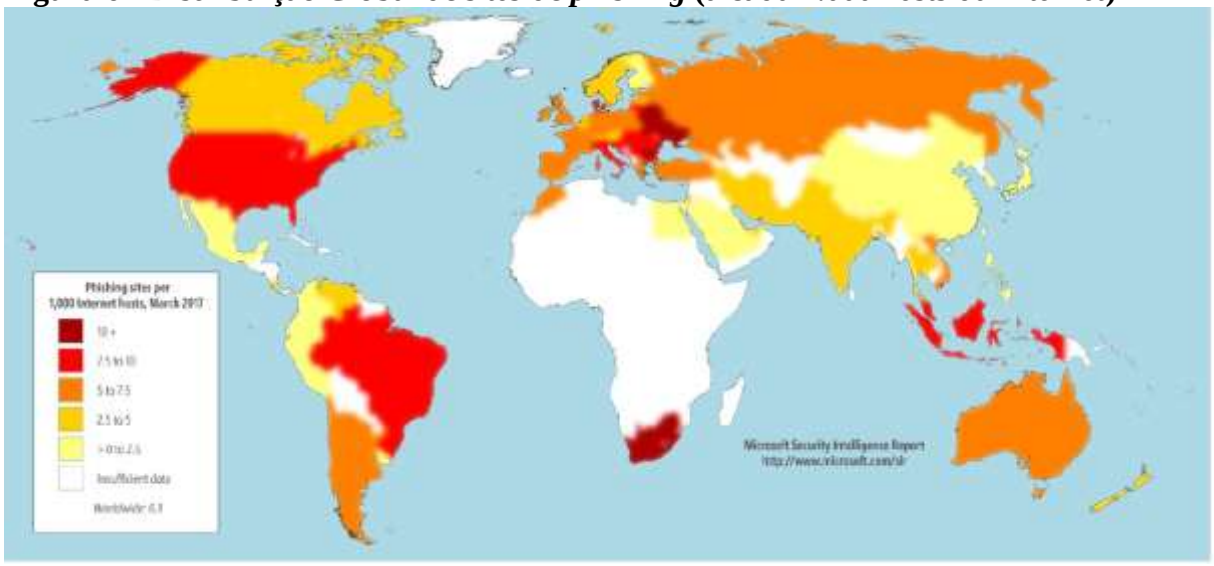


Fonte: Relatório de Inteligência de Segurança, Volume 22, p.35 (Janeiro a Março de 2017), Microsoft.

Por meio da Figura 5 e do Relatório de Inteligência de Segurança da Microsoft, pode-se analisar que durante o primeiro trimestre de 2017, a categoria de *sites* com maior número de *phishing* detectados foi a de Serviços *Online*, e em segundo lugar ficaram os *sites* de Instituições Financeiras. Cabe ressaltar que as Instituições Financeiras sempre foram e continuam sendo foco de *phishing*, pois através deles pode-se obter dados bancários das vítimas. As outras três categorias "*E-commerce*, Redes Sociais e Jogos" não apresentaram porcentagens significativas.

A Figura 6 e o Relatório de Inteligência de Segurança da Microsoft demonstram que os locais que apresentaram concentrações de *phishing* acima da média foram: Ucrânia, África do Sul, Indonésia e Dinamarca. Já locais como: China, Taiwan, Coréia e México apresentaram locais com baixa concentração de *phishing.* A Figura 6 demonstra a distribuição global de *sites* com conteúdo de *phishing.*

Figura 6 - Distribuição Global de *sites* de *phishing* (a cada 1.000 *hosts* da *Internet*)



Fonte: Relatório de Inteligência de Segurança, Volume 22, p. 37 (Março de 2017), Microsoft.

Conforme mencionado anteriormente, uma das formas de ataque mais utilizadas pelos engenheiros sociais é através de *e-mails* fraudulentos, na Figura 7 se ilustra um exemplo deste tipo de *e-mail*.

Figura 7 - Exemplo de um *e-mail phishing*

Fonte: Extraído da conta de *e-mail* do autor (2018).

Com relação a Figura 7, se percebe que o endereço de *e-mail* do remetente não condiz com a instituição financeira em questão, podendo o destinatário constatar a fraude apenas observando este detalhe. Também, vale ressaltar, que instituições sérias jamais solicitam alterações cadastrais via *e-mail*, redirecionando para *links*.

Juntamente com as vantagens proporcionadas pelos recursos disponibilizados pela *internet*, também há uma gama de códigos maliciosos (*malwares*) que pode trazer danos significativos aos usuários. Esses *malwares* após instalados nos dispositivos, tem o propósito de infectar e modificar arquivos dentro do sistema operacional. Além disso, induzem a instalação de *spyware* que é capaz de roubar dados confidenciais, enviando-os diretamente para quem os criou. Há também o risco de o hospedeiro malicioso estar incluso em uma rede de computadores vinculada por uma pessoa ou grupo, cujo objetivo é realizar ataques simultâneos para prejudicar o alvo, sendo denominada *botnet* (BASTA; BASTA; BROWN, 2014; KUROSE; ROSS, 2014).

Os *malwares* propagam-se pela rede de forma rápida, visto que se autorreproduzem, ou seja, caso um computador conectado à *internet* seja infectado, o *malware* vai realizando buscas e entrando em mais hospedeiros. Essa propagação se dá por meio de vírus ou *worm*. Os vírus têm sua atuação a partir de uma interação de usuário para executá-lo, os casos mais comuns são de *e-mails* contendo anexos executáveis, estes anexos quando são abertos, infectam o dispositivo. Neste exemplo, quando há sucesso na sua instalação, o vírus envia mensagens maliciosas automaticamente, para todos os contatos contidos no *e-mail* da vítima, facilitando sua disseminação. Por outro lado, há *malwares* que não necessitam de interação do usuário para se instalar no dispositivo, são os chamados *worm.* Basicamente, *worm* é uma aplicação que se instala, na maioria das vezes, quando um usuário está utilizando um programa em uma rede vulnerável, e o próprio programa, sem autorização do usuário, deixa o *malware* entrar, tornando-o um *worm*. Para se espalhar, o *worm* atua enviando cópias de si mesmo, e passa automaticamente, de um computador para outro sem precisar da ajuda de demais componentes, diferentemente dos vírus (KUROSE; ROSS, 2014).

Uma variação de *malware* muito comum e de fácil infecção é o chamado Cavalo de Troia. É uma aplicação que "[...] disfarçada de arquivo legítimo, procura enganar a vítima fazendo-a aceitar sua instalação", também pode ser entendido como "[...] um código *malware* oculto em uma atividade aparentemente inofensiva" (BASTA; BASTA; BROWN, 2014, p. 179). Os danos que um Cavalo de Troia pode ocasionar envolvem o registro de teclas digitadas, capturas de tela e acesso de arquivos. Em suma, este *malware* se esconde dentro de uma aplicação que está sendo executada pelo usuário e realiza sua atividade maliciosa de forma oculta (BASTA; BASTA; BROWN, 2014).

3 PROCEDIMENTOS METODOLÓGICOS

Neste capítulo, inicialmente, se descreve o enquadramento metodológico do estudo. Posteriormente, são apresentados os métodos utilizados para a coleta e análise dos dados.

3.1 ENQUADRAMENTO METODOLÓGICO

No que diz respeito à análise dos dados, se utiliza a pesquisa qualitativa. O método qualitativo, de acordo com Richardson (1999) é utilizado para estudar cenários complexos e rigorosamente específicos, possibilitando descrever um problema de difícil compreensão, analisar a relação entre variáveis e, abstrair, além de classificar, processos vividos por grupos sociais. Deste modo, as informações obtidas junto aos colaboradores da Cooperativa de Crédito em estudo, partiram da análise qualitativa e permitiram identificar as atitudes dos colaboradores em relação às práticas de engenharia social que podem afetar a manutenção da segurança da informação da entidade.

Quanto aos objetivos, este estudo define-se como descritivo, uma vez que, para Gil (2002), têm como finalidade principal descrever as particularidades de uma determinada população ou, a formação de relações entre variáveis. Assim, por meio desta pesquisa são ilustradas as características dos colaboradores da Cooperativa de Crédito quanto a Segurança da Informação e Engenharia Social.

Com relação aos procedimentos, devido ao uso do questionário para coleta de dados, se efetua um estudo do tipo levantamento, e um estudo de caso com base na Cooperativa de Crédito. Segundo Gil (2002), a pesquisa na forma de levantamento, se caracteriza pela interrogação direta das pessoas das quais a conduta se deseja conhecer. O método estudo de caso consiste na análise de um ou poucos objetos, para que seja possível ter o conhecimento maior e mais detalhado acerca de um determinado assunto.

3.2 PROCEDIMENTOS DE COLETA E ANÁLISE DE DADOS

Para a coleta de dados, foi elaborado um questionário na plataforma *Google Docs*, e posteriormente enviado para o *e-mail* dos colaboradores da Cooperativa de Crédito, dos quais 90 (noventa) retornaram com as respostas.

