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

GABRIELA CRISTINA RODRIGUES

A BRECHA HUMANA DA SEGURANÇA DA INFORMAÇÃO:
ENGENHARIA SOCIAL E POLÍTICAS DE SEGURANÇA

Americana, SP
2018

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

GABRIELA CRISTINA RODRIGUES

A BRECHA HUMANA DA SEGURANÇA DA INFORMAÇÃO:
ENGENHARIA SOCIAL E POLÍTICAS DE SEGURANÇA

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

Americana, SP
2018

GABRIELA CRISTINA RODRIGUES

A BRECHA HUMANA DA SEGURANÇA DA INFORMAÇÃO:
ENGENHARIA SOCIAL E POLÍTICAS DE SEGURANÇA

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

Americana, 11 de julho de 2018.

Banca Examinadora:

Benedito Luciano Antunes de França (Presidente)
Mestre
Faculdade de Tecnologia de Americana

Wladimir da Costa (Membro)
Mestre
Faculdade de Tecnologia de Americana

Clerivaldo José Roccia (Membro)
Mestre
Faculdade de Tecnologia de Americana

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

R613b RODRIGUES, Gabriela Cristina

A brecha humana da segurança da informação: engenharia social e políticas de segurança. / Gabriela Cristina Rodrigues. – Americana, 2018.

74f.

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

Orientador: Prof. Ms. Benedito Luciano Antunes de França

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

CDU: 681.518.5

Em memória de meus avôs, Nande e Dito, pelas lições e histórias. Meus maiores exemplos de amor e empatia.

AGRADECIMENTOS

Agradeço, primeiramente, à minha mãe e meu tio Mauro, por sempre estimularem a minha curiosidade, busca pelo conhecimento e por serem os grandes responsáveis pela minha tenra paixão pela leitura.

Agradeço também à FATEC Americana, a qual me deu dois presentes para a vida, ao longo desses anos de estudo: fascínio pela tecnologia e grandes amizades.

Agradeço ainda ao meu orientador, pela paciência, pelos conselhos e por todo cuidado para me ajudar produzir este trabalho.

À IBM Brasil, por acreditar no meu potencial desde o início de minha jornada acadêmica e me fornecer minha primeira oportunidade de desenvolvimento profissional e pessoal.

Aos meus amigos, pelo suporte, pelo companheirismo e por nunca me deixarem fraquejar diante das adversidades.

À Manuela, minha mãe italiana durante o ano de intercâmbio, por ter sido a grande facilitadora dessa experiência tão singular em minha vida. *Grazie mille*.

Enfim, agradeço a todos que, de certa forma, contribuíram para que eu concluísse essa etapa em minha vida.

A famous explorer once said, that the extraordinary is in what we do, not who we are. […] In our darkest moments, when life flashes before us, we find something; Something that keeps us going. Something that pushes us.

(Crystal Dinamics. *Tomb Raider*. Square Enix, 2013. Versão para *Windows*.)

RESUMO

Este trabalho acadêmico tem como foco de estudo a Engenharia Social e seus mais diversos métodos de investida contra a Segurança da Informação, utilizando-se do fator humano como brecha. Visa analisar técnicas tanto de ataque como de defesa a ambientes físicos e virtuais de empresas dos mais diversos ramos comerciais. O estudo tem por finalidade mensurar a brecha de vulnerabilidade que o fator humano causa para a Segurança da Informação e propõe aumentar a conscientização quanto ao desenvolvimento de Políticas de Segurança de no ambiente empresarial, bem como manter tais políticas atualizadas e devidamente instruídas para todos os funcionários que compõem uma corporação, por tratar-se de um item essencial para a preservação dos três pilares da segurança: disponibilidade, integridade e confidencialidade (NBR ISO/IEC 27002). Este trabalho apoia-se, principalmente, nos autores Mitnick e Simon (2003), Marciano (2006) e Skinner (2003). Como instrumento de pesquisa, utilizou-se um questionário que foi aplicado a 151 funcionários de empresas variadas, os quais receberam a pesquisa por meio de divulgação por redes sociais. Ao final do presente trabalho, pretende-se atestar a importância das Políticas de Segurança no ambiente corporativo, seja no âmbito físico como no virtual.

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

ABSTRACT

This academic research focuses on Social Engineering and its various methods of investing against Information Security, using the human factor as a gap. It aims to analyze both attack and defense techniques to physical and virtual environments of companies of the most diverse commercial branches. The study aims to measure the vulnerability gap that human factor causes for Information Security and proposes to raise awareness about the development of Security Policies in the business environment, as well as keep such policies updated and properly informed for all employees, since it is an essential item for the preservation of the three pillars of security: availability, integrity and confidentiality (NBR ISO/IEC 27002). This work is based mainly on the authors Mitnick and Simon (2003), Marciano (2006) and Skinner (2003). As a research tool, a questionnaire was used and applied to 151 employees of various companies, who received the research through social networks. At the end of this essay, it is intended to attest the importance of Security Policies in the corporate environment, both physically and virtually.

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

LISTA DE ILUSTRAÇÕES: FIGURAS E GRÁFICOS

LISTA DE TABELAS

SUMÁRIO

INTRODUÇÃO

Com os avanços tecnológicos ao longo das décadas, a troca de informações entre empresas e pessoas tem se tornado cada vez mais veloz. Com o advento da Internet disponível à grande maioria da população, o comércio eletrônico tem se tornado cada vez mais difundido e se solidificando como uma forma de competitividade de mercado, sendo, assim, utilizado pelas organizações dispostas a manterem vantagem comercial.

De acordo com Sêmola (2003), a informação tem se tornado um ativo cada vez mais valorizado, vista que nos tornamos a sociedade do conhecimento. Concluímos, pois, que seja imperativo implementar Políticas de Segurança de modo a evitar ou apaziguar vulnerabilidades, fraudes ou perdas de informações, a fim de sustentar o bom funcionamento de uma empresa e a troca dessas informações de forma efetiva e segura.

Porém, nem sempre os sistemas de segurança de informações estão suscetíveis a falhas técnicas. Muitas vezes, ataques à integridade das informações dão-se através a Engenharia Social. Dentro da área de segurança de sistemas computacionais, a Engenharia Social é um termo utilizado para definir tipos de intrusão efetuadas a partir do fator humano. Como explicado por Silva Filho (2009, *In*.: SOFTWARE LIVRE, 2009), um engenheiro social compreende que os indivíduos podem não estar conscientes do valor que uma informação possui e, portanto, não possuem uma preocupação proporcional a este valor. Ainda de acordo com Silva Filho (2009, *In*.: SOFTWARE LIVRE, 2009), “o elemento mais vulnerável de qualquer sistema é o ser humano”.

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

O fator humano encontra-se preparado para manusear informações confidenciais e servir de barreira para protege-las da Engenharia Social?

Como justificativa para o tema e para o problema de pesquisa, considera-se o contexto explicado como força motriz, a fim de averiguar o quão preparados estão funcionários do setor terciário, no que diz respeito a lidar com Engenharia Social e seus malefícios para troca e preservação seguras das informações com as quais lidam todos os dias, sejam de seus próprios locais de trabalho, sejam de clientes, bem como

mensurar o quão importante se faz, não só as Políticas de Segurança em si, como mantê-las sempre atualizadas e informadas a esses mesmos funcionários.

Como objetivo geral do trabalho, pretende-se conduzir uma pesquisa de campo, distribuída para funcionários de empresas de setores variados com perguntas variadas acerca do problema de pesquisa.

Já os objetivos específicos da pesquisa são:

a) Conceituar Engenharia Social, bem como seus métodos mais comuns de ataque e malefícios para os três pilares da Segurança da Informação;

b) Conceituar Políticas de Segurança e principais métodos efetivos de proteção física e virtual;

c) Por meio da pesquisa, estabelecer um paralelo entre o fator humano e a brecha, que pode ser prejudicial à Segurança da Informação;

Em termos metodológicos, pretende-se utilizar como instrumento de coleta de dados uma pesquisa anônima realizada com funcionários de diversos ramos comerciais, apresentada em gráficos. Ainda, deve-se realizar o levantamento de literatura a fim de corroborar com o estado da arte do tema e delimitar a proposta de pesquisa, conforme melhor detalhado no Capítulo IV.

O Capítulo I terá como objetivo definir o tema Engenharia Social, suas técnicas, ciclos de desenvolvimento e malefícios, por ser a base conceitual deste trabalho.

O Capítulo II irá discutir Políticas de Segurança, organismos, leis e padrões regulamentadores vigentes.

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

O Capítulo IV irá discorrer sobre o estudo de caso realizado, por meio de questionários divulgados via Rede Social (Facebook e Instagram), via ferramenta *Google Forms*, captando 151 colaboradores atuantes em empresas de diversos ramos de negócio.

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

CAPÍTULO I – ENGENHARIA SOCIAL

Entende-se por Engenharia Social como sendo uma prática que visa obter informações sensíveis por meio da manipulação daqueles que possuem acesso às mesmas, ou seja, trata-se de técnicas para enganar pessoas a fim de fazê-las fornecerem informações ou executar alguma ação, como explicado por Mann (2008).

Desta forma, o Engenheiro Social é definido por Souza (2015) como um golpista aproveitador, cujo objetivo principal é tirar vantagem de relacionamentos ou ferramentas tecnológicas para manipular pessoas bem-intencionadas, uma vez que os mesmos compreendem as brechas do comportamento humano e tendem a abusar de características oriundas a isso, como:

- Vaidade (pessoal e profissional);
- Autoconfiança, mostrar-se “bom” em determinado assunto;
- Busca pela valorização da formação profissional;
- Vontade de ser útil;
- Busca por novas amizades;
- Propagação de responsabilidade;
- Persuasão (ROSA *et al*., 2012, p. 3);

A Engenharia Social também pode ser compreendida, dentro do âmbito da informática, como técnicas utilizadas por criminosos *online* que se utilizam da tecnologia sofisticada ou não, para obterem acesso ao computador de suas vítimas. É comum os mesmos utilizarem softwares maliciosos instalados secretamente em um sistema, para agir como *spywares* e, dessa forma, coletar dados e informações confidenciais de uma organização. Um exemplo divulgado pela Microsoft (2018), descreve um engenheiro social se passando pelo suporte do Skype a fim de convencer um usuário a lhe passar sua senha, ou até mesmo utilizando-se de *bots* programados para aumentar seu alcance de vítimas.

Sobre segurança coorporativa, Mitnick e Simon (2003), declaram o seguinte:

> Todos da organização devem ser treinados para ter um grau apropriado de suspeita e cuidado ao serem contactados por alguém que não conhecem pessoalmente, sobretudo quando alguém pede algum tipo de acesso a um computador ou rede. É da natureza humana querer confiar nos outros, mas com dizem os japoneses, os negócios são uma guerra. Os seus negócios não podem permitir que você baixe a guarda. A política de segurança corporativa deve definir claramente o comportamento apropriado e inapropriado. [...] A segurança não tem tamanho único. O pessoal dos negócios tem regras e responsabilidades diferentes e cada posição tem vulnerabilidades próprias. Deve haver um nível básico de treinamento que todos da empresa devem ter e, depois, as pessoas também devem ser treinadas de acordo com o perfil do seu cargo para seguir determinados procedimentos que reduzem as chances de elas se tornarem parte do problema. As pessoas que trabalham com informações confidenciais ou que são colocadas em posições de confiança devem ter treinamento especializado adicional (MITNICK; SIMON, 2003, p. 67).

Logo, tem-se que a segurança é responsabilidade de todos, porém é exercida de modo diferente dependendo da área do negócio no qual o funcionário se encontra, já que um funcionário do setor financeiro, por exemplo, não detém as mesmas responsabilidades e tarefas de um funcionário de TI (Tecnologia da Informação). Ainda de acordo com Mitnick e Simon (2003, p. 6), “um engenheiro social pode aproveitar-se das pessoas para obter as informações com ou sem o uso da tecnologia”.

A Engenharia Social representa um dos maiores riscos para o fluxo de informações entre pessoas e organizações. Ainda de acordo com Mitnick e Simon, os indivíduos podem atuar numa empresa que obteve as melhores tecnologias de segurança, terem recebido o melhor treinamento, vigiar muito bem as informações e ainda assim, estarão completamente vulneráveis, uma vez que a Engenharia Social consiste na manipulação inteligente que um criminoso efetua na tendência natural humana de confiar, já que seus objetivos são obter acesso a informações valiosas (GRANGER, 2001, *In*.: SYMANTEC, 2001).

A Engenharia Social também se aproveita do fato de seus usuários, principalmente os posicionados mais abaixo em uma hierarquia organizacional, não terem ideia da importância das informações que manuseiam diariamente (MITNICK; SIMON, 2003). Usuários devem estar bem informados e conscientizados, independente de sua posição na empresa. Dessa forma, terão muito menos chances de serem alvos de um ataque, e, podem, ainda, ajudar com intervenções aos demais, pois tem ciência do fator humano ser o “elo mais fraco” de um sistema de segurança.

1.1 Ciclo de desenvolvimento de um ataque de Engenharia Social

De acordo com Allen (2007, p. 5, *In.*: SANS INSTITUTE, 2007), um ataque de Engenharia Social ocorre em 4 fases, após o atacante definir seu alvo e objetivo, estando as mesmas explicitadas abaixo:

1. Coleta de informações: o atacante deverá buscar o máximo de informações possíveis a respeito da vítima da qual pretende-se extrair informações para atingir o objetivo. Nesta fase, o atacante normalmente vasculha lixos, espionagem, pesquisas em redes sociais, dentre outros.
2. Desenvolvimento da relação: o indivíduo malicioso tenta utilizar as informações coletadas na fase anterior de modo a desenvolver um relacionamento amigável com a vítima, criando, assim, um vínculo de confiança.
3. Exploração da relação: o atacante, após desenvolver confiança, manipula sua vítima de modo a obter a informação ou conjunto delas que permita atingir seu objetivo já pré-definido.
4. Execução do objetivo: nesta fase, o objetivo pré-definido será executado com base em tudo que foi coletado nas fases anteriores. Isso pode ocorrer em um ciclo ou vários.[1]

A próxima seção terá por objetivo detalhar diversas formas de ação do Engenheiro Social, uma vez que é de suma importância conhecer a mais variadas formas de ataques e suas execuções, de modo a preparar-se mais adequadamente e estar sempre alerta para evitá-las.

[1] "1. Information Gathering: a variety of techniques can be used by an aggressor to gather information about the target(s). Once gathered, this information can then be used to build a relationship with either the target or someone important to the success of the attack. Information that might be gathered includes, but is not limited to: a phonelist; birthdates; an organization's chart.
2. Developing Relationship: an aggressor may freely exploit the willingness of a target to be trusting in order to develop rapport with them. While developing this relationship, the aggressor will position himself into a position of trust which he will then exploit.
3. Exploitation: the target may then be manipulated by the 'trusted' aggressor to reveal information (e.g. passwords) or perform an action (e.g. creating an account or reversing telephone charges) that would not normally occur. This action could be the end of the attack or the beginning of the next stage.
4. Execution: once the target has completed the task requested by the aggressor, the cycle is complete." (ALLEN, 2007, p. 5, *In.*: SANS INSTITUTE, 2007. *Tradução nossa*!)

1.2 Técnicas de Engenharia Social

Abaixo, explicam-se técnicas de Engenharia Social que podem ser utilizadas em qualquer uma das fases citadas na seção anterior, bem como podem ser utilizadas em conjunto por um engenheiro social disposto a extrair informações de suas vítimas. É válido, também, apontar que várias técnicas podem ser aplicadas tanto no âmbito físico, quanto no âmbito *online*.

1.2.1 Impersonation e *Pretexting*

Em seu artigo, Redmon (2005, p. 1, *In*: INFOSECWRITERS, 2005) define *impersonation* como o ato de personificar um colega ou qualquer figura de autoridade que possa intimidar outrem com ameaças, se porventura determinada informação não for fornecida. Já se mostrando como suposta colega de trabalho, o atacante conseguiria obter informações dos demais. Desse modo, a responsabilidade seria transferida uma vez que a identidade do atacante permanece anônima.

Já *pretexting* é o ato de forjar determinado pretexto para obter uma informação que, em qualquer outra circunstância, não seria fornecida[2] (ALEXANDER, 2016, *In.*: SANS INSTITUTE, 2016). Pode ser utilizada em conjunto à técnica mencionada anteriormente.

1.2.2 *Dumpster Diving* (ou *Trashing*)

Dumpster Diving também é conhecido como *trashing*. Trata-se do engenheiro social aproveitar-se do fato que as pessoas dão pouca importância àquilo que descartam no lixo, muitas vezes podendo jogar informações confidenciais que podem ser facilmente acessadas pode alguém mal-intencionado. *Dumpster diving* é a arte de coletar informações (pré-*hacking*). É comum fazer esta pesquisa de forma a pré-determinar o alvo e as melhores oportunidades de exploração (*Cf.* GRANGER, 2001, *In*.: SYMANTEC, 2001).

[2] "Pretexting is another form of social engineering where attackers focus on creating a good pretext, or a fabricated scenario, that they can use to try and steal their victims' personal information." (ALEXANDER, 2016, *In.*: SANS INSTITUTE, 2016. *Tradução nossa*!)

1.2.3 *Shoulder Surfing* e *Eavesdropping*

Eavesdropping, em sua forma mais básica, trata-se de ouvir sem permissão conversas entre indivíduos dos quais pretende-se extrair informações. No contexto da TI, esse conceito abrange, também, escutas e gravações remotas, interceptação de chamadas de telefone, transmissões de fax, *email* ou qualquer tipo de transmissão de dados[3] (MANJAK, 2006, *In*.: SANS INSTITUTE, 2006).

