PONTIFÍCIA UNIVERSIDADE CATÓLICA DO RIO GRANDE DO SUL
FACULDADE DE ADMINISTRAÇÃO, CONTABILIDADE E ECONOMIA
PROGRAMA DE PÓS-GRADUAÇÃO EM ADMINISTRAÇÃO
MESTRADO EM ADMINISTRAÇÃO E NEGÓCIOS

RODRIGO HICKMANN KLEIN

AMEAÇAS, CONTROLE, ESFORÇO E DESCONTENTAMENTO DO USUÁRIO NO COMPORTAMENTO SEGURO EM RELAÇÃO À SEGURANÇA DA INFORMAÇÃO

Porto Alegre
2014

RODRIGO HICKMANN KLEIN

AMEAÇAS, CONTROLE, ESFORÇO E DESCONTENTAMENTO DO USUÁRIO NO COMPORTAMENTO SEGURO EM RELAÇÃO À SEGURANÇA DA INFORMAÇÃO

Dissertação apresentada como requisito parcial para a obtenção do grau de Mestre em Administração, pelo Mestrado em Administração e Negócios da Faculdade de Administração, Contabilidade e Economia da Pontifícia Universidade Católica do Rio Grande do Sul.

Orientadora: Profª. Drª. Edimara Mezzomo Luciano

Porto Alegre

2014

Dados Internacionais de Catalogação na Publicação (CIP)

K64a Klein, Rodrigo Hickmann
Ameaças, controle, esforço e descontentamento do usuário no comportamento seguro em relação à segurança da informação / Rodrigo Hickmann Klein. – Porto Alegre, 2014.
100 f.

Dissertação (Mestrado em Administração e Negócios) – Faculdade de Administração, Contabilidade e Economia, PUCRS
Orientador: Profª. Drª. Edimara Mezzomo Luciano.

1. Segurança da informação. 2. Comportamento seguro. 3. Vulnerabilidade. I. Luciano, Edimara Mezzomo. II. Título.

CDD 341.2

Aline M. Debastiani
CRB 10/2199

Rodrigo Hickmann Klein

Ameaças, Controle, Esforço e Descontentamento do Usuário no Comportamento Seguro em relação à Segurança da Informação

Dissertação apresentada como requisito parcial para a obtenção do grau de Mestre em Administração, pelo Mestrado em Administração e Negócios da Faculdade de Administração, Contabilidade e Economia da Pontifícia Universidade Católica do Rio Grande do Sul.

Aprovado em 27 de março de 2014, pela Banca Examinadora.

BANCA EXAMINADORA:

Profa. Dra. Edimara Mezzomo Luciano
Orientadora e Presidente da sessão

Profa. Dra. Marie Anne Macadar Moron

Prof. Dr. Maurício Gregianin Testa

Prof. Dr. Antonio Carlos Gastaud Maçada

AGRADECIMENTOS

Dentre as várias pessoas que me auxiliaram nesta pesquisa há duas pessoas que gostaria de agradecer primeiramente, à minha orientadora, Dra. Edimara Mezzomo Luciano, pois seus inúmeros auxílios foram cruciais e imprescindíveis, e à minha esposa Deisy C. Barbiero Klein, que me apoiou e auxiliou na digitação dos dados coletados e na revisão.

Gostaria de agradecer também aos Drs. que participaram da validação de face e conteúdo do instrumento de pesquisa, pela sua prontidão em me auxiliar, mesmo perante tantos compromissos paralelos. Agradeço em especial ao Dr. Maurício Testa, à Dra. Marie Anne Macadar Moron e agradeço principalmente à Dra. Denise Lindstrom Bandeira da PPGA UFRGS, que me auxiliou nesta fase de validação, em coletas e também na análise de dados. Nesse ponto, agradeço também ao Dr. João Luiz Becker pelas suas dicas fundamentais.

Por fim, agradeço à secretária da PPGAd, Sra. Janaína R. Marques, por tantos e diversos auxílios, e a todos os respondentes que preencheram os questionários de forma sincera e por completo, bem como aos vários professores que cederam alguns minutos de suas aulas para realização das coletas.