O questionário contou com perguntas abertas e fechadas, e foi dividido em seis sessões. A primeira sessão, possui quatro questões e visa identificar informações sobre o perfil de cada colaborador. A segunda, possui quatro perguntas voltadas para as atitudes na utilização de senhas. A terceira, têm cinco perguntas que dão ênfase ao comportamento do usuário a respeito da divulgação de informações. Seguindo para a quarta sessão, tem-se duas questões abertas e uma fechada, cujo o foco é, coletar qual foi a atitude tomada quando o colaborador foi vítima de um ataque de alguém mal intencionado. A quinta sessão, é composta por quatro questões para identificar, de maneira geral, o nível de conhecimento dos colaboradores sobre o funcionamento da segurança da informação na Cooperativa. Por fim, a sexta sessão, conta com quatro perguntas de cunho pessoal, nas duas primeiras, sobre o comportamento do colaborador direcionado à proteção da Segurança da Informação e, nas duas seguintes, sobre a visão do colaborador quanto a importância das informações.

Em um segundo momento, como forma de buscar evidências sobre a importância da constante conscientização a respeito da Segurança da Informação, foi elaborado um *e-mail* de *phishing* e direcionado aos endereços eletrônicos de todos os colaboradores para verificar quais clicariam apenas no *link* ou, ainda mais grave, clicariam no *link* e preencheriam as informações solicitadas. O remetente do *e-mail* aparentava ser do Setor de Tecnologia da Informação e solicitava o preenchimento de dados para a atualização no sistema. O *phishing* foi criado na forma de um *hiperlink* que, ao ser clicado, redirecionava o usuário para uma página de formulário e, nesta página, a vítima tinha as opções de informar o nome, CPF e a senha do sistema corporativo. O pseudo *e-mail*, se analisado de forma correta, não tinha característica alguma no seu nome, domínio e assinatura, que estivesse de acordo com os padrões adotados pela Cooperativa.

4 APRESENTAÇÃO E ANÁLISE DOS RESULTADOS

4.1 OBJETO DE ESTUDO

A pesquisa foi realizada tendo como objeto de estudo os colaboradores de uma Cooperativa de Crédito localizada no sul de Santa Catarina, cujo nome fictício adotado será Cooperativa de Crédito Alfa.

4.1.1 Caracterização da Cooperativa de Crédito

A Cooperativa de Crédito Alfa, atua há aproximadamente 29 anos no sul de Santa Catarina, possui 22 (vinte e duas) agências distribuídas em 18 (dezoito) cidades e conta com cerca de 150 colaboradores, obtendo destaque pela credibilidade e satisfação dos seus 32.000 (trinta e dois mil) associados.

A lista de produtos e serviços é diversificada, contendo desde serviços mais comuns, como por exemplo, contas correntes e cartões, até alguns serviços mais específicos, como recargas telefônicas e previdência privada.

Diariamente, a Cooperativa trabalha para que seja reconhecida pela sua eficiência e como uma das melhores opções do mercado financeiro, prezando pelo comprometimento com o crescimento econômico dos associados.

4.1.2 Política da segurança da informação adotada pela cooperativa em estudo

A Cooperativa de Crédito Alfa possui internamente uma Política de Segurança da Informação que foi criada em 2013 e, aprovada pelos responsáveis Administrativos.

Em tese, a Política possui orientações a respeito de Segurança Lógica e Segurança Física, com o objetivo de conscientizar os colaboradores a adotarem as melhoras práticas para a proteção dos ativos de informação.

Em seu regulamento, também estão previstas sanções para os usuários que descumprirem às normas. É um passo muito importante para conscientizá-los sobre a responsabilidade da utilização dos recursos de TI, ou seja, que devem aplicá-los apenas para o trabalho e benefício da organização, pois as imprudências ou negligências evidenciadas resultarão em repreensões.

Atrelada a esse contexto, a Política determina que os incidentes ocorridos envolvendo a Segurança da Informação devem ser direcionados ao setor responsável, para que este possa divulgá-los, de modo que sirvam de alerta aos demais colaboradores.

4.2 DESCRIÇÃO E ANÁLISE DOS DADOS COLETADOS

4.2.1 Questionário

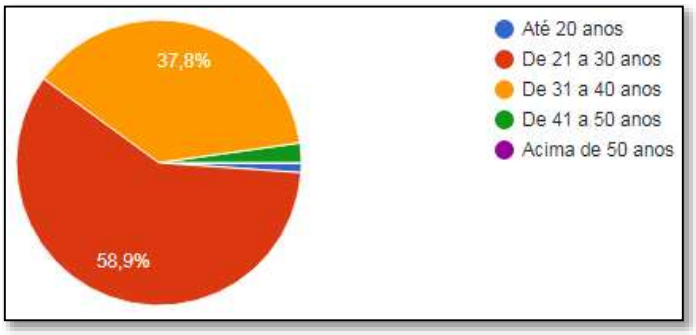
Após a coleta dos dados por meio do questionário e do teste de *phishing*, tem-se a base para analisar as atitudes dos colaboradores da Cooperativa de Crédito Alfa em relação às práticas de engenharia social que podem afetar a manutenção da segurança da informação da entidade. Primeiramente será apresentado os dados obtidos com a aplicação do questionário e, posteriormente, os dados obtidos com o envio do teste de *phishing*.

A amostra do questionário é composta por 90 (noventa) respondentes.

Na primeira sessão, composta por quatro questões, foi possível identificar o perfil dos colaboradores.

O Gráfico 1 demonstra a classificação dos colaboradores por faixa etária.

Gráfico 1 - Idade

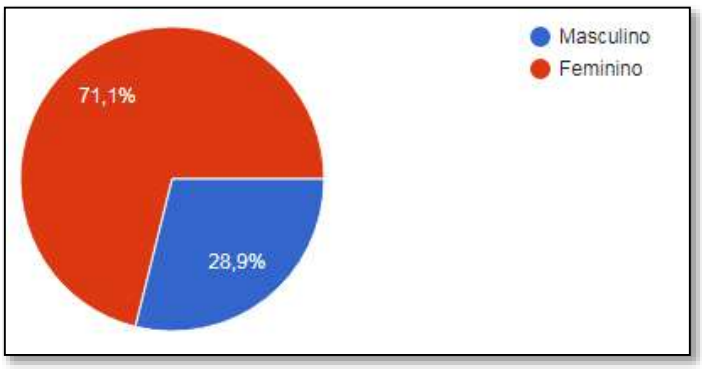


Fonte: Dados da pesquisa (2018).

A faixa etária com maior representatividade foi de 21 a 30 anos de idade, com 58,9%, seguida por 37,8% de 31 a 40 anos e as menos representativas foram 2,2% de 41 a 50 anos e 1,1% para colaboradores de até 20 anos. Portanto, ressalta-se que, a maioria do quadro de funcionários é integrado por jovens e adultos, com idades entre 21 a 40 anos de idade.

O Gráfico 2 demonstra a segregação dos colaboradores por gênero.

Gráfico 2 - Gênero

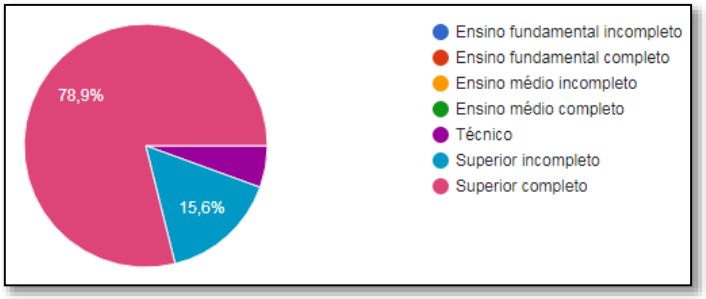


Fonte: Dados da pesquisa (2018).

Dos pesquisados, 71,1% são do sexo feminino e apenas 28,9% do sexo masculino, demonstrando a relevante presença feminina nos quadros da instituição.

O Gráfico 3 se refere ao grau de escolaridade.

Gráfico 3 - Grau de Escolaridade

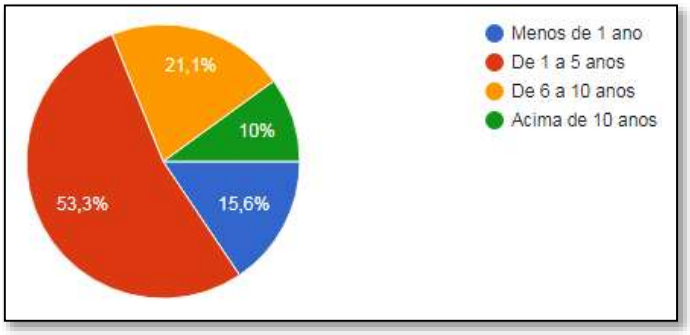


Fonte: Dados da pesquisa (2018).

De acordo com o Gráfico 3, é notória a preocupação da Cooperativa em contratar funcionários que tenham grau de escolaridade acima do ensino médio, já que 78,9% dos respondentes possui nível de formação de ensino superior, 15,6% estão cursando ensino superior e 5,6% possuem o nível técnico.

O Gráfico 4 apresenta o tempo de trabalho na organização.

Gráfico 4 - Tempo de trabalho na Cooperativa



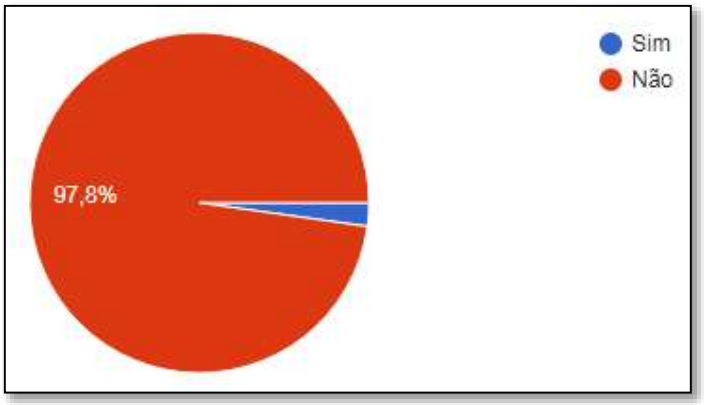
Fonte: Dados da pesquisa (2018).

