# SEGURANÇA DA INFORMAÇÃO: UM ESTUDO SOBRE O PROCESSO DE SEGURANÇA DA INFORMAÇÃO EM INSTITUIÇÕES FINANCEIRAS LOCALIZADAS NA REGIÃO CENTRO-OESTE DE MINAS GERAIS

**Nayara Santos Andrade[1], Maria Helena Silva Rabelo[1,2]**

*[1] Departamento de Administração, Faculdade de Filosofia Ciências e Letras do Alto São Francisco. Avenida Laerton Paulinelli 153, CEP 35595-000, Monsenhor Parreiras, Luz, Minas Gerais, Brasil.*
*[2] Autor correspondente. E-mail: mhrabelo@fasf.edu.br*

## RESUMO

Este trabalho teve por objetivo compreender como o processo de segurança da informação pode contribuir para aprimoramento de procedimentos e técnicas de segurança em âmbito institucional. A pesquisa realizou-se em setembro de 2016, aplicando questionários aos colaboradores e gestores de duas instituições financeiras. Sendo assim, buscou-se identificar quais as técnicas de segurança utilizadas, quais orientações são fornecidas, quais as principais ameaças e vulnerabilidades, entre outros aspectos. Os resultados obtidos foram que as instituições adotam métodos e procedimentos que visam à segurança das informações como um todo, entretanto, mesmo que forneçam meios de orientação para seus colaboradores, 50% deles afirmam possuir pouco conhecimento sobre segurança da informação no geral, mesmo que entendam e saibam o papel que exercem em relação às informações utilizadas. As principais vulnerabilidades foram a falta de conhecimento dos colaboradores e de controle de acessos, e as principais ameaças foram vazamento de informações, programas e usuários mal intencionados. Dessa forma, concluiu-se que ambas as instituições se preocupam e buscam adotar métodos que vão proteger suas informações garantindo a realização de processos de maneira segura e estão fornecendo orientação aos colaboradores visando prover o conhecimento necessário para serem efetivos no processo de segurança da informação implantado no âmbito institucional.

**Palavras-chave:**segurança da informação, ameaças, vulnerabilidades.

## ABSTRACT

The objective of this work was to understand how the information security process can contribute to the improvement of procedures and security techniques in the institutional scope. The survey was conducted in september 2016, applying questionnaires to employees and managers of two financial institutions. Thus, we sought to identify the security techniques used, which guidelines are provided, which are the main threats and vulnerabilities, among other aspects. The results obtained were that institutions adopt methods and procedures that aim at information security as a whole. However, even if they provide guidance to their employees, 50% of them claim to have little knowledge about information security in general, even if they understand and know the role they play in relation to the information used. The main vulnerabilities were lack of employee knowledge and access control, and the main threats were leaking information, programs and malicious users. Thus, it was concluded that both institutions are concerned and seek to adopt methods that will protect their information by ensuring that processes are carried out in a secure manner and are providing guidance to

employees in order to provide the knowledge necessary to be effective in the information security process implemented within the institutional framework.

**Keywords:** information security, threats, vulnerabilities.

## INTRODUÇÃO

Com um mercado altamente competitivo, a informação tornou-se um dos bens mais preciosos da organização, sendo essencial para todas as atividades desenvolvidas no meio empresarial. Dessa forma, as organizações que buscam inovação e sucesso em seus negócios, precisam ter esse elemento como aliado cuidando para o bom gerenciamento do processo de criação, armazenamento e disseminação, pois cada vez mais dependem desse recurso.

A partir disso, as tecnologias em conjunto com os sistemas de informação têm desempenhado um espaço importante dentro das organizações por meio de recursos que possibilitam a integração de atividades organizacionais, capazes de detectar e disseminar de forma adequada as informações dentro das mesmas, sendo um diferencial quando precisam ser buscadas de maneira certa, no momento certo.

Com isso, a utilização constante da tecnologia da informação caracteriza um novo perfil de usuários cada vez mais informados e conectados aos recursos disponíveis, além de que a troca de informações se tornou mais rápida. Isso trouxe grandes mudanças em termos de segurança da informação e consequentemente uma mudança de postura por parte das organizações que passaram a adotar procedimentos e mecanismos de segurança mais precisos e complexos visando suprir a necessidade crescente de proteção de informações.

Dessa forma, devido às informações representarem um fator de grande importância dentro das organizações, visto que estão sujeitas a ameaças e vulnerabilidades cada vez maiores, estas passaram a dar atenção para a gestão de riscos relativos às informações utilizadas, criando métodos como políticas e normas estabelecidas e estruturadas que sejam capazes de garantir a segurança da informação, vista agora como um processo crucial para as mesmas.

Percebe-se que há uma mudança de contexto em que as organizações estão inseridas e que as mesmas já estão se preocupando e tomando medidas conscientes pois a segurança da informação é de fato uma variável importante que deve ser levada em consideração quando se pensa na perpetuação do negócio.

Pensando nisso, a escolha das instituições analisadas neste estudo foi feita observando esse contexto envolvendo a proteção de informações em que as organizações se encontram

atualmente. Trata-se de instituições financeiras, as quais trabalham frequentemente com informações sigilosas, que podem ser consideradas como um fator crítico e sujeito a ameaças e vulnerabilidades, como o próprio vazamento de informações.