RESUMO

A popularização de softwares que visam mitigar as ameaças à Segurança da Informação acabou produzindo uma noção exacerbada nos usuários a respeito da plena eficácia desses softwares na proteção das organizações e na supressão de qualquer ameaça. Essa noção equivocada pode ser originada pela obtenção de informações parciais sobre o assunto, ou pela falta da conscientização adequada, e é um fator humano que pode provocar acréscimo de vulnerabilidade, pois ocasiona um comportamento imprudente dos usuários em relação aos Sistemas de Informação. Entretanto, somente o equívoco em relação à percepção da ameaça e a sua severidade não explica as brechas na Segurança da Informação provocadas por fatores humanos. Outra percepção importante é o esforço percebido no cumprimento de ações que conduzem a um comportamento responsável em relação à Segurança da Informação, que somados aos aspectos como a indiferença às orientações da Segurança da Informação e o erro humano, também podem ser fatores indutores de vulnerabilidade e brechas na Segurança da Informação. Na presente pesquisa optou-se pelo embasamento em teorias que tratam da Segurança da Informação através de uma abordagem comportamental do usuário. A combinação dos principais conceitos dessas teorias, previamente validados em suas respectivas pesquisas e aplicáveis à abordagem da presente pesquisa, foi utilizada buscando compreender até que ponto a percepção humana sobre ameaça, esforço, controle e o descontentamento podem induzir a um comportamento responsável perante a Segurança da Informação e como esse comportamento humano pode gerar vulnerabilidade e possíveis violações na Segurança da Informação. Os resultados demonstraram que há influência da orientação em Segurança da informação, fornecida pelas organizações, na percepção e severidade da ameaça. Além disso, através da aplicação da técnica de regressão linear, foi verificada a relação entre o descontentamento e o Comportamento Seguro em relação à Segurança da Informação. Com base nesses resultados foram elaboradas contribuições para o conhecimento acadêmico e gerencial.

Palavras-chave: Comportamento Seguro. Fator humano em Segurança da Informação. Percepção de ameaça. Vulnerabilidade e brechas em Segurança da Informação.

ABSTRACT

The popularization of softwares intended to mitigate the threats to Information Security ended up producing an incorrect notion that such artifacts can protect organizations from attack and overcome any threat. This mistaken notion may be caused by obtaining partial information on the subject or the lack of adequate awareness, being a human factor that can cause increased vulnerability, because induce a reckless behavior of users in relation to Information Systems. However, only the misconception regarding the perception of the threat and its severity does not justify the in Information Security breaches caused by human factors. Another important insight is the perceived exertion of performing actions that lead to responsible behavior in relation to Information Security, which added to aspects such as indifference to the rules of information security and human error can also be inducing factors of vulnerability and breaches in Information Security. In the present study we opted for the grounding in theories on Information Security through a behavioral approach to the user. The combination of the key concepts of these theories, previously validated in their research and applied to the present study approach, was used in order to understand the extent to which human perception of threat, stress, and disgruntlement control can induce responsible behavior before the Information Security and how that human behavior can generate vulnerability and potential breaches in Information Security. The results showed that there is an influence of Information Security orientation, provided by organizations in the perception and severity of the threat. Furthermore, by applying the linear regression technique, it was verified the relationship between disgruntlement and in relation to Information Security Safe Behaviour. Based on these findings contributions to the academic and practioneer knowledge were developed.

Keywords: Safe behavior. Human Factor in Information Security. Threat perception. Vulnerability and breaches in Information Security.

LISTA DE ILUSTRAÇÕES

LISTA DE QUADROS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
AGFI	*Adjusted Goodness-of-Fit Index*
ANOVA	*Analysis of variance*
AVE	*Average Variance Extracted* (Variância Média Extraída)
CC	Confiabilidade Composta
ISACA	*Information Systems Audit and Control Association*
ISO	*International Organization for Standardization*
ITGI	*IT Governance Institute*
ITIL	*Information Technology Infrastructure Library*
KMO	Teste de Kaiser-Meyer-Olkin
MEE	Modelagem de Equações Estruturais
PLS	*Partial Least Squares*
RMSEA	*Root Mean Square Error of Approximation*
SPSS®	*Statistical Package for Social Sciences*
SEGINF	Segurança da Informação
TI	Tecnologia da Informação
TIC	Tecnologia da Informação e Comunicação
VME	Variância Média Extraída