Por meio do Gráfico 4, os colaboradores em sua maioria, 53,3%, estão na Cooperativa entre 1 a 5 anos e, 15,6% há menos de 1 ano, o que representa uma maioria de funcionários com poucos anos de serviço, pois, se somado as duas faixas, resultam num percentual de 68,9%. Os dados menos expressivos foram 21,1% dos que trabalham de 6 a 10 anos, seguido de apenas 10% com relação aos colaboradores de mais de 10 anos de trabalho na Cooperativa.

A segunda sessão é composta por quatro questões e diz respeito à utilização de senhas.

O Gráfico 5 é relacionado ao compartilhamento de senhas, no qual foi questionado se além do respondente, alguém mais tinha conhecimento das senhas pessoais utilizadas na organização.

Gráfico 5 - Compartilhamento de Senhas

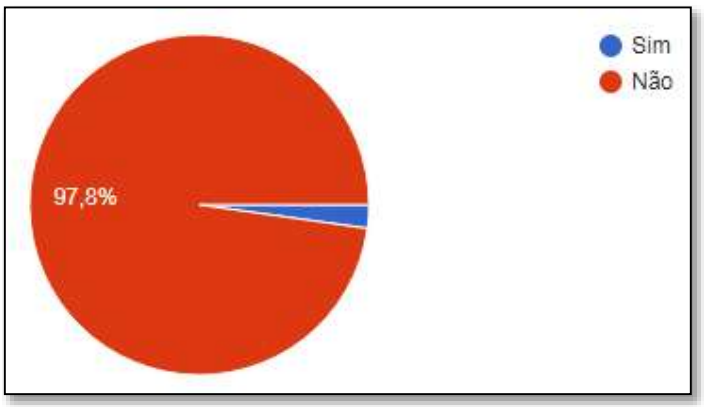


Fonte: Dados da pesquisa (2018).

Por meio do Gráfico 5, é possível verificar que grande parcela dos pesquisados não compartilha suas senhas com outros colegas de trabalho (97,8%), o que é um ponto positivo para a manutenção da Segurança da Informação. Apenas 2,2% compartilham suas senhas com outros colegas, ponto que ainda deve ser melhorado.

O Gráfico 6 diz respeito à utilização de senhas de outros colaboradores, no qual foi perguntado se o respondente utiliza senhas de outro colaborador para acessar aos sistemas e aplicações da organização.

Gráfico 6 - Utilização de Senhas de Terceiros

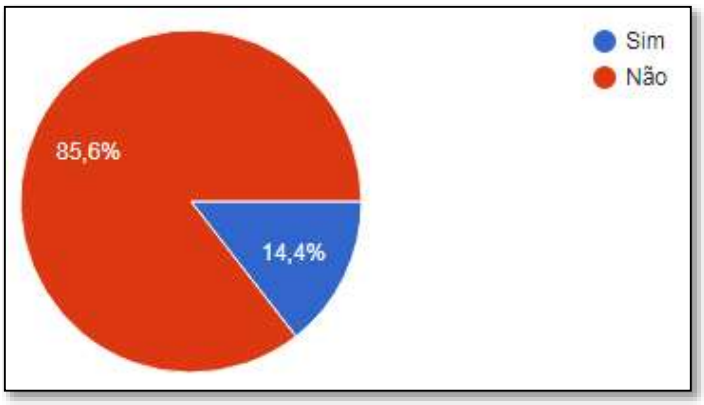


Fonte: Dados da pesquisa (2018).

É evidente, através da observação do Gráfico 6, que a utilização de senhas de terceiros para acesso aos sistemas da organização, é proporcional ao Gráfico 5, onde 97,8% dos colaboradores não utilizam e somente 2,2% alegaram utilizar.

O Gráfico 7 contempla um aspecto importante da Segurança da Informação, que se refere ao local onde são anotadas as senhas. Foi questionado se o colaborador anota suas senhas em alguma agenda ou local próximo ao computador.

Gráfico 7 - Anotações de Senhas

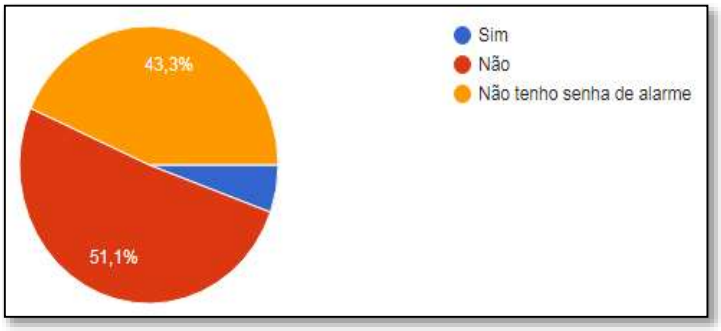


Fonte: Dados da pesquisa (2018).

Quanto a anotação de senhas em agendas ou locais próximos do computador, conforme demonstra o Gráfico 7, apesar da maioria dos respondentes, 85,6%, serem cuidadosos, constata-se que 14,4% dos funcionários adota esta prática, sendo necessário aplicar métodos de conscientização acerca das consequências que isto pode ocasionar, uma vez que cada usuário é responsável pela sua senha, e toda e qualquer alteração nos sistemas serão de responsabilidade do funcionário cadastrado com o *login* que realizou o procedimento.

O questionamento do Gráfico 8 tem a ver com a segurança física, na qual, é perguntado se o colaborador já emprestou a senha de alarme para que um colega pudesse resolver um assunto de emergência.

Gráfico 8 - Compartilhamento da senha de alarme



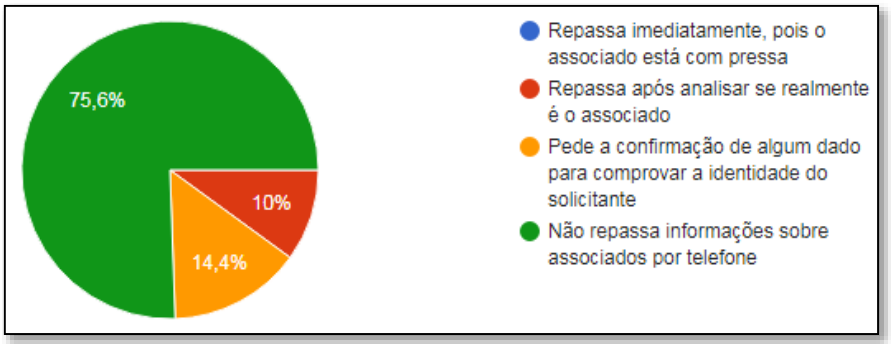
Fonte: Dados da pesquisa (2018).

Referente ao Gráfico 8, não será levado em consideração os 43,3% que responderam não ter senha de alarme, uma vez que, a senha de alarme é designada apenas para colaboradores específicos, como os responsáveis pelos departamentos ou agências, por exemplo. Por outro lado, é identificado que 51,1% dos pesquisados nunca emprestaram a sua senha de alarme para outro colega, contribuindo assim, com a proteção da informação, principalmente voltada ao meio físico. Uma parcela, 5,6%, responderam que já emprestaram sua senha de alarme, ou seja, ainda é necessário reforçar aos colaboradores sobre os riscos que isso pode acarretar para a Cooperativa ou, mesmo para o funcionário que a emprestou. Na ocasião, assim como citado no Gráfico 7, o usuário é o responsável pelas ações da utilização do seu *login.*

A terceira sessão é composta por cinco questões e diz respeito à divulgação de informações.

O Gráfico 9 buscou identificar qual seria a atitude de cada colaborador ao receber uma ligação de um associado (da Cooperativa) solicitando uma informação.

Gráfico 9 - Repasse de informações por telefone



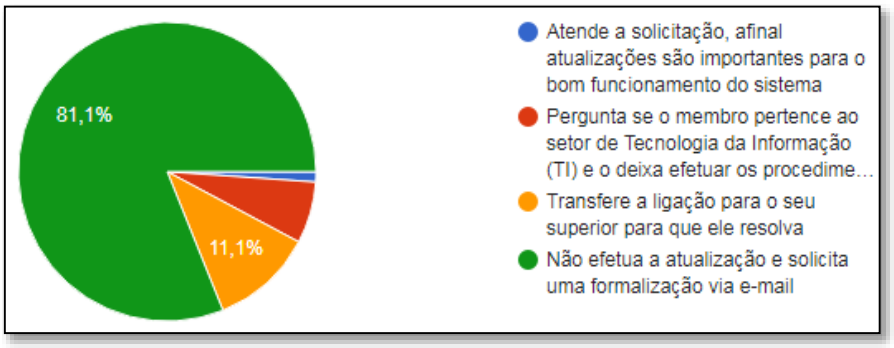
Fonte: Dados da pesquisa (2018).

Entre os pesquisados, de acordo com o Gráfico 9, 75,6% não repassam informações de associados por telefone, o que é considerado um ponto favorável contra ataques de Engenheiros Sociais, pois na maioria das vezes, o golpe acaba sendo bem sucedido por conta da exploração das vulnerabilidades humanas.