Diante do exposto, teve como objetivo compreender como o processo de segurança da informação pode contribuir para aprimoramento de procedimentos e técnicas de segurança em instituições financeiras localizadas na região Centro-Oeste de MinasGerais, no decorrer do ano de 2016, a fim de entender quais são os impactos desses processos realizados pelas instituições.

A segurança da informação torna-se ferramenta fundamental para que esse processo seja realizado de forma segura dentro da empresa, fazendo com que as possíveis invasões aos sistemas ou acesso a informações sigilosas, por exemplo, sejam evitadas. Com isso, surgiu a seguinte questionamento: como o processo de segurança da informação pode contribuir para o aprimoramento de procedimentos e técnicas de segurança em âmbito institucional?

Além disso, a pesquisa teve como objetivos específicos: verificar se existe uma política de segurança da informação adotada e de que forma é disseminada dentro da instituição; analisar o conhecimento dos colaboradores sobre os procedimentos e técnicas, adotados pela instituição, que envolvem segurança da informação e; identificar quais são as vulnerabilidades e ameaças potenciais em relação ao ambiente institucional, no que se refere à segurança da informação.

A base teórico-metodológica foi construída mediante abordagem quantitativa e qualitativa, específica a um estudo de caso. A base teórico-conceitual teve como suporte os estudos de Rezende e Abreu (2011), sobre Tecnologia da Informação, Oliveira (2011) referente a Sistemas e Informação, Machado (2014), Sêmola (2014) e Laureano (2012), sobre Segurança da Informação.

Este estudo está estruturado em 6 partes, que são: a primeira trata-se desta Introdução, a qual está sendo finalizada neste momento; a segunda compreende o Desenvolvimento, que é base conceitual deste estudo; a terceira trata-se da Metodologia, onde são apresentados os procedimentos metodológicos; a quarta trata-se dos Resultados e Discussão, que consta os resultados da aplicação dos questionários; a quinta compreende as Considerações Finais que trata do desfecho deste estudo bem como suas finalizações; a sexta trata-se da listagem de referências utilizadas no corpo deste trabalho de toda base conceitual utilizada.

## DESENVOLVIMENTO

Essa seção está dividida da seguinte forma: referencial teórico, metodologia e resultados e discussão.

## 1 REFERENCIAL TEÓRICO

### 1.1DADOS E INFORMAÇÃO

Quando o assunto é informação, inicialmente é necessário que se estabeleça a diferença existente entre dado e informação. Normalmente, o que distingue dados de informação pode-se dizer que é a capacidade de cada um em prover entendimento às pessoas que deles farão uso, ou seja, os tomadores de decisões. (OLIVEIRA, 2011).

Laudon e Laudon (2014, p. 13) definem dados como uma "sequência de fatos ainda não analisados, representativos de eventos que ocorrem nas organizações ou no ambiente físico, antes de terem sido organizados e dispostos de forma que as pessoas possam entendê-los e usá-los".

A partir disso, pode-se dizer que o dado não é capaz de fornecer base para decisões importantes em âmbito empresarial, visto que ainda não foi transformado da maneira em que será útil para a organização, ou seja, tornando-se informação. Dessa forma, dá-se a relevância de compreender o que se entende por informação (OLIVEIRA, 2011).

Para Laudon e Laudon (2014, p. 13), a informação corresponde aos "dados que foram modelados em um formato significativo e útil para os seres humanos".

Nesse contexto, pode-se dizer que os dados não viabilizam nem proporcionam elementos suficientes para a tomada de decisão empresarial e, por outro lado, a informação pode ser vista como sendo a transformação dos dados de maneira que possibilite a interpretação e utilização pelos usuários, capaz de possibilitar o entendimento de forma que seja útil e possa ser base para a tomada de decisão empresarial (OLIVEIRA, 2011).

Visto a necessidade que as organizações têm de informação e principalmente que ela seja precisa e fornecida em tempo hábil, o próximo conceito a ser tratado aborda tecnologia da informação.

### 1.2TECNOLOGIA DA INFORMAÇÃO

Cruz (1998)*apud* Rezende e Abreu (2011, p. 54) definem tecnologia da informação como "todo e qualquer dispositivo que tenha capacidade para tratar dados e ou informações,

tanto de forma sistêmica como esporádica, quer esteja aplicada ao produto, quer esteja aplicada no processo".

Os autores Laudon e Laudon (2014) e Rezende e Abreu (2011) abordam que a tecnologia da informação pode ser vista como métodos e processos tecnológicos que tem por objetivo criar e utilizar de maneira efetiva a informação. Diante disso, a tecnologia da informação está fundamentada nos seguintes componentes, que de acordo com Rezende e Abreu (2011, p. 54) são: "*hardware* e seus dispositivos e periféricos; *software* e seus recursos; sistemas de telecomunicações e gestão de dados e informações".

Para Rezende e Abreu (2011), os componentes citados se comunicam entre si e por sua vez, tem a necessidade do componente que trata as pessoas, ou seja, os usuários, que, em sua concepção, não se enquadram como parte da tecnologia da informação, entretanto, sem o fator humano a tecnologia não seria efetiva para os resultados esperados.

Albertin e Albertin (2010) abordam que as organizações utilizam a tecnologia da informação para administrar processos, buscar crescimento e interagirem com o mercado como um todo. Diante disso, de acordo com os autores, percebe-se que se encontram sujeitas a tecnologia da informação o que traz maiores riscos visto que esse recurso tem se tornado mais crítico e difícil, fazendo com que busquem formas de administrar esse fator de maneira que seus esforços envolvendo tecnologia da informação tragam os fins esperados.