SUMÁRIO

1 INTRODUÇÃO

A popularização de softwares que visam mitigar as ameaças à Segurança da Informação acabou produzindo uma noção exacerbada nos usuários a respeito da plena eficácia desses softwares na proteção das organizações e na supressão de qualquer ameaça. Essa noção equivocada pode ser originada pela obtenção de informações parciais sobre o assunto ou pela falta da conscientização adequada (LIANG e XUE, 2009) e é um fator humano que pode provocar acréscimo de vulnerabilidade, pois ocasiona um comportamento imprudente dos usuários em relação aos Sistemas de Informação (LIGINLAL et al., 2009). Entretanto, somente esse equívoco em relação à percepção da ameaça e a sua severidade não explica as brechas na Segurança da Informação provocadas por fatores humanos. Outra percepção importante é o esforço percebido no cumprimento de ações que conduzem a um comportamento responsável em relação à Segurança da Informação, que somados aos aspectos como a indiferença às orientações da Segurança da Informação e o erro humano, também podem ser fatores indutores de vulnerabilidade e brechas na Segurança da Informação.

Na presente pesquisa optou-se pelo embasamento em teorias que tratam da Segurança da Informação através de uma abordagem comportamental. A combinação dos principais conceitos dessas teorias, previamente validados em suas respectivas pesquisas e aplicáveis a abordagem da presente pesquisa, foi utilizado buscando compreender até que ponto a percepção humana sobre ameaça, esforço, controle e o descontentamento, podem induzir a um comportamento responsável perante a Segurança da Informação e como esse comportamento humano pode gerar vulnerabilidade e possíveis violações na Segurança da Informação.

1.1 TEMA E FOCO

A presente pesquisa propõe abordar o tema Segurança da Informação, especificamente sobre o aspecto do comportamento individual do usuário de artefatos da Tecnologia da Informação (TI) e sua influência no incremento ou redução de vulnerabilidades na Segurança da Informação, que são consideradas as fraquezas de um ativo ou controle e que podem ser exploradas por ameaças (ABNT, 2005). Diferencia-se de pesquisas que enfocam em aspectos técnicos ou de geração de políticas e implantação de sistemas de gestão da Segurança da Informação, pois aborda a Segurança da Informação com um processo de gestão e não apenas um processo tecnológico. Um processo que abrange a segurança física, técnica, de processos e de pessoas, visando à preservação dos princípios básicos de confidencialidade, integridade,

disponibilidade, autenticidade, irrefutabilidade e confiabilidade da informação (ABNT, 2005). Dessa forma, propõe estudar as vulnerabilidades na Segurança da Informação produzidas por condutas inadequadas ou imprudentes, embasadas em percepções relacionadas às ameaças, ao controle e ao esforço percebido em manter um comportamento responsável perante a Segurança da Informação.

Vance et al. (2012) conceituam a vulnerabilidade como a probabilidade de um incidente indesejado acontecer se não forem tomadas medidas para evitá-lo. Albrechtsen e Hovden (2009) consideram os usuários uma vulnerabilidade quando esses não possuem habilidades e conhecimentos, provocando dessa forma o uso imprudente das conexões de rede e das informações, ou ao praticarem atos inseguros dentro da organização. Bulgurcu et al. (2010) afirmam que a vulnerabilidade é um estado importante que decorre de um funcionário que não segue a Política de Segurança da Informação (PSI). No entanto, se um empregado executa o que está prescrito na PSI, ele contribui para a proteção da informação da organização e dos recursos tecnológicos, portanto a segurança é um estado que resulta do cumprimento das orientações do PSI pelos funcionários.

Segundo Herath e Rao (2009a) brechas são violações de segurança e muitas vezes a negligência e não conformidade do empregado com as regras da Segurança da Informação causam muitos prejuízo às organizações. Entretanto o comportamento dos usuários pode ajudar a reduzir essas brechas, ao seguir as práticas recomendadas, como, por exemplo, proteger os dados com senhas adequadas (NG et al., 2009) ou fazer *logoff* ao se afastar do computador que está sendo utilizado (SON, 2011).