Já o termo *Shoulder Surfing* refere-se a qualquer observação direta de informações sensíveis pelo atacante, bem como indivíduos digitando senhas, o que aparece na tela de seus computadores, papéis deixados em suas mesas, dentre outros. De acordo com Manjak (2006), o *shoulder surfing* não mais se limita a presença física do intruso, uma vez que, com o advento tecnológico, um sistema de vigilância com câmeras, por exemplo, pode ser invadido e utilizado em favor do engenheiro social.[4]

1.2.4 *Hoaxing*

Hoaxing ou boato é uma técnica que consiste em espalhar um rumor não-verdadeiro, na intenção de influenciar a tomada de decisões e também comportamentos. Muitas vezes é utilizado como forma de causar medo e ou receio, haja vista que a informação falsa se espalha sob autoria de empresas, organizações, figuras de autoridade num geral.

O *hoaxing* também pode ocorrer *online*, como *spams* de mensagens alarmantes encaminhadas a diversos usuários, a fim de espalhar códigos maliciosos, comprometer a credibilidade de instituições e pessoas, dentre outros (CERT.br, 2012, p.15).

---

[3] "Eavesdropping in the context of information security is defined as listening in on conversations among individuals associated with the target organization. In its most basic form, it amounts to one person keeping within earshot of a conversation between two other persons, but in the security and IT worlds it extends to remote listening and recording devices, including the interception of telephone calls, fax transmissions, e-mails, data transmissions, data-scoping, and even radio scanning for mobile communications." (MANJAK, 2006, p. 9-10, *In*.: SANS INSTITUTE, 2006. *Tradução nossa*!)

[4] "The term shoulder surfing refers to any direct observation of sensitive information such as individuals keying in passwords or PINs, the display of information on computer monitors, or simply personnel forms with SSNs left exposed on someone's desk. Shoulder surfing is no longer limited by the physical presence of the intruder." (MANJAK, 2006, p. 9, *In*.: SANS INSTITUTE, 2006. *Tradução nossa*!)

1.2.5 *Tailgating*

Tailgating consiste em uma técnica de ataque onde o indivíduo, sem autorização para acessar determinado prédio ou sala, aguarda por alguém que possua tal autorização para, dessa forma, entrar junto. É possível utilizar qualquer pretexto para ganhar a confiança do funcionário real (*Cf.* ALEXANDER, 2016, p. 11, *In*.: SANS INSTITUTE, 2016). Também é chamado de “Acesso Carona”.

1.2.6 *Baiting*

Baiting consiste em uma técnica de Engenharia Social onde o atacante finge esquecer qualquer dispositivo ou mídia de armazenamento (CDs, *pendrives*, HDs externos), o qual, na verdade, possui qualquer *spyware* ou programa malicioso que infectará o computador ou rede da vítima que conectá-lo (*Cf.* ALEXANDER, 2016, p. 10, *In*.: SANS INSTITUTE, 2016).

A técnica de *baiting* pode ser classificada como física e virtual. No âmbito virtual, *baiting* ocorre, por exemplo, sites que prometem prêmios atraentes a usuários que passarem informações[5] (ALEXANDER, 2016, p. 10, *In*.: SANS INSTITUTE, 2016). É bastante similar ao *phishing*, a qual será abordada posteriormente.

1.2.7 Engenharia Social Inversa

A Engenharia Social Inversa dá-se quando o atacante coloca a vítima em uma posição de precisar pedir ajuda a ele, pois o mesmo age como especialista. A Engenharia Social Inversa acontece em três etapas:

a) Sabotagem: consiste em forjar algum erro ou manipular alguma situação em que a vítima precisa recorrer ao engenheiro social.

b) Propaganda: o engenheiro social posa como capaz de resolver o problema forjado acima.

c) Auxílio: o engenheiro social mostra-se prestativo em ajudar a vítima, o que faz com que se estabeleça o já supracitado laço de confiança vítima e atacante (*Cf.* ALLEN, 2007, p. 7, *In*.: SANS INSTITUTE, 2007).

A Engenharia Social Inversa também se aplica no âmbito *online*.

---

[5] “Baiting attacks are not restricted to online schemes, either. Attackers can also focus on exploiting human curiosity via the use of physical media” (ALEXANDER, 2016, p. 10, *In*.: SANS INSTITUTE, 2016. *Tradução nossa*!)

1.2.8 *Phishing*

Phishing é um tipo de fraude eletrônica muito comum onde o atacante tenta obter informações confidenciais de um usuário através do envio de *emails* que podem conter que:

- Forjam comunicação oficial de instituições conhecidas ou sites populares.
- Procuram despertar a curiosidade do usuário, seja utilizando-se de caridade ou prêmios.
- Tentam incutir receio ao anunciar que o não cumprimento de alguns processos acarretará em sérias consequências, como cancelamento de cadastros, cartões, dentre outros.
- Tentam fazer com que o usuário transmita seus dados pessoais copiando sites oficiais de instituições conhecidas (CERT.br, 2012, p. 9).

O *phishing* também possui suas variantes como o *Smishing* (fraudes via SMS) e *Vishing* (fraudes via telefone), conforme explicita a CERT norte-americana (US-CERT, 2010, p. 5).

Como mostrado no decorrer das seções do presente trabalho, o *modus operandi* dos engenheiros sociais é, deveras, amplo. Tendo em vista os 4 ciclos da Engenharia Social supracitados, e partindo do princípio que estes ciclos podem ocorrer aliados às mais diversas técnicas descritas, é imperativo que haja conscientização e treinamento acerca de como agir em face de cada uma dessas técnicas, porque só assim o fator humano conseguiria evitá-las e prevenir que os pilares da Segurança da Informação sofressem qualquer abalo. De acordo com Mitnick e Simon (2003), o único meio efetivo de evitar a Engenharia Social é aliar a conscientização às Políticas de Segurança, as quais estabelecem as regras de conduta dos funcionários, os educa e treina precisamente para reconhecer as técnicas já citadas e, assim, terem consciência de como agir. O segundo capítulo deste trabalho deverá, portanto, abordar Política de Segurança e discorrer a fundo sobre conceitos, normas e órgãos regulamentadores já em atividade pelo Brasil e mundo.

CAPÍTULO II – POLÍTICAS DE SEGURANÇA

Entende-se por Políticas de Segurança um conjunto de regras, práticas e mecanismos que tem por objetivo alcançar o estado do sistema chamado de “estado seguro”. É considerada consistente a Política de Segurança que, se seguida à risca, torna impossível chegar ao “estado inseguro” (*Cf.* MARCIANO, 2006, p. 78).

No âmbito virtual, a chamada Política de Segurança da Informação ainda necessita atender a um requisito a mais, que é o de prover equilíbrio entre funcionalidade e segurança, o que faz ser necessário um estudo cuidadoso dos processos e fluxos de informação de cada um dos sistemas a qual será aplicada, de modo a determinar quais são suas vulnerabilidades, na chamada análise de vulnerabilidades. E também de suma importância que tais Políticas sejam adaptáveis, de modo a não gerar discrepâncias entre a situação real e a prevista no ambiente organizacional (*Cf.* MARCIANO, 2006, p. 79).

De acordo com Marciano (2006, p. 79), uma Política de Segurança da Informação deve conter os seguintes elementos:

> - Elementos básicos, os quais descrevemos diferentes indivíduos, objetos, direitos de acesso e atributos presentes na organização ou no sistema, e que definem o vocabulário segundo o qual a política é construída;
>
> - Os objetivos da segurança, ou seja, as propriedades desejadas dos sistemas com respeito à segurança, definida em termos dos atributos desta (confidencialidade, integridade e disponibilidade);
>
> - Um esquema de autorização, na forma de um conjunto de regras descrevendo os mecanismos do sistema relevantes à segurança, com a descrição das eventuais modificações no estado da segurança.

Ainda de acordo com Marciano (2006), o estudo para se aplicar uma Política de Segurança deve ser progressivo, inicialmente aplicado somente em teoria para então ser aplicado a determinados grupos dentro da organização, para que gradativamente se alcance um resultado satisfatório quando colocadas em prática num contexto geral.

Portanto, conclui-se que uma Política de Segurança da Informação faz parte da Segurança da Informação e Sêmola (2003) descreve Segurança da Informação como uma prática de gestão de riscos e incidentes, que deve se embasar em três conceitos básicos (confidencialidade, integridade e disponibilidade). Esta definição,

conforme se pode ver, está em conformidade com o que diz Peixoto (2006), a respeitos destes três conceitos básicos:

Confidencialidade: toda a informação deve ser protegida de acordo com seu grau de sigilo.

Integridade: toda informação deve ser mantida íntegra e sem alterações de quando foi disponibilizada.

Disponibilidade: toda informação deve estar disponível no momento em que os usuários a que se destina precisarem. (*Cf.* PEIXOTO, 2006, p. 38-39)

2.1 Planejamentos e Elementos

De acordo com Nakamura e Geus (2007), o planejamento de uma Política de Segurança não deve vir antes que os riscos sejam entendidos de modo abrangente; constatação já efetuada por Marciano (2006). A abordagem de segurança deve ser proativa e não reativa, pois isso pode trazer problemas graves para a organização, por se tratar de "quando" um incidente ocorrerá, e não "se" ocorrerá (NAKAMURA; GEUS; 2007).

De acordo com Mann (2008), risco pode ser definido como a probabilidade de algo indesejado ocorrer. Os componentes essenciais para compreender o que é risco e o que não é, ainda de acordo com Mann (2008, p. 23-24), são:

1) Impacto: para que algo seja considerado um risco, faz-se necessário que sua ocorrência resulte em um impacto ou dano para algum sistema.

2) Probabilidade: algo não é considerado risco, também, se há a certeza de sua ocorrência. Um risco real precisa ser determinado por chances de ocorrer.

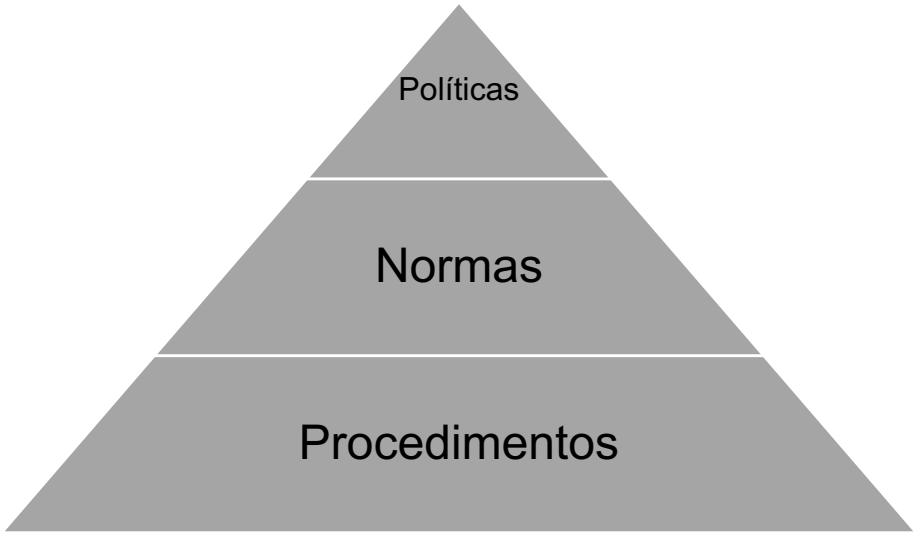
Logo, a combinação de probabilidade e impacto resulta num risco, independente da intensidade.[6]

A Figura 1, abaixo, apresenta uma visão geral do planejamento de uma política, uma vez que a mesma deve ser abrangente a todos os pontos e processos que fazem parte do negócio e servir como elemento que tem por responsabilidade guiar ações futuras. As normas, por sua vez, abordam os detalhes dessas mesmas ações, passos,

[6] 1. Impact – there must be some impact on the system in question. You could replace the word impact with damage. Without impact there is no risk.
2. Probability – if the risk is guaranteed never to happen, then again, we are not interested. There must be some chance of an event happening to create a real risk.
Thus, the combination of some impact (however small) and a real probability (however unlikely) gives us a risk (however small). (MANN, 2008, p. 23-24. *Tradução nossa*!)

conceitos e projetos. Por fim, os procedimentos servem para que os administradores cumpram com aquilo que foi definido e estabeleçam o sistema de acordo com as necessidades do negócio.

Figura 1 – O Planejamento da Política de Segurança



Fonte: Imagem adaptada de Nakamura e Geus (2007, p. 175).

Ainda de acordo com Nakamura e Geus (2007), quatro são os elementos essenciais para uma Política de Segurança de sucesso, a qual servirá para combater qualquer espécie de adversidade. Sendo eles, a vigilância, a atitude, a estratégia e a tecnologia.

A respeito da vigilância, Nakamura e Geus (2007) expõem ser um elemento que permeará tanto o âmbito físico, quanto o âmbito virtual, no sentido de que todos os usuários deverão estar cientes quanto à importância da informação com a qual lidam todos os dias e estarem proativos no que diz respeito a enxergar e denunciar quaisquer discrepâncias entre o descrito nas Políticas de Segurança vigentes e o que ocorre na prática. Já no âmbito técnico, refere-se as definições de alarmes, alertas de acesso indevido, captura de logs, dentre outros (NAKAMURA; GEUS, 2007, p. 177).

A atitude, por exemplo, é muitas vezes estimulada nos funcionários, em decorrência de treinamento recebido e do grau de conscientização, como também diz respeito à importância da Segurança da Informação em si. Uma Política de Segurança que estimula cumplicidade entre funcionários e é devidamente instruída aos mesmos, segundo estes autores, tem grandes chances de inspirar atitude para que suas normas e procedimentos sejam cumpridos efetivamente.

Acerca da estratégia, Nakamura e Geus (2007) atrelam à criatividade para definir a Política e os planos de recuperação de desastres e continuidade de negócios, que serão discutidos posteriormente. Uma estratégia efetiva faz com que as normas e procedimentos presentes na Política de Segurança sejam adaptativos e levem em conta a produtividade dos funcionários (NAKAMURA; GEUS, 2007, p. 177).

O último item discorrido por Nakamura e Geus (2007) assegura que tecnologia de boa qualidade e o dinamismo se fazem essenciais para a efetividade de uma Política de Segurança. Por mais que entre em conflito com o pensamento de Mitnick e Simon (2003), muitas vezes um elemento tecnológico defasado e de péssima qualidade pode trazer o falso sentimento de proteção, o que coloca em risco todos os aspectos da organização (NAKAMURA; GEUS, 2007, p. 177).

Outro elemento importante que será refletido a respeito da Segurança da Informação vincula-se à CERT.br, o qual prevê variantes para a implantação de uma Política de Segurança, no tocante à:

> - Política de senhas: define as regras sobre o uso de senhas nos recursos computacionais, como tamanho mínimo e máximo, regra de formação e periodicidade de troca.
>
> - Política de backup: define as regras sobre a realização de cópias de segurança, como tipo de mídia utilizada, período de retenção e frequência de execução.
>
> - Política de privacidade: define como são tratadas as informações pessoais, sejam elas de clientes, usuários e funcionários.
>
> - Política de confidencialidade: define como são tratadas as informações institucionais, ou seja, se elas podem ser repassadas a terceiros.
>
> - Política de uso aceitável (PUA) e Acceptable Use Policy (AUP): também chamada de "Termo de Uso" e "Termo de Serviço", define as regras de uso dos recursos computacionais, os direitos e as responsabilidades de quem os utiliza e as situações que são consideradas abusivas (CERT.br, 2012, p. 48).

Logo, vê-se que a implantação de uma Política de Segurança é maleável e se adequa aos mais variados setores que compõe uma empresa ou negócio, podendo ser implementada em um ou mais itens de acordo com as especificações, necessidades e objetivos de cada setor.

2.2 Ameaças e Vulnerabilidades

Nos negócios, o fluxo de informações, processos e ativos encontram-se constantemente ameaçados por investidas que buscam explorar suas vulnerabilidades e, assim, consumar a quebra de segurança (SÊMOLA, 2003).

De acordo com Sêmola (2003, p. 47), ameaças são definidas como agentes ou condições que podem violar as informações, bem como ativos nos quais ela circula, através de incidentes que são provocados após a exploração das vulnerabilidades dos processos. Elas ocorrem em detrimento dos conceitos básicos nos quais se ampara a Segurança da Informação. O conceito de ameaça ainda é corroborado por Peixoto (2006), o qual as descreve como consequências de vulnerabilidades pré-existentes. Em relação aos tipos de ameaça, têm-se:

- Ameaças naturais: fenômenos da natureza, como enchentes, tempestades, furacões, etc.
- Ameaças involuntárias: ameaças inconscientes, decorrentes de desconhecimento ou acidentes.
- Ameaças voluntárias: ameaças propositais, causadas por agentes humanos mal-intencionados (PEIXOTO, 2006, p. 43).

Com base em Peixoto (2006) e Sêmola (2003), as vulnerabilidades são frutos de ameaças generalizadas, mas elas, por si só, não provocam os incidentes, necessitando, assim, de um catalisador ou condição favorável (ameaças) para desencadear o supracitado incidente.

Abaixo, vê-se alguns exemplos de vulnerabilidades citados por Peixoto (2006) e Sêmola (2003) que podem comprometer um ambiente corporativo:

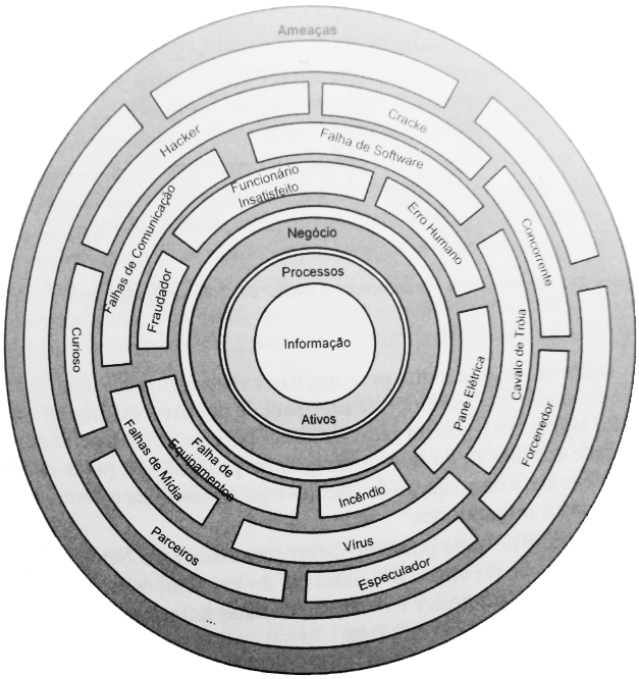
- Física: infraestrutura precária e/ou mal planejada;
- Naturais: equipamentos com danos decorrentes de fenômenos naturais;
- Hardware: equipamento obsoleto, mal utilizado ou desgastado;
- Software: erros de instalação, configuração, falta de atualizações, uso indevido por desconhecimento;
- Mídias: dispositivos de armazenamento que podem ser danificados ou não possuem um local seguro para serem guardados;
- Comunicação: escutas não autorizadas, perdas;

- Humanas: ataques de engenheiros sociais, falta de treinamento e/ou conscientização, ausência de Políticas de Segurança, dentre outros (PEIXOTO, 2006, p. 43-44; SÊMOLA, 2003, p. 48-49).