Entretanto, em razão dos Engenheiros Sociais terem como característica fundamental a capacidade de se passar por outra pessoa, é identificado um percentual preocupante, de 14,4%, que solicitam a confirmação de algum dado para comprovar a legitimidade do associado e 10% que repassam a informação após analisar se realmente é o associado. Um Engenheiro Social pode ter o conhecimento de informações, inclusive, privadas, acerca de uma determinada pessoa, sendo que o procedimento correto nesse caso, é não passar qualquer informação a respeito de associados por telefone.

Continuando a sessão da divulgação de informações, o Gráfico 10, apresenta o conjunto de dados sobre qual a seria a atitude do colaborador ao receber uma ligação de um membro ligado a Cooperativa que deseja efetuar uma atualização do sistema.

Gráfico 10 - Telefonema para atualizar o sistema



Fonte: Dados da pesquisa (2018).

Conforme disposto no Gráfico 10, é possível interpretar que dos entrevistados, 81,1% não efetua a atualização, solicitando então, uma formalização via *e-mail* para dar continuidade ao pedido. Logo, fica evidente a conscientização da maioria dos colaboradores. Contudo, ainda há uma fragilidade que se deve melhor trabalhar para evitar eventuais consequências, a de 6,7%, sendo a parcela de colaboradores que perguntam se o membro pertence ao setor de TI, para finalmente permitir que a atualização seja feita. Isso é um risco à organização, pois engenheiros sociais podem se disfarçar de um funcionário da empresa e aplicar o golpe.

Continuando com a análise do Gráfico 10, foi obtido que 11,1% dos respondentes não sabem o que fazer nessa situação e transferem a ligação para o seu superior, ainda que em um primeiro momento esta resposta não aparente ser tão importante quanto a prevenção de golpes de Engenharia Social, através dela se demonstra que uma pequena parte dos funcionários não tem a noção de como lidar com a situação perante um engenheiro social e, ao transferir a ligação, está aumentando as chances de um ataque ser bem sucedido, pois, o colega em questão, pode não ter o preparo necessário para evitar o ataque. Por fim, apenas 1,1% responderam que atenderiam à solicitação sem questionar.

O Gráfico 11, diz respeito a um *e-mail* do setor de TI que solicita informações para cadastrar no sistema, para isso é preciso clicar no *link* presente no *e-mail*.

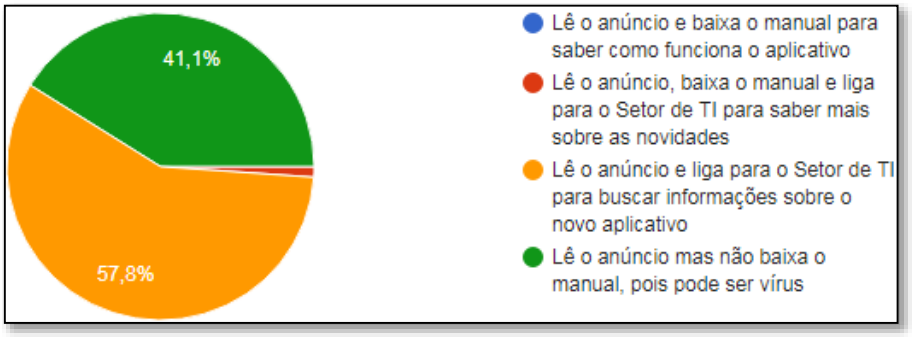
Gráfico 11 - Recebimento de *e-mail* com *link*

Fonte: Dados da pesquisa (2018).

Conforme o Gráfico 11, nota-se que 94,4% dos usuários analisam o endereço de *e-mail* e a assinatura para atender ao pedido, fator relevante na proteção das Informações. Já 3,3%, clicam no *link* com o intuito de saber quais dados estão sendo solicitados, um ponto que deve ser melhorado, devido ao risco de submeter-se a um vírus somente pelo ato de clicar no endereço. Para 2,2%, a confiança no setor de TI faz com que todo e qualquer *e-mail* que represente ser do tal departamento, seja atendido sem questionamento prévio. Por menor que seja o percentual, a sua existência sempre será significativa para a manutenção da segurança da informação, uma vez que fraudadores se baseiam em várias características de um remetente confiável para persuadir a vítima.

O Gráfico 12 demonstra a atitude dos colaboradores ao receber um *e-mail* de uma entidade relacionada à Cooperativa divulgando um novo aplicativo para controle de finanças, sendo que para visualizar o manual de como o aplicativo funciona, é necessário baixar o arquivo anexado.

Gráfico 12 - Recebimento de *e-mail* com anexo



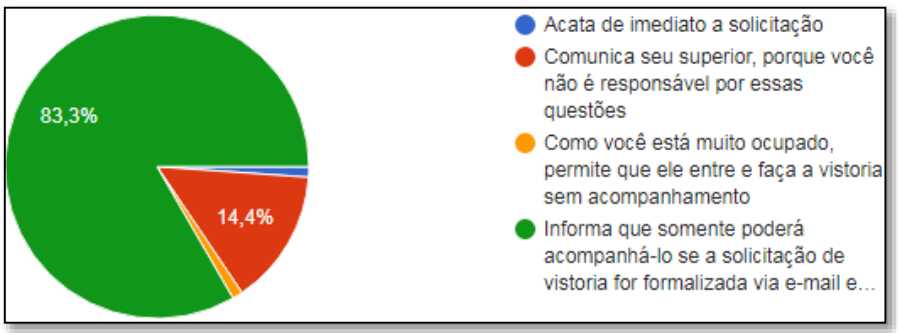
Fonte: Dados da pesquisa (2018).

Por meio do Gráfico 12, é ilustrado que 57,8% dos usuários leem o anúncio e ligam para o setor de TI com o objetivo de buscar mais informações. Embora a resposta não seja considerada errada, devido a não baixarem o anexo, o problema está no fato de que os responsáveis pelos anúncios de novos aplicativos ou sistemas, são do departamento de TI ou, responsáveis por aquele produto na qual o aplicativo tem relação.

Na pesquisa, 41,1% informaram que não baixam o manual, pois pode ser vírus, sendo a resposta correta para a proteção das informações e, somente 1,1% baixam o manual ligando posteriormente, para o setor de TI para saber mais a respeito do aplicativo. Apesar de pequeno, este percentual de 1,1% pode comprometer a todos com a negligência de não se atentar aos riscos que anexos suspeitos podem trazer, como por exemplo, infectar a rede com um vírus.

O Gráfico 13 se refere à segurança física. Foi perguntado qual seria a atitude tomada pelo pesquisado ao receber uma solicitação de um bombeiro para acompanhá-lo a uma vistoria pelas dependências da organização.

Gráfico 13 - Acompanhamento de terceiros



Fonte: Dados da pesquisa (2018).

Por meio do Gráfico 13, é visível que grande parte da amostra está consciente da atitude correta quanto a essa questão, já que 83,3% dos pesquisados responderam que só acompanham o bombeiro pelas dependências da organização após a solicitação ser formalizada por e-mail e aprovada pelo setor responsável. Outra parcela, 14,4%, responderam que não são responsáveis por essas questões e repassam para o superior resolver, o que não estaria incorreto, porém, cabe frisar, que todos devem estar cientes dos procedimentos e formalizações necessárias para um terceiro transitar no prédio. Apesar de a maioria ter conhecimento a respeito da segurança física, 2,2% dos respondentes está agindo de forma equivocada, ao ponto de que 1,1% acataria de imediato à solicitação, sem verificar se a pessoa realmente era um bombeiro e 1,1% permitiria que o bombeiro fizesse a vistoria sozinho, caso o respondente estivesse ocupado. Os dois últimos comportamentos resultariam em consequências para a segurança física da organização.

A quarta sessão do questionário foi relativa aos incidentes ocorridos sobre a segurança da informação.

A primeira pergunta foi aberta e visava identificar se os respondentes já haviam sido vítimas de pessoas mal intencionadas tentando extrair informações confidenciais relacionadas à Cooperativa e solicitava uma breve descrição do ato. Para tal, obteve-se 11 (onze) respostas positivas, sendo que, para 1 (uma), não foi especificado o ato. As 10 (dez) descrições de tentativa de golpe foram:

Quadro 2 - Descrições de tentativas de golpe

1	Tentativa de extrair informações financeiras e cadastrais de associados.
2	Tentativa de manter contato com os caixas para pedir informações sobre transferência de valores.
3	Solicitação de saldos, dívidas e solicitação de empréstimos de INSS.
4	A pessoa ligou se passando por um associado e precisava que desbloqueasse seu cartão.
5	Uma ligação se passando pela Central de Suporte, e queria manter contato com o caixa, tesoureiro ou gerente.
6	Uma ligação solicitando falar com o tesoureiro para realizar uma TED.
7	Uma ligação para efetuar transferência no caixa de uma conta de terceiro.
8	Ligações tentando fazer transferências bancárias.
9	Golpe da transferência.
10	Tentativa de fraude de INSS.

Fonte: Dados da pesquisa (2018).

A segunda pergunta também foi aberta, e se direcionou aos respondentes que já haviam sido vítimas de tentativas de golpe, e solicitava a descrição da atitude tomada quando ocorreu o caso. As respostas da segunda questão estão organizadas conforme a enumeração do quadro da primeira questão.