Diante do exposto, Albertin e Albertin (2010) concluem que é preciso que as organizações revejam suas estratégias de maneira que estejam de acordo com os resultados buscados, visando obter destaque no mercado utilizando os recursos disponíveis da tecnologia da informação.

Com isso, ao obter o conhecimento a respeito de tecnologia da informação, seus conceitos e aplicabilidades em âmbito organizacional, faz-se necessário compreender o que se entende por sistemas de informação, apresentado na próxima seção.

## 1.3SISTEMAS DE INFORMAÇÃO

Um sistema de informação pode ser definido segundo Laudon e Laudon (2014, p. 13), como "um conjunto de componentes inter-relacionados que coletam (ou recuperam), processam, armazenam e distribuem informações destinadas a apoiar a tomada de decisões, a coordenação e o controle de uma organização".

O’Brien (2004, p. 6) define sistemas de informação como “um conjunto organizado de pessoas, *hardware*, *software*, redes de comunicações e recursos de dados que coleta, transforma e dissemina informações em uma organização”.

A partir dessas definições pode-se dizer que os sistemas de informação desempenham papel fundamental desde quando são inseridos na organização, pois alteram a forma em que os negócios são estabelecidos e gerenciados, além de trazer mudanças significativas nas atividades organizacionais (O’BRIEN, 2004).

Com isso, os sistemas de informação tornaram-se ferramentas essenciais por contribuírem para a administração da informação de forma que seja útil para a organização como um todo (LAUDON E LAUDON, 2014).

Franco, Rodrigues e Cazela (2009) afirmam que o papel que os sistemas de informação desempenham na organização é estabelecido de acordo com a necessidade da organização. É preciso estabelecer quais informações precisam ser geradas e qual será a utilização necessária nos variados processos da mesma, o que abrange os objetivos a serem alcançados bem como o ambiente em que está inserida.

Pode-se dizer que existem variadas definições sobre sistemas de informação além das que aqui foram citadas, porém todas no geral, concluem que, o foco maior é a informação e a maneira como é manipulada, transformada e repassada visando que sejam criadas informações que vão fornecer elementos suficientes para decisões e atividades organizacionais (JOÃO, 2012).

A partir desse contexto, é relevante dizer que as organizações e os sistemas de informação possuem uma grande interação. As organizações estão utilizando os sistemas de informação com o objetivo de coletar informações relevantes que vão auxiliar tanto seus colaboradores como nos mais variados processos existentes na mesma (JOÃO, 2012).

Após descrever a respeito do que é um sistema de informação e suas aplicações em âmbito organizacional, é relevante compreender o papel da segurança da informação no meio organizacional, o que será exposto na próxima seção.

## 1.4SEGURANÇA DA INFORMAÇÃO

De acordo com Fontes (2006, p. 11), a segurança da informação pode ser definida como um “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”.

A partir disso, de acordo com Laureano (2012), a segurança da informação deve ser um processo capaz de proporcionar às organizações meios eficientes para evitar possíveis riscos relacionados ao ambiente em que se encontram.

Fontes (2006) aborda que a segurança da informação visa fornecer os meios para evitar os riscos e proporcionar para as organizações a possibilidade de reduzi-los, pois cada vez mais dependem de processos que fazem uso de informações. Isso se explica, pois ao deixar de obter uma informação ou obtê-la de maneira equivocada, consequentemente traz prejuízos diretos para o negócio que faz uso da mesma.

Machado (2014) afirma que, a gestão que envolve todo o processo de segurança da informação vai além de se limitar apenas a sistemas e recursos tecnológicos. Ela abrange também a criação de normas, regras e procedimentos que visam à redução de risco, o treinamento de funcionários, que vão ser o alicerce para que as organizações sejam capazes de criar seus próprios programas de segurança da informação.

Dessa forma, Sêmola (2014) destaca que, mesmo que exista uma conscientização da organização como um todo, é preciso que as regras e normas estabelecidas através da política de segurança estejam conectadas com os processos que envolvem o ciclo de vida da informação, bem como a todos os fatores que atuam sobre esse elemento, visando fazer da segurança da informação um processo eficiente dentro da organização.

Com o que foi abordado a respeito de segurança da informação, é importante compreender o que se entende por política de segurança da informação, tratado na próxima seção.

## 1.5 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Dantas (2011, p. 133) define política de segurança como “um documento que estabelece princípios, valores, compromissos, requisitos, orientações e responsabilidades para com a segurança da informação”.

A partir disso, Silva (2012) explica que quando se fala em segurança da informação no meio organizacional, estabelecer uma política de segurança é o primeiro passo para que esse processo seja de fato efetivo. Isso se explica, pois é através dela que serão definidas quais serão as regras, normas e procedimentos visando a utilização de recursos de maneira confiável seja interna ou externamente.

Ainda de acordo com Silva (2012, p. 60), a política de segurança envolve a normatização de todos os assuntos que tratam a segurança da informação, como “uso do e-

mail corporativo, o uso da internet, classificação da informação, uso de computadores móveis, incidentes de segurança, acordos de confidencialidade" entre outros.