A série de normas ISO/IEC 27000, publicadas pela ABNT no Brasil, definem aspectos que devem ser considerados ao se elaborar políticas de segurança nas organizações e que são dedicadas à segurança dos Sistemas de Informação. Entre elas se sobressaem as normas ISO/IEC 27001 (ABNT, 2006), que aborda os requisitos para os sistemas de gestão da Segurança da Informação e a norma ISO/IEC 27002 (ABNT, 2005), que trata das práticas de sistemas de gestão da Segurança da Informação, substituindo a norma anterior ISO/IEC 17799:2005 e estabelecendo diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de Segurança da Informação em uma organização.

A ISO/IEC 27002 (ABNT, 2005) define Segurança da Informação como a proteção da informação contra diversos tipos de ameaças, garantindo a continuidade dos negócios, minimizando os danos aos negócios, maximizando o retorno dos investimentos e as oportunidades de negócio. Segundo essa norma, a Segurança da Informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos,

procedimentos, estruturas organizacionais e funções de software e hardware. Esses controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados quando e onde for necessário, para garantir que os objetivos de negócio e de segurança da organização sejam atendidos.

Dentro desse contexto, a ISO/IEC 27001 (ABNT, 2006) destaca três princípios importantes da informação: a) a confidencialidade que assegura que a informação é acessível somente para pessoas autorizadas; b) a integridade que protege a exatidão e a completeza (ou completude) da informação e dos métodos de processamento; c) a disponibilidade que assegura acesso à informação e ativos associados aos usuários autorizados, quando necessário.

Entretanto, cada um desses preceitos pode ser comprometido a partir do momento que um usuário de artefato de TI comporta-se de forma imprudente e inadequada em relação à Segurança da Informação, devido a diferentes percepções ou por fatores atenuantes do comportamento responsável. Um exemplo de um comportamento inadequado é o empréstimo de senha a outra pessoa, para delegar ou agilizar parte de uma atividade em um momento de urgência, sobrecarga de trabalho, ou até mesmo, pela falta de comprometimento com a segurança, por descontentamento (WILLISON e WARKENTIN, 2013) ou baixa motivação em relação às organizações ou pessoas que estipularam normatizações de segurança (KELLOWAY et al., 2010).

Para estruturar hipóteses relacionadas à pesquisa propõem-se uma combinação de diversas teorias e conceitos atuais na área de Sistemas de Informação e através da reutilização dos construtos dessas teorias, aplicadas à área de Segurança da Informação, enseja entender os comportamentos que provocam vulnerabilidades na Segurança da Informação, com foco nas percepções humanas em relação às ameaças, normas, políticas da Segurança da Informação e o esforço percebido, que podem ser atenuadas por fatores psicológicos e ambientais.

1.2 SITUAÇÃO PROBLEMÁTICA

Vários comportamentos imprudentes ou inconsequentes perante a Segurança da Informação, originados por percepções embasadas em informações parciais ou incorretas, ou derivada de fatores atenuantes ao comportamento responsável, podem provocar acréscimo de vulnerabilidade na Segurança da Informação (ABNT, 2005; LIANG e XUE, 2009), tornando os fatores humanos uma das principais origens de vulnerabilidades na Segurança da Informação (ABNT, 2005).

A percepção equivocada ou parcialmente embasada em informações corretas, sobre os danos que, por exemplo, o empréstimo de senha ocasiona, pode estar relacionado à falta de

conscientização em relação às ameaças, ou até mesmo ser o resultado de uma ponderação na tomada de decisão racional (FISCHBEIN e AZJEN, 1975), na qual os fatores de esforço versus a ameaça, ou esforço versus a percepção de controle e relação à ameaça, resultam na tomada de decisão em prol do menor esforço. Nesta situação todos os três principais preceitos da informação estão sendo comprometidos. A confidencialidade já estaria comprometida pelo simples empréstimo da senha, além disso, a senha em si contém um padrão cognitivo de formação (BANG et al., 2012), que poderia permitir a dedução das senhas do usuário em demais Sistemas de Informação. A integridade pode ser comprometida, pois a pessoa que recebeu a senha emprestada, para auxiliar na tarefa solicitada pode não estar capacitada para lidar com o sistema de informação em questão, podendo causar danos às informações armazenadas durante a operação, como também comprometer a disponibilidade. A confiabilidade da informação, que garante a autoria das informações armazenadas nos Sistemas de Informação (ABNT, 2005), bem como a conformidade com regulações, são comprometidas devido à refutabilidade das informações nessa situação.