Quadro 3 - Atitudes tomadas ao ser vítima de tentativa de golpe

1	Seguindo procedimentos e normas, não foram repassadas as informações solicitadas.
2	Manteve o posicionamento relativo a não passar ligações para os caixas.
3	Informou que não era possível realizar este tipo de atendimento via telefone e que a Cooperativa possui canais de atendimento para tal situação, bem como, poderiam procurar a agência mais próxima. A respeito do empréstimo INSS, foi solicitado documentação, porém não retornaram mais.
4	Informou que o procedimento deveria ser feito somente via 0800.
5	Informou que não iria passar a ligação para os caixas, e que o fraudador poderia falar qual era o assunto. Ele insistiu várias vezes, xingou e desligou o telefone.
6	Desligou o telefone.
7	Não foi repassada a ligação para o caixa, pois o caixa não pode atender ligações e desligou o telefone.
8	Repassou a ligação para o gerente da agência.
9	Desligou o telefone e avisou o Setor de TI.
10	Solicitou a confirmação dos dados.

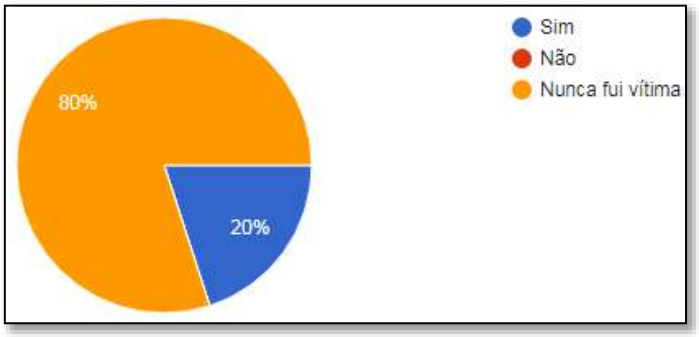
Fonte: Dados da pesquisa (2018).

Ademais, o respondente que não descreveu o caso, afirmou na segunda questão que não repassou nenhuma informação.

Pode-se afirmar que, mesmo sendo poucas as tentativas de golpe até então registradas, os colaboradores agiram de forma correta para proteger a informação da Cooperativa e de seus associados.

A terceira questão foi fechada e visava identificar, para os casos de fraudes ocorridos, se as vítimas haviam repassado a situação aos responsáveis pela Segurança da Informação, para servir de alerta a outros colaboradores.

Gráfico 14 - Alerta aos colegas



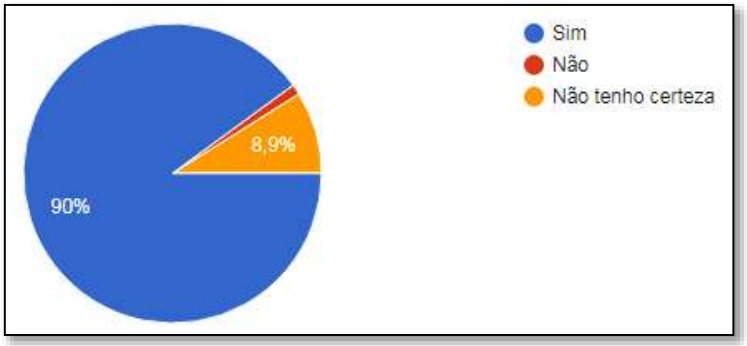
Fonte: Dados da pesquisa (2018).

De acordo com o Gráfico 14, 20% dos pesquisados reportaram ao Setor de TI o ocorrido e 80% afirmaram nunca terem sofrido qualquer tentativa de golpe.

Observa-se uma discrepância de dados em relação às duas questões anteriores desta sessão, na qual apenas 11 (onze) respondentes afirmaram terem sido vítimas, e para esta terceira questão o total de 20% está englobando 18 (dezoito) respondentes, que, para afirmarem que repassaram ao Setor de TI informações sobre a tentativa de golpe, obrigatoriamente deveriam ter sido vítimas.

A quinta sessão está composta de quatro (4) perguntas. No Gráfico 15, o objetivo é identificar se os usuários têm conhecimento das informações que são indispensáveis para o negócio da empresa.

Gráfico 15 - Informações indispensáveis para o negócio



Fonte: Dados da pesquisa (2018).

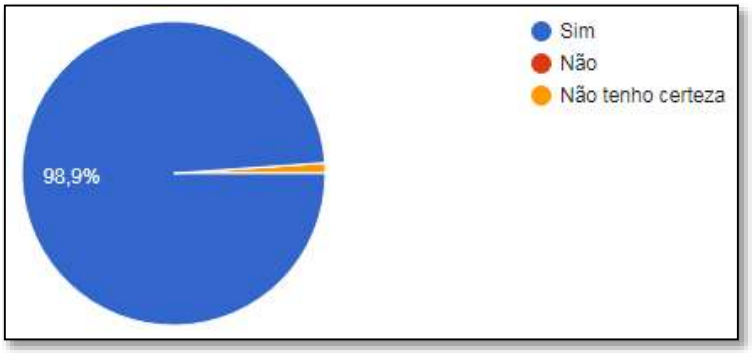
No Gráfico 14, 8.9% dos usuários responderam que não tem certeza de quais informações são vitais para o negócio da organização e somente 1,1% respondeu não saber. Por se tratar de uma instituição financeira, grande parte das informações são confidenciais e no caso de perda ou, alteração indevida desses dados, o negócio da instituição sofrerá impactos negativos. Exemplo: se o extrato de um associado é exposto ao público, a imagem

da Cooperativa estará comprometida, fazendo com que outros associados percam a confiança do trabalho prestado pela organização e consequentemente, resultando no encerramento ou transferência de suas contas. Portanto, é fundamental que todos os usuários tenham conhecimento de quais dados são importantes para a continuidade dos negócios e para a credibilidade da Cooperativa.

O percentual mais expressivo foi de 90% que alegaram ter conhecimento de quais informações são vitais para o negócio da empresa.

Dando andamento à quinta sessão, o Gráfico 16 apresenta os resultados da pergunta sobre se a Cooperativa disponibiliza orientação sobre a divulgação de informação.

Gráfico 16 - Orientação sobre a divulgação de informação



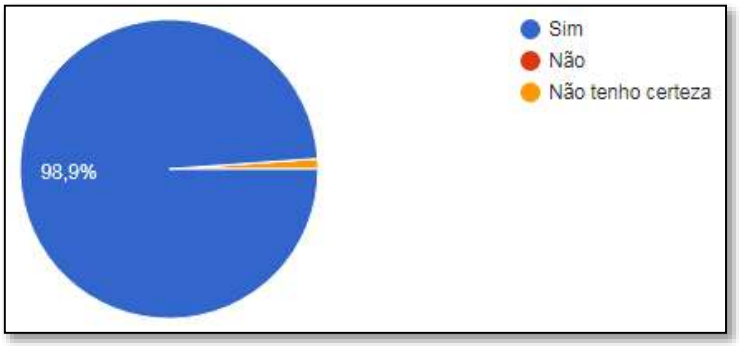
Fonte: Dados da pesquisa (2018).

Foi coletado através da pesquisa ilustrada no Gráfico 16, que 98,9% dos usuários afirmam que a Cooperativa efetua orientações acerca da divulgação de informação.

Em contrapartida, apenas 1,1% não tem certeza se a Cooperativa faz esse tipo de orientação. Nesse caso, um reforço na campanha de conscientização poderá elevar o percentual, facilmente, aos 100%.

O Gráfico 17 teve como finalidade questionar aos usuários se a Cooperativa tem uma Política de Segurança da Informação.

Gráfico 17 - Existência de uma Política de Segurança da Informação

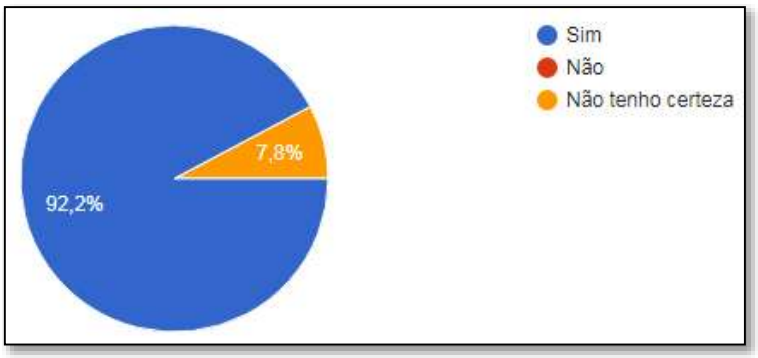


Fonte: Dados da pesquisa (2018).

Mediante o Gráfico 17, é evidente que a grande maioria dos colaboradores tem conhecimento da existência da Política, sendo um total de 98,9%, contra apenas 1,1% alegando não ter certeza. Assim como citado a respeito do Gráfico 16, para sanar este percentual de 1,1%, é necessário um reforço na campanha de conscientização acerca da Segurança da Informação.

A próxima questão exemplificada por meio do Gráfico 18, perguntou se a Cooperativa possui controle de acesso físico para os prestadores de serviço.

Gráfico 18 - Existência de um controle de acesso físico



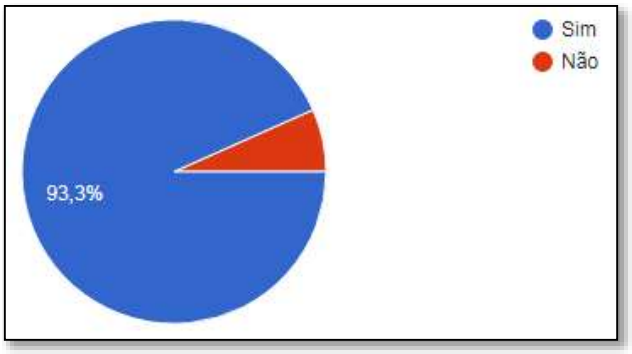
Fonte: Dados da pesquisa (2018).