Machado (2014) destaca que se pode dizer que a política de segurança é projetada e constituída com o objetivo de que a tríade de segurança (integridade, confidencialidade e disponibilidade), seja mantida. Assim, de acordo com o autor, os profissionais responsáveis por gerenciar a organização vão estipular quais os fatores e princípios que vão constar nessa política, quais os objetivos a serem alcançados, quais os deveres e obrigações a serem cumpridos, entre outros.

Dessa forma, Sêmola (2014) ressalta que a política de segurança tem grande influência no âmbito organizacional, sendo o alicerce que fundamenta as atividades que envolvem a questão da segurança.

Sendo assim, o autor destaca que a política de segurança da informação pode ser dividida em três grandes grupos, que são: "diretrizes, normas, procedimentos e instruções, sendo destinados, respectivamente, às camadas estratégica, tática e operacional" dentro da organização (SÊMOLA, 2014, p. 129).

Laureano (2012) afirma que para a organização estabelecer uma política de segurança é fundamental identificar quais informações necessitam de proteção para que não sejam feitos investimentos desnecessários. Dessa forma, o autor ressalta que para facilitar esse processo de identificação é preciso classificar as informações, pois cada uma foi criada de maneira distinta o que pede monitoramento distinto.

Entretanto, Silva (2012) afirma que a política de segurança só poderá trazer os resultados esperados em âmbito organizacional quando seus principais objetivos forem entendidos, ou seja, fornecer mecanismos que permitam que as informações utilizadas estejam seguras para atender as demandas da organização. Sendo assim, é preciso que o conjunto de regras, normas, procedimentos, etc., sejam disseminados e incorporados por toda organização e não somente em um determinado setor. Entretanto, o autor ressalta que essa conscientização é um processo demorado e que exige trabalho contínuo.

Na próxima seção, serão tratados os processos e instrumentos metodológicos utilizados para a realização desta pesquisa.

## 2 METODOLOGIA

Esta seção tem como objetivo descrever os processos e instrumentos metodológicos utilizados para a realização da pesquisa sobre segurança da informação em instituições

financeiras localizadas na região Centro-Oeste de Minas Gerais. Dessa forma, esta seção seguiu a estrutura proposta por Silva e Menezes (2005) descrita a seguir: quanto à abordagem, quanto ao ponto de vista dos objetivos, quanto aos procedimentos técnicos, sujeitos da pesquisa, quanto aos instrumentos de coleta de dados e a forma de tratamento dos dados.

## 2.1 Sob o ponto de vista da abordagem

A pesquisa sob o ponto de vista da abordagem foi de caráter qualitativo e quantitativo. Sua elaboração seguiu os estudos de Fontes (2006) com a proposta de uma releitura de questões reflexivas abordadas pelo autor.

De acordo com Silva e Menezes (2005, p. 20) a pesquisa qualitativa é “a interpretação de fenômenos e a atribuição de significados [...] não requer o uso de métodos e técnicas estatísticas. O ambiente natural é a fonte direta para coleta de dados e o pesquisador é o instrumento chave. É descritiva”. Com esse enfoque os dados foram tratados através de análise e interpretação das questões abertas do questionário.

Silva e Menezes (2005, p. 20) afirmam que a pesquisa quantitativa “considera tudo que pode ser quantificável, o que significa traduzir em números opiniões e informações para classificá-las e analisá-las. Requer o uso de recursos e de técnicas estatísticas”. Nesta abordagem os dados foram tratados através das questões fechadas do questionário.

## 2.2 Sob o ponto de vista dos objetivos

A pesquisa sob o ponto de vista dos objetivos apresentou caráter exploratório e descritivo.

De acordo com Gil (2010, p. 27), a pesquisa exploratória tem por objetivo “proporcionar maior familiaridade com o problema, com vistas a torná-lo mais explícito ou a construir hipóteses”. Assim, foi buscado através da consulta ao acervo bibliográfico da FASF e consulta externa a pesquisa sobre segurança da informação da PWC e outros livros, que permitiram a interpretação e identificação dos pontos principais apresentados neste estudo, bem como a melhor compreensão acerca do assunto abordado.

Para Bertucci (2011, p. 50), a pesquisa descritiva pode ser entendida como aquela que “tem como objetivo principal estabelecer relações entre as variáveis analisadas e levantar hipóteses ou possibilidades para explicar essas relações”. Desta forma, no presente estudo, foi descrita a importância da segurança da informação dentro das organizações e buscou-se

compreender de que forma este processo contribui no aprimoramento de técnicas, mecanismos, normas e políticas, bem como quais os riscos, ameaças e vulnerabilidades a que as organizações estão expostas.

### 3.3 Sob o ponto de vista dos procedimentos técnicos

A pesquisa quanto aos procedimentos técnicos foi caracterizada como bibliográfica e estudo de caso.

Para Marconi e Lakatos (2010, p. 166), a pesquisa bibliográfica "abrange toda bibliografia já tornada pública em relação ao tema de estudo". A pesquisa utilizou como base teórica-conceitual os estudos de Oliveira (2011), Laudon e Laudon (2014) e Rezende e Abreu (2011), sobre tecnologia e sistemas de informação, Machado (2014), Laureano (2012) e Sêmola (2014), sobre Segurança da Informação.

