UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL

ESCOLA DE ADMINISTRAÇÃO

DEPARTAMENTO DE CIÊNCIAS ADMINISTRATIVAS

GABRIEL MARQUES CARVALHO

DIAGNÓSTICO DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO EM EMPRESAS NACIONAIS DO SETOR FINANCEIRO

Porto Alegre

2018

GABRIEL MARQUES CARVALHO

DIAGNÓSTICO DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO EM EMPRESAS NACIONAIS DO SETOR FINANCEIRO

Trabalho de conclusão de curso de graduação apresentado ao Departamento de Ciências Administrativas da Universidade Federal do Rio Grande do Sul, como requisito parcial para a obtenção do grau de Bacharel em Administração.

Orientador: Prof. Dr. Luciano Ferreira

Porto Alegre

2018

GABRIEL MARQUES CARVALHO

DIAGNÓSTICO DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO EM EMPRESAS NACIONAIS DO SETOR FINANCEIRO

Trabalho de conclusão de curso de graduação apresentado ao Departamento de Ciências Administrativas da Universidade Federal do Rio Grande do Sul, como requisito parcial para a obtenção do grau de Bacharel em Administração.

Orientador: Prof. Dr. Luciano Ferreira

Aprovado em ..... de ..... de ..... .

BANCA EXAMINADORA

_____

Prof. Dr. Pablo Cristini Guedes

_____

Orientador – Prof. Dr. Luciano Ferreira

Dedico este trabalho aos meus pais, responsáveis por minha educação e caráter.

Sem eles, nada disso seria possível.

RESUMO

O atual avanço tecnológico está presente em um contexto no qual as pessoas e as organizações não possuem conhecimento nem experiência para lidar com uma segurança eficaz em tecnologia da informação. Assim, os crimes cibernéticos se apresentam como uma ameaça em constante evolução, dado o seu aumento no Brasil e em escala mundial. Por essa razão, este trabalho objetivou analisar em que medida as empresas nacionais de serviços financeiros utilizam práticas de segurança da informação, apresentando o modelo de segurança em TI proposto por Turban e Volonino (2013), relacionando-o com o fator humano e as fraudes. Dessa forma, realizou-se uma pesquisa do tipo *survey,* por meio de um questionário, para compreender e avaliar as etapas do modelo e os fatores específicos. Foram realizadas vinte e seis perguntas subdivididas em sete tópicos e respondidas por funcionários do setor de serviços financeiros. Com os resultados encontrados, foi diagnosticado que os usuários representam o chamado elo mais fraco da empresa, que o fator humano é mais importante que a adoção de ferramentas de segurança e que os usuários não conhecem as políticas e as normas das organizações de modo completo, nem são monitorados para garantir que não utilizem recursos para fins pessoais, bem como existem falhas na divulgação das políticas por parte da alta administração, demonstrando que os gestores também representam um risco iminente. Portanto, este trabalho demonstra a importância de que medidas para segurança da informação são necessárias para vitalidade empresarial.

Palavras-chave: Segurança da informação. Tecnologia da informação. Modelo de segurança. Fraudes. Fator humano.

ABSTRACT

The current technological advance is present in a context in which people and organizations do not have the knowledge or experience to deal with an effective security in information technology. Thus, cybercrime presents itself as a constantly evolving threat, given its increase in Brazil and worldwide. For this reason, this work aimed to analyze the extent to which national financial services companies use information security practices, presenting the IT security model proposed by Turban and Volonino (2013), relating it to the human factor and fraud. In this way, a research of the type survey was carried out, through a questionnaire, to understand and evaluate the stages of the model and the specific factors. Twenty-six questions were subdivided into seven topics and answered by employees in the financial services industry. With the found results, it was diagnosed that users represent as we call the company's weakest bond, that the human factor is more important than the introduction of security tools and that users do not know the policies and standards of organizations in a complete way, neither they are monitored to ensure that they do not use resources for personal purposes, as well as exist failures in disclosure of policies by part of senior management, demonstrating that managers also pose an imminent risk. Therefore, this work demonstrates the importance that measures for information security are necessary for business vitality.

Keywords: Information security. Information Technology. Safety model. Frauds. Human factor.

LISTA DE ILUSTRAÇÕES

LISTA DE QUADROS E TABELA

SUMÁRIO

1 INTRODUÇÃO

Empresas do ramo financeiro enfrentam grandes desafios no mundo contemporâneo, não basta apenas que sobrevivam, elas precisam ter uma atenção especial em relação à segurança da informação, pois absolutamente todos os dados encontram-se inseridos em uma rede global de computadores interligados, a *Internet*, de modo que esse grande volume de dados é representado pelo termo *Big Data*. De acordo com o estudo de Ferreira *et al.* (2016), é necessário que as organizações saibam administrar a segurança da informação de forma estratégica, possibilitando que o negócio da organização seja realizado e a sua missão alcançada.

Considerando que esta seja uma preocupação recorrente das organizações, é necessário que elas se previnam e tenham elementos necessários para autoavaliação e diagnóstico quanto à gestão da segurança da informação, para que o risco quanto às fraudes seja relativamente baixo. Conforme é apresentado por Turban e Volonino (2013, p. 121), a "segurança da informação envolve os riscos aos dados, aos sistemas de informação e às redes. Esses incidentes geram riscos legais à empresa, como quando as operações são interrompidas ou as leis de privacidade violadas".

Nesse sentido, podemos verificar que a maturidade das empresas em relação à segurança da informação ainda é baixa, conforme demonstra o estudo da IDC Brasil, realizado em 2017, encomendado pela *Level 3 Communications*, mediante o qual se verifica que as empresas no Brasil possuem, em média, apenas dois profissionais dedicados à segurança da informação e apenas 42% das organizações alegam praticar e gerir métricas sobre o cumprimento de suas políticas de segurança da informação. Isso reflete na pontuação que o Brasil recebeu no índice (64,9 pontos de um total de 100 possíveis).

Segundo a pesquisa *Global Economic Crime and Fraud Survey,* realizada em 2018, pela empresa de consultoria PwC, metade das empresas brasileiras foram vítimas de crimes econômicos nos últimos dois anos (o crime cibernético representa 22% desses crimes). Os controles corporativos são os principais meios de detecção desses crimes, visto que no Brasil 59% dos participantes da pesquisa relataram que os delitos econômicos mais graves foram detectados dessa forma. Já nos próximos

dois anos, 14% dos participantes da pesquisa acreditam que o crime cibernético será de maior impacto para os negócios (no mundo, esse percentual sobe para 26%). Portanto, o crime cibernético, ao que parece, será o de maior relevância para os negócios, visto que são facilmente convertidos em dinheiro e de difícil percepção.

Aliado a isso, a pesquisa *Norton Cyber Security Insights Report*, realizada em 2017, aponta que o Brasil é o 2º país que mais perdeu dinheiro com os chamados *cibercrimes* (termo que se refere às atividades ilegais que ocorrem por meio de redes de computadores) naquele ano, visto que as perdas totalizaram US$ 22 bilhões e aproximadamente 62 milhões de brasileiros foram vítimas desses crimes no ano, ante a 42 milhões de brasileiros atingidos em 2016. O grande descuido da população, conforme a pesquisa, também se faz presente nas empresas, em virtude de que a segurança de uma companhia depende, dentre tantos aspectos, da própria postura de seus profissionais.

Com a finalidade de verificar quais ramos empresariais são os mais afetados por crimes virtuais para centralizar o estudo, foi identificado que, de acordo com o estudo da *Accenture e Ponemon Institute,* realizado em 2018, os *cribercrimes* acontecem, em sua maioria, no setor de serviços financeiros. Associado a esse estudo, verificou-se que o custo efetivo para gerir *ciberataques* em empresas de serviços financeiros é mais alto do que comparado com outros setores, pois elas são as mais visadas para a prática de delitos, não obstante, o número de incidentes relacionados aos crimes cibernéticos triplicou ao longo dos últimos cinco anos.

Em razão de tal contexto, torna-se importante que as organizações, sobretudo do setor de serviços financeiros, desenvolvam modelos e métricas para defesa cibernética, evitando maiores prejuízos. Os crimes cibernéticos se apresentam como uma ameaça em constante evolução, dado o aumento desse crime nos últimos anos, tanto no Brasil como em escala mundial. Desse modo, Mandarino (2010, p. 49), diz que “estratégia de segurança cibernética é a arte prática de assegurar a existência e a continuidade da sociedade da informação de uma nação, garantindo e protegendo, no espaço cibernético, seus ativos de informação e suas infraestruturas críticas”.

Portanto, é imprescindível que a segurança da informação tenha grande relevância dentro das organizações, uma vez que os crimes cibernéticos estão em constante crescimento e sua prevenção é considerada baixa. Assim, faz-se

necessário que o presente estudo aborde os temas de maior impacto na segurança da informação, principalmente como as empresas – sobretudo no ramo de serviços financeiros -, sejam capazes de combater os crimes cibernéticos através de mecanismos de gestão que possibilitem a estruturação de controles eficientes, de modo que procure conscientizar as empresas nacionais da importância e do cumprimento de uma política de normas e procedimentos para prevenção.

A preocupação decorre então de desenvolver uma autoavaliação e diagnóstico para as organizações, por meio das percepções de seus colaboradores quanto às fraudes, crimes, violações e fator humano, além da análise destes aspectos sobre a gestão de segurança da informação, mais precisamente ao modelo de segurança em tecnologia da informação, presente em sua instituição. Por meio dessa proposta, surge o seguinte questionamento: **“Em que medida as empresas nacionais de serviços financeiros utilizam práticas de segurança da informação? ”.**

1.2 JUSTIFICATIVA

Em um momento em que a prevenção contra *cibercrimes* torna-se cada vez mais necessária, as ações de caráter preventivo e de detecção dos crimes cibernéticos ganham destaque e são tidas como fontes eficazes de combate às fraudes no sistema financeiro. Nesse sentido, as ferramentas de controle corporativo passam a ser primordiais para estabelecer sistemas de gestão integrados e eficazes, assim como é fundamental o suporte da alta administração para que a estrutura seja implementada e respeitada, além de políticas, procedimentos e normas de segurança, que serão demonstradas no decorrer do estudo.

Com o objetivo de nortear o melhor gerenciamento de segurança da informação nas organizações, o presente trabalho procura desenvolver uma metodologia de autoavaliação e diagnóstico com base no modelo de defesa em profundidade de segurança em tecnologia da informação proposto por Turban e Volonino (2013), que também foi implementado no estudo de Ferreira *et al*. (2016). Assim, este estudo servirá de base para que organizações verifiquem a grande importância em relação à gestão da segurança da informação, às fraudes e ao fator humano, bem como demonstrar a importância de um modelo de segurança em TI, que busca auxiliar na sobrevivência da organização neste atual ambiente de constante aperfeiçoamento tecnológico.

1.3 OBJETIVOS

1.3.1 Objetivo geral

- Identificar em que medida as empresas nacionais de serviços financeiros utilizam práticas de segurança da informação.

1.3.2 Objetivos específicos

- Apresentar as etapas em relação à gestão estratégica da informação presente nas organizações;
- Descrever sobre os sistemas de informações que são responsáveis pela manipulação da informação no contexto organizacional;
- Demonstrar as etapas e os fatores necessários para uma eficiente e eficaz gestão de segurança da informação;
- Analisar o desempenho das empresas selecionadas em relação à adoção de medidas de segurança da informação.

2 REFERENCIAL TEÓRICO

Na revisão teórica se faz necessário um esclarecimento sobre a gestão estratégica da informação, os sistemas de informações e a gestão da segurança da informação, que tratam de aspectos norteadores para fundamentação e construção da análise final do presente trabalho. Necessariamente, serão apresentados estudos e pesquisas acadêmicas de diversos autores do ramo como fonte de compreensão e assimilação deste estudo.

2.1 GESTÃO ESTRATÉGICA DA INFORMAÇÃO

Atualmente vivencia-se a era da informação, na qual as informações representam patrimônios inestimáveis, sendo a informação necessária para que se possa inovar a ponto de não ser engolido pela mudança. Desta forma, é de grande importância administrar para que o fluxo informacional ocorra de maneira eficiente e eficaz na organização, sendo essa gestão indispensável nos mais diversos ramos de negócio (BEAL, 2008). No entanto, há muitas informações em excesso e, por isso, é necessário selecionar as informações de maior qualidade pelos meios e tecnologias adequadas, além de se comprometer com uma segurança necessária para isso. Em vista disso, Beal (2008) demonstra que as organizações, com objetivo de ter um processo decisório eficaz, procuram selecionar as informações de maior qualidade para garantir um sucesso corporativo, além de uma boa relação entre custo e benefício, satisfazendo os clientes internos e externos.

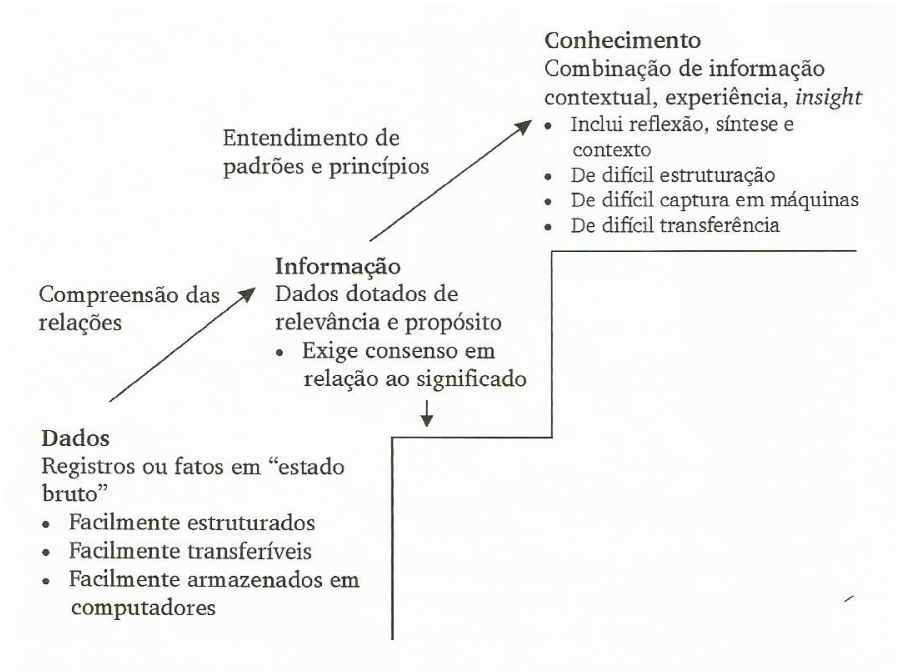
Deste modo, conforme o avanço tecnológico se faz existente em todos os ramos do negócio, a informação e a comunicação são responsáveis por novas formas significativas de mudanças nas organizações (BEAL, 2008). Para conhecer essas novas formas, a presente seção procura desenvolver sobre as diferenças entre dado, informação e o conhecimento, além de demonstrar o valor da informação para as

organizações, bem como o fluxo informacional presente nas empresas e as suas estratégias em tecnologia da informação como forma de demonstrar o avanço tecnológico e as efetivas responsabilidades para uma segurança que atualmente é indispensável.

2.1.1 Dado, informação e conhecimento

Compreender a diferença entre dado, informação e conhecimento, torna-se importante na medida em que os termos são constantemente confundidos e representam certa importância para entendimento deste estudo. Como forma de relação entre os termos, Beal (2008, p. 11), acredita que “um conjunto de dados não produz necessariamente uma informação, nem um conjunto de informações representa necessariamente um conhecimento”. Isso ocorre porque Beal (2008) entende que dados só serão transformados em informação e, posteriormente, esta só será transformada em conhecimento caso exista a agregação de valor ou de outros elementos, conforme demonstrado na figura 1.

Figura 1 – Os “níveis hierárquicos” da informação



Fonte: Beal (2008, p. 12)

A partir dessa relação em que dados são considerados registros ou fatos brutos, informação é considerada dados de relevância e propósito; e conhecimento é considerado a combinação de informação e experiência, é necessário demonstrar as diferenças conceituais entre dado, informação e conhecimento. Deste modo, foram selecionadas as conceituações desses termos pelos autores Stair e Reynolds (2016), e Rainer e Cegielski (2012).

Dados – Rainer e Cegielski (2012, p.8), dizem que “dados se referem a uma descrição de coisas elementares, eventos, atividades e transações que são gravadas, classificadas e armazenadas, mas não são organizadas para transmitir um significado específico”.

Informação – Para os autores Stair e Reynolds (2016, p. 5), a “informação é uma coleção de fatos organizados e processados de modo que tenham valor adicional, que se estende além do valor dos fatos individuais”.