Segundo Mitnick e Simon (2003), uma empresa estará mais suscetível ao ataque de engenheiros sociais se possuir um número grande de funcionários, se tiver muitas instalações, se possuir informações sobre o paradeiro dos funcionários deixadas na secretaria eletrônica de telefones, se ter informações de ramal muito acessíveis, não possuir treinamento em segurança, não ter sistema de classificação de dados e nenhum plano de recuperação de desastres ou plano de continuidade de negócios (*Cf.* MITNICK; SIMON, 2003, p. 267)

A seguir, apresenta-se uma figura extraída de Peixoto que trata a respeito das ameaças em um ambiente corporativo:

Figura 2 – Panorâmica de ameaças



Fonte: Peixoto (2006, p. 41).

Na imagem, observa-se como a informação encontra-se ao centro e é tratada por ativos e processos, os quais são a força motriz de um negócio. As ameaças, por sua vez, circundam todos estes elementos, já que que podem afetá-los em quaisquer aspectos, seja física ou virtualmente, bem como causadas de modo intencional ou

não. Logo, é de suma importância a realização de uma auditoria cuidadosa em todos os processos e ativos, de modo a determinar quais devem ser prioridade, quais estão mais suscetíveis, a fim de elaborar uma Política de Segurança abrangente e eficaz.

2.3 Plano de recuperação de desastres e continuidade de negócios

De acordo com Marciano (2006), o Plano de Recuperação de Desastres (também chamado de DRP – Disaster Recovery Plan) prevê a recuperação de atividades de um negócio, em caso de interrupções seja lá qual forem sua natureza. Dentre as vantagens da formalização de um Plano de Recuperação de Desastres, estão:

> - Eliminar possível confusão e erro;
> - Reduzir interrupções às operações da organização;
> - Prover alternativas durante eventos desastrosos;
> - Reduzir a dependência a determinados indivíduos;
> - Proteger os dados da organização;
> - Garantir a segurança do pessoal;
> - Apoiar uma restauração ordenada das atividades (MARCIANO, 2006, p. 85).

Como apontado por Marciano (2006), é importante frisar que um Plano de Recuperação de Desastres envolve custos, bem como a formação de uma equipe capacitada ou contratação de terceiros, e também a aquisição de equipamento sobressalente.

Já o Plano de Continuidade de Negócios (também chamado BCP – Business Continuity Plan) tem por objetivo proteger as operações e ativos de uma organização, não somente no âmbito virtual e também englobando os indivíduos que nela operam. (MIORA, 2002, *Apud* MARCIANO, 2006, p. 86).

Segundo Marciano (2006), um BCP é construído da seguinte maneira:

> Uma análise dos ativos indica o grau de criticidade de cada um destes, o que, associado ao número de dias durante os quais a organização pode prosseguir sem o ativo considerado, gera a chamada matriz de análise de impacto nos negócios. Esta matriz é então utilizada como índice para apontar os ativos críticos e o tempo máximo suportável de indisponibilidade, orientando prioridades e investimentos (MARCIANO, 2006, p. 86).

De acordo com Marciano (2006), conclui-se, portanto, que um BCP, assim como uma Política de Segurança, deve ser elaborado após uma auditoria que deverá mapear a criticidade dos ativos de um negócio, para, então, ser determinado o tempo máximo que este pode permanecer indisponível, sem que hajam perdas significativas.

2.4 Leis, Padrões e Organizações regulamentadoras

No decorrer dessa seção, discorre-se acerca de órgãos regulamentadores, a instituição de regras e leis que se aplicam a Segurança da Informação no Brasil, além dos modos de conduta e penas, em caso de sua violação. Nesta seção, indica-se alguns dos principais órgãos presentes no mundo, que também são ou foram fundamentais para a padronização de regras, no decorrer dos anos em que a Tecnologia evoluiu como ferramenta essencial para o funcionamento de negócios, instituições e governos. Apresenta-se, ainda, alguns dos modelos mais conhecidos de Governança de TI, os quais trazem consigo material para elaboração de uma Política de Segurança no ambiente coorporativo.

2.4.1 Órgãos regulamentadores de Segurança da Informação no Brasil

No Brasil, somente no final da década de 1990 os eventos de Segurança da Informação têm recebido sua importância, pois até então eram classificados conforme os pré-existentes conceitos de fraude ou falsificação. Logo, leis têm sido propostas especificamente para o tema no âmbito digital, porém, a legislação brasileira segue deveras abrangente (MARCIANO, 2006).

2.4.1.1 CERT.br

Em 1995, a partir de uma iniciativa do Ministério de Ciência e Tecnologia e Ministério das Comunicações, foi criado o Comitê Gestor da Internet no Brasil (CGI.br), a fim de coordenar atividades que estivessem relacionadas com a Internet brasileira. Então, só em 1997, como resultado de um estudo realizado pelo mesmo Comitê, foi fundado o NBSO, o qual evoluiu para o atual CERT.br (Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil), em 1999 (NIC.br, 2015-2018).

2.4.1.2 Constituição Federal de 1988

A Carta Magna brasileira foi aprovada pela Assembleia Nacional Constituinte em 22 de setembro de 1988 e promulgada em 5 de outubro de 1988, ao fim do Regime Militar no Brasil (1964-1985) e tem por objetivo assegurar direitos coletivos e individuais, bem-estar, segurança, a fim de obter uma sociedade fraterna, pluralista e sem preconceitos (BRASIL, 1988).

Todas as políticas e ações coercivas formuladas em território brasileiro deverão agir em conformidade com os textos legais presentes na Constituição. O Código Penal brasileiro, que segue vigente até os dias de hoje, foi criado pelo Decreto-Lei no 2.848, em 7 de dezembro de 1940 pelo então presidente Getúlio Vargas, sendo esse o 3º código da história do Brasil (BRASIL, 1940). Algumas leis, então, foram implementadas ao Código Penal, a fim de alterá-lo e torná-lo abrangente a crimes cibernéticos.

2.4.1.3 Leis nº 12.735/12 e 12.737/12

A Lei nº 12.735/12, publicada no Diário Oficial da União em 30 de dezembro de 2012, tem por intuito "tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências" (BRASIL, 2012). Esta Lei também é conhecida como Lei Azeredo.

Já a Lei nº 12.737/12, também publicada no Diário Oficial da União na mesma data que a supracitada, é chamada de Lei Carolina Dieckmann, em virtude de um incidente ocorrido com a atriz em 2012, visto que a mesma teve dados e fotos pessoais vazados de seu dispositivo móvel. Esta Lei, assim como a supracitada, altera o Código Penal Brasileiro, acrescentando ao mesmo os arts. 154-A e 154-B, nos quais lê-se:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
>
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
>
> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput. [...]

> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
>
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave [...] (BRASIL, 2012).

2.4.1.4 NBR ISO/IEC 27002:2013

A norma técnica de auditoria de Segurança da Informação NBR ISO/IEC 27002:2013 é um documento homologado pela Associação Brasileira de Normas Técnicas (ABNT), em sintonia com a International Organization for Standardization (ISO) e International Electrotechnical Commission (IEC) denominado “Tecnologia da Informação: Técnicas de segurança: Código de prática para a gestão da Segurança da Informação”.

A norma está dividia em 11 seções, sendo elas: a) Política de Segurança da Informação; b) Organizando a Segurança da Informação; c) Gestão de ativos; d) Segurança em recursos humanos; e) Segurança física e do ambiente; f) Gestão das operações e comunicações; g) Controle de acessos; h) Aquisição, desenvolvimento e manutenção de sistemas de informação; i) Gestão de incidentes de Segurança da Informação; j) Gestão da continuidade do negócio; k) Conformidade (ABNT ISO/IEC 27002: 2013).

2.4.1.5 Decreto nº 3.505, de 13 de junho de 2000

O supracitado Decreto tem por objetivo instituir a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal. Nos artigos 1º e 2º são instituídos:

> Art. 1 º Fica instituída a Política de Segurança da Informação nos órgãos e nas entidades da Administração Pública Federal, que tem como pressupostos básicos:
> I - Assegurar a garantia ao direito individual e coletivo das pessoas, à inviolabilidade da sua intimidade e ao sigilo da correspondência e das comunicações, nos termos previstos na Constituição;
> II - Proteção de assuntos que mereçam tratamento especial;
> III - Capacitação dos segmentos das tecnologias sensíveis;
> IV - Uso soberano de mecanismos de segurança da informação, com o domínio de tecnologias sensíveis e duais;
> V - Criação, desenvolvimento e manutenção de mentalidade de segurança da informação; [...]
> das entidades da Administração Pública Federal sobre a importância das informações processadas e sobre o risco da sua vulnerabilidade.
> Art. 2º Para efeitos da Política de Segurança da Informação, ficam estabelecidas as seguintes conceituações: [...]

> II - Segurança da Informação: proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento (BRASIL, 2000).

É importante apontar que o decreto, ainda, foi responsável pela criação do Comitê Gestor da Segurança da Informação.

2.4.2 Órgãos regulamentadores de Segurança da Informação no mundo

Nesta seção, abordam-se quatro órgãos, sendo eles: NIST, US-CERT, Sans Institute e OCDE.

2.4.2.1 NIST

O Instituto Nacional de Padrões e Tecnologia (NIST – National Institute o Standars and Technology) foi fundado em 1901 e faz parte do Departamento de Comércio dos Estados Unidos. Trata-se de um dos laboratórios de ciências físicas do país, mas que também gerencia nanomateriais, chips de computadores, registros de saúde eletrônicos, dentre outros produtos que dependem de tecnologia, medições ou padrões fornecidos pelo próprio NIST (NIST.GOV, 2015-2017)

2.4.2.2 US-CERT

O US-CERT (United States Computer Emergency Readiness Team) é uma organização norte-americana e também uma das ramificações do chamado NCCIC (National Cybersecurity and Communication Integration Center). Trata-se de um órgão que tem por objetivo analisar e reduzir riscos cibernéticos, bem como reduzir vulnerabilidades, disseminar conscientização a respeito de segurança e coordenar medidas de respostas à incidentes (US-CERT.GOV, 2018). Para fins de informação, o Brasil possui sua própria versão do CERT, o denominado CERT.br.

2.4.2.3 SANS Institute

A SANS (System Administration, Networking and Security) Institute foi fundada em 1989 como uma organização privada de pesquisa e educação. A SANS Institute é especializada em Segurança da Informação, Cibersegurança e emissão de

certificados para estas áreas de conhecimento. A organização também mantém e desenvolve um vasto repositório com diversos documentos e publicações acerca de Segurança da Informação, gratuitamente. Um dos certificados mais conhecidos que pode ser obtido através da SANS é o GIAC, Global Information Assurance Certification (SANS.ORG, 2000-2018).

2.4.2.4 OCDE

A OCDE (Organização para a Cooperação e Desenvolvimento Econômico) trata-se de uma organização internacional composta por 36 países, o qual o Brasil é parceiro-chave desde 2015, e tem por finalidade entender mudanças econômicas, sociais e ambientais através de análises de dados e estudos com os governos participantes. Tem sua sede em Paris, na França (OECD.ORG, 2018).

2.4.3 Padrões técnicos e de infraestrutura para a implantação de Políticas de Segurança

Nesta seção, abordam-se três Padrões, sendo eles: a ITSEC, COBIT e ITIL.

2.4.3.1 ITSEC

O ITSEC é um acrônimo para Information Technology for Security Evaluation Criteria e foi um dos primeiros padrões propostos para recuperação de sistemas inoperantes de computador. Seu desenvolvimento ocorreu em meados dos anos 1980, num esforço conjunto de França, Alemanha, Reino Unido e Holanda, a fim de gerenciar sistemas governamentais. Serviu como referência para criação de padrões utilizados ainda hoje, como o COBIT (FORD, 1994 *Apud* MARCIANO, 2006, p. 100)

2.4.3.2 COBIT

O COBIT (Control Objectives For Information and Related Technology) é um guia de boas práticas para a governança da Tecnologia da informação, criado pela ISACA, em 1998. Os recursos apresentados no COBIT servem como modelo de referência para a governança da tecnologia e do negócio e independe de plataformas adotadas por empresas (IT GORVERNANCE INSTITUTE, 2005 *Apud* MARCIANO, 2006).

Os componentes do COBIT são, de acordo com Marciano (2006), Sumário executivo; Framework; Objetivos de controle; Práticas de controle; Linhas mestras de gestão; Linhas mestras de auditoria.

Acerca da Framework, trata-se do suporte que guia os demais componentes. Está dividido em quatro grandes domínios: a) Planejamento e organização; b) Aquisição e implementação; c) Entrega e suporte; d) Monitoração e avalição (IT GORVERNANCE INSTITUTE, 2000; 2004 *Apud* MARCIANO, 2006).

No tocante aos Objetivos de controle, Marciano apresenta que cada processo de TI precisa ser gerenciado, a fim de atingir os objetivos do negócio (IT GORVERNANCE INSTITUTE, 2000 *Apud* MARCIANO, 2006).

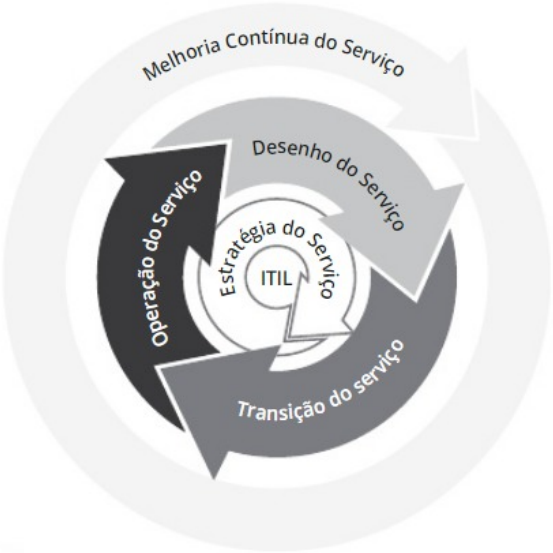
As Linhas mestras de gestão são, de acordo com Marciano (2006), ferramentas de suporte para gestores de TI, enquanto que as Linhas mestras de auditoria são objetivos de auditoria de TI.

2.4.3.3 ITIL

A ITIL (Information Technology Infrastructure Library) trata-se de uma biblioteca de processos que tem por objetivo gerenciar os serviços de TI e seus ciclos de vida no negócio. Foi desenvolvida na década de 1980 pelo órgão britânico CCTA (Central Computer and Telecommunications Agency) e hoje trata-se de uma marca registrada da OGC (Office of Government Commerce) (CESTARI FILHO, 2012, p. 3).

A ITIL apresenta os seguintes conjuntos de processos: Estratégia do Serviço, Projeto de Serviço, Transição de Serviço, Operação do Serviço e Melhoria Contínua do Serviço (CESTARI FILHO, 2012, p. 5). Estes processos estão representados na Figura 3, através de um ciclo de vida de um serviço:

Figura 3 – Ciclo de vida de um serviço



Fonte: Cestari Filho, 2012, p. 5.

De acordo com Cestari Filho (2012), no tocante a Estratégia do Serviço, este volume tem por objetivo conceituar um conjunto específico de serviços para ser desenvolvido de acordo as necessidades e requisitos do negócio.

Já o Projeto de Serviço projeta os serviços estabelecidos pelo volume anterior, baseando-se principalmente em suas respectivas utilidades e garantias. Enquanto a Transição de Serviço deverá transpor estes serviços para os ambientes de teste e produção.

Acerca da Operação do Serviço, o objetivo é monitorar e assegurar que a utilidade e garantia supracitadas estejam sendo atingidas como foi estabelecido pelo Projeto de Serviço.

Por fim, a Melhoria Contínua do Serviço prevê uma avaliação dos serviços a fim de melhorar seu suporte aos objetivos do negócio.

Atualmente, a biblioteca ITIL encontra-se em sua terceira versão.

Definida a Política de Segurança, sua utilização e importância na relação de prevenção e de recuperação de incidentes, nota-se a importância da contribuição dada por Mitnick e Simon (2003), pois ela auxilia na prevenção de ataques de Engenharia Social. Contudo, tratando-se de fator humano, como um fator gerador de risco, conforme foi refletido no capítulo primeiro, neste foi analisado como o fator humano influencia diretamente na Segurança da Informação, apesar de ser tratado

como fator externo. A seguir, o terceiro capítulo deste trabalho terá por objetivo analisar o fator humano atuando na Segurança da Informação, tomando por base os estudos de caso de Mitnick e Simon (2003) e utilizando aspectos importantes do pensamento de Marciano (2006) e Skinner (2003).