Para Gil (2010, p. 37), o estudo de caso consiste "no estudo profundo e exaustivo de um ou poucos objetos, de maneira que permita seu amplo e detalhado conhecimento". Dessa forma, o estudo de caso foi realizado em duas instituições financeiras localizadas na região Centro-Oeste de Minas Gerais, no ano de 2016, a fim de compreender sob o ponto de vista da segurança da informação de que forma esse processo contribui para o aprimoramento de técnicas e mecanismos utilizados pelas organizações no que tange à proteção de informações.

### 3.4 Sujeitos da Pesquisa

Foram escolhidas para aplicação da pesquisa duas instituições financeiras localizadas na região Centro-Oeste de Minas Gerais.

As instituições atualmente são administradas por 1 presidente, 1 vice-presidente, 2 diretores cada uma, totalizando 4 gestores em cada instituição. Além disso, possuem juntas 59 colaboradores.

O método adotado foi o de amostragem não probabilística intencional, que de acordo com Mattar (2008, p. 134), "uma estratégia muito utilizada na amostragem intencional é a de se escolherem casos julgados como típicos da população em que o pesquisador está interessado".

Diante disso, a pesquisa foi realizada, do total de 8 gestores considerando as duas instituições, com apenas 2 gestores, um de cada instituição que efetivamente participaram. E, do total de 59 colaboradores, foram aplicados 5 pré-testes e 42 colaboradores participaram da

pesquisa, exceto a pesquisadora, considerando que são as pessoas que possuem contato direto e influenciam nos processos operacionais, além do acesso constante a informações das instituições através de sistemas e demais recursos.

Assim, os demais colaboradores não foram incluídos na pesquisa por não possuírem acesso a esses elementos na instituição pela função que exercem o que representam 6 colaboradores e 5 estavam ausentes. Considerando que a pesquisadora por fazer parte do quadro de colaboradores de uma das instituições não respondeu à pesquisa, não sendo incluída nos dados coletados.

### 3.5 Instrumentos de coleta de dados

Quanto aos instrumentos de coleta de dados a pesquisa foi feita a partir de aplicação de questionário.

O instrumento para a coleta de dados foi o questionário estruturado fechado para os colaboradores e também o questionário estruturado aberto para os gestores. De acordo com Marconi e Lakatos (2011, p. 86), o questionário "é um instrumento de coleta de dados constituído por uma série ordenada de perguntas, que devem ser respondidas por escrito e sem a presença do entrevistador".

Com isso, os autores Marconi e Lakatos (2011, p. 89) afirmam que relacionado aos tipos de perguntas a serem utilizadas nos questionários, existem três categorias: "abertas, fechadas e de múltipla escolha".

As perguntas abertas podem ser definidas como "livres ou não limitadas, são as que permitem ao informante responder livremente, usando linguagem própria, e emitir opiniões", enquanto que as fechadas são consideradas "limitadas ou de alternativas fixas, são aquelas em que o informante escolhe sua resposta entre duas opções" e, por último, as de múltipla escolha que podem ser explicadas como "perguntas fechadas, mas que apresentam uma série de possíveis respostas, abrangendo várias facetas o mesmo assunto" (MARCONI; LAKATOS, 2011, p. 89-91).

O questionário fechado e o questionário aberto foram elaborados através do referencial teórico apresentado neste estudo, mais especificamente do autor Fontes (2006), que foi base para a elaboração das questões dos questionários onde foram adaptadas, visando o cumprimento dos objetivos deste estudo.

Foi aplicado um pré-teste no mês de setembro do questionário com cinco colaboradores a fim de analisar se as questões eram claras e objetivas de forma a garantir que

as informações desejadas fossem de fato obtidas e foram realizadas algumas alterações no questionário visando atender as observações e correções obtidas na aplicação do pré-teste.

Para a aplicação dos questionários nas instituições estudadas foi necessário solicitar autorização para os setores responsáveis para posteriormente realizar a pesquisa.

Assim, os dados foram coletados através da aplicação do questionário fechado em setembro de 2016, pela pesquisadora nas duas instituições pessoalmente, com os colaboradores e através de questionário aberto aplicado no mesmo período, com os gestores das organizações. Os dados coletados foram tratados, analisados e tabulados.

### 3.6 Tratamento de dados

Quanto ao tratamento de dados da pesquisa, este foi através dos dados coletados pelos questionários aplicados aos colaboradores, utilizando de análises e técnicas estatísticas, que depois foram disponibilizados em forma de gráficos, tabelas e quadros a fim de fornecer uma melhor compreensão dos dados coletados.

Para Marconi e Lakatos (2011, p. 117), a análise de conteúdo “é uma técnica que visa aos produtos da ação humana, estando voltada para o estudo de ideias e não das palavras em si”. Dessa forma a análise das questões abertas do questionário aplicado aos gestores tratou do conteúdo e buscou-se a interpretação dos dados coletados, a fim de relacionar os conceitos defendidos pelos autores no referencial teórico com as respostas obtidas no questionário aberto, visando atingir os objetivos deste estudo e responder à questão problema.

## 3RESULTADOSEDISCUSSÃO

Esta seção tem por objetivo apresentar os resultados e as discussões referentes aos dados levantados em campo, onde foi aplicado um questionário fechado a 42 colaboradores e realizada aplicação de questionário aberto com 2 gestores.

### 3.1 Dados dos colaboradores

Nesta seção são apresentados os resultados levantados mediante a aplicação de questionário a 42 colaboradores das instituições investigadas. O questionário abrange o total de 14 perguntas e as perguntas de 1 a 4 tiveram por objetivo caracterizar o perfil dos

colaboradores das instituições em estudo e as demais trataram da segurança da informação nas instituições.