Conhecimento – Os autores Rainer e Cegielski (2012, p. 8) dizem que o “conhecimento consiste no dado e/ou informação que tenha sido organizada e processada para transmitir entendimento, experiência, aprendizado acumulado e perícia, os quais são aplicados a um problema de negócio atual”.

Tipologia da Informação

Conforme demonstrados os conceitos de dado, informação e conhecimento, pode ser concluído que as informações se fazem presentes em todas as organizações e, para melhor entendimento sobre a estrutura organizacional, torna-se necessário compreender os níveis em que as informações se encontram na estrutura organizacional. Assim, conforme é exposto por Beal (2008), a natureza da informação pode se apresentar em três níveis:

a) Informação de nível institucional – São as informações destinadas às decisões de alto nível, que monitoram e avaliam o desempenho e o planejamento para tomar decisões;

b) Informação de nível intermediário – São as informações destinadas às decisões tomadas em nível gerencial, que monitoram e avaliam os processos para tomar decisões;
c) Informação de nível operacional – São as informações destinadas a executar as atividades e tarefas, além de monitorar o espaço geográfico sob sua responsabilidade.

Desta maneira, compreender a origem das fontes possibilita representar um importante aprofundamento, podendo elas se originar de duas maneiras, de acordo com Beal (2008):

a) Fonte formal - Podem ser caracterizadas como advindas da imprensa, de informações científicas e técnicas, de base de dados e de documentos empresariais;
b) Fonte informal - São provenientes de informações por meio de visitas a clientes, exposições, agências de publicidade, fornecedores.

A partir do conhecimento quanto aos níveis em que as informações se apresentam e aos tipos de fontes, o valor da informação é apresentado, de modo que se possa compreender o fluxo da informação nas organizações e as estratégias tomadas no âmbito organizacional aliadas à tecnologia.

2.1.2 O valor da informação para as organizações

Historicamente, as empresas têm sido influenciadas por informações aplicadas aos negócios, pois desde a revolução industrial a informação se faz presente possibilitando a geração de novos conhecimentos, modelos, métodos e técnicas em constante evolução, assim como a tecnologia aplicada aos negócios. Neste contexto, a informação é progressivamente mais valorizada, pois as informações de qualidade trazem muitos benefícios ao negócio, como o apoio à tomada de decisões, a redução de custos e uma melhor produtividade empresarial, o que torna uma gestão informacional de qualidade como um diferencial competitivo nos diversos ramos de negócio (SÊMOLA, 2014).

Nesse aspecto, compreender o valor que a informação possui no âmbito organizacional se constitui como um passo necessário para tomar providências eficientes e eficazes. Assim, o valor da informação, conforme Stair e Reynolds (2016, p. 8), é “diretamente ligado a como ela ajuda os tomadores de decisões a alcançar os objetivos da organização”. Dessa maneira, conforme ela ajuda ao alcance dos objetivos da organização, o seu valor aumenta, podendo ser, inclusive, negociado. Como demonstrado, saber gerir a informação de forma adequada se torna um diferencial competitivo para as organizações, uma vez que é necessário administrar a informação de maneira adequada para a sobrevivência. Podemos verificar tamanha importância que a informação possui, servindo nos diferentes contextos como fatores significativos para as organizações, conforme classifica Beal (2008):

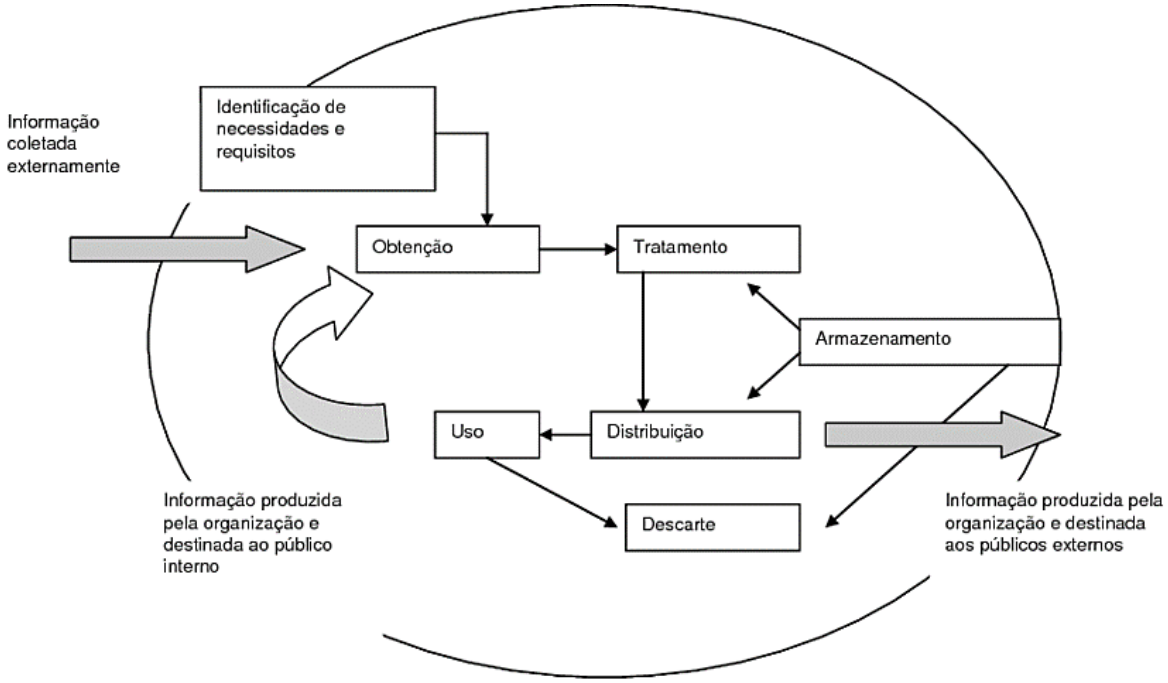
a) Fator de apoio à decisão – A informação aumenta a probabilidade de sucesso na tomada de decisão;
b) Fator de produção – A informação possibilita adicionar um elemento de maior valor no mercado de produtos (bens ou serviços), gerando um ganho maior;
c) Fator de sinergia – Uma maior qualidade no fluxo informacional entre as unidades organizacionais proporciona um melhor desempenho da organização;
d) Fator determinante de comportamento – A informação atua como peça fundamental no comportamento interno e externo, influenciando para que as ações sejam condizentes com os objetivos corporativos.

Dessa forma, a informação é considerada como um fator determinante para o funcionamento de uma organização, na qual, Sêmola (2014) demonstra tamanha importância, comparando que a informação está para a empresa assim como o sangue para o ser humano, e o coração está para o ser humano assim como os grandes computadores e servidores estão para as empresas. Tamanha comparação, além do demonstrado anteriormente, justifica a necessidade de ações corporativas para a segurança da informação organizacional.

2.1.3 O fluxo da informação nas organizações

Considerado o valor da informação, que é de extrema importância organizacional, se faz necessário compreender o seu caminho nas organizações. Esse caminho é denominado por Beal (2008) como o fluxo da informação nas organizações e por Sêmola (2014) como o ciclo de vida da informação, pois relaciona a informação nas organizações com o funcionamento do corpo humano. Assim, o ciclo de vida da informação, conforme Sêmola (2014), corresponde aos momentos que a colocam em risco, como quando ela é utilizada pelo meio empresarial, passando pelos ativos físicos, humanos e tecnológicos. Desse modo, o fluxo que a informação percorre nas organizações pode ser visto na figura 2, de acordo com o modelo proposto por Beal (2008).

Figura 2 – Modelo proposto para representar o fluxo da informação nas organizações



Fonte: Beal (2008, p. 29).

De maneira objetiva, a atividade do fluxo inicia pela identificação de necessidades e requisitos, passando pelas etapas de obtenção, tratamento, distribuição, uso, armazenamento e descarte, conforme demonstrado acima.

Resumidamente, as etapas do fluxo podem ser descritas do seguinte modo, de acordo com Beal (2008):

a) Identificação de necessidades e requisitos – Identificar as necessidades de informação dos usuários internos e externos para melhorar os produtos e processos ou fortalecer o vínculo de relacionamento;
b) Obtenção – Obter as informações que podem suprir as necessidades, desenvolvendo as atividades de criação, recepção ou captura de informação, por meio de fontes internas ou externas;
c) Tratamento – A informação pode passar por processos de organização que exijam torná-la mais acessível aos usuários, como formatação, estruturação, análise;
d) Distribuição – A distribuição permite levar informações a quem precisa, seja internamente ou para públicos externos;
e) Uso – Se refere à etapa mais importante de todo o processo, podendo servir para gerar novos conhecimentos que podem realimentar o ciclo da informação, conforme demonstrado na figura 2;
f) Armazenamento – Necessária para a conservação dos dados e informações em diferentes meios, como documentos de papel ou bases de dados informatizadas, visando manter a integridade e disponibilidade da informação;
g) Descarte – O descarte é efetuado quando uma informação se torna obsoleto ou perde a utilidade para a organização, cuidando sempre para descartar de acordo com as políticas da organização.

2.1.4 Estratégia e tecnologia da informação

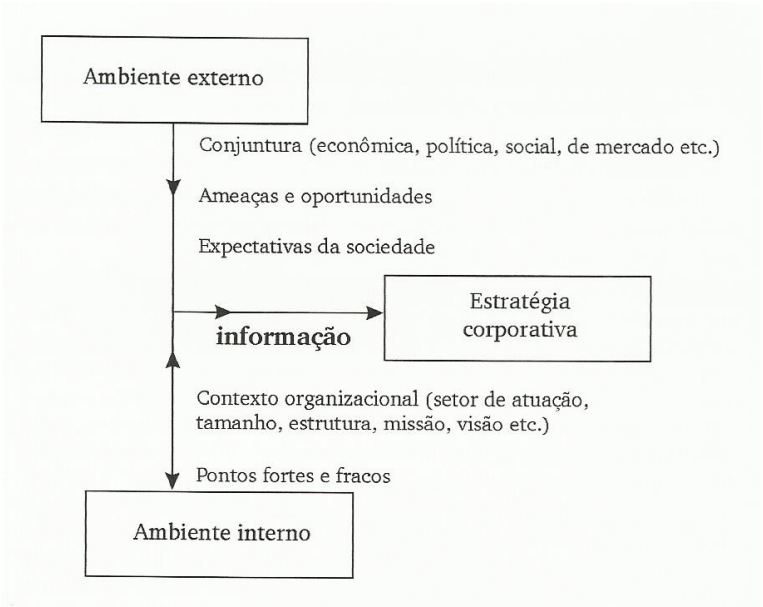
Conforme o fluxo da informação é transmitido nas organizações, estas devem dispor de estratégias coerentes para lidar com tamanho fluxo, objetivando uma tomada de decisões de maneira eficaz. Em vista disso, Beal (2008), entende que a estratégia pode ser compreendida como a prática organizacional para tomar determinadas atitudes em um determinado intervalo de tempo, bem como a identificação dos meios mais eficazes para atingir os objetivos propostos. Assim, é de

grande importância ressaltar o papel de informações adequadas, no sentido de que são elementos essenciais na elaboração de uma estratégia. Por isso, Beal (2008, p. 75), acredita que:

> “Sem o acesso a informações adequadas a respeito das variáveis internas e do ambiente onde a organização se insere, os responsáveis pela elaboração da estratégia não têm como identificar os pontos fortes e fracos, as ameaças e oportunidades, os valores corporativos e toda a variedade de fatores que devem ser considerados na identificação de alternativas e na tomada de decisões estratégicas” (BEAL, 2008).

Nesse sentido, isso pode ser representado pela figura 3, na qual representa a informação em relação aos ambientes externo e interno gerando informações para a tomada de decisão estratégica.

Figura 3 – A informação como matéria prima para formulação da estratégia



Fonte: Beal (2008, p. 76).

A partir disso, Beal (2008) demonstra que surge um novo cenário em que a tecnologia da informação participa diretamente do processo, pois adiciona valor e qualidade aos produtos e/ou serviços. Nesse cenário, a TI precisa ser caracterizada para entendimento futuro, e os autores Rainer e Cegielski (2012, p. 4), descrevem que “a tecnologia da informação (TI) se refere a qualquer ferramenta baseada em

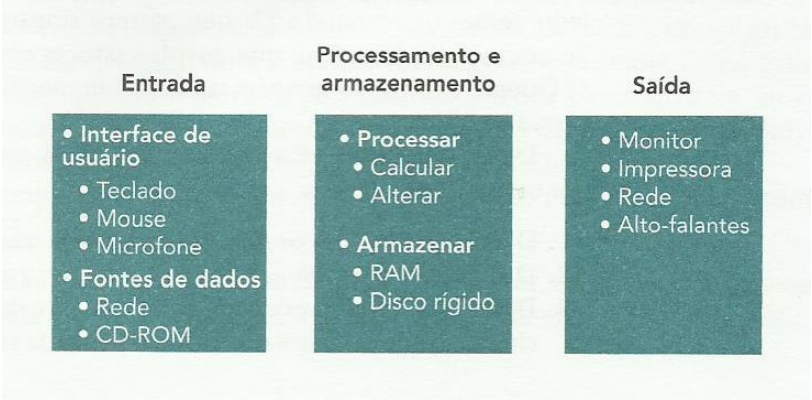
computador usado pelas pessoas para trabalhar com informações e apoiar as necessidades de informação e processamento de informações de uma organização". Portanto, Beal (2008) demonstra que a organização, como forma de impulsionar os negócios, desenvolva estratégias alicerçadas em tecnologia da informação. Desse modo, surgem os sistemas de informação para auxiliar as organizações nas estratégias, sobretudo as apoiadas à tecnologia.

2.2 SISTEMAS DE INFORMAÇÕES

Como se sabe, a informação é um ativo importante que possui grande valor para a organização, pois sem a informação a organização não realiza seu negócio; desta maneira, procura-se entender sobre o sistema de informações, que é responsável pela manipulação da informação no contexto organizacional. Nesse sentido, entender sobre o sistema de informação (SI) é fundamental, pois de acordo com Perottoni e*t al.* (2001), as empresas só conseguem tomar decisões adequadas se estas provêm de informações corretas, nesse sentido é que surgem os sistemas de informações como meio de transformar os dados existentes e auxiliar na tomada de decisões. Assim, o sistema de informações é conceituado do modo abaixo.

Sistemas de Informações – Conforme os conceitos dos autores O'Brien (2009), Stair e Reynolds (2016), Turban e Volonino (2013), pode se chegar à conclusão de que um sistema de informação é um conjunto de elementos que, de forma coordenada, coleta, transforma, armazena e dissemina dados e informações com a finalidade de alcançar os objetivos específicos da organização. Esses elementos podem ser verificados na figura 4, que apresenta um exemplo de funções básicas de um sistema de informação.

Figura 4 – Quatro funções básicas de um sistema de informação



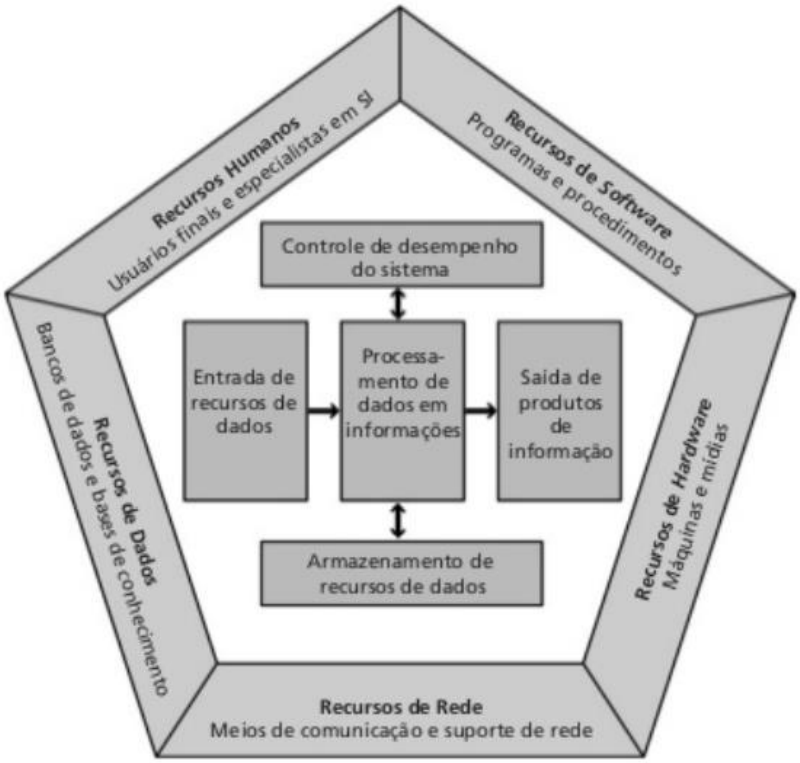
Fonte: Turban e Volonino (2013, p. 8)

Os elementos mencionados na figura acima representam o exemplo de um sistema de informações baseado em computador. De tal modo, Turban e Volonino (2013) demonstram que um SI pode ser tão pequeno quanto um smartphone ou pode se referir a vários equipamentos como a impressoras conectadas por redes sem fio. Assim, as funções básicas de um sistema de informações, mencionados anteriormente em seu conceito, são descritas conforme o entendimento de Turban e Volonino (2013):

a) Entrada – Momento em que se obtêm os dados brutos por dispositivos de entrada;
b) Processamento – Esses dados são transformados em resultados úteis para armazenamento ou transferência;
c) Saída – É resultado de dados e informações úteis, que são transmitidos para outros meios;
d) Feedback – Refere-se a um instrumento para supervisionar as atividades e possíveis mudanças.