CAPÍTULO III – O FATOR HUMANO NA SEGURANÇA DA INFORMAÇÃO

De acordo com análises dos estudos de caso apresentados por Mitnick e Simon (2003), entende-se o motivo pelo qual ambos definem o fator humano como o elo mais fraco da Segurança da Informação. Em complementação ainda a este pensamento, Marciano (2006, p. 109) diz que:

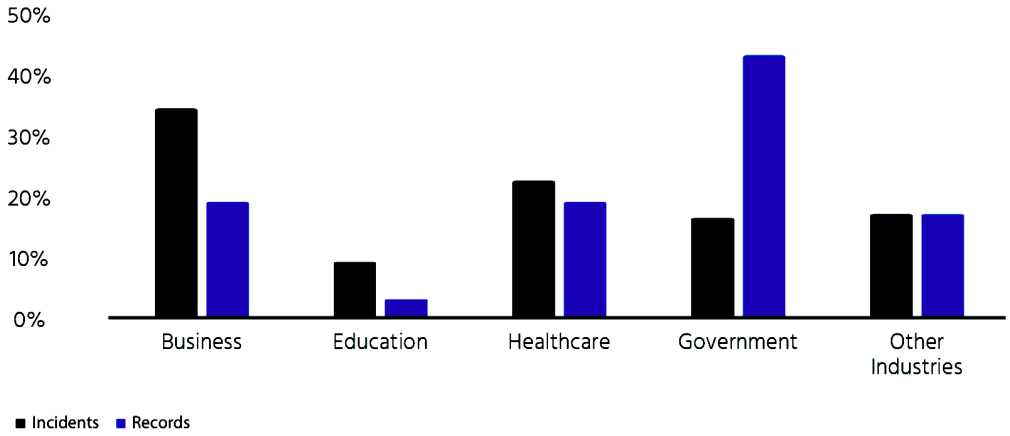
> Não se vê uma discussão adequada sobre o grau de receptividade a estas políticas, nem se apresentam, de modo metódico, questões sobre o impacto, usualmente considerável, por elas causado sobre o ambiente e sobre o comportamento daqueles que as devem seguir.

A informação, de acordo com Sêmola (2003), trata-se do sangue da empresa e circula por todos os seus ativos, ambientes, tecnologias, cumprindo, desse modo, um papel essencial no fornecimento de instrumentos para a gestão do negócio. Retomando a discussão apresentada no Capítulo I do presente trabalho, é imperativo que os usuários tenham ciência do valor das informações que manuseiam diariamente, seja deles próprios ou de terceiros.

Marciano (2006) defende que a Segurança da Informação deve ser um domínio multidisciplinar das Ciências Sociais, o que é corroborado por Rosa, Silva e Silva (2012), quando relacionada a Análise de Redes Sociais aplicadas à Engenharia Social, no que diz respeito a observar padrões de comportamentos de indivíduos para saber a melhor maneira de abordá-los.

De acordo com estatísticas divulgadas pela Organização Internet Society em 2016, denominado “Global Internet Report 2016”, o meio mais comum de se obter acesso aos dados de uma organização é por meio da Engenharia Social. O histograma apresentado no Gráfico 1 mostra os alvos mais visados para violação de dados:

Gráfico 1 – Alvos de violação de dados



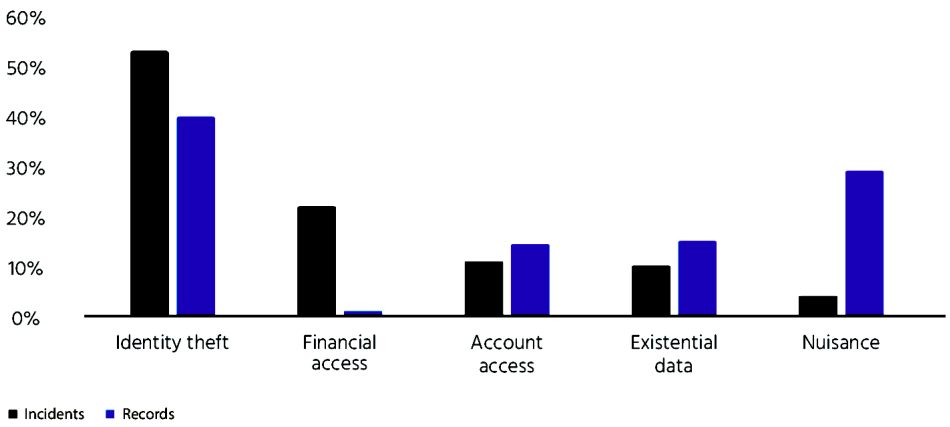
Fonte: Imagem adaptada de Breach Level Index; Gemalto, 2016 *Apud* Internet Society, 2016, p. 41.

No gráfico, é possível visualizar como os negócios tratam-se dos alvos mais visados pelos ataques, seguidos de violação de dados da saúde e informações governamentais. Por mais que este setor tenha tido uma porcentagem baixa de violações, algo em torno de 18%, este percentual é irrisório se comparada a taxa das invasões recordes anteriores (INTERNET SOCIETY, 2016, p. 41).

Mais a fundo no relatório, tem-se que, dentro dos Negócios, o setor de varejo representa com 13% de todas as violações reportadas e 6% de registros. O setor financeiro, por sua vez, representa 15% das violações, porém só 0,1% dos registros, enquanto a Tecnologia trouxe 6% de violações e 12% de registros. Nenhum outro setor, além dos Negócios, foi explicitamente detalhado (INTERNET SOCIETY, 2016, p. 40).

Conforme as informações estatísticas explicitam, muitas vezes as organizações não arcam totalmente com as consequências de suas violações de segurança, daí entendermos o porquê das altas taxas de violações e o baixo percentual dos registros, visto que, por mais que a reputação empresarial seja posta em desconfiança por seus clientes, o que gera uma espécie de impacto indireto, o custo financeiro destas vulnerabilidades recaem às instituições bancárias, fornecedoras, por exemplo, dos cartões de crédito dos clientes, cujos dados estavam somente armazenados na organização empresarial violada (INTERNET SOCIETY, 2016, p. 129).

Gráfico 2 – Tipos de Informação almejados nas violações

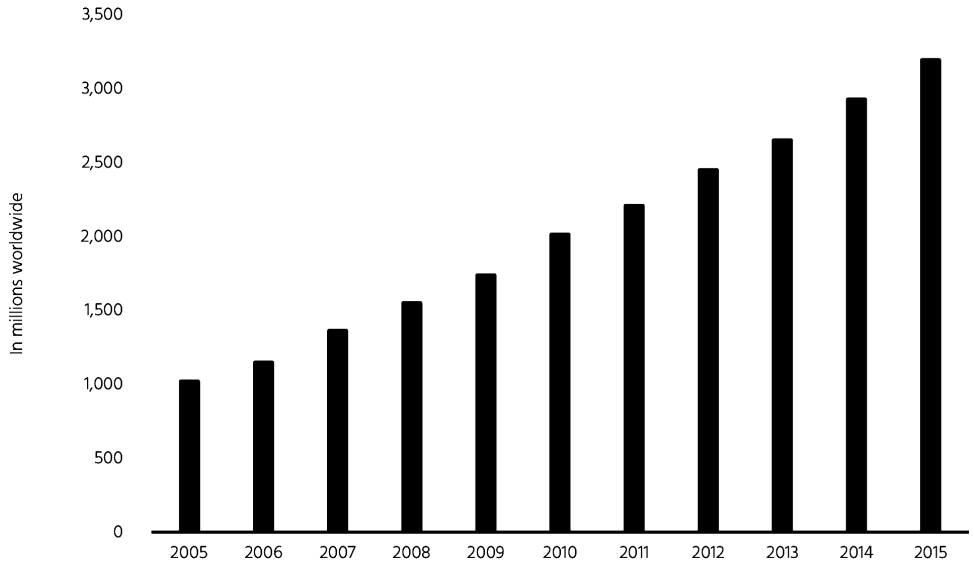


Fonte: Imagem adaptada de Breach Level Index; Gemalto, 2016 *Apud* Internet Society, 2016, p. 42.

Dentre as informações listadas no “Global Internet Report 2016”, o qual utilizou-se da definição de Gemalto, têm-se que o roubo de identidade (Identity theft) que possui altas porcentagens de incidentes (algo em torno de 53%) e, também, de registros (quase 40%) se compararmos às demais eventualidades cibernéticas. No tocante ao acesso financeiro, que, de acordo com o Relatório é constituído por contas bancárias e cartões de crédito, a taxa de incidentes é proporcionalmente altíssima se comparada aos índices de registros anteriores, conforme se pode analisar no segundo tabulamento deste gráfico. No que se refere ao acesso às contas, as quais dizem respeito a *logins* e senhas, serviços *online* de qualquer cunho, as informações estatísticas ficam na casa dos 10% de incidentes, mas com índice estatístico superior no número de registros. Quanto aos dados existenciais, definidos no Relatório como dados da segurança nacional ou essenciais para a existência do negócio, o percentual de incidentes é em torno dos 10%, ao passo que o número estatístico de registros é superior ao de incidentes. Transtornos virtuais, como *spams* e afins, são denominados neste gráfico de “Dados de perturbação” (Nuisance): conforme se observa há um alto número de registros, porém baixo número de incidentes.

No Gráfico 3 verificar-se-á o aumento de usuários na Rede Mundial de Computadores, tendo em vista os dados coletados entre os anos de 2005 e 2015 e expostos no Relatório da Internet Society (2016):

Gráfico 3 – Indivíduos utilizando a Internet pelo mundo (em milhões)



Fonte: Imagem adaptada de ITU, 2016, *Apud* Internet Society, 2016, p. 32.

Em consonância às informações estatísticas apresentadas, entre os anos de 2005 e 2015, houve um progressivo aumento na quantidade de usuários da Internet, de algo em torno de 1 milhão, em 2005, para algo em torno de 3,2 e 3,3 milhões de usuários, o que representa um dado estatístico altamente expressivo (quase 330%).

Com o advento da Internet das Coisas (também chamado de IoT – Internet of Things), a empresa de consultoria Gartner estipula que, até 2020, o número de conexões de dispositivos dos mais variados tipos chegará aos 20,8 bilhões, baseando-se em estatísticas coletadas nos últimos anos.

Tabela 1 – Dispositivos conectados através da IoT por categoria (em milhões de unidades)

Categoria	2014	2015	2016	2020
Usuários comuns	2,277	3,023	4,024	13,509
Negócios: Genéricos	632	815	1,092	4,408
Negócios: Específicos	898	1,065	1,276	2,880
Total	3,807	4,902	6,392	20,797

Fonte: Tabela adaptada de Meulen, *In.*: Gartner (2015).

Ainda de acordo com a Gartner, na Tabela 1, no ramo dos negócios, considera-se genéricos os dispositivos que são usados por múltiplas indústrias, como lâmpadas conectadas a IoT, sistemas de refrigeração, dentre outros cujo objetivo principal é redução de custos. Já os categorizados dentro da indústria vertical, estão os dispositivos específicos, utilizados em âmbitos particulares, como por exemplo equipamentos especializados de hospitais, rastreadores de navios, dentre outros.

É imperativo que, em vista do crescimento das conexões e a velocidade com que a Informação se propaga, as empresas pensem em soluções e Políticas de Segurança que se adaptem às novas tecnologias. De acordo com Mitnick e Simon (2003), não existe solução definitiva para a Engenharia Social enquanto o fator humano for o elo mais fraco da Segurança da Informação, porém, podem-se obter meios para dificultar a ação dos criminosos.

De acordo com o Relatório emitido pela Internet Society (2016), os usuários estão cada vez mais conscientes a respeito de privacidade de problemas de segurança em geral, especificamente quando relacionados com violação de informações, em face do número de incidentes reportados, o qual vem aumentando. Porém, a mesma consciência faz com que os mesmos usuários percam a confiança em serviços *online* que requerem o uso de informações pessoais.

3.1 Segurança da Informação aplicada às Ciências Sociais

De acordo com Marciano (2006), a Segurança da Informação aplica-se às Ciências Sociais, pelo simples fato de que “a informação é gerada, armazenada, tratada e transmitida com o fim de ser comunicada e a comunicação é inerentemente um processo grupal” (MARCIANO, 2006, p. 110). Um estudo que tem por finalidade observar o comportamento de um grupo diante de situações e ações coletivas é responsabilidade da Sociologia.

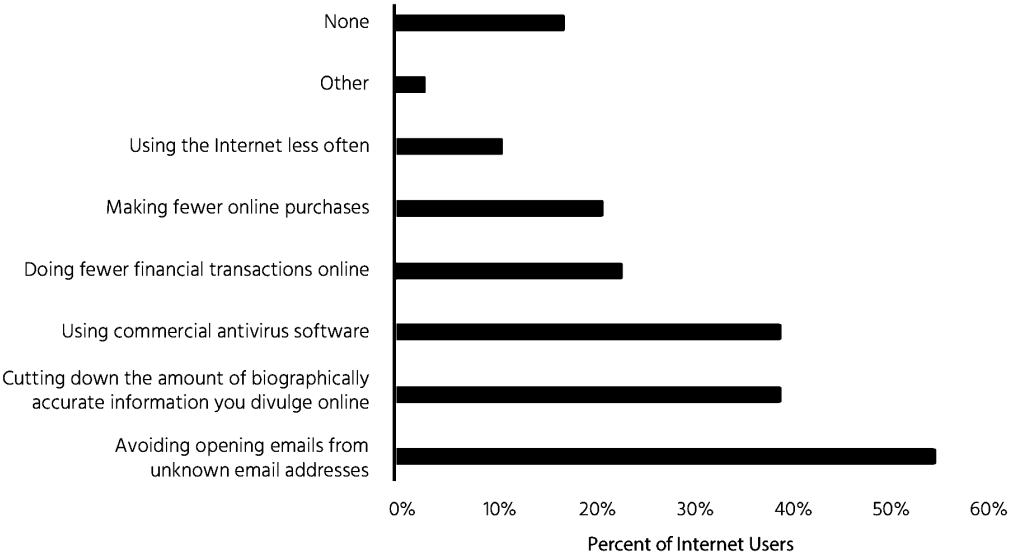
Como discutido no início do Capítulo 3, de acordo com o Relatório da Internet Society (2016), a conscientização a respeito de segurança e privacidade vem aumentando, e, junto com ela, a desconfiança na utilização de serviços *online*, tendo em vista os inúmeros incidentes de violação de dados. No último deles, que ocorreu no Facebook, ainda no começo deste ano, estima-se que 87 milhões de usuários tenham tido suas informações inadvertidamente coletadas pela Cambridge Analytica

através de um aplicativo conectado ao Facebook. Porém, ainda em 2015, outra violação de dados ocorreu na mesma rede social, contudo, o fato não foi amplamente divulgado, o que custou ao CEO uma intimação para depor no Congresso dos Estados Unidos (BADSHAH, 2018, *In.*: THE GUARDIAN, 2018). De acordo com a CNN, o prejuízo monetário em virtude do escândalo de segurança no Facebook, para a própria companhia, foi de quase 80 milhões de dólares (LA MONICA, 2018, *In.*: CNN MONEY, 2018).

De acordo com a Internet Society (2016), no ano de 2015, em uma pesquisa realizada pelo CIGI (Centre for International Governance Innovation), com 24 mil usuários de diferentes países, 57% dos participantes mostraram-se preocupados com sua privacidade *online*; a porcentagem, em 2014, foi de 64%, o que demonstra crescimento ano por ano. Quando perguntados se mudaram o comportamento *online* ao saberem de casos de violação de privacidade, apenas 17% dos participantes da pesquisa responderam que não.

Abaixo será apresentado o Gráfico 4 com informações concernentes às mudanças de comportamento para proteger informações de cunho pessoal:

Gráfico 4 – Mudanças de comportamento para proteger informações pessoais



Fonte: Imagem adaptada de CIGI-Ipsos Global Survey on Internet Security and Trust, 2016 *Apud* Internet Society, 2016, p. 45.

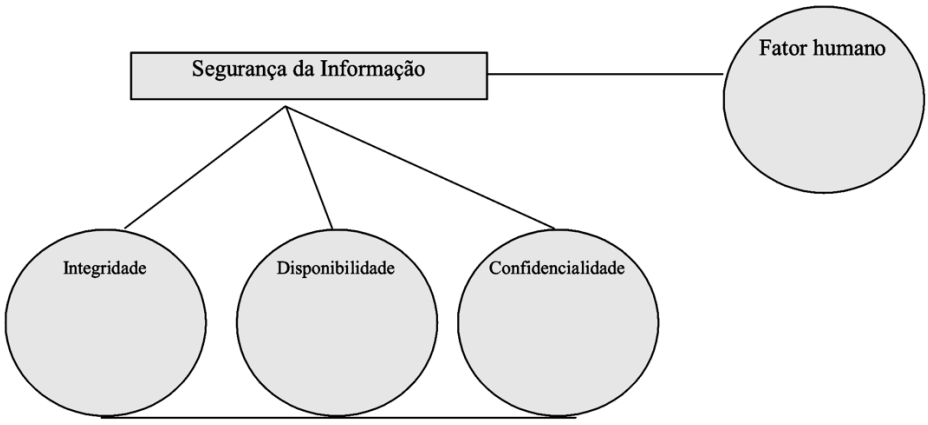
De acordo com os dados apresentados neste gráfico acima, estão os seguintes comportamentos: 17% disseram que não mudaram de comportamento no ambiente virtual, ao passo que aproximadamente 11% afirmaram que estão usando a Internet com menos frequência; algo em torno de 20% estão efetuando menos compras *online* e mais ou menos 22% efetuam menos transações *online*. Por outro lado, como fator de prevenção, aproximadamente 40% dos usuários passaram a usar programas antivírus e, por conseguinte, quase o mesmo número de usuários diminuiu a quantidade de informações pessoais divulgadas em ambiente virtual e, consideravelmente, algo em torno de 55% das pessoas começaram a se precaver, como, por exemplo, evitando abrir *emails* de origens desconhecidas.

É importante salientar que a perda de confiança dos usuários nos serviços *online* pode ter um impacto altamente negativo para os negócios em geral, visto que passaram a conceber o ambiente virtual como um espaço de incertezas e de vulnerabilidades, e como se sabe, se o espaço gera desconfiança, abre-se a porta para o medo.