Traçando um paralelo entre os Sistemas de Informações e o cotidiano, é perceptível que os procedimentos que buscam uma maior segurança física ocasionam um acréscimo de ações e tarefas que outrora eram desnecessárias. Esses procedimentos suscitam no uso e transporte de chaves, crachás e controles eletrônicos, além de onerar em um dispêndio de tempo recorrente nas ações de fechamento e abertura dos dispositivos associados. Dessa forma, similarmente como qualquer outro procedimento que produza maior segurança física no cotidiano, os procedimentos na Segurança da Informação ocasionam em um maior número de procedimentos e tarefas a serem realizadas, acarretando em um maior esforço potencial para a realização das ações adicionais, que podem ser percebidas equivocadamente como um empecilho desproposital (HERATH e RAO, 2009a).

Quando as ameaças à segurança não são percebidas como eminentes, os esforços em seguir normas e boas práticas em Segurança da Informação podem ser considerados desnecessários, improdutivos e apenas uma formalização normativa (HERATH e RAO, 2009a). Nessa circunstância, os procedimentos que proporcionam a Segurança da Informação podem ser preteridos ou burlados, dependendo da percepção em relação ao controle e à punição em contraponto aos benefícios. Além disso, o descontentamento de um usuário de Sistemas de Informação com organizações ou pessoas que estabeleceram normas de segurança pode produzir ações que burlam a segurança, como forma de demonstração do descontentamento (WILLISON e WARKENTIN, 2013), ou apenas pela baixa motivação em cumpri-las (KELLOWAY et al., 2010).

Portanto, as maneiras como os usuários se comportam em relação à Segurança da Informação podem decorrer das percepções acerca de ameaças, dos controles e punições percebidos e do esforço percebido, bem como de fatores ambientais, como sobrecarga de trabalho, fadiga (KRAEMER e CARAYON, 2007) e o descontentamento (WILLISON e WARKENTIN, 2013; KELLOWAY et al., 2010), que podem gerar vulnerabilidade e brechas da Segurança da Informação, comprometendo todos os princípios da Segurança da Informação e tornando a informação um dado inútil devido à sua inverossimilidade.

Da Veiga e Eloff (2010) argumentam que a abordagem de uma organização na Segurança da Informação deve se concentrar no comportamento do empregado, pois o sucesso ou o fracasso depende efetivamente do que os funcionários fazem ou deixam de fazer.

Desta forma, a questão que essa pesquisa propõe responder é: qual a influência da percepção do usuário a respeito da ameaça, do controle, do esforço e do descontentamento no comportamento seguro em relação à Segurança da Informação?

1.3 OBJETIVOS

A fim de propiciar um melhor entendimento sobre os motivos que conduze a situação problemática e visando atender ao tema e ao foco da pesquisa foram estabelecidos os seguintes objetivos de pesquisa.

1.3.1 Objetivos Gerais

Identificar a influência da percepção do usuário sobre a ameaça, o controle, o esforço e o descontentamento no comportamento seguro em relação à Segurança da Informação.

1.3.2 Objetivos Específicos

a) Elaborar e validar um instrumento estruturado de pesquisa a ser utilizado em uma pesquisa tipo *survey*.
b) Identificar se as percepções dos usuários sobre a suscetibilidade e severidade de uma ameaça à Segurança da Informação, e sobre o controle e a severidade da punição em não seguir as orientações organizacionais, influenciam positivamente no comportamento responsável desse usuário perante a Segurança da Informação.
c) Identificar se o esforço percebido pelo usuário em seguir as orientações de Segurança da Informação influencia negativamente no comportamento responsável desse usuário em relação à Segurança da Informação.

d) Identificar se o descontentamento de um usuário com a organização onde trabalha, com superiores ou com colegas, influencia negativamente no comportamento responsável desse usuário, em relação à Segurança da Informação.