Em vista disso, pode ser entendido que os componentes básicos de um sistema de informação com base em um computador são os procedimentos, as pessoas, banco de dados, telecomunicações, *software* e *hardware*, conforme demonstra a figura 5, representada por O’Brien (2009).

Figura 5 – Componentes de um sistema de informação



Fonte: Adaptado de O'Brien (2009, p. 10).

Desse modo, o modelo apresentado por O'brien (2009), reforça as relações entre os componentes que fazem parte de um sistema de informações e as suas atividades. Assim, é necessário conhecer os principais tipos de SI e para que servem.

2.2.1 Tipos e ênfases na atuação

Os principais tipos de sistemas informações são caracterizados conforme Perottoni *et al.* (2001):

a) **Sistema de Informação Transnacional (SIT)** – Foi o primeiro sistema desenvolvido e atualmente é utilizado na maioria das organizações, servindo como base para os demais sistemas, pois o seu foco principal é o fornecimento de todas as informações legais ou organizacionais referentes à empresa;

b) **Sistema de Informação Gerencial (SIG)** – É um sistema que possibilita transformar dados em informações empresariais para auxiliar na tomada de decisões gerencias, possibilitando que os objetivos sejam alcançados, influenciando diferentes áreas funcionais da organização no nível tático;
c) **Sistema de Automação de Escritório (SAE)** – Surge como forma principal para organizar os relatórios empresariais de forma informatizada, melhorando e agilizando as atividades básicas, auxiliando no aumento da produtividade, redução de custos e um aumento na qualidade;
d) **Sistema de Apoio à Decisão (SAD)** – É um sistema para apoiar no aumento de qualidade da tomada de decisão, servido como suporte às decisões semiestruturadas (procedimentos padrões) e não-estruturadas (processos vagos e problemas complexos);
e) **Data Warehouse e Data Mining** – O data warehouse é, basicamente, um grande banco de dados que possibilita o acesso a informações que demonstram melhor as operações da organização. Por outro lado, o data mining serve para selecionar os dados que o usuário precisar dentro da grande quantidade de dados do data warehouse;
f) **Sistemas Especialistas (SE)** – São necessários para disponibilizar conhecimentos específicos em determinadas áreas, sendo uma das técnicas de inteligência artificial, que possibilitam uma maior agilidade na conclusão das operações organizacionais como forma de aumentar a capacidade de solucionar problemas, a produtividade, entre outros aspectos;
g) **Sistemas de Informação para Executivos (EIS)** – Surge com o objetivo de uma maior filtragem de dados relevantes para os executivos, permitindo um maior controle organizacional, com capacidade para gerar relatórios de diversos tipos analisando, sobretudo, os fatores críticos de sucesso, daí que se origina a ferramenta *Business Intelligence* (BI), responsável, resumidamente, pela inteligência de negócios;
h) **Sistema de Gestão Empresarial (ERP)** – É um sistema que procura cobrir todas as atividades de negócio dentro da empresa, com a finalidade de administrar diversas operações, como financeira contábil, recursos humanos e englobando as funções contidas no SIT, SIG e EIS, além de características do CRM.

i) **Customer Relationship Management (CRM**) – A gestão de relacionamento com o cliente é uma busca pela melhora contínua entre a relação das empresas e de seus clientes, possibilitando que as informações fiquem à disposição de todos os setores empresariais para satisfazer a necessidade do consumidor.

2.2.2 A organização, seus sistemas de informações e o ambiente externo

Os sistemas e tecnologias de informação tornaram-se componentes vitais quando se pretende alcançar o sucesso das organizações e, por essa razão, constituem um campo de estudo essencial em administração e gerenciamento de empresas (O'BRIEN, 2009). Esse contexto também é destacado por Sêmola (2014), no qual ele afirma que as ferramentas de apoio alteraram a forma de como as organizações usam a informação e administram seus negócios.

Em vista disso, os autores Turban e Volonino (2013) acreditam que as inovações em tecnologias da informação (que se refere ao conjunto de sistemas computacionais), estão evoluindo a forma como as empresas fazem negócio, como os gestores e colaboradores trabalham, redesenhando o design dos processos e a estrutura dos mercados. Desse modo, não acompanhar a evolução tecnológica significa ficar de fora dos negócios.

A evolução tecnológica é alvo do estudo de muitos autores, tal como Rainer e Cegielski (2012), eles resumem que os impactos da TI frente às organizações estão demonstrando que para ter sucesso atualmente é necessário mudar os modelos e as estratégias de negócios, pois a TI permite que as organizações sobrevivam e prosperem nas mais adversas situações. De tal maneira, isso pode exigir um grande investimento por um longo período de tempo, assim, as tecnologias podem ser usadas, por exemplo, para criar novos aplicativos, como forma de aprimorar os produtos e serviços para proporcionar um excelente serviço ao cliente.

Nesse contexto, O'Brien (2009) demonstra que as tecnologias da informação, entre as quais os sistemas de informações baseados sobretudo na Internet, estão desempenhando um papel vital no desenvolvimento das organizações, pela

ampliação dos negócios, além de validar que a tecnologia da informação pode ajudar todos os tipos de empresas a melhorarem a eficiência e eficácia de seus processos, a tomada de decisões gerenciais e a colaboração de grupos de trabalho, como forma de se fortalecer em um contexto de rápida transformação tecnológica. Portanto, é demonstrada a constante evolução das tecnologias da informação e, assim, surgem as preocupações relativas à segurança das informações.

2.3 GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Após ser evidenciado a gestão estratégica da informação (destacando o valor e o fluxo da informação), e os sistemas de informações (destacando o contexto atual das tecnologias), manifesta-se o objetivo de manter isso de forma protegida, respeitando os princípios éticos de segurança. Conforme é demonstrado pela autora Beal (2008, p. 52), “uma área da gestão da informação que diz respeito a todas as etapas do fluxo informacional é a segurança, cujo objetivo é garantir proteção da informação de acordo com seus requisitos (princípios) ”.

De acordo com Fontes (2015), a informação é um ativo extremamente importante para as organizações e, nesse sentido, os seus ambientes e equipamentos devem ser protegidos. Desse modo, Ferreira *et al.* (2016) demonstra que a gestão de segurança da informação é um meio eficaz para proteção, tendo em vista que é necessário se adequar às normas, obter certificações e ferramentas de proteção para os sistemas de informações. Assim, Fontes (2015) acredita que o assunto segurança da informação tem atraído cada vez mais atenção na medida que três fatores acontecem:

- Quase que a totalidade das informações organizacionais se fazem presentes em ambiente computacional.
- O negócio da organização depende invariavelmente do ambiente computacional.

- Os colaboradores da organização possuem livre acesso às informações da empresa no ambiente computacional.

2.3.1 Princípios e conceitos

Os conceitos de segurança da informação adotados pelos mais diferentes autores, de maneira geral, representam os meios para proteção do ativo informacional, que assim pode ser demonstrado:

Segurança da Informação – Para Fontes (2015, p. 11), a segurança da informação representa “o conjunto de orientações, normas, procedimentos, políticas e demais ações que tem por objetivo proteger o recurso informação, possibilitando que o negócio da organização seja realizado e a sua missão seja alcançada”. Além disso, Fontes (2015) também demonstra que o objetivo principal da segurança da informação é a diminuição dos riscos informacionais, que afetam diretamente os negócios e, consequentemente, a organização, o que compromete o lucro. Assim, Turban e Volonino (2013) concluem que a segurança da informação é um conjunto de medidas que envolvem os principais riscos aos quais a informação está vulnerável, e isso gera riscos no sentido de que os negócios, assim como suas políticas, podem ser afetados. Já Sêmola (2014, p. 43), expressa a segurança da informação como “uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade”.

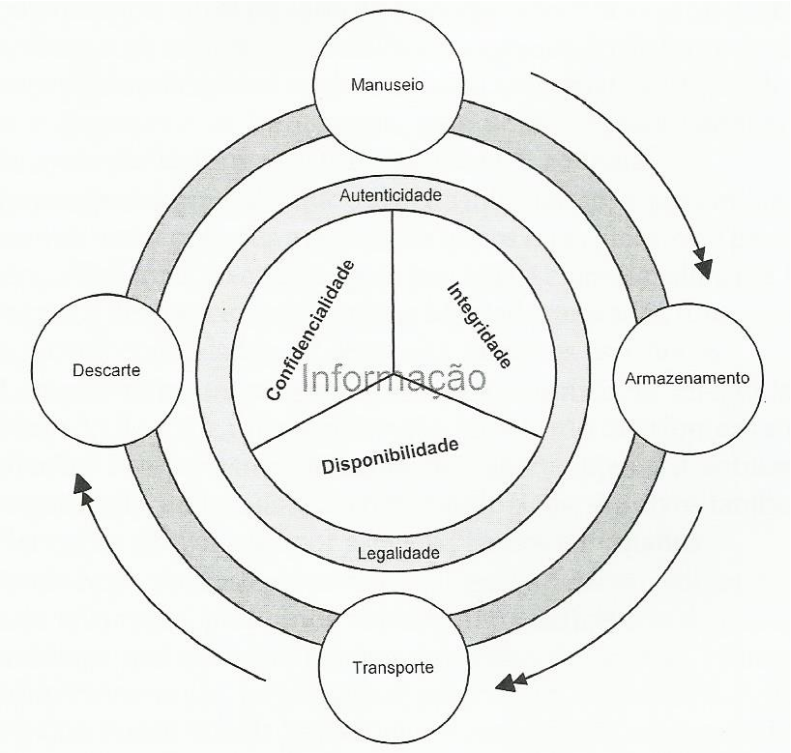
Além disso, Sêmola (2014, p. 43), diz que:

> “De forma mais ampla, podemos também considerá-la como a prática de gestão de riscos de incidentes que impliquem no comprometimento dos três principais conceitos de segurança: confidencialidade, integridade e disponibilidade da informação. Desta forma, estaríamos falando da definição de regras que incidiram sobre todos os momentos do ciclo de vida da informação: manuseio, armazenamento, transporte e descarte, viabilizando a identificação e o controle de ameaças e vulnerabilidades”.

O atestado por Sêmola (2014) relaciona-se com o funcionamento dos sistemas de organização, demonstrados no capítulo anterior, assim como os princípios de segurança, que serão vistos neste capítulo. Essa relação pode ser demonstrada

conforme a figura 6, que ilustra o ciclo de vida da informação com os conceitos básicos de segurança da informação.

Figura 6 – Quatro momentos do ciclo de vida da informação, considerando os conceitos básicos da segurança e aspectos complementares



Fonte: Sêmola (2014, p. 11).

Assim, é importante o conhecimento dos princípios essenciais de segurança da informação, que são desta forma caracterizados por Sêmola (2014):

Confidencialidade - O princípio da confidencialidade diz respeito que todas as informações devam ser mantidas conforme o grau de sigilo necessário, de forma que o seu conteúdo possa ser acessado apenas às pessoas que têm direito.

Integridade - O princípio da integridade diz respeito que todas as informações devam ser mantidas de maneira íntegra conforme o disponibilizado pelo proprietário, ou seja, de modo que seu conteúdo não seja alterado ou violado indevidamente.

Disponibilidade - Demonstra que a informação, gerada ou adquirida, deva estar acessível sempre que necessário a todos os usuários que forem autorizados a acessá-la.

Além dos princípios mencionados, Fontes (2015) acrescenta mais três princípios caracterizados como essenciais:

Legalidade - As informações precisam estar de acordo com as normas vigentes, como leis, regulamentos e licenças, além de respeitarem os princípios perante a sociedade.

Auditabilidade – Demonstra que a informação deve ter a possibilidade de ser auditada, ou seja, deve ser registrado quem usou ou acessou determinada informação.

Não repúdio de autoria – Esclarece que o usuário deve agir responsavelmente, não podendo negar caso tenha alterado ou gerado qualquer tipo de informação.

Dessa forma, ficam entendidos os princípios fundamentais de segurança da informação, os quais as organizações devem seguir para preservar as informações de maneira que se possa trazer uma série de benefícios para as empresas e para a sociedade. Portanto, de acordo com Fontes (2015), a segurança da informação se traduz de um grande interesse dos acionistas, além da continuidade do negócio, pois o trabalho, a segurança e o crescimento profissional estão diretamente vinculados à existência organizacional.

2.3.2 Normas de segurança da informação

As normas de segurança da informação servem para explicar as melhores práticas, bem como os princípios e as diretrizes, para que ao adotá-las, as organizações disponham de uma segurança eficaz, o que consequentemente possibilita o ganho a uma série de benefícios empresariais. Este tema de grande relevância é apresentado por Fontes (2015, p. 104), no qual ele demonstra que “assim como no mundo real, você deve conhecer todas as normas e regulamentos da organização e a legislação vigente sobre o uso da informação no mundo virtual”. Pois

além de conhecer para que serve e os ganhos de segurança que as normas possibilitam, as punições aplicadas no chamado mundo virtual são tratadas e sancionadas no mundo real.

É importante destacar que existem diversas normas reconhecidas nacional e internacionalmente de diversas instituições padronizadoras. Porém, as mais adotadas e reconhecidas nacionalmente, pertencem à família ISO/IEC 27000 (é um padrão publicado pela *International Organization for Standardization* e pela *International Electrotechnical Commission*), que trata sobre gestão de segurança da informação. Nesse contexto, conforme a norma ISO9000 (referente à gestão de qualidade), ficou amplamente conhecida e se tratou de um diferencial competitivo para as empresas; acredita-se que a norma da família ISO/IEC 27000, referente à segurança da informação, será amplamente conhecida e adotada na medida em que as organizações, assim como as pessoas, compreenderem o tamanho de sua importância. Essa relevância é demonstrada por Sêmola (2013, p. 72), de acordo com o autor, “teremos seguramente um novo movimento no meio corporativo em busca de sintonia, conformidade e, consequentemente, certificação com base na norma de segurança da informação”.

Nesse contexto, foi realizado um estudo por Galegale *et al.* (2017), no qual todas as organizações examinadas usam como base a norma ABNT NBR ISO/IEC 27002:2005 (norma pertencente à família ISO/IEC 27000), para elaboração da sua política. A norma 27002 exemplifica os controles e mecanismos para implementações de segurança da informação e foi criada a partir de uma transição da norma ISO/IEC 17799, que é a norma tratada por Sêmola (2013) em seu livro, criada no ano de 2000, possibilitando que segurança da informação passasse a ser mais conceituada no ambiente empresarial.

2.3.3 Ameaças, vulnerabilidades, medidas de segurança e análise de risco

Ameaças e vulnerabilidades se constituem como tema recorrente para entender a segurança da informação, no sentido que se deve conhecer os riscos tecnológicos que existem para as organizações e, assim, tomar as medidas de segurança necessárias. Para os autores Turban e Volonino (2013), entre os principais

erros que os gerentes ou diretores comentem é não dar a devida importância ao assunto, não conhecendo as vulnerabilidades e ameaças presentes na organização. Assim, como forma de entendimento, serão demonstradas o que são ameaças e vulnerabilidades, além de medidas de segurança e análise de risco.

Ameaças – De acordo com Rainer e Cegielski (2012, p. 75), “uma ameaça a um recurso de informação é qualquer perigo ao qual um sistema pode estar exposto”. Como demonstrado ao decorrer do trabalho, o sistema exposto pode trazer prejuízos para a organização. Sêmola (2014, p.47), também classifica as ameaças e, de acordo com ele, elas se referem a “agentes ou condições que causam incidentes que comprometem as informações e seus ativos por meio da exploração de vulnerabilidades”.