Nota-se, pois, a ligação indiscutível já mencionada por Marciano (2006) entre Segurança da Informação aplicada às Ciências Sociais, uma vez que “quando se quer observar o indivíduo e suas interações com o meio, está-se no campo da Psicologia; quando se pretende observar o comportamento de grupos diante de situações e suas ações coletivas, recorre-se à Sociologia; por fim, o estudo cultural, partindo de sua gênese e evolução, é o campo da Antropologia” (BATES, 1999 *Apud* MARCIANO 2006, p. 110).

Nos moldes atuais, a Segurança da Informação se apoia nos três pilares conceituados por Peixoto (2006) e também corroborados por Sêmola (2003), tendo o Fator Humano como elemento externo, agindo como o elo entre as informações e a segurança das mesmas. Na Figura 4, a seguir, tem-se o modelo de Segurança da Informação embasado pelos três pilares:

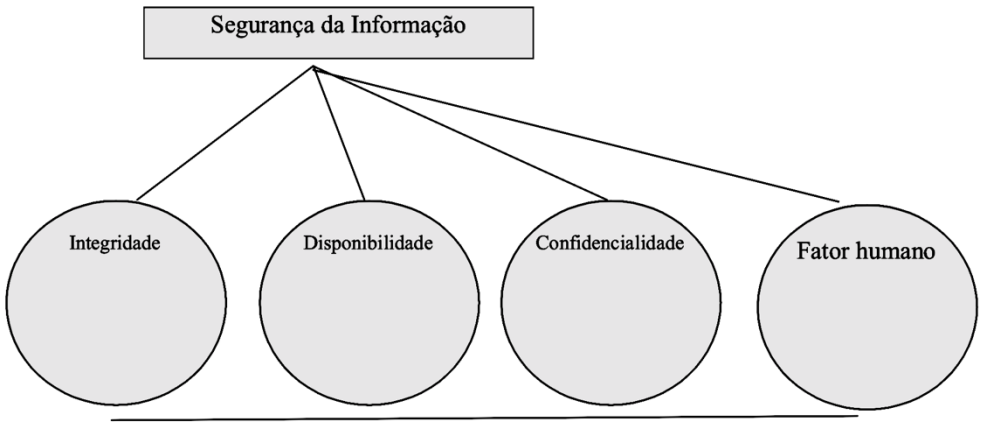
Figura 4 – Modelo clássico da Segurança da Informação



Fonte: Imagem adaptada de Silva; Costa, 2009, p. 3.

Porém, em um modelo alternativo proposto por Silva e Costa (2009), o Fator Humano deve encaixar-se também como um dos pilares da Segurança, dada sua importância para a causa, como demonstrado na figura abaixo:

Figura 5 – Modelo proposto por Silva e Costa (2009) da Segurança da Informação



Fonte: Imagem adaptada de Silva; Costa, 2009, p. 3.

E o Fator Humano, uma vez classificado como o elo mais fraco por Mitnick e Simon (2003), não possui um modo concreto de ser protegido e/ou trabalhado. Diferentemente de sistemas binários de computação, o Fator Humano possui diversos outros agentes que podem afetá-lo, porquanto, deve ser encarado de uma perspectiva social.

3.2 Gestão da Segurança da Informação

De acordo com o psicólogo Skinner (2003), o comportamento dos indivíduos molda-se ao ambiente social no qual estes se inserem, conforme certas respostas são reforçadas, ou seja, estimuladas ou não. O ambiente social, propriamente dito, insere-se dentro da definição de cultura, por se tratar de um procedimento que abrange a influência de agências e subagências controladoras com as quais o indivíduo se depara ao longo de sua vida, as quais servirão para formatar seu comportamento para que esteja em consonância com o grupo no qual se insere (SKINNER, 2003, p. 455-456).

Nesta linha de pensamento, Marciano (2006) prevê que a falha na gestão da segurança pode ser extremamente nociva, uma vez que influenciará no comportamento de seus geridos, visto que as decisões tomadas pelos gestores, bem como os treinamentos expedidos, deverão manifestar-se no comportamento dos ditos "usuários comuns" (RHODEN, 2002; GUZ- MAN; KAARST-BROWN, 2004 *Apud* MARCIANO, 2006, p. 189).

O homem como ser social, de acordo com Skinner (2003), tem seu comportamento fortemente influenciado pelo grupo que pertence e esse mesmo comportamento pode ser alterado se ele for inserido em um grupo diferente do seu original. O grupo, neste sentido, possui pleno poder de influência, de acordo com Skinner, pois "o indivíduo está sujeito a um controle mais poderoso quando duas ou mais pessoas manipulam variáveis que têm um efeito comum sobre seu comportamento" (SKINNER, 2003, p. 352). Logo, em concordância com o pensamento de Skinner, Marciano (2006) infere que uma Política de Segurança bem implementada é aquela melhor aceita individualmente, uma vez que isso influenciaria os demais membros de um grupo do qual se espera o seguimento de tal política, pois a regulamentação coletiva é dependente, primeiramente, da autorregulamentação (KAROLY, 1993 *Apud* MARCIANO, 2006, p. 190)

3.3 Impactos para credibilidade e confiança

Ainda de acordo com os estudos realizados pela Internet Society, em 2016, e retomando o que foi mencionado no início deste capítulo, os usuários estão cada vez mais preocupados com a segurança de suas informações, e uma série de escândalos envolvendo vazamento de dados alterou seu comportamento *online*, conforme foi exposto no Gráfico 4.

No Gráfico 5, a seguir, a Organização Internet Society revela a incipiente indisposição dos usuários em fazer negócios com empresas que tiveram seus dados vazados:

Gráfico 5 – Disposição para fazer negócios com uma companhia que teve dados financeiros e sensíveis “roubados”

Fonte: Imagem adaptada de SafeNet, 2016 *Apud* Internet Society, 2016, p. 59.

Neste gráfico, têm-se os seguintes resultados: 40% dos usuários responderam que “nunca mais” fariam negócios com empresas que tiveram dados invadidos; 25% disseram que a relação comercial seria “muito improvável”; 15% asseguraram que a relação comercial seria “um pouco improvável”; 14% “talvez”; na contramão dos dados estatísticos apresentados, apenas 4% responderam que “muito provavelmente” fariam negócios e 2% “definitivamente”, portanto, sendo indiferentes ao vazamento dos dados sigilosos).

A pesquisa foi aplicada nos Estados Unidos, Reino Unido, Alemanha, Austrália e Japão. Ainda de acordo com o mesmo estudo, 49% dos respondentes concordavam ao afirmar que as empresas não levavam a Segurança da Informação a sério o suficiente (INTERNET SOCIETY, 2016, p. 58).

E dada as mudanças comportamentais expostas no início deste capítulo, conclui-se que a cada brecha na segurança, a cada vazamento e a cada escândalo, as empresas perdem a credibilidade de seus clientes, gerando ainda possível impacto financeiro indireto, uma vez que, de acordo com o Gráfico 4, eventos de falta de segurança afetaram o comportamento *online*, visto que os usuários passaram a efetuar menos compras *online* e diminuíram as transações virtuais. De acordo com a Internet Society, a totalidade dos custos ainda não serve para fornecer a uma organização a completa dimensão deste tipo de desastre (INTERNET SOCIETY, 2016, p. 58).

3.4 O círculo da segurança

De acordo com as informações apresentadas, é impreterível que se dê a devida atenção ao desenvolvimento e aplicação efetiva de uma Política de Segurança em harmonia com as necessidades, cultura e missão de um negócio. A informação, como visto, é um bem precioso que deve ser preservado e, nos tempos atuais em que a conexão com a Internet segue aumentando, a atenção deve ser redobrada em todas as áreas, uma vez que a Engenharia Social não se restringe somente a ataque virtuais.

De acordo com Peixoto (2006, p. 20):

> Se todo funcionário fosse tão questionador como uma criança, demonstrando interesse nos mínimos detalhes, ouvindo mais, estando fortemente atento a tudo à sua volta, e principalmente fazendo o uso dos poderosos “por quês”, com certeza as empresas transformariam os frágeis cadeados em legítimos dispositivos dificultantes de segurança da informação.

E, em conformidade com Marciano, a respeito de Políticas de Segurança dentro de um grupo, “quanto mais rapidamente a prática se torna um ritual, mais facilmente a norma é obedecida, evitando assim o individualismo e os comportamentos aversivos às práticas prescritas como adequadas” (2006, p. 190), uma vez que o comportamento do grupo influenciará todos os seus membros, e como assegurou Skinner (2003), o comportamento do grupo só é moldado através de interações com seus próprios indivíduos.

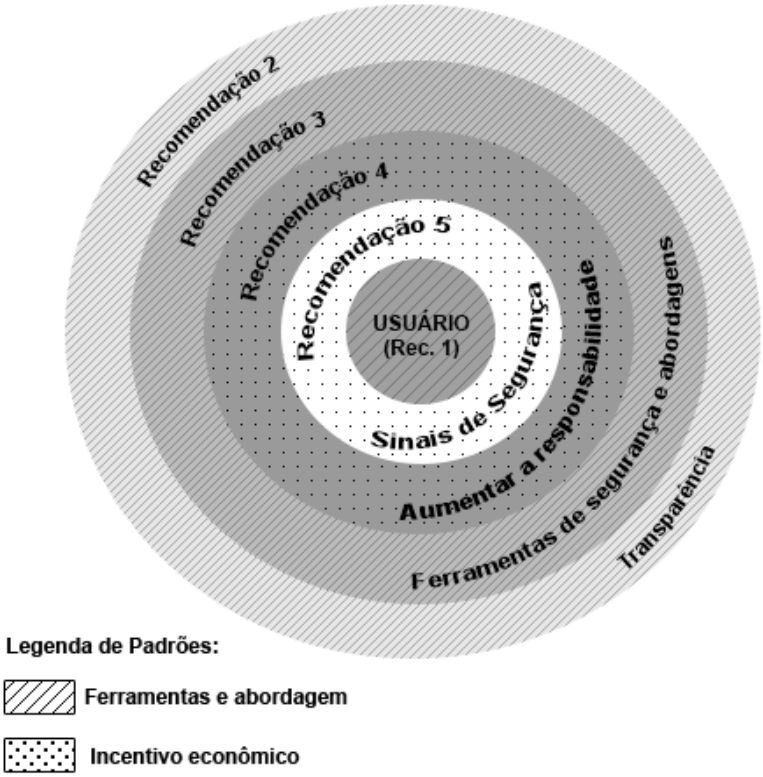
Partindo desse princípio, ainda no estudo divulgado pela Internet Society, são feitas cinco recomendações para as empresas, no intuito de lidar com Segurança da Informação, sendo elas:

> 1. Colocar os usuários sempre no centro de todas as soluções;
> 2. Aumentar a transparência a respeito de violação de dados e divulgação;
> 3. Segurança da Informação deve ser prioridade e as organizações devem possuir altos padrões de práticas e segurança;
> 4. Organizações devem se responsabilizar por suas violações; e
> 5. Aumentar incentivo de mercado para o desenvolvimento de métodos de segurança[7](INTERNET SOCIETY, 2016, p. 19).

[7] "1- Put users at the centre of solutions; and include the costs to both users and organisations when assessing the costs of data breaches.
2- Increase transparency through data breach notifications and disclosure.
3- Data security must be a priority. Better tools and approaches should be made available. Organisations should be held to best practice standards when it comes to data security.
4- Organisations should be accountable for their breaches. General rules regarding the assignment of liability and remediation of data breaches must be established up front.
5- Increase incentives to invest in security by catalysing a market for trusted, independent assessment of data security measures." (INTERNET SOCIETY, 2016, p. 19. *Tradução nossa*!)

A primeira das recomendações endossa o que vem sido discutido neste trabalho a de que Fator Humano influencia diretamente a segurança das informações. Como mostrado na imagem abaixo, oriunda do Relatório da Internet Society (2016), o círculo da segurança baseia-se nas cinco recomendações supracitadas, têm-se:

Figura 6 – O Círculo da Segurança da Informação



Fonte: Imagem adaptada de Internet Society, 2016, p. 21.

Conforme o círculo indica a Segurança está centralizada no usuário e dividida entre “Ferramentas e Abordagem” e “Incentivo Econômico”. A primeira recomendação (Rule 1) está contida dentro de “Ferramentas e Abordagem”, colocando o fator humano ao centro. Já a segunda recomendação engloba todos os demais itens, por tratar-se da transparência que deve haver entre organizações e usuários.

A terceira recomendação também está inserida em “Ferramentas e Abordagem”, uma vez que as organizações devem ter a Segurança da Informação em alta consideração dentro de sua cultura de governança corporativa. A quarta recomendação está contida no “Incentivo Econômico”, pois ela defende que as organizações devem ser totalmente responsabilizadas por suas brechas de

segurança; sendo assim, esta recomendação é expedida precisamente para que isso se altere e sirva de incentivo para que todas as organizações tomem ciência do real valor de todas as informações que nelas circulam, sejam de clientes, sejam de terceiros (INTERNET SOCIETY, 2016, p. 18). Já a quinta recomendação (Rule 5) diz respeito a incentivos financeiros para que a novos métodos de segurança sejam desenvolvidos, catalisando um mercado específico, especialista e independente a respeito do assunto.

O cenário atual, de acordo com os estudos da Organização Internet Society (2016), revela consideravelmente uma maior preocupação com a Segurança da Informação após tantos sinistros virtuais ocorridos, como o supracitado vazamento de dados do Facebook (LA MONICA, 2018, *In.*: CNN MONEY, 2018), juntamente a uma mudança de comportamento *online*, em virtude destas mesmas vulnerabilidades no mundo virtual. Em contrapartida, vale ressaltar que os componentes de uma organização são, de fato, outros indivíduos. Corroborando com a linha de pensamento de Skinner (2003), conforme já citado, o grupo molda o comportamento individual e este também se altera se for deslocado para um outro grupo diferente do original, logo, entende-se porque trata-se de "indivíduo" separado de "organização", mesmo sendo uma organização um grupo de indivíduos regidos pela mesma cultura, regras e padrões de comportamento. No estudo divulgado da Internet Society (2016, p. 135) pressupõe-se que, por mais que sejam os usuários as maiores vítimas das violações de segurança, não são eles os maiores focos quando se discute Segurança da Informação[8]. Logo, o então classificado "elo mais fraco" não obtém o foco que lhe é devido.

Embora esta reflexão não constitua o cerne desta monografia, é interessante notar que as violações a dados financeiros não representam tão grande ameaça como o possível "roubo ou furto de identidade", questão fundamentalmente de cunho ético-moral, que pode ser indiscutivelmente preocupante para os indivíduos e para os sistemas governamentais, haja vista que, de acordo com o Relatório da Internet Society, o número de usuários com acesso à Internet aumentou consideravelmente

[8] "While users are the ultimate victims of data breaches, and their trust is affected, currently, users, and their trust, are not the main focus of approaches to data breaches." (INTERNET SOCIETY, 2016, p.135. *Tradução nossa*!)

de 2005 a 2015. Não obstante, estas linhas não têm a intenção de debruçar sobre a temática proposta, elemento que poderá ser discutido em outras futuras pesquisas.

Para o próximo capítulo, será exposta uma pesquisa no intuito de entender, por meio de uma amostra de 151 usuários, o que estes julgam como importante para se preservar as informações dentro de um ambiente corporativo.

CAPÍTULO IV – ESTUDO DE CASO

No presente capítulo, deve-se analisar acerca do nível de ciência, esperado e desejado, dos funcionários de diversos ramos do setor terciário sobre Segurança da Informação e Engenharia Social. A análise que será apresentada foi amparada por uma pesquisa realizada por meio de uma ferramenta *online* gratuita do Google (Google Forms). A pesquisa buscou coletar dados que serão tratados de forma quantitativa e qualitativa, foi realizada entre os meses de abril e junho de 2018, e contou com 151 (cento e cinquenta e um) respondentes.

A pesquisa foi conduzida de forma anônima, de modo a preservar a identidade dos respondentes, sob o intuito de não comprometer de maneira alguma as empresas nas quais os respondentes-colaboradores atuam. Julgou-se imprescindível a coleta de respostas provenientes de respondentes que, de fato, trabalhassem, desconsiderando, portanto, os usuários e demais colaboradores que não tivessem um vínculo empregatício formal ou informal. Foram elaboradas dezesseis perguntas das quais duas destinavam-se para a coleta de respostas abertas (questões 1 e 14):

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

1. Você trabalha em qual ramo de negócio? (Informática, Contabilidade, Gestão, Saúde, Comércio, etc)

2. Você tem acesso a informações confidenciais de clientes ou até mesmo da própria empresa onde você trabalha? (e.g. registros de funcionários, documentos, pagamentos, contas, etc)

3. Seu local de trabalho possui algum controle de acesso físico, como porteiros, portas liberadas somente com crachás, leitor de biometria, etc?

4. Sua empresa possui sistemas de vigilância e/ou alarmes contra acesso indevido?

5. Seu local de trabalho possui controles de acesso virtuais nos computadores, como antivírus, firewalls, login/senha, etc?

6. Em caso de antivírus e firewalls, os mesmos são mantidos sempre atualizados? (desconsiderar se não houver)

7. Em caso de login/senha, existe uma política de senha vigente (e.g. obrigatório letra maiúscula, símbolos, números, trocas de senha a cada x período de tempo)? (desconsiderar se não houver)

8. Existe, em seu local de trabalho, algum local seguro (e.g. uma gaveta com tranca, cofre, armários com tranca, etc) para funcionários guardarem dispositivos eletrônicos pessoais ou empresariais, ou qualquer objeto de valor?

9. Em caso de laptops, existem cable lockings (como na imagem)[9] para mantê-los presos à mesa?

10. Olhe em volta, no ambiente de trabalho: existe algum papel contendo informações sigilosas à vista? Ou mesmo algum instrumento/dispositivo/documento de trabalho que pudesse ser furtado, causando problemas para a empresa?