Dos que responderam à pesquisa, 92,2% confirmaram saber da existência deste documento. Aspecto positivo na manutenção da Segurança Física, uma vez que este documento tem como finalidade registrar os dados pessoais do prestador de serviço, a data e horário do atendimento, o serviço realizado e o nome do funcionário que o acompanhou. Os usuários que responderam não ter certeza, correspondem a 7,8%, o que demonstra um risco à Segurança, pois, se os funcionários não têm certeza, podem deixar alguém entrar sem a devida autorização e acompanhamento.

A sexta e última sessão apresentou quatro perguntas quanto ao acesso às informações. Sendo dividida em duas partes, a primeira sobre o comportamento do usuário e as duas seguintes, acerca da opinião pessoal do colaborador.

A primeira questão da sexta sessão está ilustrada no Gráfico 19. A pergunta é, se ao sair, o usuário costuma deixar a mesa limpa, sem papéis importantes.

Gráfico 19 - Mesa sem papéis importantes

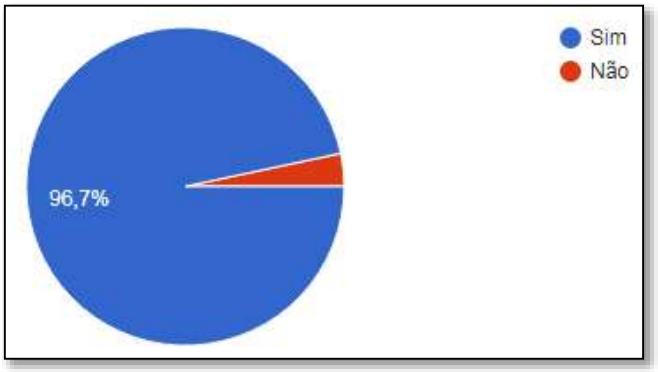


Fonte: Dados da pesquisa (2018).

No exposto pelo Gráfico 19, para 6,7% dos colaboradores, deixar papéis importantes sobre a mesa ainda é um hábito corriqueiro. Por outro lado, a maioria dos colaboradores, 93,3% não adota esta prática que pode trazer riscos a organização.

Na segunda questão foi perguntado se ao sair do ambiente de trabalho, o colaborador deixava seu computador bloqueado, impedindo assim, o acesso de terceiros às suas informações.

Gráfico 20 - Bloqueio da estação de trabalho

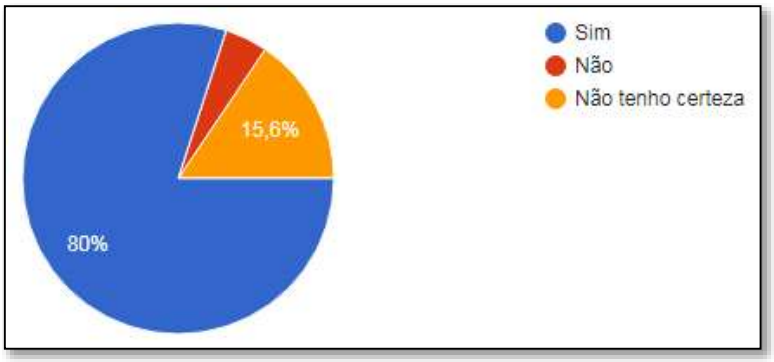


Fonte: Dados da pesquisa (2018).

Conforme a pesquisa, 96,7% costumam bloquear a estação de trabalho, enquanto 3,3% afirmaram não fazer o procedimento. Evidencia-se que a maior parte dos colaboradores está atenta à proteção de seus dados, em contrapartida, ainda há uma parcela que não está seguindo rigorosamente os conceitos de Segurança da Informação.

O Gráfico 21 representa a terceira questão que buscou avaliar se na opinião do funcionário, todos os demais colaboradores do mesmo setor sabem a importância das informações da Cooperativa.

Gráfico 21 - Importância das informações



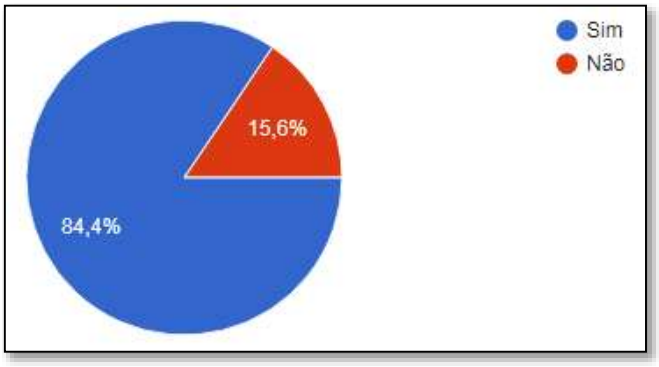
Fonte: Dados da pesquisa (2018).

Ainda que a resposta a esta pergunta seja uma questão de concepção, é importante levá-la em consideração, pois o engenheiro social obtém sucesso na maior parte das vezes, explorando pessoas com poucas informações, para posteriormente, alcançar às pessoas que verdadeiramente possuem o conhecimento acerca das informações importantes.

Dos pesquisados, 80% tem certeza de que todos os colaboradores de seu setor estão cientes da importância das informações, 15,6% não tem certeza e 4,4% afirmaram que nem todos têm conhecimento sobre o valor que as informações da Cooperativa possuem. Deste modo, se compreende que ainda deve ser disseminada essa concepção entre todos, para que haja um aprendizado mútuo, a fim de evitar que informações, muitas vezes consideradas irrelevantes por alguns indivíduos, possam trazer prejuízos para a imagem e credibilidade da Cooperativa.

A última questão, teve como propósito, perguntar se na opinião do colaborador, seria difícil que pessoas externas conseguissem informações importantes da Cooperativa.

Gráfico 22 - Divulgação das informações



Fonte: Dados da pesquisa (2018).

Apesar de 84,4% responderem que seria difícil o roubo de informações importantes da Cooperativa, o percentual de 15,6% faz com que a organização passe a impressão de que não está oferecendo a devida segurança às suas informações, pois elas podem ser fornecidas por *e-mail*, telefone ou pessoas entrando na Cooperativa. A atenção com relação a isso deve ser melhorada.

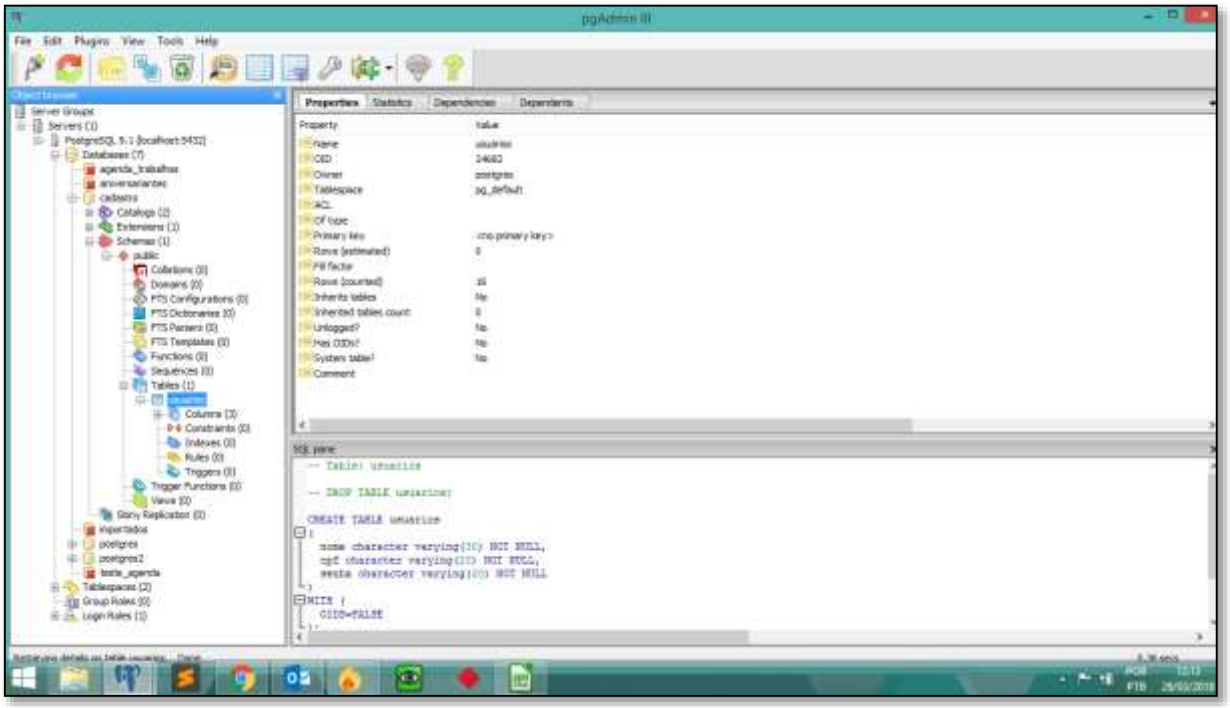
4.2.2 Teste de *phishing*

O segundo mecanismo de coleta de dados, foi por meio de um teste de *phishing.* O teste foi um pseudo *e-mail* enviado aos colaboradores da Cooperativa e tinha como finalidade, averiguar quantos usuários cairiam no golpe.

Primeiramente, se implementou um código em *PHP* e *HTML*, cujo foco era a criação de um formulário simples. Neste formulário, era possível cadastrar o nome, CPF e a senha. Após o cadastramento das informações, estas eram armazenadas no banco de dados com a utilização do *PostgreSQ*L.