Assim, Sêmola (2014) relaciona as ameaças de acordo com a sua intencionalidade, sendo:

a) Naturais – São as ameaças ocasionadas por fenômenos da natureza, como incêndios, enchentes;
b) Involuntárias – As ameaças involuntárias são causadas de modo inconsciente em função do desconhecimento das pessoas, como erros ou falta de energia;
c) Voluntárias – São causadas por agentes invasores, como hackers, ladrões, espiões.

Vulnerabilidades – Conforme demonstram Rainer e Cegielski (2012, p. 76), “a vulnerabilidade de um sistema é a possibilidade de ele sofrer algum dano devido a uma ameaça”. O mesmo também é caracterizado por Sêmola (2014, p.48), como “fragilidade presente ou associada a ativos que manipulam e/ou processam informações que, ao ser explorada por ameaças, permite a ocorrência de um incidente de segurança”. Portanto, pode ser concluído, de acordo com Sêmola (2014), que as vulnerabilidades necessitam de um agente causador ou das ameaças para que os incidentes sejam provocados.

Da mesma forma, são demonstrados exemplos de vulnerabilidades, conforme apresenta Sêmola (2014):

a) Físicas – Correspondem à falta de planejamento na prevenção de possíveis incêndios, explosões, como não instalar detector de fumaça;
b) Naturais – Desastres naturais podem acontecer, como enchentes e terremotos;
c) Hardware – São as falhas que ocorrem por desgaste, falta de atualização dos equipamentos físicos ou a má utilização;
d) Software – São os erros que ocorrem durante a instalação e configuração, possibilitando que dados sejam perdidos, recursos alterados por acessos indevidos;
e) Mídias – As mídias, como CD's, pendrive, relatórios, que podem ser extraviadas ou danificadas, impossibilitando o acesso;
f) Comunicação – Correspondem à falha ou falta de comunicação ou os chamados acessos não autorizados;
g) Humanas – Refere-se à não aplicação de segurança necessária, vazamento de informações, omissões, roubos.

Medidas de segurança – Podem ser entendidas conforme o demonstrado Sêmola (2014, p.49), em que "são as práticas, os procedimentos e os mecanismos usados para a proteção da informação e seus ativos, que podem impedir que ameaças explorem vulnerabilidades.

Nesse sentido, as medidas possuem as seguintes características, conforme entendido por Sêmola (2014):

a) Preventivas – Referem-se às medidas que a organização possa implementar para evitar possíveis ataques ou acidentes;
b) Detectáveis – Referem-se às medidas de segurança que visem identificar as ameaças e impedir que as mesmas explorem possíveis vulnerabilidades;
c) Corretivas – Referem-se às medidas que no geral corrigem determinadas estruturas deficitárias, seja reduzindo os impactos ou se recuperando de desastres.

Análise de Riscos - Sêmola (2014, p. 109), também conceitua a análise de riscos, sendo, de acordo com ele, a "probabilidade de ameaças explorarem vulnerabilidades, provocando perdas de confidencialidade, integridade e disponibilidade, causando, possivelmente, impactos nos negócios". Assim, Sêmola

(2014) acredita que a análise de riscos é um mecanismo essencial para o diagnóstico atual de segurança da informação. Nesse sentido, para Turban e Volonino (2013, p. 125), a gestão de risco corresponde ao “processo de identificação, avaliação e redução do risco a um nível aceitável”.

Após demonstrado o que são ameaças, vulnerabilidades, medidas de segurança e análise de riscos, surgem as fraudes, crimes e violações, responsáveis em sua maioria pela criação das medidas de segurança.

2.3.4 Fraudes, crimes e violações

Conforme demonstra Mandarino (2010), o mundo está perante uma crescente ameaça de ataques cibernéticos, de modo que as empresas, pessoas físicas e governos estão expostos a riscos imensuráveis. Assim, é necessário compreender os elementos que estabelecem o espaço cibernético e as fraudes, crimes e violações presentes. Dessa forma, de acordo com Turban e Volonino (2013), pode-se dizer que os crimes se subdividem em dois tipos, os considerados violentos e os não violentos; assim, as fraudes, por utilizar a ilusão e truques não são consideradas como um crime violento, pois elas são realizadas por meio de vantagens, ignorância ou preguiça dos outros.

No aspecto dos crimes não violentos, manifestam-se os *cibercrimes* (crimes por intermédio de computador), que possibilitam um roubo considerado fácil com pouco esforço de tempo e com perspectiva de ganhos elevados. Nessa situação, Stair e Reynolds (2016, p 641), admitem que “a capacidade de um computador para processar milhões de sequências de dados em menos de um segundo pode ajudar um ladrão a roubar dados que valem milhões de dólares”. Portanto, para Stair e Reynolds (2016), pode ser considerado que os criminosos aos quais se utilizam deste meio, são mais audaciosos e criativos, pois cometem crimes a nível global com o auxílio da internet.

Nesse contexto é importante mencionar que, apesar da grande quantidade de *cibercriminosos* (pessoas que cometem o *cibercrime*) presentes no mundo, a maior parte das fraudes que acontecem nas organizações são com o auxílio de pessoas

internas. Isso é demonstrado por Fontes (2015), o qual conclui que os agentes internos possuem informações privilegiadas e necessárias para realização de fraudes corporativas, assim, uma pessoa de fora da organização que procure obter essas informações irá gastar mais tempo e aparatos financeiros. Nesse sentido, Turban e Volonino (2013) acreditam que os funcionários internos podem penetrar as barreiras de segurança física (meios de acesso a empresa) e lógica (uso de senhas, por exemplo), sendo responsáveis pelos maiores prejuízos das organizações.

Em um contexto de fraudes, crimes e violações, destacam-se três atualmente notáveis: a engenharia social, o *ciberterrorismo* e o roubo de identidade, além dos populares conceitos de hacker e cracker. Assim, são delimitados abaixo.

Engenharia Social – Para os autores Stair e Reynolds (2016, p 642), a engenharia social refere-se ao “uso de habilidades sociais para fazer com que os usuários forneçam dados, permitindo aos hackers terem acesso a um sistema de informação ou a seus dados”. Assim, Fontes (2015, p.121) demonstra que os “engenheiros sociais agem e buscam informações da organização usando pessoas como você: falam com conhecimento, adquirem a confiança do interlocutor, prestam favores”. Dessa maneira, por meio da conquista de confiança, é que eles adquirem acesso aos dados e cometem fraudes.

Ciberterrorismo – Conforme Stair e Reynolds (2016, p 642), corresponde a “qualquer ataque premeditado e com motivação política contra sistemas de informações, computadores, programas de dados, que resultem em ataques contra alvos não resistentes realizados por grupos subnacionais ou agentes clandestinos”.

Roubo de Identidade – Para Turban e Volonino (2013), o roubo de identidade refere-se a um dos piores crimes e atualmente bem comum. Stair e Reynolds (2016, p 644) dizem que “roubo de identidade é um crime no qual um impostor obtém importantes informações sobre identificação pessoal, como os números de seguro social ou de cartas de motorista, para se passar por outra pessoa”.

Hacker ou Cracker – Para Stair e Reynolds (2016, p 648) o termo “Hacker: Uma pessoa que gosta de tecnologia da computação e gasta seu tempo aprendendo e usando os sistemas operacionais”. Os autores Stair e Reynolds (2016, p 648) dizem que “Hacker criminoso (Cracker): É uma pessoa habilidosa no uso de computadores que tenta obter acesso não autorizado ou ilegal a sistemas computacionais para

roubar senhas, corromper arquivos e programas, ou mesmo para transferir dinheiro". De forma ampla, o autor Mandarino (2010, p. 83) correlaciona os termos no sentido de que "hackers invadem sistemas com o único objetivo de conhecê-lo melhor e aprimorar as técnicas. Crackers invadem sistemas, em geral, com objetivos financeiros ou, simplesmente, para causar algum dano ao computador da vítima".

2.3.5 O fator humano

Estudos revelam que gastos elevados em TI não indicam uma segurança eficaz, pois quem realmente faz toda a diferença é o usuário, visto que ele pode simplesmente negligenciar todo esforço e dedicação da organização em criar uma política eficiente. Portanto, o fator humano é um aspecto fundamental no presente estudo, sendo essencial que o usuário entenda o real valor da segurança da informação e, assim, compreenda a necessidade de se prevenir. Nesse contexto, Turban e Volonino (2013, p.124) demonstram que os maiores riscos advêm dos funcionários e gestores, conforme o representado abaixo:

> "Em geral, medidas de segurança em TI têm focado em proteger a empresa de malwares e de pessoas de fora. Ainda que controlar o acesso físico e remoto aos bancos de dados e redes continue sendo um desafio, a maioria das violações de dados envolve algum tipo de erro ou ação interna – intencional ou não intencional. **Isso quer dizer que os maiores riscos em seginfo são os funcionários e os gestores**. As empresas sofrem perdas tremendas com fraudes cometidas por seus funcionários. É um problema geral que afeta todas as empresas, independentemente do seu tamanho, localização ou setor" (TURBAN, VOLONINO, 2013).

O mesmo demonstrado por Turban e Volonino (2013), também é encontrado em Davenport *et al.* (2004), pois de acordo com os autores, muitas pesquisas expõem que os investimentos em TI não demonstram retornos representativos, porque o usuário não aprendeu a usufruir corretamente da tecnologia ou os gestores não conseguiram administrar como forma a se tirar proveito.

Nesse sentido, Silva e Stein (2007), evidenciam que as corporações já gastaram muitos recursos em meios de proteção, porém, acredita-se que esses recursos foram desperdiçados, pois não foi analisado o fator humano que compreende

os usuários do sistema, assim, por conta das limitações, o fator humano representa o elo mais fraco. Desse modo, Sêmola (2014, p. 129) também destaca que “os recursos humanos são considerados o elo mais frágil da corrente, pois são responsáveis por uma ou mais fases de processo de segurança da informação”. Portando, Sêmola (2014) considera o ser humano uma máquina complexa que sofre interferência de fatores externos, não sendo possível prever seus comportamentos.

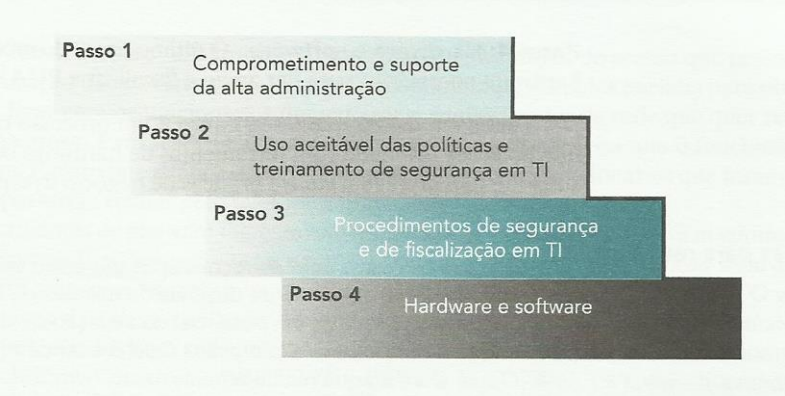
Logo, apesar de todas as funcionalidades da tecnologia da informação, Davenport *et al.* (2004) fazem uma crítica na qual, segundo eles, a TI auxilia diversos processos do fluxo informacional, mas não é a principal ferramenta para criação e exploração das informações como se imaginava, pois o domínio da informação ainda é uma tarefa particularmente humana. Desse modo, o fator humano é determinante na adoção de estratégias em TI e também será analisado neste estudo.

Portanto, pode-se concluir, conforme Davenport *et al.* (2004), que as pesquisas dão suporte a razão pelas quais os grandes investimentos em TI não produzem resultados deve-se ao fato de que as empresas não conseguem entender os funcionários, sendo assim, um bom modo de corrigir esse erro é pelo entendimento de como as pessoas processam e adquirem as informações. Nesse sentido, Fontes (2015) corresponde dizendo que com base em sua experiência, na medida em que o usuário conhece os sentidos de segurança da informação, ele as adota como meio de proteção.

2.3.6 Modelo de segurança em TI

Conforme demonstrado, o sucesso no âmbito empresarial depende da proteção dos dados, informações e conhecimentos, e, por esse motivo, o controle interno da tecnologia da informação requer um modelo que apresente métricas para estruturação da TI na organização. Nesse sentido, Fontes (2015) demonstra que o comportamento do usuário é imutável, porém os controles para uma segurança eficaz de TI são necessários para evitar situações de fraudes e crimes. Dessa maneira, o modelo proposto por Turban e Volonino (2013) propõe estruturar a segurança da informação com base em uma combinação de pessoas, processos e tecnologia, de acordo com a figura 7.

Figura 7 – Modelo de defesa em profundidade de segurança em TI



Fonte: Turban e Volonino (2013, p.131).

Esses passos fazem referência aos procedimentos que um projeto de segurança em TI precisa seguir para atingir o sucesso, como referência à alta administração, ao uso aceitável das políticas e procedimentos de segurança, além de uma preocupação com ferramentas de segurança, assim, pode-se dizer que todas as etapas são essenciais para o bom funcionamento organizacional. A representação de todas as etapas é demonstrada por Turban e Volonino (2013, p. 130), e eles resumem dizendo que “o princípio básico é que, quando uma camada ou nível de defesa falha, outra camada ou nível da a proteção”. A seguir, os níveis ou etapas do modelo serão descritas, como pretexto para melhor assimilação do mesmo.

2.3.6.1 Etapa 1: Comprometimento e suporte da alta administração

A primeira etapa corresponde ao total comprometimento e suporte da alta administração, porém, atualmente nem todos os gestores possuem conhecimentos necessários sobre a segurança da informação, pois muitos não conhecem nem ao menos os princípios básicos e as suas importâncias. Isso é altamente necessário, de modo que é papel dos gestores dar suporte e demonstrar ao restante da organização as políticas, normas e métodos para se seguir, objetivando uma competente segurança da informação organizacional.

No sentido de promover a segurança em TI, Turban e Volonino (2013, p. 130) acreditam que “a influência dos superiores é necessária para implementar e manter a segurança, os padrões éticos, as práticas de privacidade e o controle interno”. Além deles, Ferreira *et al.* (2016) também entendem que os gestores devem utilizar as suas posições hierárquicas para definir as principais práticas de segurança a serem abordadas de maneira ética, de acordo com os recursos destinados e necessários para uma aplicação eficaz frente aos riscos organizacionais. Isso também é presente no estudo de Galegale *et al.* (2017, p. 87), no qual eles concluíram que o assunto de segurança da informação, mais precisamente, a política das organizações referente ao assunto, são tratados em níveis estratégicos das instituições.

Esses estudos são demonstrados no que expõe Beal (2008, p. 86), sendo de acordo com a autora:

> “A participação da cúpula estratégica (pessoas com responsabilidade global sobre a organização) é fundamental nos processos de planejamento estratégico da informação e da TI. Sem o envolvimento da direção nas decisões de alto nível a respeito dos investimentos e prioridades na alocação de recursos, a organização corre o sério risco de deixar de investir em informação e tecnologia necessária e desperdiçar recursos em projetos sem grande retorno para o negócio, em decorrência da falta de parâmetros para se analisar corretamente o custo-benefício envolvido” (BEAL, 2008).

Portanto, nota-se que a alta administração possui papel fundamental na adoção de estratégias de segurança em TI que sejam eficientes, possibilitando que as organizações cumpram os regulamentos e que a organização tenha uma boa visão perante os clientes internos e externos. Turban e Volonino (2013) também entendem assim, pois de acordo com eles, os órgãos reguladores veem com bons olhos as empresas que praticam a adoção de métodos de governança corporativa na prevenção de crimes e fraudes.

De tal modo, é importante relacionar que a segurança da informação é um papel fundamental da governança de TI, que de acordo com Turban e Volonino (2013), é responsável pela supervisão e monitoramento dos controles em TI. Assim, muitas normas que o instituto de governança em TI publica podem ser seguidas, como o COBIT (guia de governança), e a lei *Sarbanes-Oxley* (lei que requer provas para validar os relatórios financeiros). Sendo assim, Turban e Volonino (2013), garantem

que uma prevenção de TI começa com uma cultura de governança corporativa por parte da alta administração das organizações.

2.3.6.2 Etapa 2: Uso aceitável das políticas e treinamento de segurança em TI

Após a etapa de comprometimento e suporte da alta administração, o próximo passo consiste no uso aceitável das políticas e treinamento de segurança em TI, de acordo com as normas que a organização procurar seguir. As políticas de segurança da informação servem para definir diretrizes e modelos a serem seguidos pelos colaboradores da organização, que necessitam de orientação e treinamento referente à segurança da informação, como forma de prevenir quanto a possíveis crimes, fraudes e violações. Dessa forma, Turban e Volonino (2013) demonstram que conforme for o entendimento de como a segurança afeta a organização, maior será a adoção de políticas de segurança pelas empresas.