Entre os 42 colaboradores participantes da pesquisa, 55% possuem faixa etária entre 18 e 28 anos, 26% entre 29 e 39 anos, 12% entre 40 e 50 anos, 2% entre 51 e 61 anos e 5% com mais de 61 anos e 40% são do gênero masculino e 60% do gênero feminino. Quanto à escolaridade, 38% possuem curso superior incompleto, 33% possuem curso superior completo, 24% possuem pós-graduação, 5% possuem ensino médio completo. Além disso, 15% trabalham na empresa há menos de um ano, 33% entre 1 a 4 anos, 33% entre 5 a 9 anos, 7% entre 10 a 14 anos, 5% entre 15 a 19 anos e 7% há mais de 19 anos.

A pergunta 9 teve por objetivo identificar os meios pelos quais as instituições orientam seus colaboradores sobre os procedimentos e técnicas que adotam referente à segurança da informação.

Entre os 42 colaboradores participantes da pesquisa, 38% afirmam que o meio mais utilizado para orientação sobre segurança da informação é através de cursos, 25% afirmam serem palestras, 2% debates, 81% afirmam que são reuniões, 40% através de manuais e 2% afirmam que a orientação é feita por outros meios que não os citados neste estudo.

Com isso, através dos resultados obtidos, foi observado que um dos meios mais utilizado para orientar os colaboradores são as reuniões, seguido de manuais e cursos. Com isso, constata-se que as instituições em estudo ainda não possuem métodos de orientação para seus colaboradores de forma estruturada, pois a maioria das orientações são passadas através de reuniões.

A pergunta 5 teve por objetivo avaliar o grau de conhecimento dos colaboradores no que diz respeito à segurança da informação, em geral. Entre os 42 colaboradores participantes da pesquisa, 50% alegaram possuir muito conhecimento e 50% alegaram possuir pouco conhecimento sobre segurança da informação no geral, a terceira opção de nenhum conhecimento não foi marcada pelos colaboradores.

Nesse sentido, pode-se dizer que apenas metade dos colaboradores reconhece possuir o conhecimento necessário do que é segurança da informação, enquanto a outra metade afirma ter pouco conhecimento do que se trata. Dessa forma, é possível afirmar que essa parcela que não possui totalmente o conhecimento necessário seria preciso alguma ação por parte da instituição para instruir esses colaboradores, no sentido de fazer com que obtenham as informações essenciais sobre o que vem a ser o processo de segurança da informação de forma consciente e que possam contribuir para o desenvolvimento de procedimentos e técnicas envolvendo a segurança das informações acessadas nas instituições.

A pergunta 13 teve por objetivo identificar quais são as maiores vulnerabilidades internas por parte dos colaboradores que possam vir a trazer prejuízos para as organizações no que tange à segurança da informação.

Entre os 42 colaboradores participantes da pesquisa, 31 afirmam conhecer a diferença existente entre ameaça e vulnerabilidade no que diz respeito a segurança da informação, 9 afirmam não saber essa diferença e 2 não tem nenhum conhecimento sobre o assunto. Enquanto que, 38 afirmam terem assinado termos e/ou documentos sobre sigilo de informações, 2 relatam não ter assinado e 2 afirmam não conhecer o assunto tratado.

34 dos colaboradores que afirmaram ter assinado um documento a respeito de sigilo de informações afirmam que se lembram do que esses documentos tratam e sabem as suas obrigações referentes aos mesmos, por outro lado 4 afirmam ter assinado, porém não se lembram do conteúdo desses documentos.

42 colaboradores consideram a criação de documentos e mecanismos de defesa como algo importante. Entretanto, 18 afirmam que não é possível dizer que somente eles detêm o conhecimento a respeito dos próprios acessos, enquanto 21 relatam ter certeza que somente eles sabem de seus acessos e 3 relatam não ter conhecimento se existe ou não a possibilidade de mais pessoas além deles terem conhecimento de seus acessos.

40 dos colaboradores afirmam não possuir o hábito de comentar assuntos das instituições em outro ambiente que não o organizacional e 2 afirmam que comentam a respeito de questões das instituições em outros lugares.

Com os resultados obtidos, pode-se dizer que a instituição tem procurado fornecer o conhecimento necessário para seus colaboradores, no sentido de que 31 deles sabem do que se tratam alguns termos de segurança da informação. Além disso, 38 deles assinaram documentos sobre sigilo de informações, sendo assim pode-se dizer que as instituições têm se preocupado e tomado medidas preventivas para que seus colaboradores criem o hábito de manterem as questões referentes à instituição, na instituição somente.

A pergunta 14 teve por objetivo identificar quais são as maiores ameaças do ponto de vista dos colaboradores, para a organização no que se refere à segurança da informação, visto que foi uma adaptação das ameaças potenciais citadas pelo autor Machado (2014).

Entre os 42 colaboradores participantes da pesquisa, 98% apontam como a maior ameaça a segurança da informação na instituição o vazamento de informações, 17% as modificações sem autorização, 17% o desfalque de recursos tecnológicos, 24% o usuário ou programa utilizando mecanismos de disfarce, 36% o usuário autorizado utilizando recursos ou sistemas para fins em que não possui permissão, 50% os programas instalados com a intenção

de violar a segurança de recursos tecnológicos e 5% outras ameaças que não as citadas neste estudo.