No banco de dados, foi criado um *database* com uma tabela denominada “usuários”, possuindo três colunas: nome, CPF e senha. O *database* é apresentado na Figura 8.

Figura 8 - *Database*



Fonte: Dados da pesquisa (2018).

Após os devidos testes quanto à eficiência do programa, foi então enviado o *e-mail* para todos os colaboradores da Cooperativa, conforme ilustrado na Figura 9.

Figura 9 - Falso *E-mail*

De: tecnologia [tecnologia[redacted]@gmail.com]
Enviado: quarta-feira, 28 de março de 2018 10:57
Para: todos@[redacted].coop.br
Assunto: Atualização de Usuários

Bom dia, Pessoal!

Estamos atualizando a lista de usuários do sistema, informe os dados solicitados no link abaixo para que possamos efetuar as atualizações necessárias.

http://ti:8080/tecnologia

Atenciosamente,

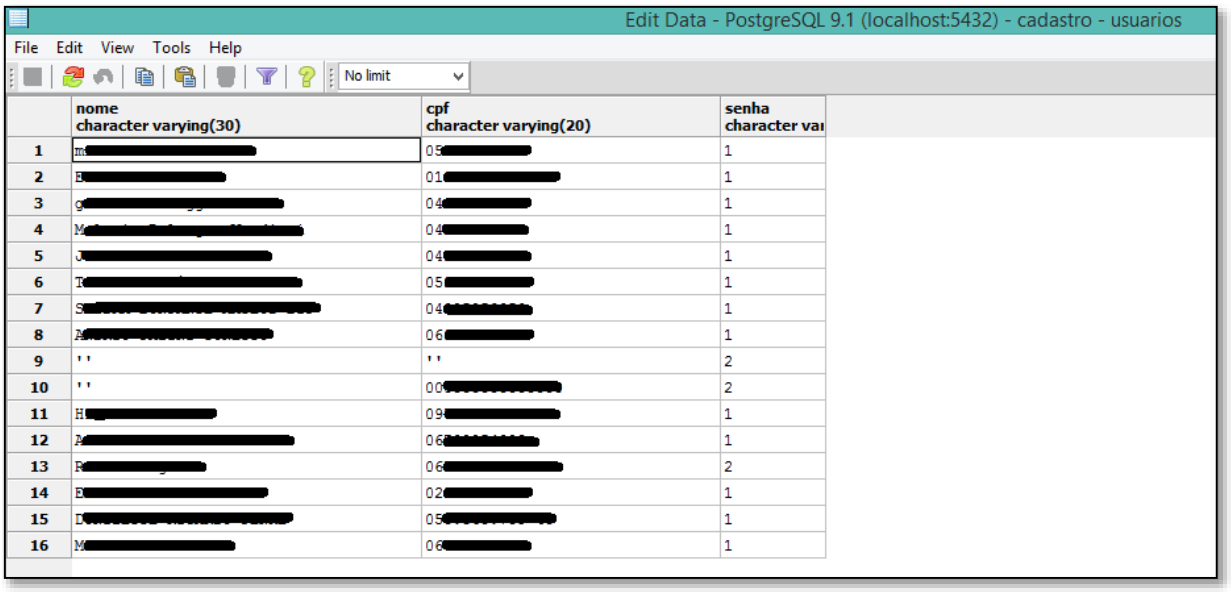
Setor de Tecnologia da Informação

Fonte: Dados da pesquisa (2018).

Se o *e-mail* for analisado com um pouco de atenção, se pode notar que o remetente não faz parte do domínio que a Cooperativa utiliza, sendo o correto o "coop.br", ao invés de "gmail.com". Além do mais, o *e-mail* não contém assinatura, impedindo assim, saber qual o nome e departamento da pessoa que o enviou e, o *link* inserido no corpo do *e-mail*, não é uma mensagem interativa com o usuário, fazendo com que seja mais um ponto a se suspeitar.

O total de usuários que foram vítimas do falso golpe foi de 16 (dezesseis) pessoas, ilustradas por meio da Figura 10.

Figura 10 - Tabela de usuários



	nome character varying(30)	cpf character varying(20)	senha character var
1	[redacted]	[redacted]	1
2	[redacted]	[redacted]	1
3	[redacted]	[redacted]	1
4	[redacted]	[redacted]	1
5	[redacted]	[redacted]	1
6	[redacted]	[redacted]	1
7	[redacted]	[redacted]	1
8	[redacted]	[redacted]	1
9	''	''	2
10	''	[redacted]	2
11	[redacted]	[redacted]	1
12	[redacted]	[redacted]	1
13	[redacted]	[redacted]	2
14	[redacted]	[redacted]	1
15	[redacted]	[redacted]	1
16	[redacted]	[redacted]	1

Fonte: Dados da pesquisa (2018).

Vale ressaltar que por questão de ética, o programa não foi construído para mostrar a senha dos usuários. Sendo assim, os usuários que não digitaram a senha, independente de terem cadastrado o nome ou CPF, o código atribuído na coluna "senha" da tabela foi 2 (dois) e, os que cadastraram a senha, o código foi 1 (um).

Dos que foram vítimas do golpe, 13 (treze) digitaram todas as informações (nome, CPF e senha), 1 (um) apenas digitou nome e CPF, mas não a senha, 1 (um) informou somente o CPF, e 1 (um) apenas abriu o formulário e enviou sem cadastrar as informações.

5 CONSIDERAÇÕES FINAIS

O objetivo desta pesquisa, foi identificar as atitudes dos colaboradores de uma Cooperativa de Crédito localizada no Sul de Santa Catarina em relação às práticas de engenharia social que podem afetar a manutenção da segurança das informações da entidade. Pode-se afirmar que o objetivo foi atingido, por meio dos objetivos específicos estabelecidos e da metodologia aplicada.

Primeiramente, foram apresentados os elementos que integram a segurança da informação no ambiente corporativo. Desta maneira, foram explanados os conceitos físicos, lógicos e humanos da segurança da informação. Para tal, foi abordado a teoria pertinente à definição de informação, ativos de informação, segurança da informação nas organizações, seus princípios básicos e a política de segurança da informação, além de destacar as ameaças e vulnerabilidades encontradas no ambiente corporativo.

Depois, foram expostas as características da Engenharia Social aplicada às organizações. Foi apresentado o conceito de Engenharia Social, o perfil que os engenheiros sociais possuem, as vulnerabilidades humanas exploradas por eles e os métodos utilizados para os ataques.

Simultaneamente aos conteúdos de Segurança da Informação e Engenharia Social elucidados, foi destacada a importância de administrar os componentes da segurança da informação, sejam estes físicos, lógicos e, principalmente humanos. A Engenharia Social explora, em sua maioria, as vulnerabilidades dos indivíduos, com o intuito de obter dados confidenciais para utilizá-los em seu benefício ou, simplesmente, para causar algum tipo de dano. É fundamental que as organizações conscientizem todos seus colaboradores a respeito das consequências que a divulgação indevida de dados pode acarretar, sobretudo voltando a sua política interna para a redução dos índices de fraudes e golpes.

Em análise às atitudes do colaboradores e identificação dos pontos negativos e positivos, foi constatado que, embora a maior parte dos funcionários aja de acordo com as normas de segurança de informação, uma parcela ainda adota hábitos incorretos, os quais podem ser prejudiciais à Cooperativa.

Alguns pontos a serem melhorados se referem ao compartilhamento de senhas com outros colegas de trabalho e anotações de senhas em locais próximos à mesa de trabalho. Outra característica observada, é sobre o repasse de informações por telefone, em que houve um alto percentual de funcionários que solicitam a confirmação de dados e depois repassam a

informação, entretanto, pode-se tratar de um golpe proveniente de Engenharia Social, no qual o fraudador pode ter em posse, os dados de um associado.

Além disso, um aspecto que precisa ser trabalhado é em relação à conscientização sobre os *phishing*, pois tanto no questionário e, principalmente, no teste de *phishing* aplicado, há um percentual preocupante de funcionários que clicam em *links* ou baixam anexos antes de confirmar sua autenticidade, o que pode comprometer seriamente à rede corporativa e, consequentemente, colocar toda a organização sob risco.

Quanto às limitações da pesquisa, ressalta-se que, por se tratar de um estudo de caso, os resultados obtidos aplicam-se apenas ao objeto de estudo e, portanto, não podem ser utilizados para análises e interpretações de outras organizações.

Sugere-se que, com base nessa pesquisa, sejam replicados estudos em outras instituições financeiras ou, até mesmo, organizações de outros segmentos, visando identificar quais aspectos são importantes para a Segurança da Informação, com ênfase na prevenção de ataques de Engenharia Social. Atrelado a isso, é relevante analisar quais públicos podem estar mais propensos aos ataques de Engenharia Social, como forma de identificar e propor métodos de conscientização voltados aos públicos mais vulneráveis.

REFERÊNCIAS

ABNT NBR ISO/IEC 17799:2005. **Tecnologia da informação:** código de prática para a gestão da informação. ABNT, 2005. Disponível em < http://www.aulasemparedes.com.br/wp-content/uploads/2014/09/215545813-ABNT-NBR-177991.pdf> Acesso em: 05 mar. 2018.

ABNT NBR ISO/IEC 27001:2013. **Tecnologia da informação:** sistema de gestão da segurança da informação. ABNT, 2013.