Nesse sentido, Sêmola (2014) alega para a importância das diretrizes, pois de acordo com ele, as empresas precisam comunicar de forma clara aos usuários sobre a importância que destinam para a informação, com a finalidade de que isso seja implementado em sua cultura organizacional. Dessa maneira, Beal (2008) acredita que ao divulgar os valores que a empresa dispõe ao fluxo informacional, possibilita que parceiros de negócio conheçam os limites éticos a serem seguidos, como a distribuição e manipulação adequadas da informação.

Nesta etapa, os autores Turban e Volonino (2013) definem que uma política de uso aceitável (PUA), é amplamente necessária, na medida em que delimita as responsabilidades e as consequências dos funcionários, bem como as ações aceitáveis e inaceitáveis. Dessa maneira, é demonstrado por Beal (2008, p. 53) que as “políticas de informação e de segurança da informação orientam a análise de riscos, processo no qual são avaliadas as ameaças existentes, as probabilidades de sua concretização e os respectivos impactos para o negócio”.

Assim, Sêmola (2014) caracteriza a relevância que uma política de segurança da informação possui, demonstrando tamanha importância conforme relaciona que a política de segurança está para as organizações assim como a Constituição Federal

está para um País, além de subdividir a política em 3 blocos: diretrizes, normas, procedimentos e instruções, representados conforme os níveis estratégico, tático e operacional. Nesse sentido, Fontes (2015), conclui ilustrando que “cada colaborador faz parte do processo de segurança da informação, que busca garantir para a organização a sua continuidade no mercado e a proteção de sua informação como um recurso crítico para a realização do negócio”. Portanto, além definir diretrizes e normas, se faz necessário treinar os funcionários quanto aos procedimentos e instruções para implementação e continuidade do negócio.

2.3.6.3 Etapa 3: Procedimentos de segurança e de fiscalização em TI: orientação, normas e controle

A terceira etapa corresponde aos procedimentos de segurança e de fiscalização em TI, ou seja, orientação, normas e controle, com a finalidade de que os usuários sigam os procedimentos como forma de minimizar os riscos. Assim, conforme demonstrado no referencial teórico, o fator humano é o elo mais vulnerável da organização, dado que o comportamento humano é de certa forma imprevisível, portanto, estar em permanente controle dos funcionários e atualizar periodicamente as orientações e normas é de grande necessidade para a eficácia empresarial.

Novamente, o fator humano é colocado em risco, pois Sêmola (2014) acredita que conforme sejam demonstradas as normas referentes ao fluxo informacional e descarte de senhas, serão implementados recursos para auditoria e autenticação de acesso, porém, isso pode ser posto em perigo, por exemplo, se um fator humano divulga a sua senha pessoal. Assim, Sêmola (2014) acredita que somente com o compartilhamento de responsabilidades entre os indivíduos, como forma de desenvolver uma cultura de segurança, é que as empresas terão funcionários competentes na gestão de segurança da informação e atuando na diminuição de riscos.

Nesse contexto, Turban e Volonino (2013) acreditam que o desempenhado pelos funcionários precisa ser monitorado permanentemente, como forma de verificar o cumprimento das políticas da organização, como a política de uso aceitável (PUA), por exemplo, sendo necessários métodos para monitoramento, treinamento e

fiscalização. Nesse sentido, Beal (2008) demonstra que a política de segurança da informação deverá estar constantemente atualizada, como maneira de ser considerada efetiva, porém, Sêmola (2014) acredita ser muito complexo desenvolver e manter atualizada a PSI, pois o meio tecnológico é muito dinâmico, com alterações frequentes e, dessa forma, pode ser viável ter representantes de diferentes setores contribuindo com diferentes visões e necessidades para construção da política institucional de segurança da informação. Pode se concluir que se é necessário monitorar o comportamento humano para garantir que as políticas sejam eficazes, além de constantemente atualizar as orientações e normas.

2.3.6.4 Etapa 4: Ferramentas de segurança - *hardware* e *software*

No presente contexto, após o comprometimento da alta diretoria, o uso de políticas aceitáveis e os procedimentos de segurança e de fiscalização, é iniciada a última etapa, na qual, Turban e Volonino (2013) demonstram que é necessária a implementação de ferramentas de segurança correspondentes a hardware (refere-se a equipamentos, como computador, processador) e software (refere-se a programas que instruem o hardware a processar os dados), indispensáveis para fiscalizar as políticas e apoiar as práticas seguras. Além disso, é alertado por Turban e Volonino (2013) de que a segurança é um processo contínuo e essas ferramentas não protegem das práticas irresponsáveis.

Desse modo, Sêmola (2014) demonstra que a implementação necessária de software e hardware consiste na aplicação dos controles de segurança para alcançar o nível de risco essencial. Assim, Sêmola (2014, p. 116) acredita que:

> “Destinados a suprir a infra-estrutura tecnológica com dispositivos de software e hardware de proteção, controle de acesso e consequente combate a ataques e invasões, esta família de mecanismos tem papel importante no modelo de gestão de segurança, à medida que as conexões eletrônicas e tentativas de acesso indevido crescem exponencialmente. Nesta categoria, existem dispositivos destinados ao monitoramento, filtragem e registro de acessos lógicos, bem como dispositivos voltados para a segmentação de perímetros, identificação e tratamento de tentativas de ataque” (SÊMOLA, 2014).

Nesse sentido, as ferramentas de hardware e software contribuem para a fiscalização das políticas de segurança da informação, sendo necessárias para combate a ataques e invasões, logo, as ferramentas devem estar em constante atualizações e disponíveis para que o usuário as usufrua de maneira responsável e ética.

3. PROCEDIMENTOS METODOLÓGICOS

A presente pesquisa apresenta a avaliação e diagnóstico quanto à gestão de segurança da informação. De acordo com Gil (2010, p. 1), “pode-se definir a pesquisa como o procedimento racional e sistemático que tem como objetivo proporcionar respostas aos problemas que são propostos”. Nesta pesquisa, são apresentados estudos e pesquisas acadêmicas para traçar um problema e, após isso, o referencial teórico é desenvolvido para embasar modelos e demonstrar o diagnóstico das respostas. Desse modo, a pesquisa quanto à utilização de práticas de segurança da informação por parte das empresas nacionais tem por objetivo verificar as gestões de segurança nas empresas nacionais de acordo com a pesquisa do tipo *survey* aplicada.

3.1 Método e estratégia de pesquisa

Conforme mencionado, este trabalho se utiliza do método de pesquisa *survey*, em que procura descrever quantitativamente uma população, fazendo uso de um instrumento para coleta de dados previamente definido (FREITAS *et al*. 2000). Assim, o instrumento escolhido para análise foi o questionário, o modelo utilizado neste estudo pode ser encontrado em apêndice e foi realizado por meio da plataforma formulários *google*. As perguntas foram realizadas com base no modelo de segurança em TI proposto por Turban e Volonino (2013), descrito na revisão teórica do presente trabalho e como fonte nas pesquisas aplicadas por Ferreira *et al*. (2016) e Fontes (2015) em seus estudos.

3.2 População alvo e amostragem

A população alvo foram pessoas que trabalham com serviços financeiros (fundo de investimento, corretora de ações, banco de varejo e de investimentos, cooperativa de crédito, companhia de cartões de crédito, consultoria financeira, etc.). No entanto, foram encontradas barreiras para atingir esse público, por ser de difícil acesso e pela

complexidade do assunto, além de que muitos não são autorizados a responder este tipo de pesquisa, pois ela pode violar as políticas de algumas organizações. Por isso, o número total de participantes foi de 23, sendo que a mesma foi enviada para um número muito superior, demonstrando as barreiras já mencionadas para atingir o público específico. As empresas que participaram do estudo foram necessariamente as do setor de serviços financeiros, visto que são mais afetadas por crimes virtuais - conforme identifica a pesquisa *Accenture e Ponemon Institute,* realizada em 2018 -, além de que o custo efetivo para gerir *ciberataques* nesse setor é maior do que comparados aos outros.

3.3 Coleta e análise de dados

Para coleta de dados, os questionários foram enviados via correio eletrônico a empresas consideradas a responder, a conhecidos que trabalham no ramo e através do *mailing* dos cursos de Administração e de Ciências da Computação da Universidade Federal do Rio Grande do Sul. Os itens de preenchimento foram operacionalizados conforme a escala *Likert,* de 5 pontos, variando de (1) discordo totalmente a (5) concordo totalmente. Conforme mencionado, o procedimento metodológico coletou os dados empíricos de empresas brasileiras por meio de um questionário aplicado no tipo de pesquisa *survey*, para analisar como as empresas adotam e se preocupam com medidas que auxiliam na gestão de segurança da informação, a detecção e combate às fraudes, além da percepção quanto ao fator humano. Após a coleta dos dados e informações, realizou-se a análise dos mesmos por meio do software *Qlik Sense*, que possui as habilidades de ler, trabalhar, analisar os dados. Desse modo, foram desenvolvidos gráficos, quadros e tabelas para ilustrar os dados e as informações e, assim, gerar conhecimento.

4 ANÁLISE DOS RESULTADOS

Os resultados apresentados ao longo da pesquisa *survey* serão tratados neste capítulo, que aborda o perfil dos respondentes, a percepção dos mesmos quanto aos fatores humanos e às fraudes, além da avaliação sobre o modelo de defesa em profundidade de segurança em TI, que está presente nas organizações pesquisadas. Ao todo, foram 26 perguntas subdivididas em sete tópicos (perfil dos respondentes, percepção quanto ao fator humano e às fraudes, avaliação sobre a alta administração, políticas de segurança, procedimentos e ferramentas). Assim, nesta análise de resultados existe uma argumentação dos dados e informações por meio de uma relação com estudos e pesquisas acadêmicas, para demonstrar a importância das relações existentes com destino a desenvolver um modelo de segurança em TI eficaz.

4.1 Perfil dos respondentes

O objetivo da pesquisa foi aplicá-la a funcionários do setor financeiro, com idades diversas, escolaridades e cargos distintos, variados tempos de experiência no setor financeiro, além de diferentes departamentos, para relacionar variáveis que apresentam mais criteriosamente a possível influência dessas diferenças em uma adoção eficaz de um modelo se segurança em TI. A partir das respostas referentes ao perfil, foi produzida a tabela 1, para demonstrar as diferentes características dos respondentes à pesquisa. O número total de participantes foi de 23, sendo que a mesma foi enviada para um número muito superior, comprovando as barreiras de atingir um público específico que conheça, esteja disposto e seja autorizado a responder.

Tabela 1 - Características da amostra

Características		**Absoluta (n)**	**Relativa %**
Gênero			
	Feminino	8	34,8%
	Masculino	15	65,2%

Idade			
	Entre 16 e 25 anos	9	39,1%
	Entre 26 e 33 anos	7	30,4%
	Entre 34 e 41 anos	6	26,1%
	Acima de 42 anos	1	4,3%
Cidade			
	Porto Alegre	16	69,6%
	São Paulo	5	21,7%
	Eldorado do Sul	1	4,3%
	Rio de Janeiro	1	4,3%
Escolaridade			
	Ensino Superior Incompleto	13	56,5%
	Ensino Superior Completo	6	26,1%
	Pós-Graduação	3	13,0%
	Mestrado	1	4,3%
Cargo			
	Estagiário	6	26,1%
	Auxiliar/Assistente	5	21,7%
	Analista	8	34,8%
	Supervisão/Coordenação	3	13,0%
	Gerência	1	4,3%
Tipo de Empresa			
	Privada	18	78,3%
	Pública	5	21,7%
Tamanho da Empresa			
	Até 9 colaboradores	3	13,0%
	De 10 a 49 colaboradores	3	13,0%
	De 50 a 99 colaboradores	4	17,4%
	Mais de 100 colaboradores	13	56,5%
Tempo de Experiência em Instituições Financeiras			
	Até 2 anos	10	43,5%
	Entre 2 e 5 anos	6	26,1%
	Entre 5 e 10 anos	3	13,0%
	Entre 10 e 15 anos	2	8,7%
	Acima de 15 anos	2	8,7%
Setor da Empresa			
	Fundo de Investimento	6	26,1%
	Corretora de ações	5	21,7%
	Banco de Varejo e de Investimentos	5	21,7%
	Cooperativa de Crédito	4	17,4%
	Companhia de Cartões de Crédito	2	8,7%
	Consultoria Financeira	1	4,3%
Departamento			
	Departamento Administrativo	4	17,4%

	Departamento de Comunicação	5	21,7%
	Departamento de Informática	8	34,8%
	Departamento Financeiro	6	26,1%

Fonte: Elaborado pelo autor.

Diante do exposto na tabela 1, pode ser verificado que os dados são distintos em praticamente todas as categorias, representando uma boa distribuição nos itens de idade, escolaridade, cargo, experiência, ramo da empresa e departamento em que trabalha. De acordo com os dados relevantes dos respondentes, pode ser verificado que homens correspondem a **65,2%**, empresas residentes na cidade de Porto Alegre correspondem a **69,6%**, grau de escolaridade em ensino superior incompleto corresponde a **56,7%**, funcionários de empresa privada correspondem a **78,3%**, e funcionários de empresa com mais de 100 colaboradores correspondem a **56,5%**.

4.2 Percepção quanto ao fator humano

Como demonstrado no referencial teórico do presente trabalho, o usuário representa um fator determinante para efetividade da segurança em TI nas organizações, pois conforme Silva e Stein (2007), o usuário representa o chamado elo mais fraco das empresas. Assim, foi procurado verificar em que medida se dá a atuação dos usuários nas organizações em relação à segurança. A escala de medida do tipo *Likert* foi adotada, de 5 pontos, variando de (1) discordo totalmente a (5) concordo totalmente. As perguntas, bem como as médias, podem ser verificadas no quadro 1 assim, a escala das respostas em gráfico pode ser demonstrada na figura 9.

Quadro 1 - Perguntas de 1 a 4

Perguntas	**Média (n)**
1. Em que medida você consegue comunicar ao setor de TI qualquer ocorrência ou suspeita que comprometa a segurança da informação na organização financeira em que você atua?	**4,26**
2. Em que medida você considera que o usuário é fator essencial no combate aos crimes cibernéticos?	**3,91**
3. Em que medida você acredita que são monitorados os acessos realizados pelos usuários (e-mail, sites, sistemas corporativos)?	**3,83**

4. Em que medida você considera que os funcionários seguem corretamente as recomendações da área de segurança da informação?	**2,87**

Fonte: Elaborado pelo autor.

Em relação à pergunta de número 1, foi questionada a comunicação do usuário com o setor de TI em qualquer ocorrência suspeita, desse modo, é importante mencionar que o usuário deva ter ampla comunicação com os responsáveis no auxílio de possíveis vulnerabilidades e ameaças existentes. Nesta perspectiva, a média apresentada (4,26) foi considerada alta neste estudo, concluindo que a comunicação existente é eficiente, o que representou a maior média da categoria de percepção quanto ao fator humano.

Conforme a pergunta de número 2, foi indagou-se em que medida se considera o usuário como fator essencial no combate a *cibercrime*; nesse contexto, Silva e Stein (2007) demonstram que o usuário é a parte mais vulnerável na segurança em TI e o mesmo é representado por Turban e Volonino (2013), pois demonstram que os maiores riscos advêm dos funcionários e gestores. Assim, conforme a média apresentada (3,91), nem todos respondentes consideram o usuário como o fator essencial no combate aos crimes cibernéticos.

De acordo com a questão 3, foi questionada em que medida se acredita que são monitorados os acessos realizados pelo usuário; nesse sentido, conforme o proposto por Turban e Volonino (2013), o monitoramento dos acessos realizados pelos usuários é efetivo e necessário como forma de verificar o cumprimento das políticas e normas da organização. De acordo com a média apresentada (3,83), a maior parte dos respondentes da pesquisa concordam que os acessos são monitorados pelas empresas.

Conforme a pergunta de número 4, foi questionada em que proporção se considera que os usuários seguem corretamente as recomendações da área de segurança da informação. Este ponto é fundamental no entendimento deste trabalho, pois os autores Davenport *et al.* (2004), Fontes (2015), Turban e Volonino (2013) e Silva e Stein (2007), alegam para o sentido de que o fator humano possui grande importância na adoção de qualquer estratégia em TI. Assim, pode ser entendido, conforme Fontes (2015), que o usuário desconhece os motivos para segurança da informação, por isso não segue os procedimentos, ou conforme Davenport *et al.*

(2004), pelo fato de que a maioria dos programas de TI ainda negligenciam o usuário como fator fundamental em uma segurança eficaz. Além, é claro, de acordo com Turban e Volonino (2013), por motivos pessoais, em que o usuário é uma ameaça intencional e pratica fraude interna. Em vista disso, a média das repostas (2,87) causou surpresa, representando a mais baixa da pesquisa, sendo possível perceber que a maioria dos usuários não segue corretamente as recomendações de segurança da informação.