11. Seu local de trabalho já foi vítima de fraude, roubo, furto ou algum outro acesso indevido?

12. Caso tenha respondido sim à questão 11, o quão ruim foi o incidente?

13. Caso tenha respondido 'não' ou 'não sei' à questão 11, em sua opinião, o quão fácil seria, para alguém mal-intencionado, provocar qualquer incidente de segurança em seu local de trabalho?

14. Brevemente, o que você considera essencial para se preservar a integridade das informações de uma empresa?

15. Você sabe o que é Política de Segurança?

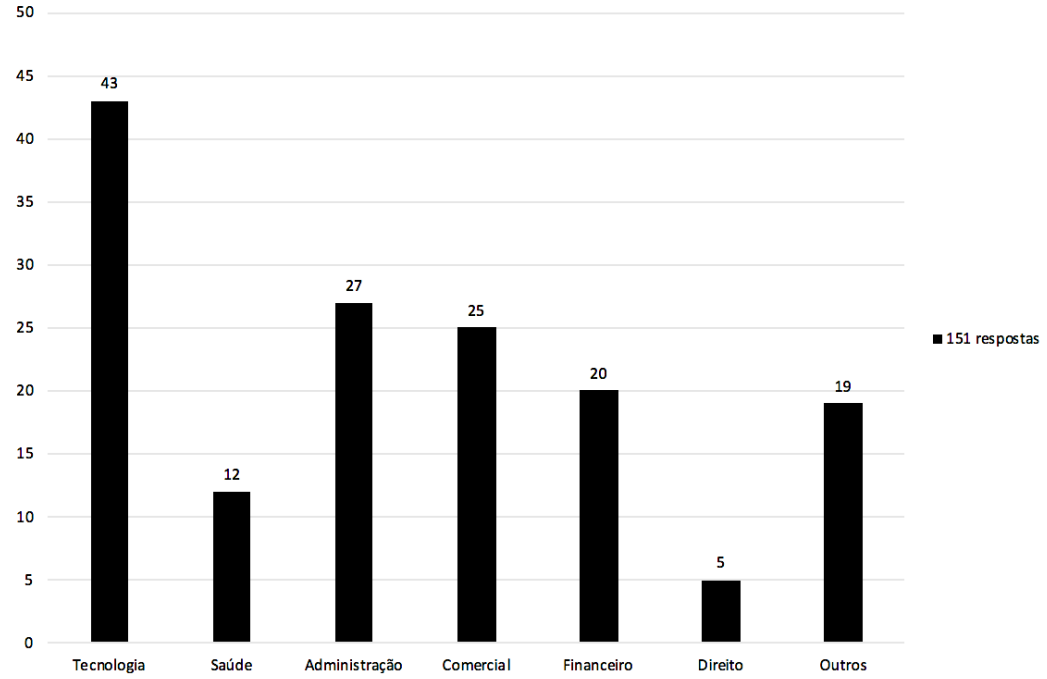
16. Você sabe o que é Engenharia Social?

Com o objetivo de clarificar as análises seguintes, neste momento, apenas será analisada qualitativamente as respostas derivadas da questão 1; quanto à questão 14, de natureza aberta, será avaliada em outra ocasião, ainda neste capítulo.

O histograma a seguir, apresentado no Gráfico 6, traz a área de atuação dos respondentes da pesquisa, de acordo com as respostas abertas dadas à primeira questão:

[9] A ilustração do *cable locking* foi obtida do Google Imagens, proveniente do site Killa Design. Disponível em: <https://www.killadesigns.co/blog/apple-releases-mac-pro-security-lock-just-no-cable>. Acesso em: 20 jun. 2018

Gráfico 6 – Grupos de atuação dos respondentes da pesquisa



Fonte: Autoria própria (2018): Dados da pesquisa.

Na intenção de separar as inúmeras respostas obtidas, muitas delas genéricas, foram criados sete grupos de áreas de atuação:

Grupo 1 – Tecnologia;

Grupo 2 – Saúde: atuantes em vários setores da área de saúde;

Grupo 3 – Administração: colaboradores da pesquisa relacionados à Gestão, Auxiliar administrativo, Recursos Humanos e Secretaria;

Grupo 4 – Comercial: colaboradores da pesquisa relacionados ao comércio, mercado, Telemarketing, vendas, balconista;

Grupo 5 – Financeiro: profissionais com atuações em Banco e em Contabilidade;

Grupo 6 – Direito: profissionais relacionados ao ramo jurídico e de advocacia;

Grupo 7 – Outros.

No Gráfico 6, observa-se que a maior parte dos respondentes, aproximadamente 29% da amostragem, atuam na área de Tecnologia (1º dos 7 grupos de respondentes), sendo estes vinculados à Tecnologia da Informação e Informática.

Há, ainda, um grande número de respondentes que atuam na área de Administração, com 18% da amostra proveniente da análise do Grupo 3.

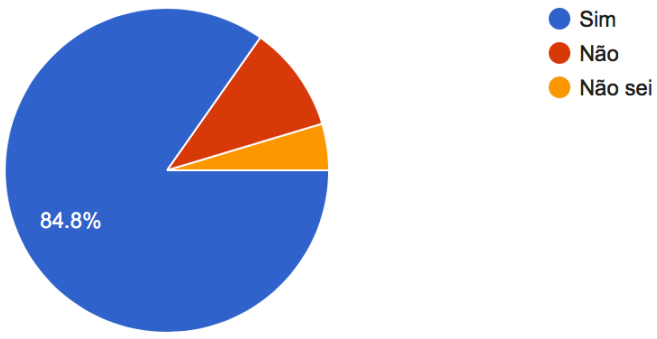
No Grupo 4 dos respondentes, aproximadamente 17% atuam no setor comercial, ao passo que no setor financeiro, Grupo 5 das respostas, algo em torno de 13% das respostas obtidas. Já para os setores de Saúde, identificados no Grupo 2, e de Direito (pertencentes ao Grupo 6), têm-se, respectivamente, 8% e 3,5% de respostas.

Na categorização genérica do Grupo 7, denominado “Outros”, foram englobadas diversas áreas de atuação, tais como “Serviços”, “Têxtil”, “Publicidade”, “Indústria de bens de capital (Máquinas)”, “Imobiliária”, “Empresas de Construção Civil”, “Serviços públicos”, “Educação”, “Jornal”, “Games/Jogos”, “Call center”, “Produção”, “Suporte técnico”.

Como as respostas à primeira questão eram demasiadamente genéricas, foi estabelecido o seguinte critério metodológico: considerar, no mínimo, quatro respostas idênticas à mesma ou similar função, ramo ou setor de atuação; estas, no Grupo 7, totalizaram, portanto, 12% do montante das 151 respostas.

Após determinar o grupo de atuação dos respondentes no mercado de trabalho, elemento essencial para a compreensão das próximas análises, agora de natureza quantitativa, a autora desta pesquisa julgou pertinente indagar aos colaboradores desta enquete se lidavam ou não, no dia a dia, com informações confidenciais no local de trabalho ou de clientes:

Gráfico 7 – Manuseio de informações confidenciais no dia a dia



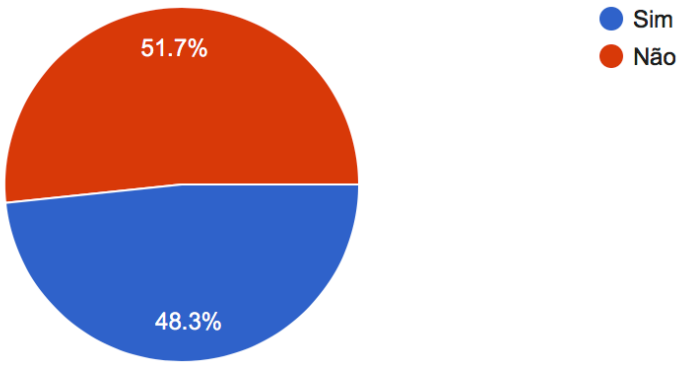
Fonte: Autoria própria (2018): Dados da pesquisa.

No tocante à proposta do Gráfico 7, 128 respondentes afirmaram lidar com informações confidencias em seu dia a dia de trabalho, o que representa aproximadamente 85% de toda a amostragem. Somente 16 de 151 dos respondentes disseram não manusear qualquer tipo de informação sensível (quase 11%), enquanto 4,5% dos participantes (7 colaboradores) não tinham certeza.

Seguindo esta linha de raciocínio, a autora buscou entender, com as próximas sete perguntas, o quão seguro é o ambiente de trabalho, no tocante a acessos físicos e virtuais.

O Gráfico 8, a seguir busca quantificar quantos dos respondentes trabalhavam em um ambiente que possuía controles de acesso físico, como biometria, porteiros, portas liberadas somente com crachá, dentre outros:

Gráfico 8 – Controles de acesso físico no ambiente de trabalho

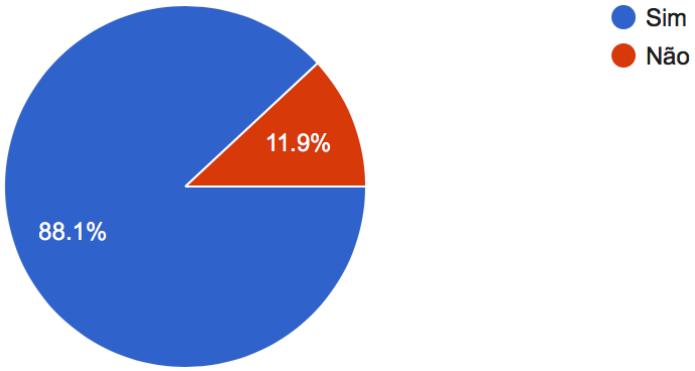


Fonte: Autoria própria (2018): Dados da pesquisa.

Para a questão proposta no Gráfico 8, aproximadamente 52% dos respondentes afirmaram que a empresa na qual atuam não possui controles de acesso físico, ao passo que quase 49% disseram que sim, ou seja, 73 dos 151 respondentes.

Seguindo a proposta da autora de compreender os controles de acesso físico e virtuais que as empresas possuíam, no tocante a sistemas de vigilância e alarmes, obteve-se o Gráfico 9, a seguir:

Gráfico 9 – Alarmes e sistemas de vigilância

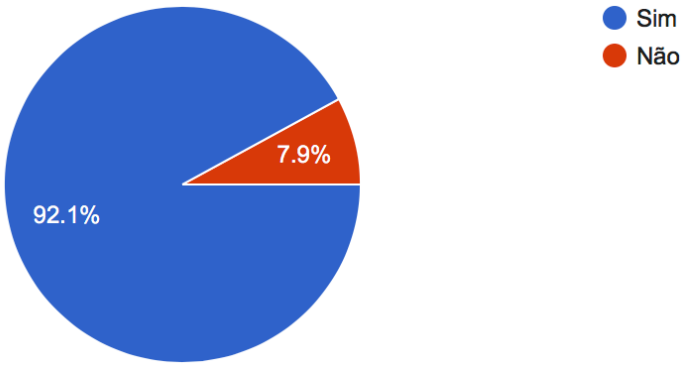


Fonte: Autoria própria (2018): Dados da pesquisa.

Neste Gráfico, pode-se observar que, enquanto aproximadamente 12% afirmavam negativamente, o restante dos participantes, representados por quase 89%, afirmam que, na empresa onde atuam, existe um sistema de vigilância e/ou um sistema de alarmes contra acesso indevido, ou seja, 133 dos 151 colaboradores.

Na análise gráfica a seguir, baseada na questão 5, buscou-se assimilar se os computadores manuseados pelos respondentes, no ambiente de trabalho, possuíam controles de acesso virtual, como *logins* e senhas, *firewalls*, antivírus e afins:

Gráfico 10 – Controles de acesso virtuais



Fonte: Autoria própria (2018): Dados da pesquisa.

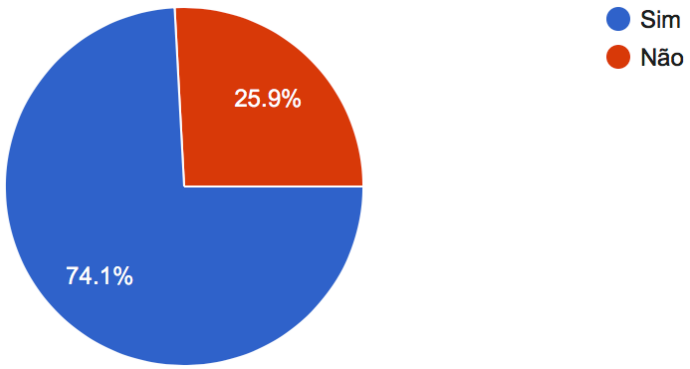
Conforme demonstrado neste Gráfico, a maioria dos respondentes (139), aproximadamente 92%, respondeu que há controles de acesso virtuais de qualquer

cunho no computador usado no ambiente de trabalho, enquanto apenas 8% respondeu que não.

Para fins de esclarecimentos quantitativos, os Gráficos 11 e 12, derivados das questões 6 e 7, não tiveram o mesmo número habitual de respondentes, visto que a questão 5 era disjuntiva, podendo os colaboradores responderem afirmativa ou negativamente à enquete. Sendo assim, não se obteve o montante de 151 respostas, mas apenas 139, visto que 12 colaboradores responderam negativamente à questão 5. As informações estatísticas estão, portanto, alicerçadas neste novo número de respondentes, ou seja, 139.

O Gráfico 11, baseado na questão 6, refere-se especificamente aos antivírus e *firewalls*, a fim de entender se estes são ou não mantidos frequentemente atualizados:

Gráfico 11 – Antivírus e *firewalls* são constantemente atualizados



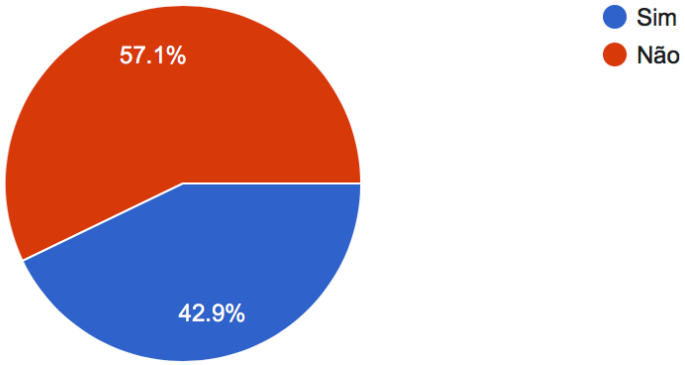
Fonte: Autoria própria (2018): Dados da pesquisa.

Este Gráfico revela que aproximadamente 26% dos 139 respondentes afirmaram negativamente, ao passo que 74% afirmaram que os antivírus e *firewalls* são constantemente atualizados, ou seja, 103 colaboradores.

A análise apresentada pelo Gráfico 12, a seguir, refere-se especificamente aos *logins* e senhas, e visa captar a informação se estes recursos de segurança são regidos por uma Política de Senha, ou seja, Política de Segurança, conforme foi

aludido no Capítulo II. A questão, assim como a anterior, não era obrigatória, destinando-se àqueles que responderam afirmativamente ao Gráfico 10.

Gráfico 12 – Existência de uma Política de Senha

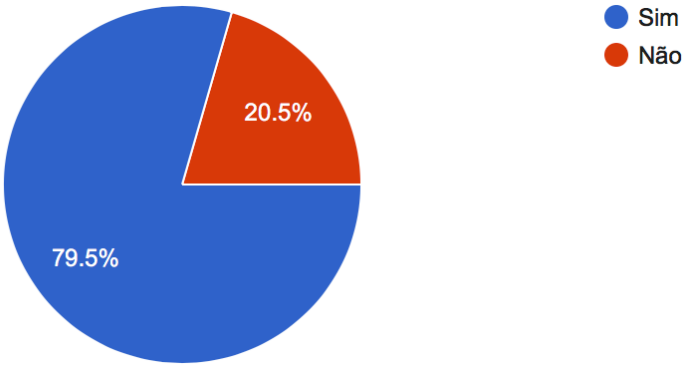


Fonte: Autoria própria (2018): Dados da pesquisa.

No Gráfico 12, assim como no anterior, obteve-se 139 respostas, das quais 57% são negativas à existência de Política de Senha (79 colaboradores), enquanto aproximadamente 43% afirmaram a vigência deste tipo de Política (60).

A análise gráfica a seguir, origina-se da questão número 8, de cunho obrigatório, por meio da qual a autora desta pesquisa inquiriu aos participantes se, em seus respectivos ambientes de trabalho, existia algum local seguro para guardar pertences pessoais ou coorporativos, como cofres, armários, gavetas com trancas, e afins. Das 151 respostas analisadas, obteve-se a informação gráfica abaixo:

Gráfico 13 – Local seguro para armazenar pertences

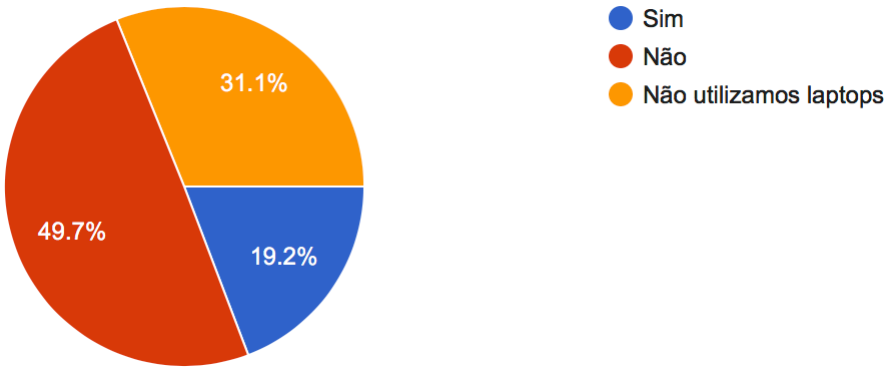


Fonte: Autoria própria (2018): Dados da pesquisa.

No Gráfico 13, 79,5% dos respondentes afirmaram existir um local seguro para armazenar pertences pessoais ou coorporativos, ou qualquer outro objeto de valor e documentos sigilosos, ao passo que 20,5% dos 151 respondentes da amostra negou (31 colaboradores).