Visto isso, buscou-se identificar quais são as ameaças sob o ponto de vista dos colaboradores, que as instituições em que trabalham estão sujeitas em relação às atividades que desempenham no mercado financeiro, objeto deste estudo. Sendo assim, a ameaça que obteve o maior número de respostas identificadas foi o vazamento de informações, seguido de programas instalados com a intenção de violar a segurança dos recursos tecnológicos e usuário autorizado que utiliza seus acessos para fins que não possui permissão.

### 3.2 Dados dos gestores

Nesta seção são apresentados os resultados levantados mediante a aplicação de questionário aberto a dois gestores das instituições investigadas. O questionário aberto é composto por 11 perguntas e as perguntas de 1 a 4 tiveram por objetivo caracterizar o perfil dos gestores das instituições em estudo e as demais trataram da segurança da informação nas instituições.

A pergunta 5 teve por objetivo identificar se as instituições em estudo possuem alguma política de segurança da informação, bem como esclarecer se esse documento é de conhecimento de todos os colaboradores.

De acordo com o G1 “A instituição possui política institucional de segurança da informação, esta política foi transmitida para os colaboradores e está disponível em nosso site para consulta, porém não acredito que todos colaboradores conheçam esta política, sabem da existência mais não do conteúdo”.

Segundo G2 “Sim, todos possuem suas senhas e controles, possuem um sistema avançado de segurança e os mesmos têm consciência de que não podem passar suas senhas e acessos a outras pessoas”.

No geral, pode-se dizer que as duas instituições se preocupam com a adoção de políticas que determinem as regras e normas que devem ser seguidas quanto à segurança da informação, por outro lado, seus colaboradores não se encontram totalmente cientes sobre o que esse tipo de documento trata, o que necessita de atenção por parte das instituições para prover a orientação necessária nesse aspecto.

A pergunta 6 teve por objetivo identificar a frequência com a qual as instituições promovem orientação aos seus colaboradores a respeito dos métodos utilizados pelas mesmas sobre segurança da informação.

Segundo **G1**, a respeito das orientações fornecidas pela instituição, esclareceu que ocorre da seguinte maneira:

> De maneira esporádica, porém o ramo de instituição financeira é muito cobrado principalmente quanto a questão do sigilo de informações isto torna-se uma cultura da organização que é facilmente entendida. Os colaboradores sempre participam de treinamentos que envolvem o tema. Quanto ao conhecimento dos colaboradores vejo que sabem que a cultura da organização exige-se segurança nas informações, porém não aprofundam quanto ao tema.

Enquanto **G2** afirma que essa orientação ocorre "mensalmente, o responsável pelo TI transfere mensalmente. Palestras feitas pelo responsável pela TI, outros funcionários vão a cursos também. Possuem muito conhecimento, estão indo sempre em cursos e são oferecidos constantemente, são bem assistidos".

Observando esses aspectos, pode-se dizer que as instituições tem se preocupado com promover instruções sobre segurança da informação para seus colaboradores como um todo, mas que a orientação feita periodicamente traz mais resultados e mantém os colaboradores atentos a essas questões.

A pergunta 11 teve por objetivo verificar quais são as principais ameaças e vulnerabilidades que as instituições estão sujeitas no ambiente em que estão inseridas, bem como identificar se estão preparadas para possíveis violações da segurança da informação.

Segundo **G1** "A instituição encontra-se sólida no quesito de segurança das informações *web* visto que possui *firewall* e monitoramento por parte da Central. Quanto a possíveis vazamentos acredito que possa ocorrer apenas do aspecto pessoal que fica mais complicado identificar estes vazamentos" (grifo da autora).

De acordo com **G2** "*Hackers*, mal intencionados. Sim, existem muitos treinamentos e acessos são bloqueados rapidamente" (grifo da autora).

Analisando as respostas dos gestores, é possível dizer que as principais ameaças encontradas pelas instituições são o vazamento de informações e a entrada de *hackers* mal intencionados, sendo que ambos estão sujeitos a ocorrer tanto de maneira interna ou externamente, ou seja, pessoas que não se incluem no ambiente institucional.

Entretanto, ambas concordam que muito se é feito para monitorar e controlar acessos, sistemas, recursos, usuários visando que essas ocorrências e consequentemente prejuízos futuros para as instituições sejam evitados.

A partir desse contexto, a próxima seção trata das principais conclusões deste estudo, bem como o alinhamento dos resultados com os objetivos e resultados buscados.

## CONSIDERAÇÕES FINAIS

A partir do contexto em que as organizações se encontram atualmente e da importância da segurança da informação para garantir que as mesmas desenvolvam suas atividades de maneira confiável e assertiva, esse estudo buscou compreender como o processo de segurança da informação pode contribuir para aprimoramento de procedimentos e técnicas de segurança em âmbito institucional.

Com base nos resultados e nas discussões realizadas, ambas as instituições estudadas adotam uma política de segurança da informação e se preocupam em disponibilizar seu conteúdo aos seus colaboradores.

A respeito do conhecimento dos colaboradores referente à segurança da informação, mesmo que as instituições estejam oferecendo orientações sobre os procedimentos que utilizam, o resultado obtido é que a maioria dos colaboradores possui consciência de suas responsabilidades, mas não possuem no todo o conhecimento necessário a respeito.