4.3 Percepções quanto às fraudes

A partir da percepção sobre fatores humanos, podemos verificar as percepções quanto às fraudes, visto que estas decorrem do auxílio de pessoas. Esta percepção corresponde ao item do referencial teórico do presente trabalho sobre as fraudes, crimes e violações, em que são demonstrados contextos dos mesmos, além de alguns crimes atualmente notáveis. Conforme mencionado por Fontes (2015), a maior parte das fraudes nas organizações ocorrem com participação dos funcionários internos, pois possuem informações privilegiadas, por isso, é necessário a adoção de políticas eficazes para evitar esse tipo de crime. Isto posto, foi perguntado sobre a percepção dos colaboradores quanto às fraudes na organização em que trabalha. A escala de medida do tipo *Likert* foi adotada, de 5 pontos, variando de (1) discordo totalmente a (5) concordo totalmente. As perguntas, bem como as médias, podem ser verificadas no quadro 2, assim, a escala das respostas em gráfico pode ser demonstrada na figura 10.

Quadro 2- Perguntas de 5 a 7

Perguntas	**Média**
5. Em que medida você conhece alguém que já foi vítima de fraude realizada por meio do ambiente computacional.	**3,96**
6. Em que medida a organização na qual você trabalha já foi vítima de fraudes.	**3,30**
7. Em que medida você considera que a sua organização tem realizado medidas para evitar as fraudes.	**4,30**

Fonte: Elaborado pelo autor.

De acordo com a questão de número 5, foi questionada em que medida os participantes conhecem alguma vítima de *cibercrimes* (fraude realizada por meio do ambiente computacional); nesse sentido, podemos conhecer casos de pessoas que já foram vítimas de fraudes por meio do ambiente computacional, seja um familiar, amigo ou conhecido. Dessa maneira, a média apresentada (3,96) representa um número elevado de respondentes que conhecem vítimas desses ataques.

Conforme a pergunta de número 6, foi questionada em que dimensão a organização na qual as pessoas trabalham já foi vítima de fraudes; nessa perspectiva, a pesquisa *Global Economic Crime and Fraud Survey,* realizada em 2018, pela empresa de consultoria PwC, aponta que metade das empresas brasileiras foram vítimas de crimes econômicos nos últimos dois anos. Dessa forma, a presente pesquisa obteve média (3,30) considerada baixa em relação às demais médias, mas relacionada com o resultado encontrado na pesquisa demonstrada. Para maior quantificação de dados, pode ser verificado, conforme a figura 10, em anexo, que 10 respondentes (43,48%) classificaram que as organizações na qual trabalham já foram vítimas de fraudes.

Em relação à questão de número 7, foi questionada em que proporção se considera que a organização na qual trabalham tem realizado medidas para evitar fraudes. Nesse contexto, Sêmola (2014) demonstra que é essencial a realização de medidas de segurança para a proteção da informação e seus ativos. Na situação analisada, a média apresentada (4,30) foi a mais alta desta pesquisa, considerando que as organizações realizam medidas de segurança. Porém, como as perguntas foram destinadas a diversos setores, procurou-se identificar como se tratou a percepção em relação a essas medidas em cada setor, isso é representado na figura 8.

Figura 8 – Relação da pergunta questão 7 com o setor

Fonte: *Qlik Sense*/Elaborado pelo autor.

O que pode ser compreendido, relacionando-se os dados, é que o setor de informática classificou em média (4,75), como alta a percepção sobre a organização estar realizando medidas para evitar fraudes, ante os setores de administração e comunicação que classificaram como a média (4,00), porém próxima à média representada pelo setor financeiro (4,17). Isso demonstra que os departamentos, pelo nível de conhecimento e outros fatores, podem ter diferentes percepções e, em vista disso, é importante realizar uma pesquisa abrangente com diferentes departamentos.

4.4 Avaliação sobre suporte da alta administração

Conforme mencionado no referencial teórico relativo à etapa 1, de comprometimento e suporte da alta administração, o resultado eficaz de uma organização em sua segurança de informação depende de uma gestão corporativa eficaz em governança de TI. Dessa forma, foram realizadas 3 perguntas referentes ao assunto, em que foi questionado sobre o grau de envolvimento da gerência em relação a gestão de segurança da informação. A escala de medida do tipo *Likert* foi adotada, de 5 pontos, variando de (1) discordo totalmente a (5) concordo totalmente. As perguntas, bem como as médias, podem ser verificadas no quadro 3, assim, a escala das respostas em gráfico pode ser demonstrada na figura 11.

Quadro 3 - Perguntas de 24 a 26

Perguntas	Média
24. Em que medida a alta administração já delimitou objetivos a serem seguidos quanto à Gestão de Segurança da Informação.	**3,61**
25. Em que medida a direção ou responsável certifica-se para que recursos destinados à segurança da informação estejam disponíveis.	**3,87**
26. Em que medida foram planejadas ações para lidar com possíveis riscos associados à segurança da informação.	**3,96**

Fonte: Elaborado pelo autor.

De acordo com pergunta de número 24, foi questionada em que medida a alta administração já delimitou objetivos a serem seguidos quanto à gestão de segurança da informação. Nesse sentido, conforme mencionado por Galegale *et al.* (2017), o assunto de segurança da informação é tratado na alta administração das organizações. Deste modo, foi verificado que a média nesta questão (3,61), é consideravelmente baixa em relação às demais médias, logo, é importante ressaltar que a alta administração deve conhecer e delimitar os objetivos a serem seguidos.

Conforme a questão de número 25, questionou-se de que forma a direção ou o responsável certifica-se de que os recursos destinados à segurança da informação estejam disponíveis. Nessa situação, Davenport *et al.* (2004), definem que os investimentos em TI não demonstram retornos efetivos, na medida que o usuário não aprende a utilizar a tecnologia, por isso, primeiramente é importante conhecer como as pessoas processam e adquirem as informações. Assim, conforme a média apresentada (3,87), representa uma média de certa forma alta em relação às demais médias, demonstrando que o nível estratégico destina os recursos necessários, mas isso não indica que necessariamente conhecem o assunto.

Em relação à questão de número 26, foi questionada de que forma são planejadas ações para lidar com possíveis riscos associados à segurança de informação, dessa forma, Fontes (2015) acredita que a diminuição de riscos informacionais é o objetivo principal da segurança da informação, pois os riscos afetam diretamente os negócios. Nesse contexto, de acordo com a média apresentada (3,96), apesar de ser a maior da seção, o ideal é que se obtivesse nota máxima em

todas as organizações, pois as medidas de segurança são essenciais para qualquer negócio.

4.5 Avaliação sobre uso aceitável das políticas

De acordo com o descrito no referencial teórico, referente à etapa 2, sobre o uso aceitável das políticas de segurança da informação, uma política de segurança eficaz serve para definir diretrizes e modelos a serem seguidos, que possibilitam um ganho para a organização nos sentidos de produção, de fluxo de receita e de segurança. Assim, conforme o tema é amplo, foram realizadas 6 perguntas. A escala de medida do tipo *Likert* foi adotada, de 5 pontos, variando de (1) discordo totalmente a (5) concordo totalmente. As perguntas, bem como as médias, podem ser verificadas no quadro 4, assim, a escala das respostas em gráfico pode ser demonstrada na figura 12.

Quadro 4 - Perguntas de 12 a 17

Perguntas	**Média**
12. Em que medida **existe uma política** de segurança da informação na sua organização?	**3,87**
13. Em que medida você acha que a política de segurança da informação da sua organização **foi divulgada** adequadamente?	**3,22**
14. Em que medida a unidade **comunica sobre a importância da segurança** da informação aos servidores.	**3,65**
15. Em que medida **a unidade tem definidas as responsabilidades** de cada usuário especificando ações aceitáveis e inaceitáveis.	**3,78**
16. Em que medida a unidade **tem definidas as consequências** do não cumprimento das normas.	**3,52**
17. Em que medida **você já assinou** o termo de compromisso na organização em que trabalha.	**4,17**

Fonte: Elaborado pelo autor.

Conforme a pergunta de número 12, foi questionada em que medida existe uma política de segurança da informação na organização. Assim, de acordo com Sêmola (2014), uma PSI é essencial para o funcionamento das organizações, demonstrando tamanha importância conforme relaciona que a política está para a empresa assim como a Constituição Federal está para um País. Conforme a média apresentada

(3,87) pode-se concluir que algumas organizações pesquisadas ainda não possuem uma política de segurança da informação, sendo considerada uma medida inaceitável.

De acordo com a pergunta de número 13, foi questionada em que proporção a política de segurança da informação das organizações foi divulgada adequadamente, assim, é extremamente importante que uma política existente seja divulga de maneira adequada para os colaboradores. Conforme a média apresentada (3,22), o que corresponde a menor desta seção, reflete que há um grave desinteresse ou desconhecimento na divulgação da política por parte da alta administração, contribuindo para a conclusão de Turban e Volonino (2013), que além dos funcionários, os gestores também correspondem aos maiores riscos em segurança da informação.

Em relação à questão de número 14, foi questionada em que escala a organização comunica sobre a importância da segurança da informação aos servidores. Nesse caso, Fontes (2015) acredita que a segurança da informação é uma forma de garantir a continuidade do negócio. Assim, a média apresentada (3,65) pode ser considerada baixa neste assunto de grande importância, demonstrando que o nível estratégico novamente deixa a desejar.

Referente às questões de números 15 e 16, foram questionadas em que medidas a unidade tem definidas as responsabilidades dos usuários sobre ações aceitáveis e inaceitáveis e as consequências do não cumprimento das normas. Nesse sentido, as questões trataram de definições que constam na política de uso aceitável (PUA), na qual Turban e Volonino (2013) a denominam sendo essencial para eficácia da segurança em TI, pois delimita as responsabilidades e consequências, além das ações aceitáveis e inaceitáveis. As médias das questões, respectivamente, (3,78 e 3,52), demonstram que podem ser melhoradas, principalmente no que tange às consequências, sendo importante mencionar que os atos praticados no mundo virtual geram consequências no mundo real.

De acordo com a questão de número 17, foi questionada em que medida o usuário já assinou o termo de compromisso na organização em que trabalha, nesse sentido, no termo de compromisso é adequado que contenham políticas de informação, abrangendo e praticando o que foi apresentado neste estudo. Assim, apesar de ser a maior média da seção (4,17), somente assiná-lo não quer dizer que o

usuário conheça sobre o assunto, além disso, ele precisa ser treinado e constantemente monitorado.

4.6 Avaliação sobre procedimentos de segurança

Após a etapa da política de segurança, chega o momento sobre os procedimentos de segurança e de fiscalização em TI, as orientações, normas e controle, conforme demonstrado no referencial teórico. Assim, Sêmola (2014) valida que é necessário desenvolver uma cultura de segurança para diminuição dos riscos. A partir do proposto, foram realizadas 6 perguntas, que abordaram, além de procedimentos de segurança, os princípios fundamentais de segurança da informação. A escala de medida do tipo *Likert* foi adotada, de 5 pontos, variando de (1) discordo totalmente a (5) concordo totalmente. As perguntas, bem como as médias, podem ser verificadas no quadro 5, assim, a escala das respostas em gráfico pode ser demonstrada na figura 13.

Quadro 5 - Perguntas de 18 a 23

Perguntas	**Média**
18. Em que medida são fornecidas orientações para que a **informação** esteja **disponível** para acesso somente àqueles que **tenham direito**.	**4,04**
19. Em que medida são fornecidas orientações para **proteger** as informações de maneira **íntegra**, garantindo que ela não sofra qualquer modificação desde a sua origem.	**3,78**
20. Em que medida são fornecidas orientações para manter as informações acadêmico-administrativas em **sigilo**.	**4,04**
21. Em que medida existem normas quanto à **definição e sigilo de senha**.	**4,09**
22. Em que medida você conhece **a política e as normas de sua organização em relação à privacidade** dos funcionários, dos prestadores de serviço e dos clientes?	**3,65**
23. Em que medida há controle para que ninguém utilize os recursos para fins pessoais.	**3,30**

Fonte: Elaborado pelo autor.

Conforme a questão de número 18, foi questionada em que medida são fornecidas orientações referentes à disponibilidade, assim, o princípio da disponibilidade, de acordo com Sêmola (2014), demonstra que a informação deva

estar acessível somente àqueles que tenham direito. Dessa forma, conforme a média apresentada (4,08), foi considerada coerente nesta pesquisa, apesar de que poderia ser maior no sentido de que isso reflete um princípio fundamental de segurança da informação.

Em relação à pergunta de número 19, foi questionada sobre outro princípio fundamental de segurança da informação, o princípio da integridade, no qual Sêmola (2014) esclarece que o conteúdo das informações seja preservado de maneira íntegra e não alterado indevidamente. Nessa questão, de acordo com a média apresentada (3,78), reflete que tal conceito não é devidamente difundido nas organizações pesquisadas, podendo-se concluir que não são fornecidas orientações necessárias para proteger as informações de maneira íntegra.

De acordo com a questão de número 20, foi questionado em que nível é fornecido orientações para manter as informações em sigilo, o que correspondente ao princípio da confidencialidade, no qual Sêmola (2014) define que todas as informações devam ser mantidas conforme o grau de sigilo necessário e acessadas somente àqueles que tenham direito. Dessa forma, conforme a média apresentada (4,04), acredita-se que são fornecidas, em grande parte das organizações, orientações para manter as informações acadêmico-administrativas em sigilo.

Conforme a questão de número 21, foi questionada em que medida existem normas para definição e sigilo de senha e, nesse sentido, Silva e Stein (2007) demonstram que a complexidade quanto à definição de senhas esbarra nas capacidades cognitivas dos usuários, deste modo, reforçam o ponto crucial neste estudo, de que o usuário é o elo mais fraco da segurança. Assim, conforme a média apresentada (4,09), representando a maior média da seção, demonstra que normas para definição e sigilo de senha são conhecidas e praticadas.

Em relação à questão de número 22, questionou-se em que medida são conhecidas as políticas e as normas da organização em relação à privacidade dos funcionários, prestadores de serviço e clientes. Por conseguinte, de acordo com a média apresentada (3,65), pode-se concluir que os respondentes conhecem as políticas e as normas em relação à privacidade, mas não de modo completo.

De acordo com a questão de número 23, foi questionado qual o nível de controle para que ninguém utilize os recursos para fins pessoais, por exemplo, usar o

telefone, a impressora, o e-mail corporativo e, nesse sentido, estas restrições devem constar na política empresarial, conforme apresentam Turban e Volonino (2013), as ações aceitáveis e inaceitáveis. Assim, conforme a média apresentada (3,30), correspondente a menor do setor, conclui-se que há falha nas empresas analisadas, pois não existe monitoramento dos usuários para garantir que não utilizem recursos para fins pessoais, representando riscos ao negócio.

4.7 Avaliação sobre ferramentas de segurança

Conforme o demonstrado no referencial teórico, referente a etapa 4 sobre ferramentas de segurança, que correspondem a hardwares e softwares, é explicitado, conforme Turban e Volonino (2013), de que as ferramentas de segurança são indispensáveis para fiscalizar e apoiar as políticas. Assim, foram realizadas 4 perguntas relacionadas a essa avaliação, e estas fazem referência às políticas de hardwares e softwares das organizações. A escala de medida do tipo *Likert* foi adotada, de 5 pontos, variando de (1) discordo totalmente a (5) concordo totalmente. As perguntas, bem como as médias, podem ser verificadas no quadro 6, assim, a escala das respostas em gráfico pode ser demonstrada na figura 14.

Quadro 6 - Perguntas de 8 a 11

Perguntas	**Média**
8. Em que medida existem ferramentas que impedem o recebimento/acesso a conteúdo externo ou de fontes desconhecidas.	**4,13**
9. Em que medida há bloqueios impedindo alterações de hardware e software.	**4,30**
10. Em que medida existe um **padrão** de segurança para uso de dispositivos conectados ao computador (Pendrive, CDs, Celulares, etc).	**3,70**
11. Em que medida as ferramentas de segurança estão em constante **atualização**.	**4,00**

Fonte: Elaborado pelo autor.

Esta seção correspondeu ao somatório de médias com as maiores notas, justamente porque é de conhecimento geral que a segurança da informação corresponde meramente a ferramentas de segurança, como softwares e hardwares,

quando, na verdade, refere-se a todo um modelo de segurança empresarial no qual foi demonstrado neste estudo.