1.4 JUSTIFICATIVA

De forma progressiva as organizações coletam, manipulam e armazenam informações, evidenciando a necessidade crescente da Segurança da Informação, que visa propiciar a proteção dos ativos informacionais da organização contra as perdas, exposição indevida ou dano e a proteção desses ativos perante as ameaças, a fim de garantir a continuidade do negócio, minimizar as perdas empresariais e maximizar o retorno dos investimentos e as oportunidades de negócios, através de procedimentos e mecanismos de proteção da informação e do atendimento dos requisitos dessa informação.

Segundo Vance et al. (2012), as organizações tipicamente sofrem ao menos anualmente uma brecha na segurança, devido a uma violação da política de Segurança da Informação. Os autores estimam que mais da metade de todas as violações de segurança são direta ou indiretamente causados por falha de um colaborador ao cumprir os procedimentos de segurança. Ainda segundo Vance et al. (2012), uma série de abordagens comportamentais têm sido propostas na literatura para explicar o cumprimento da Política de Segurança da Informação, ou para explicar as razões dos abusos.

O grau de responsabilização das pessoas em relação às falhas Segurança da Informação é tão grande que há uma norma ISO dedicada a esse tema, a ISO/IEC 27002 (ABNT, 2005), que considera as pessoas o principal fator de falhas da Segurança da Informação, além de especificar uma série de responsabilidades aos funcionários de organizações, no que tange à Segurança da Informação nas organizações. As falhas humanas são cometidas por diferentes motivos e várias delas são resultados de fatores atenuantes ao comportamento responsável, como sobrecarga de trabalho, urgência, fadiga, ou descontentamento. Outras falhas são provocadas por percepções limitadas, causadas pela falta de informações completas ou corretas em consideração às ameaças. (LIGINLAL et al., 2009)

A conscientização em relação à Segurança da Informação, por intermédio de treinamentos e pela divulgação de riscos e ameaças é uma forma de aprimorar as percepções dos usuários de sistemas de informações, em relação aos riscos e ameaças as quais estão sujeitos (ABNT, 2005). Entretanto, a percepção sobre a ameaça à Segurança da Informação não é a única que resulta em um comportamento responsável, pois a racionalização sobre a eminência da ameaça varia de indivíduo para indivíduo, dando margem a demais percepções

envolvidas, como o esforço necessário ao comportamento responsável e a percepção relativa ao controle, além dos fatores atenuantes do comportamento responsável que são resultantes do contexto vivido pelo indivíduo.

Portanto, identificar quais são as influência da percepção do usuário e de fatores ambientais no comportamento relacionado à vulnerabilidades na Segurança da Informação, através de uma pesquisa quantitativa com usuários de Sistemas de Informação, é algo fundamental para o aprimoramento do entendimento dos fatores humanos, que produzem vulnerabilidades na Segurança da Informação, proporcionando novas ideias sobre formas de redução de riscos, bem como, novas premissas para uma maior efetividade da conscientização e da gestão da Segurança da Informação.

2 REFERENCIAL TEÓRICO

A Segurança da Informação apresenta diversas abordagens e conceitos que buscam explicar seus mecanismos, práticas, aspectos humanos e comportamentais dos usuários com relação ao tema.

Neste capítulo são abordados alguns conceitos necessários para o entendimento desta pesquisa. Inicialmente é abordada a Segurança da Informação e sua importância no contexto organizacional. Posteriormente, são abordadas questões sobre privacidade e confiança em Segurança da Informação, aspectos relacionados ao ambiente organizacional e questões relacionadas a comportamento e características individuais dos usuários.

2.1 SEGURANÇA DA INFORMAÇÃO

Segurança da Informação consiste na proteção dos ativos informacionais de uma organização, em relação às perdas, exposição indevida ou dano (WILLIAMS, 2001), aplicada a toda informação armazenada, manipulada ou transmitida em uma ou entre organizações. A preocupação com a Segurança da Informação vem ganhando evidência e se popularizando em uma progressão exponencial nas últimas décadas, devido aos artefatos de TI que possibilitaram gradativamente uma geração, processamento e ubiquidade de informações sem precedentes, potencializando também as ameaças à Segurança da Informação (KING e RAJA, 2012).

O crescimento dessas ameaças gerou para a área de Segurança da Informação, no decorrer das últimas décadas, uma ampla normalização, com a consequente ampliação de procedimentos de segurança e políticas de acesso à informação (ABNT, 2006; ABNT, 2005). Apesar desse investimento, frequentemente oneroso, as políticas da Segurança da Informação, que representam a estrutura formal de Segurança da Informação sofrem resistência, por parte dos usuários, em seu uso no cotidiano das organizações (PUHAKAINEN e SIPONEN, 2010).