Em relação às vulnerabilidades encontradas nas instituições, pode-se dizer que as potenciais e que podem trazer prejuízos futuros às mesmas são: a falta de conhecimento necessário por parte dos colaboradores no que trata os procedimentos e técnicas utilizados pelas instituições. Esses dados são relevantes, pois são variáveis que podem ser exploradas para que um vazamento de informações ocorra, por exemplo, o que necessita de cuidado e monitoramento por parte das instituições.

No que se referem às ameaças potenciais, as principais identificadas foram o vazamento de informações, programas instalados com intenção de violar a segurança de sistemas e/ou recursos, usuários autorizados que utilizam os acessos para fins que não possuem autorização e usuário ou programa utilizando mecanismos de disfarce, esse último também mais conhecido como hackers. Nesse caso, pode-se dizer que ambas as instituições já adotam mecanismos de segurança e buscam instruir seus colaboradores a respeito dos riscos inerentes ao ambiente em que estão inseridas, visando minimizar a incidência de vulnerabilidades bem como de ameaças que possam vir a explorá-las.

Portanto, considerando as conclusões apresentadas, pode-se confirmar o alcance dos objetivos inicialmente propostos. Além disso, pode-se dizer que esse processo é capaz de prover o conhecimento necessário para o quadro de colaboradores, com a finalidade de mantê-

los familiarizados com as técnicas adotadas pelas próprias instituições e saber como utilizá-las em suas rotinas diárias.

Sugere-se que as instituições estudadas busquem prover o conhecimento necessário para a parcela de colaboradores que ainda afirma não conhecer o processo como um todo, visto que utilizam informações diariamente nas instituições, e se tornam peça chave para que procedimentos e técnicas adotados visando à segurança dessas informações sejam eficientes.

## REFERÊNCIAS

ALBERTIN, R. M. M.; ALBERTIN, A. L. **Estratégias de governança de tecnologia da informação**. Rio de Janeiro: Elsevier, 2010.

BERTUCCI, J. L. de O. **Metodologia básica para elaboração de trabalhos de conclusão de cursos (TCC):** ênfase na elaboração de TCC de pós-graduação Lato Sensu. 3 reimpr. São Paulo: Atlas, 2011.

CRUZ, T. **Sistemas de informações gerenciais:** tecnologia de informação e a empresa do século XXI. São Paulo: Atlas, 1998.

DANTAS, M. L. **Segurança da informação:** uma abordagem focada em gestão de riscos. Olinda: Livro Rápido, 2011.

FRANCO, D. H.; RODRIGUES, E. de A.; CAZELA, M. M. **Tecnologias e ferramentas de gestão.** São Paulo: Alínea, 2009.

FONTES, E. **Segurança da informação:** o usuário faz a diferença. São Paulo: Saraiva, 2006.
GIL, A. C. **Como elaborar projetos de pesquisa**. 5 ed. São Paulo: Atlas, 2010.

JOÃO, B. N. **Sistemas de informação**. São Paulo: Pearson Education do Brasil, 2012. Disponível em: <http://unisa.bv3.digitalpages.com.br/users/publications/9788564574533/pages/-8>.

LAUDON, K. C; LAUDON, J. P. **Sistemas de informação gerenciais**. Tradução de Luciana do Amaral Teixeira. 9 ed. São Paulo: Pearson, 2014. Disponível em: <http://unisa.bv3.digital

pages.com.br/users/publications/9788543005850/pages/-18>

LAUREANO, M. A. P. **Segurança da informação**. Curitiba: Livro Técnico, 2012.

MACHADO, F. N. R. **Segurança da informação: princípios e controle de ameaças**. 1 ed. São Paulo: Érica, 2014.

MARCONI, M. A; LAKATOS, E. M. **Fundamentos de metodologia científica**. 7 ed. São Paulo: Atlas, 2010.

MARCONI, M. A.; LAKATOS, E. M. **Técnicas de pesquisa: planejamento e execução de pesquisas, amostragens e técnicas de pesquisa, elaboração análise e interpretação de dados**. 7. ed. 5 reimpr. São Paulo: Atlas, 2011.

MATTAR, F. N. **Pesquisa de marketing:** edição compacta. 4 ed. 2 reimpr. São Paulo: Atlas, 2008.

O'BRIEN, J. A. **Sistemas de informação e as decisões gerenciais na era da internet**. Tradução: Célio Knipel Moreira e Cid Knipel Moreira. 2 ed. São Paulo: Saraiva, 2004.

OLIVEIRA, D. P. R. **Sistemas de informações gerenciais:** estratégicas, táticas, operacionais. 14. ed. São Paulo: Atlas, 2011.

REZENDE, D. A.; ABREU, A. F. **Tecnologia da informação aplicada a sistemas de informação gerenciais:** o papel estratégico da informação e dos sistemas de informação nas empresas. 8 ed. São Paulo: Atlas, 2011.

SÊMOLA, M. **Gestão da segurança da informação: uma visão executiva**. 2. ed. - Rio de Janeiro : Elsevier, 2014.

SILVA, A. E. N. da. **Segurança da informação – vazamento de informações – as informações estão realmente seguras em sua empresa?**. Rio de Janeiro: Editora Ciência Moderna Ltda, 2012.

SILVA, E.L. da; MENEZES, E. M. **Metodologia da pesquisa e elaboração de dissertação**. 4 ed. rev. atual. Florianópolis: Laboratório de Ensino a Distância da UFSC, 2005.