Conforme a pergunta de número 8, foi questionada em que medida existem ferramentas que impedem o recebimento/acesso de conteúdo externo ou fontes desconhecidas; nesse contexto, Turban e Volonino (2013) demonstram que as ferramentas são indispensáveis para apoiar as práticas seguras. Assim, conforme a média apresentada (4,13), que foi considerada alta em relação às demais médias, infere-se que existem ferramentas desse tipo nas organizações.

Em relação à pergunta de número 9, foi questionada em que medida existem bloqueios impedindo alterações de hardware e software, e, nesse sentido, é essencial que a gestão corporativa bloqueie tais alterações para a realização de medidas de segurança. Assim, conforme a média apresentada (4,30), é válido dizer que há medidas impedindo alterações nas ferramentas das organizações pesquisadas.

De acordo com a questão de número 10, foi questionada em que medida existe um padrão de segurança para uso de dispositivos conectados ao computador. Nessa circunstância, tal padrão pode estar mencionado na política de uso aceitável (PUA). Por isso, a média apontada (3,70), não configurou uma média alta em relação às outras desta seção, demonstrando ser um aspecto vulnerável, pois muitas organizações não possuem restrições quanto a equipamentos conectados ao computador.

Em relação à questão de número 11, foi questionada em que medida as ferramentas de segurança estão em constante atualização; nesta perspectiva, em um contexto de constante avanço tecnológico, as ferramentas devem sempre estar atualizadas. Assim, conforme a média apresentada (4,00), pode-se concluir que as ferramentas estão em constante atualização e representam um fato que deve existir também com as políticas de segurança das organizações.

5 CONSIDERAÇÕES FINAIS

De forma ampla, este trabalho procurou analisar como estão sendo realizadas as gestões de segurança da informação nas empresas nacionais de serviços financeiros. Nesse aspecto, foi apresentado o modelo de segurança em TI proposto por Turban e Volonino (2013), que contém quatro etapas (comprometimento da alta administração, uso aceitável das políticas, procedimentos de segurança e ferramentas de segurança). Para fortalecer o estudo referente ao modelo proposto, foram analisados mais dois tópicos específicos (o fator humano e as fraudes), pois são variáveis presentes e importantes no contexto empresarial.

Dessa forma, realizou-se uma pesquisa do tipo *survey,* por meio de questionário, para compreender e avaliar as etapas do modelo e os tópicos específicos. Foram realizadas 26 perguntas subdivididas em sete tópicos (perfil dos respondentes, percepção quanto ao fator humano e às fraudes, avaliação sobre a alta administração, políticas de segurança, procedimentos e ferramentas), respondidas por 23 funcionários do setor de serviços financeiros (fundo de investimento, corretora de ações, banco de varejo e de investimentos, cooperativa de crédito, companhia de cartões de crédito e consultoria financeira). De modo geral, nos resultados compreendeu-se que:

Os usuários representam o chamado elo mais fraco da empresa, pois não seguem corretamente as recomendações da área responsável pela segurança da informação.

Quase metade das empresas brasileiras de serviços financeiros já foram vítimas de fraudes. Porém, o nível de percepção quanto às medidas de proteção é distinto entre os departamentos das organizações (administração, comunicação, financeiro, informática).

A alta administração destina recursos necessários para a segurança da informação, mas não necessariamente delimita objetivos a serem seguidos, pois desconhece o assunto.

Parte dos funcionários desconhecem as políticas de segurança da informação de sua organização, por desinteresse ou desconhecimento, neste sentido, há falha na divulgação das políticas por parte da alta administração, demonstrando que os gestores também representam um risco iminente.

As organizações seguem os princípios básicos de segurança da informação, porém, os usuários não conhecem as políticas e as normas de modo completo, nem são monitorados para garantir que não utilizem recursos para fins pessoais, representando riscos ao negócio.

As ferramentas de segurança existem e acredita-se que uma segurança eficaz se refere somente à aplicação de ferramentas como software e hardware, no entanto, o fator humano é mais importante que a adoção de ferramentas de segurança e que estas fazem parte da última etapa a se pensar.

Nesse contexto, as organizações de serviços financeiros devem compreender que as fraudes, crimes e violações são amplamente presentes no mundo atual. Assim sendo, este trabalho demonstra a importância de que medidas para segurança da informação são necessárias para vitalidade empresarial, servindo de base para possíveis autoavaliações e diagnósticos, além de conhecimentos para estruturação da área de segurança em tecnologia da informação.

Os objetivos, de certa forma, foram cumpridos e demonstraram resultados equivalentes aos estudos e trabalhos científicos que existem referente ao assunto de segurança da informação. No entanto, a população amostrada foi limitada a empresas de serviços financeiros, que são as mais afetadas por crimes cibernéticos e as mais comprometidas com a segurança, mesmo assim, os resultados nos índices foram elevados. Outro limite refere-se ao tamanho da amostra de respondentes, devido às diversas barreiras existentes no setor, ao assunto proposto e ao público pretendido.

Novos estudos poderiam abordar organizações de diversos ramos, que não somente empresas financeiras, possibilitando que seja alcançado um número maior de respondentes. Nesse sentido, se os resultados se mostraram assustadores com empresas financeiras, o que se pode imaginar de outros ramos de negócio que não possuem a mesma preocupação com o assunto estudado.

REFERÊNCIAS

BEAL, Adriana. **Gestão estratégica da informação:** como transformar a informação e a tecnologia da informação em fatores de crescimento e alto desempenho nas organizações. 3. ed. São Paulo: Atlas, 2008. 137 p.

Cost of Cyber Crime Study 2018. **Accenture e Ponemon Institute**. Disponível em: <https://www.accenture.com/br-pt/company-news-release-crimes-virtuais> Acesso em 04. Set. 2018.

DAVENPORT, Thomas H. Marchand, Donald A. Dickson, Tim. **Dominando a gestão da informação**. Porto Alegre: Bookman, 2004. 407p.

FERREIRA, M. R.; DOLCI, D. B.; TONDOLO, V. A. G. **Uma Proposta de Diagnóstico e Autoavaliação da Gestão da Segurança da Informação**. In: XL Encontro da ANPAD, 2016, Costa do Sauípe - BA. EnANPAD 2016.

FONTES, Edison. **Segurança da Informação: o usuário faz a diferença.** São Paulo: Saraiva, 2015. 172 p.

FREITAS, H.; OLIVEIRA, M.; SACCOL, A. Z.; MOSCAROLA, J**.** O método de pesquisa survey. **Revista de Administração**, v. 35, n. 3, p. 105-112, 2000.

GALEGALE, Napoleão Verardi; FONTES, Edison Luiz Gonçalves; GALEGALE, Bernardo Perri. Uma contribuição para a segurança da informação: um estudo de casos múltiplos com organizações brasileiras. **Perspectivas em Ciência da Informação**, [S.l.], v. 22, n. 3, p. 75-97, set. 2017. ISSN 19815344. Disponível em:

<http://portaldeperiodicos.eci.ufmg.br/index.php/pci/article/view/2866/1957>. Acesso em: 6 jun. 2018.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa.** 5 ed. São Paulo: Atlas, 2010. 184 p.

Global Economic Crime and Fraud Survey 2018. **PwC**. Disponível em: < https://www.pwc.com/gx/en/services/advisory/forensics/economic-crime-survey.html> Acesso em: 10 mai. 2018.

Índice de Maturidade de Segurança na Infraestrutura Corporativa de TI. **Level 3 Communications**. Disponível em: <http://www.level3.com/SecurityIndex> Acesso em: 10 mai. 2018.

MANDARINO JUNIOR, Raphael. **Segurança e defesa do espaço cibernético brasileiro**. Recife: Cubzac, 2010. 182 p.

Norton Cyber Security Insights Report 2017. **Norton by Symantec**. Disponível em: <https://us.norton.com/cyber-security-insights-2017> Acesso em: 10 mai. 2018.

O'BRIEN, James. A. **Sistemas de informação e as decisões gerenciais na era da internet.** 3. ed. São Paulo: Saraiva, 2009. 431 p.

PEROTTONI, R.; OLIVEIRA, M.; LUCIANO, E. M.; FREITAS, H. Sistemas de Informações: um Estudo Comparativo das Características Tradicionais às Atuais. Porto Alere/RS: **Revista REAd,** v.7, n.3, Junho de 2001.

RAINER JUNIOR, R. Kelly; CEGIELSKI, Casey G. **Introdução a sistemas de informação**: apoiando e transformando negócios na era da mobilidade 3ed. Rio de Janeiro: Elsevier, 2012.

Segurança da Informação: Segurança da Informação e Comunicações. **Portal do Sisp.** <http://www.sisp.gov.br/faq_segurancainformacao/one-faq?faq_id=13941646> Acesso em: 05 jun. 2018.

SÊMOLA, Marcos. **Gestão da segurança da informação**: uma visão executiva. 2ed. Rio de Janeiro: Elsevier, 2014. 156 p.

SILVA, D. R. P.; STEIN, L. M. Segurança da Informação: uma reflexão sobre o componente humano. **Ciências & Cognição**. v.10, p.46-53, mar. 2007.

STAIR, Ralph M. e REYNOLDS George W. **Princípios de Sistemas de Informação.** 3. ed. São Paulo: Cengage Learning, 2016. 719 p.

TURBAN, E. VOLONINO, L. **Tecnologia da Informação para Gestão**: Em busca do melhor desempenho Estratégico e Operacional. 8ed. Porto Alegre: Bookman, 2013. 721 p.

APÊNDICE A – QUESTIONÁRIO APLICADO

Qual a sua faixa etária?

( ) Entre 16 e 25 anos; ( ) Entre 26 e 33 anos; ( ) Entre 34 e 41 anos; ( ) Acima de 42 anos.

Qual a sua escolaridade?

( ) Ensino Médio Completo; ( ) Ensino Superior Incompleto; ( ) Ensino Superior Completo; ( ) Pós-graduação; ( ) Mestrado; ( ) Doutorado.

Sexo

( ) Masculino; ( ) Feminino; ( ) Prefiro não responder

Há quanto tempo você atua em instituições financeiras?

( ) Até 2 anos; ( ) Entre 2 e 5 anos; ( ) Entre 5 e 10 anos; ( ) Entre 10 e 15 anos;

( ) Acima de 15 anos;

Qual o seu atual cargo?

( ) Estagiário; ( ) Auxiliar/Assistente; ( ) Analista; ( ) Supervisão/Coordenação; ( ) Gerência; ( ) Diretoria/Presidência;

Em qual departamento você atua?

( ) Departamento Administrativo; ( ) Departamento Financeiro; ( ) Departamento de Informática; ( ) Departamento de Comunicação; ( ) Outro, qual?

Você trabalha em qual tipo de instituição financeira?

( ) Privada; ( ) Pública.

Quantos funcionários a empresa em que você trabalha possui?

( ) Até 9 empregados; ( ) De 10 a 49 empregados; ( ) De 50 a 99 empregados;

( ) Mais de 100 empregados.

Qual o ramo da empresa em que você atua?

( ) Cooperativa de crédito; ( ) Banco de varejo e de investimento; ( ) Companhia de cartões de crédito; ( ) Companhia de seguros; ( ) Corretora de ações; ( ) Fundo de investimento; ( ) Outro, qual?

Em qual cidade localiza-se a sua empresa?

( ) Porto Alegre; ( ) Rio de Janeiro; ( ) São Paulo; ( ) Outro, qual?

Etapa das perguntas sobre o modelo de segurança em TI

Os itens de preenchimento foram operacionalizados conforme a escala *Likert,* de 5 pontos, variando de (1) discordo totalmente a (5) concordo totalmente.

A) Perguntas sobre o usuário

1. Em que medida você consegue comunicar ao setor de TI qualquer ocorrência ou suspeita que comprometa a segurança da informação na organização financeira em que você atua?
2. Em que medida você considera que o usuário é fator essencial no combate aos crimes cibernéticos?
3. Em que medida você acredita que são monitorados os acessos realizados pelos usuários (e-mail, sites, sistemas corporativos)?

4. Em que medida você considera que os funcionários seguem corretamente as recomendações da área de segurança da informação?

B) Perguntas sobre fraudes

5. Em que medida você conhece alguém que já foi vítima de fraude realizada por meio do ambiente computacional.
6. Em que medida a organização na qual você trabalha já foi vítima de fraudes.
7. Em que medida você considera que a sua organização tem realizado medidas para evitar as fraudes.

C) Perguntas sobre ferramentas de segurança

8. Em que medida existem ferramentas que impedem o recebimento/acesso a conteúdo externo ou de fontes desconhecidas.
9. Em que medida há bloqueios impedindo alterações de hardware e software.
10. Em que medida existe um padrão de segurança para uso de dispositivos conectados ao computador (Pendrive, CDs, Celulares, etc).
11. Em que medida as ferramentas de segurança estão em constante atualização.

D) Perguntas sobre uso aceitável das políticas

12. Em que medida existe uma política de segurança da informação na sua organização?
13. Em que medida você acha que a política de segurança da informação da sua organização foi divulgada adequadamente?
14. Em que medida a unidade comunica sobre a importância da segurança da informação aos servidores.
15. Em que medida a unidade tem definidas as responsabilidades de cada usuário especificando ações aceitáveis e inaceitáveis.
16. Em que medida a unidade tem definidas as consequências do não cumprimento das normas.

17. Em que medida você já assinou o termo de compromisso na organização em que trabalha.

E) Perguntas sobre procedimentos: orientação, normas e controle

18. Em que medida são fornecidas orientações para que a informação esteja disponível para acesso somente àqueles que tenham direito.
19. Em que medida são fornecidas orientações para proteger as informações de maneira íntegra, garantindo que ela não sofra qualquer modificação desde a sua origem.
20. Em que medida são fornecidas orientações para manter as informações acadêmico-administrativas em sigilo.
21. Em que medida existem normas quanto à definição e sigilo de senha.
22. Em que medida você conhece a política e as normas de sua organização em relação à privacidade dos funcionários, dos prestadores de serviço e dos clientes?
23. Em que medida há controle para que ninguém utilize os recursos para fins pessoais.

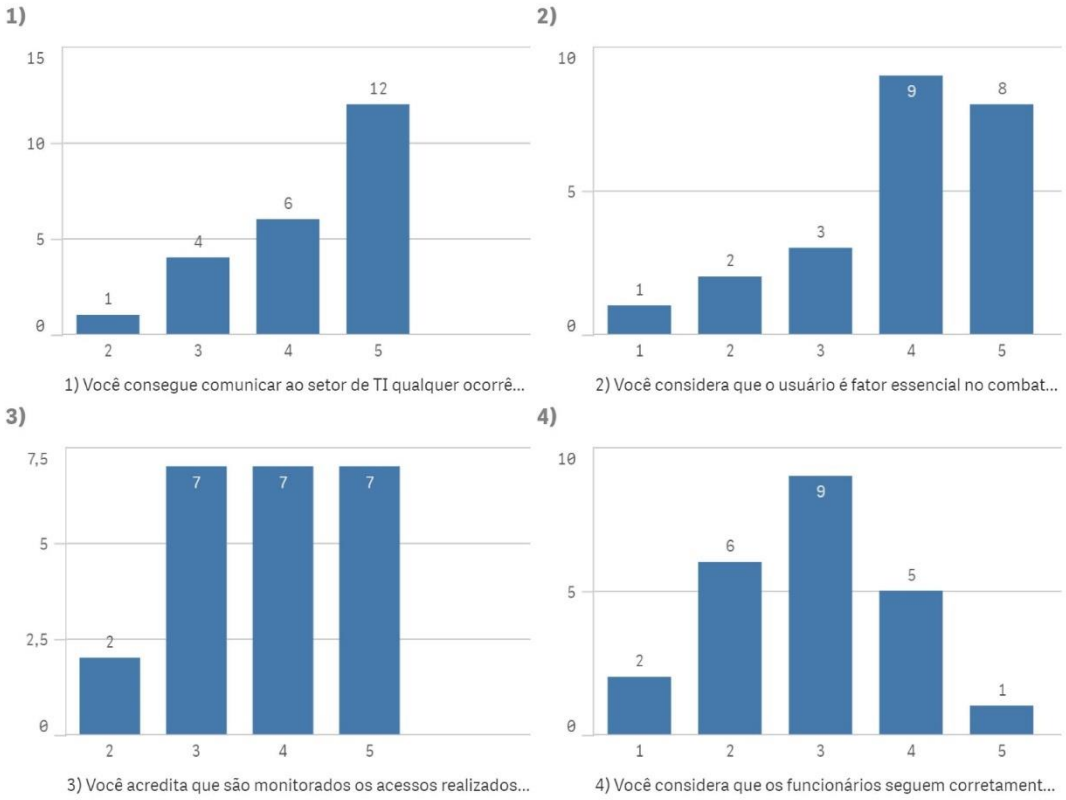
F) Perguntas sobre suporte da alta administração

24. Em que medida a alta administração já delimitou objetivos a serem seguidos quanto à Gestão de Segurança da Informação.
25. Em que medida a direção ou responsável certifica-se para que recursos destinados à segurança da informação estejam disponíveis.
26. Em que medida foram planejadas ações para lidar com possíveis riscos associados à segurança da informação.