A resistência dos usuários para a utilização das normas de Segurança da Informação tem sido identificada como uma razão importante para as brechas na Segurança da Informação (PUHAKAINEN e SIPONEN, 2010), tornando necessária a compreensão de como os usuários avaliam a mudança que essas normas produzem e porque decidem resistir a elas, possibilitando através dessa compreensão possibilidade de mitigar essa resistência. De acordo com Son (2011), uma preocupação primordial para as organizações deveria ser a medida que os empregados cumprem com as políticas de Segurança da Informação.

No âmbito da normatização da Segurança da Informação, a série de normas ISO/IEC 27000 é dedicada à segurança dos Sistemas de Informação e definem aspectos que devem ser considerados ao se elaborar políticas de segurança nas organizações. Nessa série se sobressaem as normas ISO/IEC 27001:2006 (ABNT, 2006), que aborda os requisitos para os sistemas de gestão da Segurança da Informação e a norma ISO/IEC 27002:2005 (ABNT, 2005), que trata das práticas de sistemas de gestão da Segurança da Informação, substituindo a norma anterior ISO/IEC 17799:2005 e estabelecendo diretrizes e princípios gerais para iniciar, programar, manter e melhorar a gestão de Segurança da Informação em uma organização.

A ISO/IEC 27002:2005 (ABNT, 2005) define Segurança da Informação como a proteção da informação contra diversos tipos de ameaças, garantindo a continuidade dos negócios, minimizando os danos aos negócios, maximizando o retorno dos investimentos e as oportunidades de negócio. Segundo essa norma, a Segurança da Informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Esses controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados quando e onde for necessário, para garantir que os objetivos de negócio e de segurança da organização sejam atendidos.

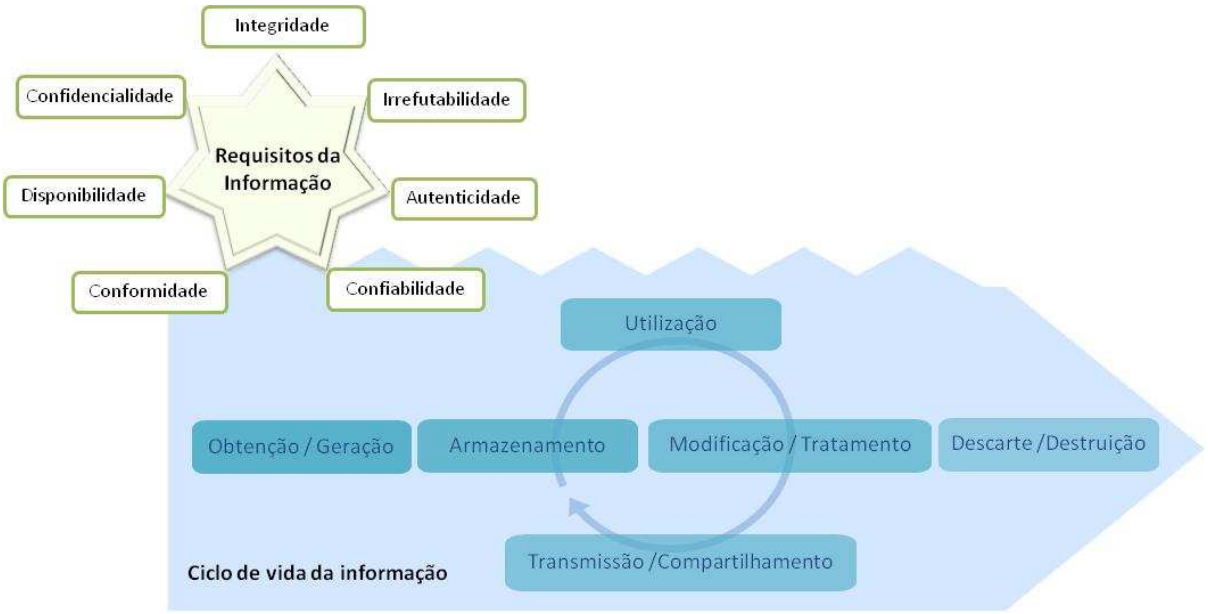
Dentro desse contexto, a ISO/IEC 27001:2006 (ABNT, 2006) destaca três aspectos importantes da informação: a) a confidencialidade que assegura que a informação é acessível somente para pessoas autorizadas; b) a integridade que protege a exatidão e a completeza (ou completude) da informação e dos métodos de processamento; c) a disponibilidade que assegura acesso à informação e ativos associados aos usuários autorizados, quando necessário.