No Gráfico 14, buscou-se especificar quantos participantes da pesquisa utilizavam-se de *cable lockings* para manter *laptops* da empresa presos à mesa ou qualquer outro local seguro, a fim de evitar furtos ao se ausentarem. Buscou-se, também, quantificar quantos deles não utilizavam *laptops*.

Gráfico 14 – Utilização de *cable lockings* nos *laptops*

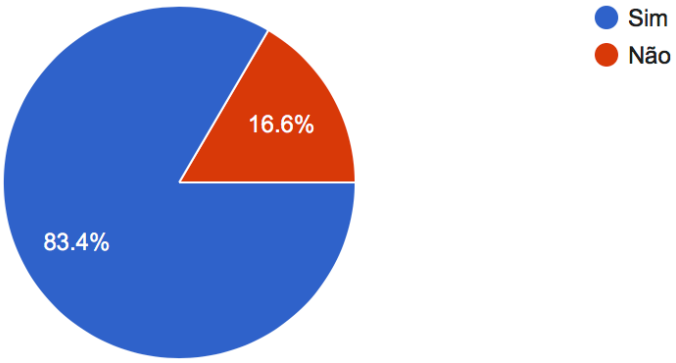


Fonte: Autoria própria (2018): Dados da pesquisa.

Como verificado neste Gráfico, somente 19,2% dos participantes afirmaram fazer a utilização de *cable lockings* a fim de manter *laptops* presos à mesa ou qualquer outro local seguro, ou seja, 29 colaboradores. Outros 49,7% respondentes utilizavam *laptops*, porém, não utilizavam *cable lockings* (75), ao passo que o restante 31,1% não utilizavam *laptops* em seus trabalhos, ou seja, 47 pessoas utilizavam outro tipo de ferramenta computacional.

Para finalizar o entendimento geral do ambiente de trabalho de seus respondentes, na proposta final, a autora deste trabalho sugere que os mesmos olhem a sua volta, em seus escritórios, e respondam se há algum documento, dispositivo de trabalho, instrumento e afins, à vista de todos, que poderia ser facilmente furtado e causar problemas de segurança para a empresa. O resultado da proposta é apresentado pelo Gráfico 15, a seguir:

Gráfico 15 – Informações sigilosas à vista de todos durante expediente

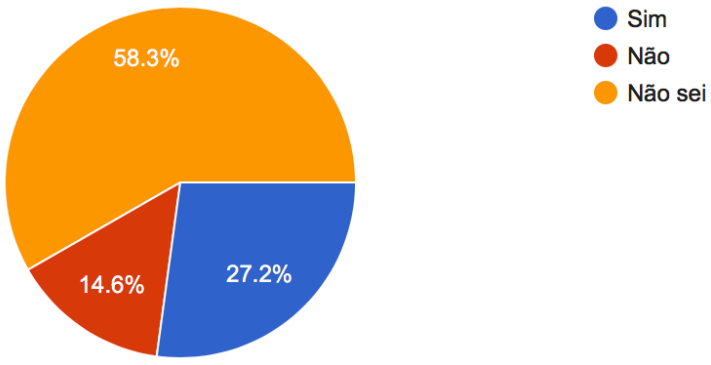


Fonte: Autoria própria (2018): Dados da pesquisa.

Como observado no Gráfico 15, aproximadamente, 84% dos respondentes afirmou existir informações sigilosas, à vista de todos, as quais poderiam ser furtadas e causar grandes problemas à empresa na qual atuam, isto é, 126 colaboradores da pesquisa. Enquanto o restante dos respondentes, quase 17%, afirmou não existir nada sigiloso à vista.

A respeito da questão 11, a autora desta pesquisa buscou compreender se os respondentes sabiam se a empresa na qual atuavam já havia sofrido algum tipo de incidente envolvendo segurança, como fraude, roubo, furto ou algum acesso indevido. As respostas foram quantificadas no gráfico a seguir:

Gráfico 16 – Incidente de segurança na empresa onde atua



Fonte: Autoria própria (2018): Dados da pesquisa.

A maioria dos 151 respondentes afirmou não ter conhecimento de qualquer incidente de segurança envolvendo a empresa na qual atuam, representados por

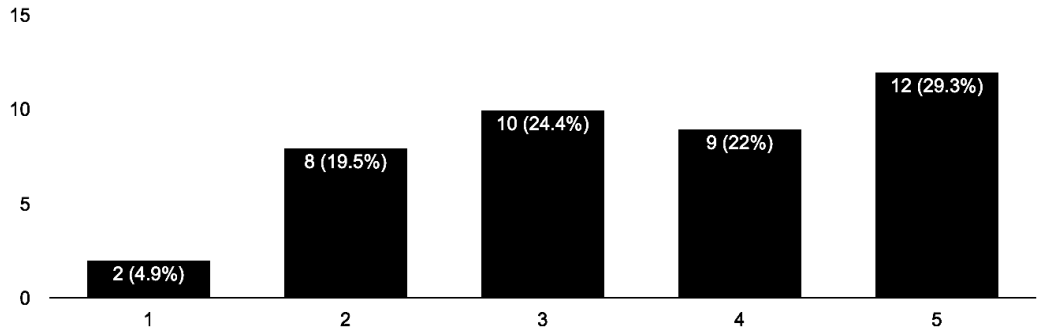
aproximadamente 58% da amostra (88). Ao passo que quase 15% responderam negativamente (22), enquanto os que asseguram ter conhecimento de algum incidente estão quantificados por volta dos 27% do total, ou seja, 41 colaboradores.

O histograma a seguir foi destinado aos participantes que responderam “Sim” à questão anterior, ou seja, explicitamente para os 41 colaboradores, e objetivou captar, de acordo com suas opiniões, o quão grave foi o incidente ocorrido em seus locais de trabalho. Destas 41 respostas, a autora desta pesquisa utilizou-se de uma escala de 1 a 5 para mensurar o impacto do incidente, sendo:

1. Impacto quase imperceptível;
2. Impacto perceptível;
3. Impacto mediano;
4. Impacto Grave; e
5. Impacto Gravíssimo.

O gráfico a seguir, baseado em 41 respostas, elucida o nível de gravidade do incidente ocorrido:

Gráfico 17 – Gravidade do incidente



Fonte: Autoria própria (2018): Dados da pesquisa.

Observa-se que, na opinião dos entrevistados, somente 2 de 41 (4,9%) responderam que o incidente sofrido pela empresa no qual atuavam foi “quase imperceptível”, dados mensurados na escala 1.

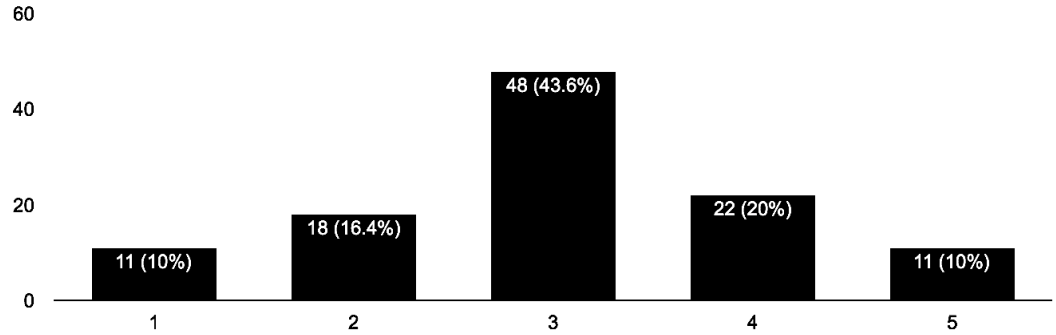
Oito dos respondentes afirmaram que se tratou de um incidente de “Impacto Perceptível” (19,5%), enquanto 10 colaboradores consideraram um “Impacto Mediano”, avaliado na escala 3, no incidente do qual tinham conhecimento, ou seja, 24,4%. A respeito da escala 4, 9 de 41 respondentes afirmaram que o impacto gerado

pelo tal incidente foi “Grave”, enquanto a maior parte dos respondentes, doze, responderam que o impacto foi de cunho “Gravíssimo”, ou seja, 29,3% dos colaboradores.

O histograma a seguir, por sua vez, traz os resultados de uma proposta da autora da pesquisa, que se direcionava aqueles que haviam respondido “Não” e “Não Sei” à pergunta do Gráfico 16, que gerou um montante de 110 respondentes, sendo 22 “Não” e 88 “Não sei”. Considerando a opinião destes respondentes, baseando-se em suas experiências e observações diárias, a pergunta buscou quantificar o quão suscetível a incidentes de segurança encontra-se os respectivos ambientes de trabalho. Para mensurar o grau destas suscetibilidades a incidentes de segurança, a partir das observações e das experiências singulares dos respondentes, utilizou-se uma escala de 1 a 5, sendo:

1. Muito suscetível;
2. Suscetível;
3. Mediano;
4. Dificilmente suscetível; e
5. Muito dificilmente suscetível.

Gráfico 18 – Suscetibilidade para um incidente de segurança



Fonte: Autoria própria (2018): Dados da pesquisa.

Como observado neste gráfico, 48 de 110 entrevistados (43,6%) responderam que, de acordo com suas experiências e observações diárias, a probabilidade de acontecer um incidente de segurança em seus ambientes de trabalho é “mediana”, dados mensurados na escala 3.

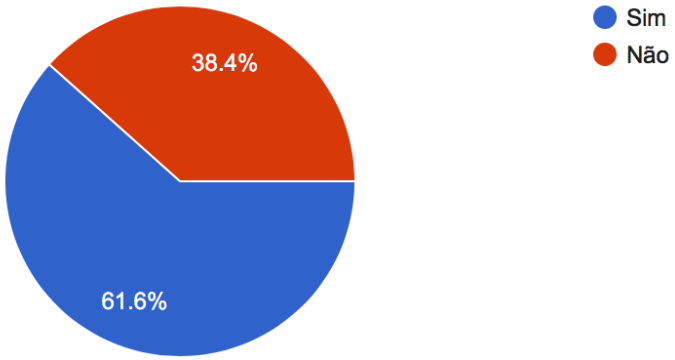
Onze dos colaboradores consideraram-se trabalhando em um ambiente “muito suscetível” ao um incidente de segurança (10%), mensurado na escala 1. E, também, 18 das 110 respostas (16,4%) estão mensuradas na escala 2, considerando seus locais de trabalho como “suscetíveis” a incidentes.

Nas escalas 4 e 5 têm-se, respectivamente, 22 colaboradores que consideram seus ambientes de trabalho como dificilmente suscetível a qualquer incidente (20%), e 11 que afirmam como sendo muito dificilmente suscetível a um incidente de segurança.

Nas últimas duas propostas de cunho quantitativo, a autora buscou compreender dos participantes se conheciam Políticas de Segurança e Engenharia Social, haja vista que todos são atuantes no mercado de trabalho e a maioria manuseia informações confidenciais em sua rotina de trabalho, conforme foi testificado no Gráfico 7.

O gráfico a seguir indica o grau de conhecimento sobre Política de Segurança:

Gráfico 19 – Você sabe o que é Política de Segurança?

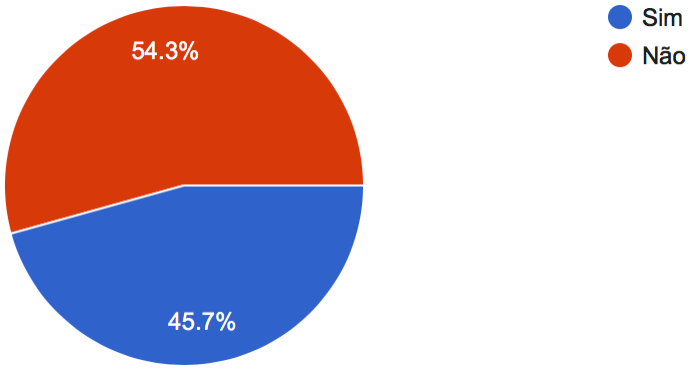


Fonte: Autoria própria (2018): Dados da pesquisa.

Como visto na informação gráfica supracitada, a maioria dos respondentes afirmou saber sobre Política de Segurança, algo em torno de 62% da amostragem, ao passo que quase 38% afirmaram desconhecer, ou seja, 58 colaboradores da pesquisa.

Por último, o gráfico a seguir explicita o grau de conhecimento sobre a Engenharia Social:

Gráfico 20 – Você sabe o que é Engenharia Social?



Fonte: Autoria própria (2018): Dados da pesquisa.

Conforme demonstrado no Gráfico 20, quase 54% afirmaram desconhecer a respeito da Engenharia Social (82 colaboradores), enquanto 45,7% dos 151 respondentes afirmaram ter conhecimento.

Concernente à pergunta no 14, de natureza aberta e qualitativa, será utilizado o recurso metodológico de Análise de Conteúdo, na intenção de separar as respostas obtidas, muitas delas genéricas, e agrupá-las por ideias similares em prioridades que atendam à proposta de pesquisa deste trabalho.

Após esta análise, os grupos obtidos pela autora são os seguintes:

Grupo 1 – Colaboradores que citaram explicitamente Políticas de Segurança;

Grupo 2 – Respostas vinculadas às normas genéricas, regras, boas práticas, instruções e afins;

Grupo 3 – Ideias que deem importância à liderança e gestão do grupo;

Grupo 4 – Respostas atreladas aos aspectos da conduta ética e moral individual ou coletiva do fator humano; e

Grupo 5 – Colaboradores que priorizem sistemas de segurança físicos e virtuais.

De acordo com a metodologia para se criar uma Análise de Conteúdo:

> O conteúdo não pode, sob nenhuma hipótese, ser passível de classificação em mais de uma categoria. Isso remete à regra número 1, que diz que a definição das categorias deve ser clara. O que está em uma categoria, não pode estar em outra. Um determinado conteúdo não pode ser passível de ser classificado uma ou outra categoria, a depender da interpretação do analista. As categorias não podem ter elementos que se sobreponham ou sejam redundantes, que possibilite que as mensagens (conteúdo) se encaixem em uma ou outra categoria. A quebra desta regra levaria à ausência de confiabilidade (CARLOMAGNO; ROCHA, 2016, p. 178-179).

Por razões didáticas e metodológicas, e também por conta da dificuldade ao separar respostas demasiadamente genéricas e passíveis de serem classificadas em duas ou mais das categorias descritas acima, a resposta obtida através de pesquisa que diz, explicitamente: “Consciência e boa Política de Segurança” foi classificada no Grupo 1, a despeito do Grupo 4, uma vez que seu conteúdo corrobora diretamente com a temática central deste trabalho. Igualmente as respostas “Boa Política de Segurança, backups e softwares de proteção”, “Boas lideranças e boa Política de Segurança”, bem como “a empresa não só ter boas políticas, mas fazer com que seus funcionários as sigam” e “Boa Política de Segurança, backups e softwares de proteção” foram classificadas no Grupo 1 pela mesma razão metodológica apresentada.

No tocante às respostas fornecidas como “boas normas de Segurança da Informação e também equipamentos de segurança”, “estar atento quanto as más intenções, manter antivírus e *firewalls* atualizados, boas práticas” e “boas normas de segurança, aparelhos/equipamentos”, estas foram inseridas no Grupo 2, e não Grupo 5, em virtude do conteúdo apresentado estar intimamente vinculado ao tema central desta pesquisa. Também no Grupo 2 estão consideradas as respostas “ser sempre consciente e seguir regras de segurança”, “boas práticas e funcionários cuidadosos”, assim como “comprometimento em cumprir normas, treinamentos, etc.”, “estar sempre comprometido em seguir boas práticas” e “manter a consciência sobre ataques tanto físicos quanto virtuais, com regras e boas práticas”, a despeito do Grupo 3, também pelo fato de a autora considerar a categorização do grupo fortemente relevante para o amparo de seu problema de pesquisa proposto.

No que diz respeito ao Grupo 3, foram inseridas as respostas ambíguas “gestão comprometida e sigilo”, “informar a todos dos riscos e como agem os infratores, estar sempre alerta”, bem como “critérios de contratação e preocupar-se com segurança”, uma vez que a autora desta pesquisa também considerou relevante

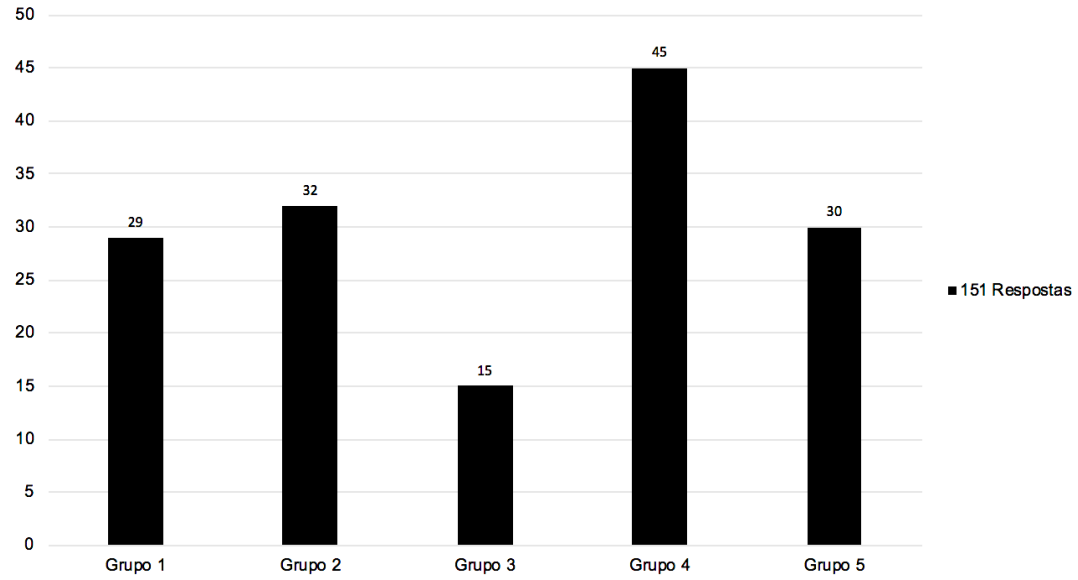
para seu problema de pesquisa a importância atribuída à gestão e à liderança dos grupos.