ANEXO A – GRÁFICO DAS ANÁLISES DOS RESULTADOS

A) Percepção quanto ao fator Humano

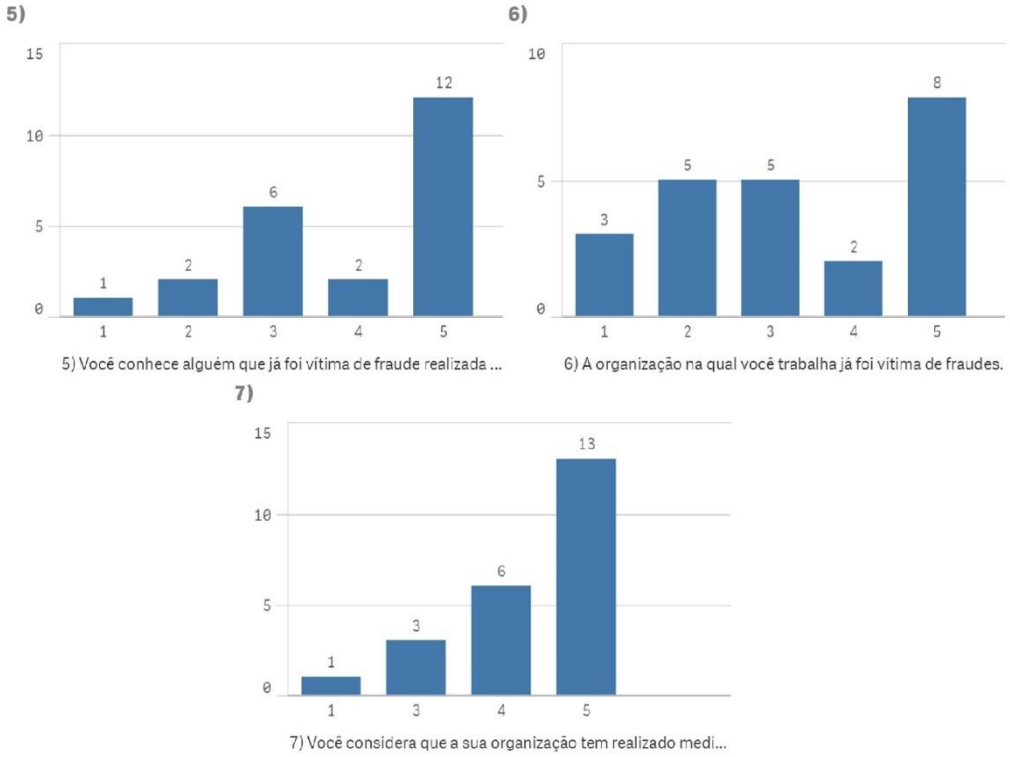
Figura 9 – Gráficos das perguntas 1 a 4



Fonte: *Qlik Sense*/Elaborado pelo autor.

B) Percepções quanto às fraudes

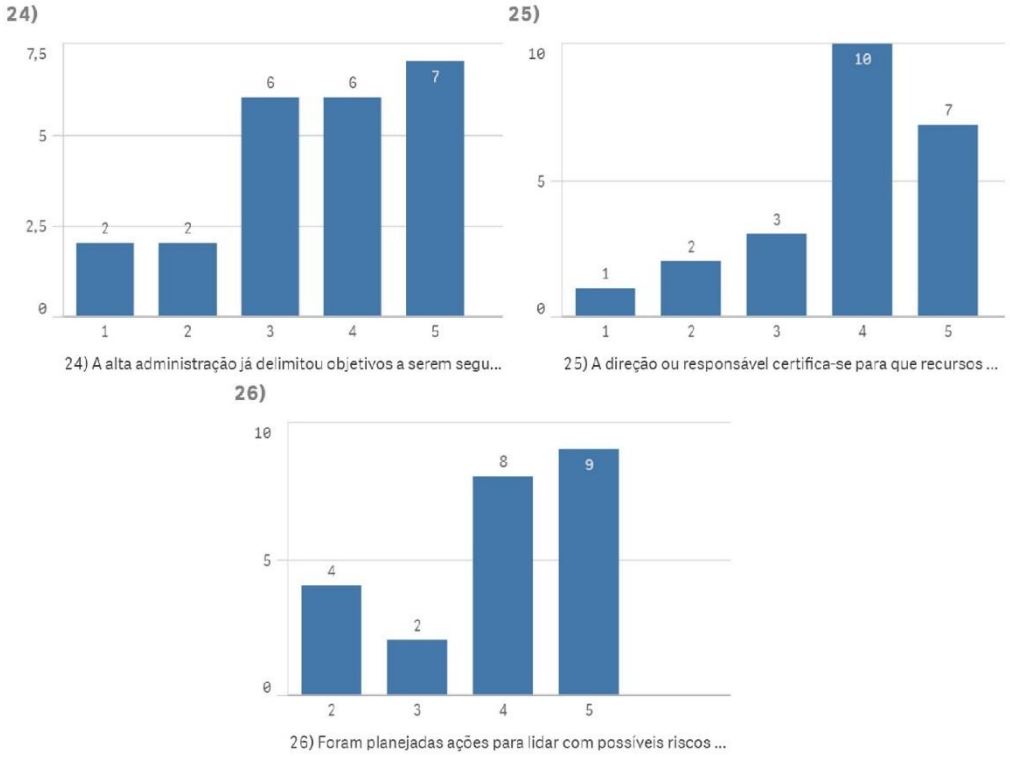
Figura 10 – Gráficos das perguntas 5 a 7



Fonte *Qlik Sense*/Elaborado pelo autor.

C) Avaliação sobre suporte da alta administração

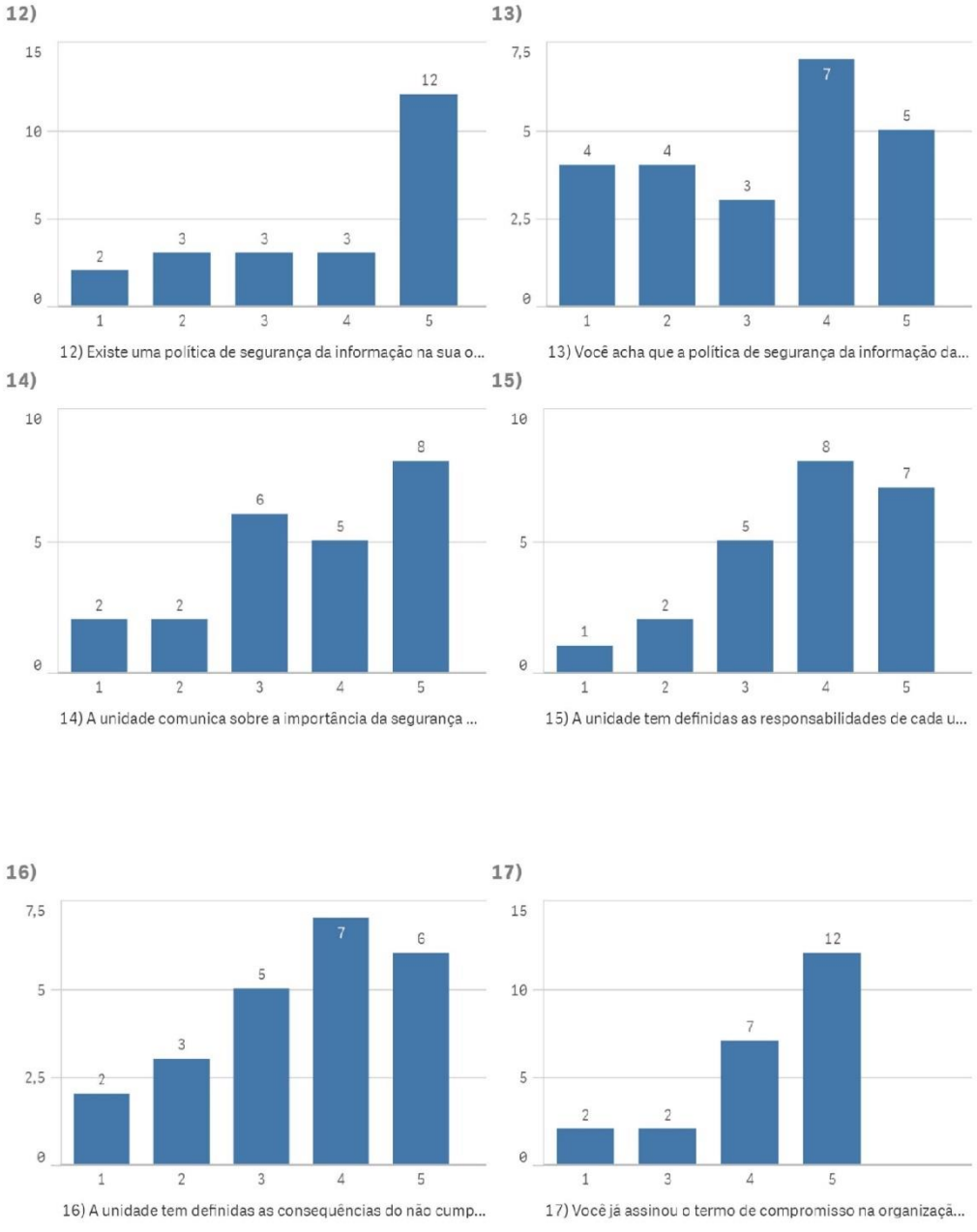
Figura 11 – Gráficos das perguntas 24 a 26



Fonte: *Qlik Sense*/Elaborado pelo autor.

D) Avaliação sobre uso aceitável das políticas

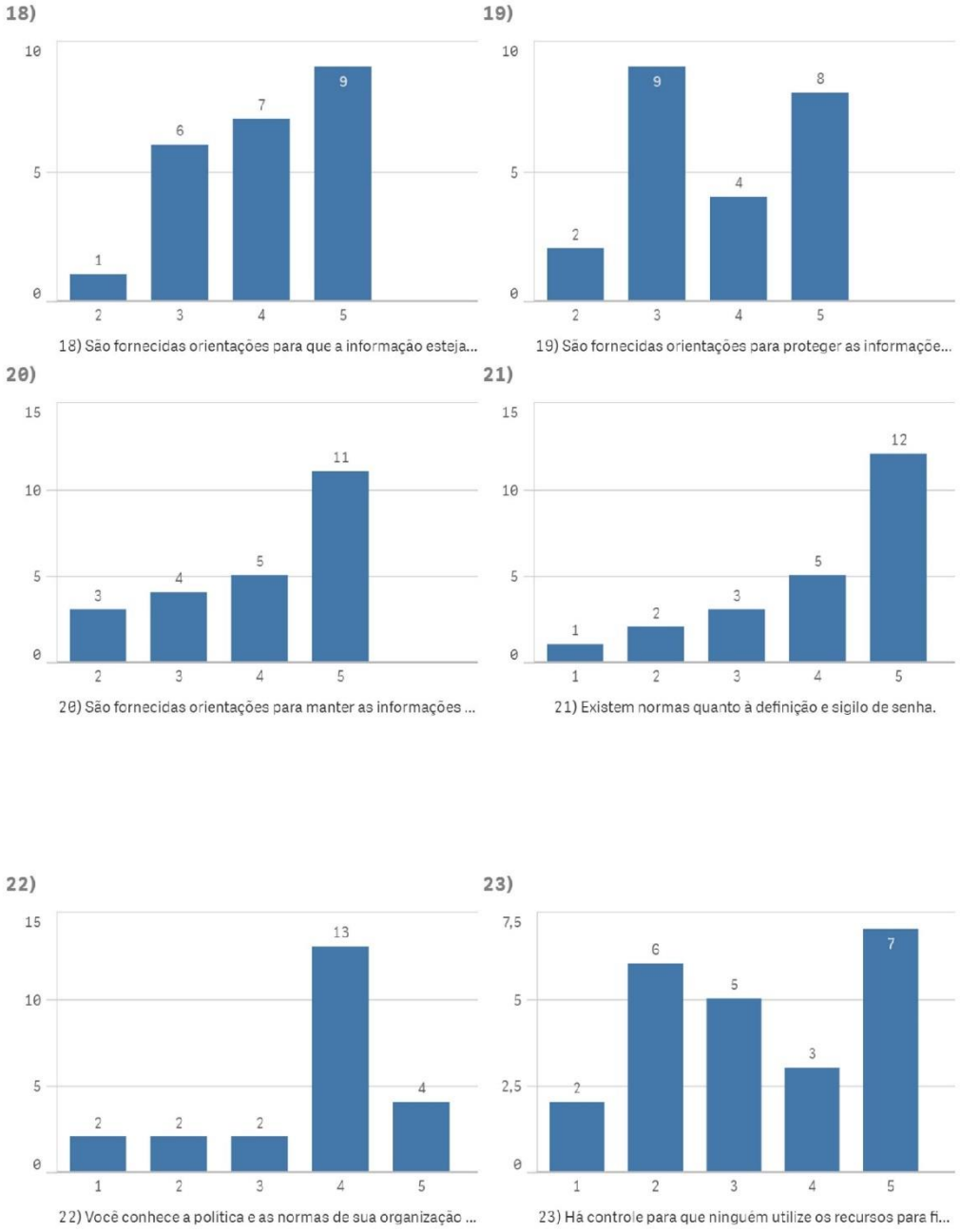
Figura 12 – Gráficos das perguntas 12 a 17



Fonte: *Qlik Sense*/Elaborado pelo autor.

E) Avaliação sobre procedimentos de segurança

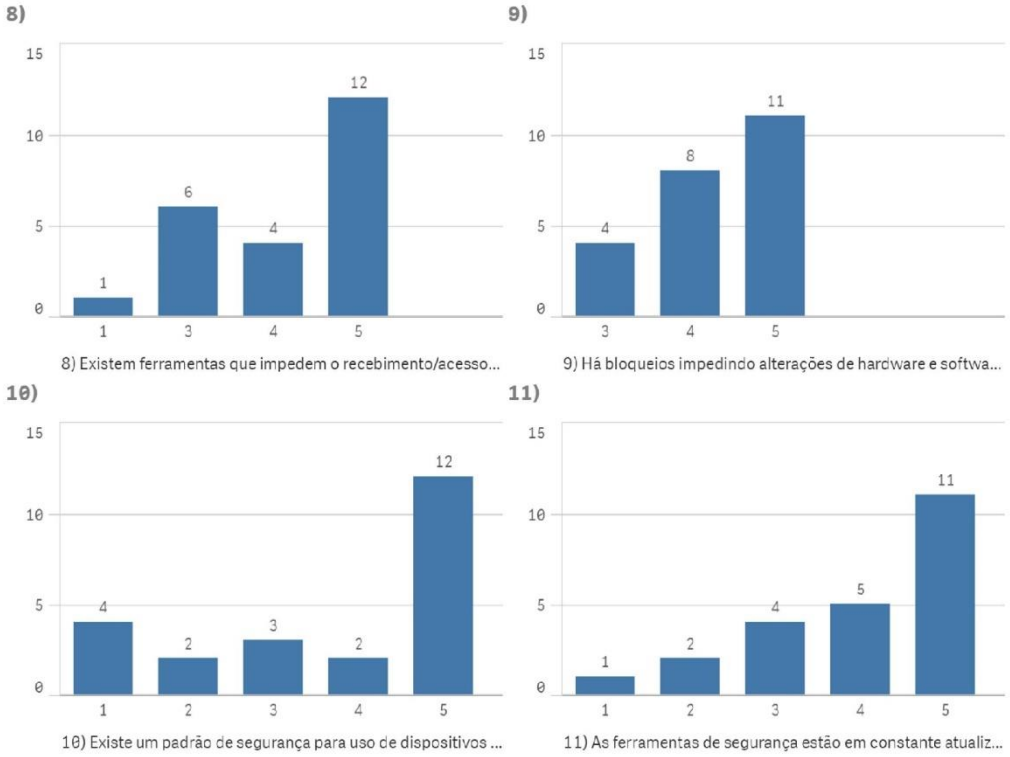
Figura 13 – Gráficos das perguntas 18 a 23



Fonte: *Qlik Sense*/Elaborado pelo autor.

F) Avaliação sobre ferramentas de segurança

Figura 14 – Gráficos das perguntas 8 a 11



Fonte: *Qlik Sense*/Elaborado pelo autor.