ABNT NBR ISO/IEC 27002:2013. **Tecnologia da informação:** código de prática para controles de segurança da informação. ABNT, 2013. Disponível em: < http://www.fieb.org.br/download/senai/NBR_ISO_27002.pdf>. Acesso em: 05 mar. 2018.

ABS JUNIOR, José Tenório; BARCAROLI, Velcir. **Engenharia social e a aleatoriedade na escolha do alvo.** UCEFF: Tecnológica, Revista Científica. v. 5, n. 2. 2016. Disponível em: < https://uceff.edu.br/revista/index.php/revista/article/view/155 >. Acesso em: 22 mar. 2018.

ADACHI, Tomi. **Gestão de segurança em internet banking:** estudo de casos brasileiros. 2004. 130 f. Dissertação (Mestrado) - Curso de Administração de Empresas, Fundação Getúlio Vargas, São Paulo, 2004. Disponível em: <http://bibliotecadigital.fgv.br/dspace/handle/10438/2339>. Acesso em: 15 dez. 2004.

AIELLO, Michael. Social engineering. In: JANCZEWSKI, Lech J.; COLARIK, Andrew M. **Cyber warfare and cyber terrorism.** New York: Information Science Reference, 2008. Cap. 24. p. 191-198.

ALEXANDRIA, João Carlos Soares. **Gestão da segurança da informação:** uma proposta para potencializar a efetividade da segurança da informação em ambiente de pesquisa científica. Tese (Doutorado) – Instituto de Pesquisas Energéticas e Nucleares, São Paulo. 2009.

AVIZIENIS, J.-C. et al. **Basic concepts and taxonomy of dependable and secure computing. Dependable and secure computing**, 2004. Disponível em < https://www.nasa.gov/pdf/636745main_day_3-algirdas_avizienis.pdf> Acesso em 08 de Março de 2018

BASTA, Alfred; BASTA, Nadine; BROWN, Mary. **Segurança de computadores e teste de invasão**. Tradução Lizandra Magon de Almeida. São Paulo: Cengage Learning, 2014.

BAZZOTTI, Cristiane; GARCIA, Elias. **A importância do sistema de informação gerencial na gestão empresarial para tomada de decisões.** Revista Unioeste, 2006. Disponível em < http://e-revista.unioeste.br/index.php/csaemrevista/article/view/368/279>Acesso em: 04 de Março de 2018.

BEAL, Adriana. **Segurança da informação:** princípios e melhores práticas para a proteção dos ativos de informação nas organizações. São Paulo: Atlas, 2008. 175 p.

CARUSO, Carlos A. A.; STEFFEN, Flávio Deny. **Segurança em informática e de informações.** 2.ed. São Paulo: SENAC/SP, 1999. 367 p.

DANTAS, Marcus Leal. **Segurança da informação:** uma abordagem focada em gestão de riscos. Olinda: Livro Rápido, 2011. 152 p. Disponível em: < http://www.marcusdantas.com.br/files/seguranca_informacao.pdf >. Acesso em: 5 de Março de 2018.

DIAS, Cláudia. **Segurança e auditoria da tecnologia da informação**. Rio de Janeiro: Axcel Books do Brasil, 2000. 218 p.

ENGEBRETSON, Patrick. **The basics of hacking and penetration testing:** ethical hacking and penetration testing made easy. USA: Syngress, 2011. 178 p.

FILHO, Antônio Mendes da Silva. **Entendendo e evitando a engenharia social:** protegendo sistemas e informações. 2009. Disponível em <http://softwarelivre.org/brasil/entendendo-e-evitando-a-engenharia-social-protegendo-sistemas-e-informacoes>. Acesso em: 03 de Março de 2018.

FONSECA, Paula Fernanda. **Gestão de Segurança da Informação: O Fator Humano.** 2009. 16 f. Monografia (Especialização) - Curso de Pós Graduação em Redes e Segurança de Computadores, Pontifícia Universidade Católica do Paraná, Curitiba, 2009. Disponível em: <https://www.ppgia.pucpr.br/~jamhour/RSS/TCCRSS08A/Paula Fernanda Fonseca - Artigo.pdf>. Acesso em: 14 mar. 2018.

FONTES, Edison. **Segurança da informação:** o usuário faz a diferença. São Paulo: Saraiva, 2006. xvi, 172 p.

GABBAY, Max. **Fatores influenciadores da implementação de ações de gestão de segurança da informação:** um estudo com executivos e gerentes de tecnologia da informação em empresas do Rio Grande do Norte. 170 f. Tese (Doutorado) – Universidade Federal do Rio Grande do Norte, Rio Grande do Norte, 2003. Disponível em: < http://repositorio.ufrn.br:8080/jspui/bitstream/123456789/14985/1/Max%20Simon%20Gabbay.pdf >. Acesso em: 07 mar. 2018.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa.** 4. ed. São Paulo: Atlas, 2002. 175 p.

GRAGG, David. **A multi-level defense against social engineering.** SANS Institute, 2002. Disponível em: <https://www.sans.org/reading-room/whitepapers/engineering/multi-level-defense-social-engineering-920>. Acesso em: 22 mar. 2018.

HADNAGY, C. **Social engineering**: the art of human hacking. Indianápolis: Willey Publishing Inc., 2011.

KUROSE, James F.; ROSS, Keith W. **Redes de computadores e a Internet**: uma abordagem top-down. Tradução Daniel Vieira; revisão técnica Wagner Luiz Zucchi. 6. ed. São Paulo: Pearson Education do Brasil, 2013.

MICROSOFT SECURITY AND PROTECTION CENTER (Eua) (Org.). **Microsoft Security Intelligence Report.** 22. ed. Redmond: Microsoft Corporation, 2017. 74 f. Disponível em: <https://www.microsoft.com/pt-br/security/Intelligence-report>. Acesso em: 23 mar. 2018.

MITNICK, Kevin D.; SIMON, William L. **A arte de enganar: ataques de hackers:** controlando o fator humano na segurança da informação. Tradução: Kátia Aparecida Roque. São Paulo: Pearson Education, 2003

NETTO, Abner da Silva; SILVEIRA, Marco Antonio Pinheiro da. **Gestão da segurança da informação:** fatores que influenciam sua adoção em pequenas e médias empresas. JISTEM J.Inf.Syst. Technol. Manag. (Online) vol.4 no.3 São Paulo, 2007

PARSONS, Kathryn et al. Human factors and information security: individual, culture and security environment. **Command, Control, Communications And Intelligence Division: DSTO Defence Science and Technology Organisation.** Edinburgh, p. 1-54. out. 2010. Disponível em: <https://pdfs.semanticscholar.org/07f8/c87e6bb79ffb3ad846168a641dc750cb85e8.pdf>. Acesso em: 23 mar. 2018.

PEIXOTO, Mário César Pintaudi. **Engenharia Social & Segurança da Informação na Gestão Corporativa**. 1ª ed. Rio de Janeiro: Brasport, 2006. 132 p.

PORTAL IPNEWS. **Serviços financeiros é o maior afetado por crimes virtuais, segundo Accenture.** 2018. Disponível em: <https://ipnews.com.br/servicos-financeiros-e-o-maior-afetado-por-crimes-virtuais-segundo-accenture/>. Acesso em: 14 abr. 2018.

RICHARDSON, Roberto Jarry. **Pesquisa social:** métodos e técnicas. 3. ed. São Paulo: Atlas, 1999.

ROWE, Neil C; CUSTY, E. John. Deception in cyber attacks. In: JANCZEWSKI, Lech J.; COLARIK, Andrew M. **Cyber warfare and cyber terrorism.** New York: Information Science Reference, 2008. Cap. 12. p. 91-96.

SCHNEIER, Bruce. **Segurança.com**: segredos e mentiras sobre a proteção na vida digital. Rio de Janeiro: Campus, 2001.

SÊMOLA, Marcos. **Gestão da segurança da informação:** uma visão executiva. Rio de Janeiro: Campus, 2003. 156 p.

SILVA, Narjara Bárbara Xavier; ARAÚJO, Wagner Junqueira de; AZEVEDO, Patrícia Morais de. **Engenharia social nas redes sociais *online:*** um estudo de caso sobre a exposição de informações pessoais e a necessidade de estratégias de segurança da informação. Revista ibero-americana de ciência da informação. V. 6. N. 2. 2013.

SILVA, Pedro A. Lemes da. **Análise de Redes Sociais aplicada à Engenharia Social.** 2012. 11 f. TCC (Graduação) - Curso de Segurança da Informação, Faculdade de Tecnologia de Guaratinguetá, Guaratinguetá, 2012. Disponível em: <http://rabci.org/rabci/sites/default/files/Artigo_ARS_e_ES.pdf>. Acesso em: 14 mar. 2018.

SYMANTEC CORPORATION. **Norton Cyber Security Insights Report 2016.** Disponível em: <https://www.symantec.com/content/dam/symantec/br/docs/reports/2016-norton-cyber-security-insights-comparisons-brazil-pt.pdf>. Acesso em: 14 abr. 2018.

WHITMAN, Michael E.; MATTORD, Herbert J. **Principles of information security.** 4ª ed. Boston: Course Tecnology, 2012. 656 p.

WORKMAN, Michael. Wisecrackers: a theory-grounded investigation of phishing and pretext social engineering threats to information security. **Journal Of The American Society For Information Science And Technology.** Melbourne, p. 1-13. jan. 2008. Disponível em: <https://pdfs.semanticscholar.org/6b4d/cbc51e891aa7a79b054dcf518d3f5f293572.pdf>. Acesso em: 24 mar. 2018.