No Grupo 4, foi inserida a resposta “sigilo, profissionais capacitados e honestos, e um ótimo sistema de vigilância e proteção, tanto aos trabalhadores quanto aos consumidores ou clientes”, uma vez que a ideia que categoriza o grupo ter sido expressada pelo colaborador antes daquela que está relacionada ao Grupo 5, o qual engloba sistemas de vigilância física e virtuais. O mesmo critério de categorização foi utilizado para inserir as respostas “programas bons que ajudem a proteger os sistemas de computador, boa conscientização para manter a segurança física e virtual” e “sistemas de câmera, seguranças e conscientização” junto ao Grupo 5.

A autora tem por primeira intenção categorizar, unificar e parametrizar as respostas, visando garantir certo grau de inteligibilidade do conteúdo, sem ter, *a priori*, nenhum intuito de gerar dados prolixos ou ambíguos, imprecisos e, sobretudo, tornar a reflexão qualitativa genérica.

O histograma a seguir apresenta os resultados obtidos após a categorização dos grupos supracitados:

Gráfico 21 – Elemento essencial para se preservar informações sensíveis



Fonte: Autoria própria (2018): Dados da pesquisa.

No Gráfico 21, observa-se que os colaboradores inseridos no Grupo 1, os quais citam as Políticas de Segurança, explicitamente, para se preservar a integridade das informações, são algo em torno de 19,2% de 151, ou seja, 29.

No Grupo 2 de respondentes, obteve-se um total aproximado de 21% (32 respostas de 151) de respostas que consideravam importantes normas, regras, instruções, boas práticas e quaisquer padronizações genéricas, a fim de manter a integridade das informações.

Já na categorização do Grupo 3, foram agrupadas respostas que consideravam importante a liderança/gestão do grupo, sob o intuito de manter a integridade das informações, o montante de respostas foi de aproximadamente 10% de 151, ou seja, 15 colaboradores com ideias similares.

A respeito do Grupo 4, o maior agrupamento de respostas, algo em torno de 30% (45) dos colaboradores atribuem à conduta ética e moral do grupo ou do indivíduo a maior importância na hora de se preservar a integridade de informações confidenciais. Ao passo que no Grupo 5, 20,5% dos 151 colaboradores consideravam que os fatores externos, ou seja, sistemas de segurança física e virtual, são elementos de vital importância para atingir este mesmo objetivo.

4.1 Análise do Estudo de Caso

Com base nos dados apresentados, o manuseio de informações sensíveis por parte de funcionários de empresas, em suas rotinas de trabalho, é constante. Quando não se está lidando com informações confidenciais de clientes ou dos próprios locais de trabalho, existem informações individuais, logo, é imperativo que se promova a consciência das mazelas ocasionadas por vazamentos e brechas em quaisquer ambientes nos quais o Fator Humano atue, virtual ou físico.

Vale ressaltar que aproximadamente 70% de 110 respondentes considerou o próprio ambiente de trabalho com segurança fraca ou mediana, considerando a opinião expressas no Gráfico 18. Como discutido no decorrer deste trabalho, é imperativo que as empresas promovam a consciência de seus funcionários e que, também, disponibilizem um ambiente seguro para seu fluxo de informações. Também de acordo com os gráficos citados, a maioria dos respondentes não sabia do que se tratava Engenharia Social, embora o resultado não tenha sido tão discrepante (54,3% não sabiam). A Engenharia Social possui diversos métodos, seus praticantes têm ciência das vulnerabilidades do comportamento humano e, além de tudo, podem analisar suas vítimas durante muito tempo, através de muitas perspectivas, até obter o meio mais eficaz de conseguir aquilo que lhe interessa.

E por mais que a consciência a respeito de Segurança da Informação esteja mudando, como discutido no decorrer deste trabalho e amparado pelo Gráfico 19 a respeito de Política de Segurança, no âmbito coorporativo, ainda se veem poucos mecanismos de defesa, os quais podem não ser suficientes para impedir que um incidente grave aconteça. Como demonstrado pelo Gráfico 15, a maior parte da amostra respondeu haver informações sigilosas à vista de todos durante o expediente (aproximadamente 85%), mas quando confrontado com o Gráfico 8, quase 52% respondeu não haver controles de acesso físico ao local onde trabalham. Por mais que na maioria dos locais de trabalho dos respondentes haja sistemas de vigilância e alarmes (vide Gráfico 9), somente esta barreira não é suficiente para proteger informações sigilosas, dado seu valor no cenário atual.

Outro aspecto importante para endossar o presente raciocínio acima, basta observar o Gráfico 14, o qual demonstrou que a maioria dos usuários de *laptops* nas empresas não utiliza *cable lockings* para mantê-los presos a locais seguros, para a eventual necessidade de ausentar-se da mesa de trabalho, baia e afins. O Gráfico 13 pode servir como possível solução para o problema apresentado no Gráfico 14, já que de acordo com o mesmo, quase 80% da amostra afirmou existir na empresa um local seguro para guardar pertences.

No entanto, é importante ressaltar que há empresas que, de fato, possuem *cable lockings*, contudo, são incompatíveis com todos os tipos de *laptops* existentes, haja vista que há certos modelos que não têm a trava de segurança, nem a abertura própria. Além do mais, ainda que a empresa gere todos os meios para garantir a absoluta segurança dos dispositivos e das máquinas, existe ainda o impasse do uso, ou seja, os funcionários podem se indispor a realizá-los cotidiana e permanentemente, quando saem ao banheiro, ao almoço ou ao cafezinho.

No que tange aos controles de acesso virtual, obteve-se um bom resultado de aproximadamente 92% de toda a amostra afirmando existir algum tipo deles, em seus computadores, sistemas da empresa, e afins. Porém, no que diz respeito a Políticas de Senha, por volta de 57% dos respondentes afirmaram não existir qualquer tipo de regra para se criar senhas fortes e/ou data para trocá-las. Políticas de Senha, como visto no decorrer deste trabalho, são variantes para a implementação de uma Política de Segurança eficaz e abrangente. No tocante a antivírus e *firewalls*, ainda por volta de 25% afirma não os manter atualizados, o que pode ser um fator de risco gravíssimo,

uma vez que códigos maliciosos estão sempre circulando pela Internet e sendo atualizados, conforme a eficácia dos controles de acesso, também é aperfeiçoada.

E, de fato, de acordo com os 41 respondentes que afirmavam ter conhecimento sobre um incidente de segurança que ocorreu em suas respectivas empresas, 31 (por volta de 75% do total) consideravam tal incidente de impacto mediano a muito grave. Conforme foi refletido no decorrer deste trabalho, nenhum controle é totalmente eficaz, e é por este motivo que existem planos de mitigação e continuidade para que o impacto não seja tão grave e, talvez, até destrutivo para um negócio.

CONCLUSÃO

De acordo com as reflexões deste trabalho, é nítido observar que a conscientização a respeito de Segurança da Informação e proteção de dados é uma pauta que vem ganhando importância entre usuários da rede.

Não existe segurança infalível ou sistema definitivo de proteção, contudo, no âmbito corporativo, muitas vezes há negligência e excesso de confiança da alta gestão, o que leva a funcionários dispersos, atuantes em ambientes inseguros nos quais a Política de Segurança é inexistente ou mesmo não faz parte da cultura da empresa, seja por estar defasada ou não ser bem aceita por aqueles que deveriam segui-la.

De acordo com a tradição empirista, as regras morais não são inatas, portanto, não se deve pautar a segurança de um bem tão valioso, como a informação, baseando-se exclusivamente na conduta individual de membros de um grupo. É importante que a gestão faça uma auditoria cuidadosa e elabore Políticas de Segurança condizentes com cada setor atuante e, principalmente, faz-se necessária a criação de regras maleáveis e adaptativas ao mundo veloz da atualidade, em virtude da tecnologia.

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

Por conta das limitações desta atual contribuição ao estado da arte, tendo em vista o curto período de tempo disponível para desenvolvê-la, bem como a limitada amostra de colaboradores para embasar o estudo de caso, espera-se que as reflexões aqui presentes fomentem e sirvam de inspiração para outras pesquisas na área, por se tratar de um assunto altamente pertinente no cenário atual.

REFERÊNCIAS

ALEXANDER, Michael. Methods for Understanding and Reducing Social Engineering Attacks. *In*.: **SANS Institute**. 30 abr. 2016. Disponível em: <https://www.sans.org/reading-room/whitepapers/critical/methods-understanding-reducing-social-engineering-attacks-36972>. Acesso: 10 abr. 2018

ALLEN, Malcolm. Social Engineering: A means to violate a computer system. *In*.: **SANS Institute**. 2007. Disponível em: <https://www.sans.org/reading-room/whitepapers/engineering/social-engineering-means-violate-computer-system-529>. Acesso: 3 abr. 2018

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS / INTERNATIONAL ORGANIZATION FOR STANDARDIZATION / INTERNATIONAL ELECTROTECHNICAL COMMISSION. **ISO/IEC 27002: 2013**. Information Technology: Security Techniques: Code of practice for information security controls. Vernier, Genebra – Suíça, 2013. Disponível em: <http://www.abntcatalogo.com.br/norma.aspx?ID=304865>. Acesso em: 29 maio 2018

BADSHAH, Nadeem. Facebook to contact 87 million users affected by data breach. *In*.: **The Guardian**. 8 abr. 2018. Disponível em: <https://www.theguardian.com/technology/2018/apr/08/facebook-to-contact-the-87-million-users-affected-by-data-breach>. Acesso em: 25 abr. 2018

BRASIL. **Constituição Federal de 1988**. Promulgada em 5 de outubro de 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 17 abr. 2018

BRASIL. Decreto-Lei 2.848, de 07 de dezembro de 1940. **Código Penal**. Diário Oficial da União, Rio de Janeiro, 31 dez. 1940. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848.htm>. Acesso em: 20 maio 2018.

BRASIL. Decreto nº 3505, de 13 de junho de 2000. Presidência da República. Brasília/DF, 2000. *In.*: **Planalto.gov.br**. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto/D3505.htm>. Acesso em: 20 maio 2018.

BRASIL. Lei nº 12735, de 30 de novembro de 2012. Presidência da República. Brasília/DF, 2012. *In.*: **Planalto.gov.br**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm>. Acesso em: 20 maio 2018.

BRASIL. Lei nº 12737, de 30 de novembro de 2012. Presidência da República. Brasília/DF, 2012. *In.*: **Planalto.gov.br**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 20 maio 2018.

CARLOMAGNO, Márcio C.; ROCHA, Leonardo Caetano da. Como criar e classificar categorias para fazer análise de conteúdo: Uma questão metodológica. **Revista Eletrônica de Ciência Política**: Revista da Universidade Federal do Paraná (UFPR), v. 7, n. 1, p.173-188. 2016. Disponível em: <https://revistas.ufpr.br/politica/article/view/45771/28756>. Acesso em: 20 jun. 2018

CENTRO DE ESTUDOS, RESPOSTAS E TRATAMENTO DE INCIDENTES NO BRASIL. **Cartilha de Segurança para Internet**. 2ª ed. São Paulo: Comitê Gestor da Internet no Brasil, 2012. 140p. Disponível em: <https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Acesso em: 7 jun. 2018

CESTARI FILHO, Felício. **ITIL v3 Fundamentos**. Rio de Janeiro: Rede Nacional de Ensino e Pesquisa (RNP), 2012. 158p.

GRANGER, Sarah. Social Engineering Fundamentals, Part I: Hacker Tactics. *In*.: **Symantec**. 18 dez. 2001. Disponível em: <https://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics>. Acesso em: 15 abr. 2018.

INTERNET SOCIETY. **Global Internet Report 2016**. Disponível em: <https://www.internetsociety.org/globalinternetreport/2016/wp-content/uploads/2016/11/ISO C_GIR_2016-v1.pdf>. Acesso em: 20 jun. 2018

LA MONICA, Paul R. Facebook has lost $80 billion in market value since its data scandal. *In*.: **CNN Money**, Nova Iorque, 27 de mar. 2018, às 16h27min. Disponível em: <http://money.cnn.com/2018/03/27/news/companies/facebook-stock-zuckerberg/index.html>. Acesso em: 15 maio 2018

MANJAK, Martin. Social Engineering Your Employees to Information Security. *In*.: **SANS Institute**. 1 jun. 2006. Disponível em: <http://www.sans.org/reading_room/whitepapers/awareness/social-engineeringemployees-information-security_1686>. Acesso em: 10 abr. 2018

MANN, Ian. **Hacking the Human**. Illustrated edition. Aldershot, Hampshire: Gower Publishing, 2008. 254p.

MARCIANO, João Luiz Pereira. **Segurança da Informação - uma abordagem social**. 2006. 211f. Tese (Doutorado em Ciência da Informação) – Colegiado do Programa de Pós-Graduação em Ciência da Informação do Departamento de Ciência da Informação e Documentação, Universidade de Brasília, Brasília, 2006. Disponível em: <http://repositorio.unb.br/handle/10482/1943>. Acesso em: 20 maio 2018

MEULEN, Rob van der. Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015. *In*.: **Gartner**. Stamford, 10 nov. 2015. Disponível em: <https://www.gartner.com/newsroom/id/3165317>. Acesso em: 20 maio 2018

MICROSOFT. **What is social engineering?**. 2018. Disponível em: <https://support.skype.com/en/faq/FA10921/what-is-social-engineering>. Acesso em: 23 abr. 2018.

MITNICK, Kevin D.; SIMON, William L. **A arte de enganar:** ataques de hackers: controlando o fator humano na segurança da informação. Trad: Kátia Aparecida Roque. São Paulo: Makron (Person Education), 2003. 284p.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **About NIST**. 2015-2017. Disponível em: <https://www.nist.gov/about-nist>. Acesso em: 24 maio 2018

NAKAMURA, Emilio Tissato; GEUS, Paulo Licio. **Segurança de Redes em ambientes Cooperativos**. São Paulo: Novatec, 2007. 482p.

NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR. **Quem somos**. 2015-2018. Disponível em: <http://nic.br/quem-somos/>. Acesso em: 23 maio 2018.

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO. **About OECD**. 2018. Disponível em: <http://www.oecd.org/about/>. Acesso em: 23 maio 2018.

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

REDMON, Kevin C. Mitigation of Social Engineering attacks in Corporate America. *In.*: **Infosecwriters**. 2005. Disponível em: <http://www.infosecwriters.com/text_resources/pdf/Social_Engineering_KRedmon.pdf>. Acesso em: 10 abr. 2018

ROSA, Adriano Carlos; SILVA, Bruno Donizete da; SILVA, Pedro Lemes da. Análise de redes sociais aplicada à Engenharia Social. *In.*: I Simpósio Internacional de Gestão de Projetos. São Paulo/SP, 12 jul. 2012. **Anais do I SINGEP**: São Paulo/SP: Programas de Pós-Graduação em Administração, Universidade Nove de Julho (UNINOVE). Disponível em: <http://repositorio.uninove.br/xmlui/bitstream/handle/123456789/163/128-360-1-DR%20analise%20de%20redes%20sociais.pdf?sequence=1>. Acesso em: 1 abr. 2018.

SÊMOLA, Marcos. **Gestão da Segurança da Informação:** uma visão executiva da segurança da informação. 9ª ed. Rio de Janeiro: Elsevier, 2003.

SILVA FILHO, Antônio Mendes da. Entendendo e Evitando a Engenharia Social: Protegendo Sistemas e Informações. *In.*: **Software Livre**. 12 nov. 2009. Disponível em <http://softwarelivre.org/brasil/entendendo-e-evitando-a-engenharia-social-protegendo-sistemas-e-informacoes>. Acesso em: 16 abr. 2018

SILVA, Maicon Herverton Lino Ferreira da; COSTA, Veridiana Alves de Sousa Ferreira. O fator humano como pilar da Segurança da Informação: uma proposta alternativa. *In.*: IX Jornada de Ensino Pesquisa e Extensão (JEPEX). Recife/PE, 23 out. 2009. **Anais do IX JEPEX**: Recife/PE: Universidade Federal Rural de Pernambuco (UFRPE). Disponível em: <http://www.eventosufrpe.com.br/jepex2009/cd/resumos/R0052-3.pdf>. Acesso em: 5 abr. 2018.

SKINNER, Burrhus Frederic. **Ciência e Comportamento humano**. Trad: João Carlos Todorov; Rodolfo Azzi. 11ª ed. São Paulo: Martins Fontes, 2003. 489p.

SOUZA, Raul Carvalho. **Prevenção para ataques de engenharia social:** um estudo sobre a confiança em segurança da informação em uma ótica objetiva, social, estrutural e interdisciplinar utilizando fontes de dados abertos. 2015. 189 f. Dissertação (Mestrado em Ciência da Informação) – Programa de Pós-Graduação em Ciência da Informação (PPGCINF), Universidade de Brasília, Brasília, 2015. Disponível em: <http://repositorio.unb.br/bitstream/10482/18863/1/2015_RaulCarvalhodeSouza.pdf> . Acesso em: 16 abr. 2018

SYSTEM ADMINISTRATION, NETWORKING AND SECURITY. **About SANS**. 2000-2018. Disponível em: <https://www.sans.org/about/>. Acesso em: 24 maio 2018

UNITED STATES COMPUTER EMERGENCY READINESS TEAM. **About us**. 2018. Disponível em: <https://www.us-cert.gov/about-us>. Acesso em: 25 maio 2018.

UNITED STATES COMPUTER EMERGENCY READINESS TEAM. **Technical Information Paper**: Cyber Threats to Mobile Devices. 15 abr. 2010. Disponível em: <https://www.us-cert.gov/sites/default/files/publications/TIP10-105-01.pdf>. Acesso em: 28 abr. 2018.