Segundo Sêmola (2003) a informação possui quatro momentos distintos dentro de um ciclo de vida, nos quais fica exposta às ameaças que colocam em risco a confidencialidade, integridade e disponibilidade e que são identificados como:

a) Manuseio: momento em que a informação é criada e manipulada.
b) Armazenamento: momento em que a informação é armazenada.
c) Transporte: momento em que a informação é transportada.
d) Descarte: momento em que a informação é descartada.

Todos estes momentos essenciais do ciclo de vida da informação, e suas características, podem ser representados como na Figura 1, a seguir.

Figura 1- Requisitos da Segurança da Informação e o Ciclo de Vida da Informação



Fonte: Elaborado a partir de Sêmola (2003) e ISACA (2012b).

Em todas as etapas do ciclo de vida da informação, que são: a geração da informação, a utilização, o armazenamento, a transmissão e o descarte, a informação deve ser mantida de forma confidencial, precisa se manter íntegra, autêntica e confiável, estar disponível e ser irrefutável, mantendo sempre conformidade a regulatórios. Esses requisitos são especificamente pertinentes à proteção da informação e se complementam aos critérios da informação correta, precisa, completa, relação custo benefício adequada, flexível, relevante, simples, em tempo e verificável e eficaz (ISACA 2012b).

Dentre os principais requisitos da informação se destacam os seguintes:

a) Confidencialidade: diz respeito à proteção de informações sensíveis contra divulgação não autorizada (ISACA, 2012a) e que as informações devem ser protegidas de acordo com o grau de sigilo de seu conteúdo (SÊMOLA, 2003). Há informações públicas e privadas, porém nem todas as informações privadas precisam ser mantidas de forma confidencial.

b) Integridade: se refere à exatidão e completude das informações, bem como a sua validade, de acordo com os valores de negócios e expectativas (ISACA, 2012a), no sentido de proteger a exatidão e a completude dos ativos de informação (ISO/IEC 27000:2012, 2012), além dos caminhos pelos quais ela é processada (SÊMOLA, 2003). A integridade da informação pode ser perdida por erros de sistemas ou acesso indevido que venha de dentro ou de fora de uma organização. As consequências da perda de integridade envolvem uma decisão tomada com base em uma informação que perdeu a sua exatidão, que não é mais fidedigna.

c) Disponibilidade: visa garantir que a informação esteja disponível no exato momento em que for necessária. Diz respeito também à salvaguarda dos recursos necessários e capacidades associadas ao acesso a esta informação (ISACA, 2012a). Uma informação que não se mostra disponível quando se precisa dela pode gerar desde problemas na tomada de decisão até indisponibilidade de serviços. As informações são fundamentais para a redução do risco na tomada de decisão, por isso a possibilidade de não obter acesso às informações durante uma decisão pode comprometer o resultado dessa decisão. Há organizações do setor público que são essencialmente empresas de informação, tais como bancos públicos, fundações de pesquisas e estatísticas. Por exemplo, um cliente acessa o site da Receita Federal e os dados do seu imposto de renda não estão disponíveis. Esta situação fere a relação de prestação de serviços entre o governo e o cidadão, em virtude da indisponibilidade da informação.

d) Autenticidade: é a propriedade que indica que uma entidade é o que afirma ser (ISO/IEC 27000:2012, 2012). Desta forma, deve-se assegurar que uma informação é autêntica, o que envolve, segundo Sêmola (2003), o processo de identificação e reconhecimento formal da identidade dos elementos que entram em comunicação ou que são parte de uma determinada transação eletrônica, permitindo o acesso à informação com o devido controle.

e) Confiabilidade: indica a prestação de informação apropriada para as organizações operarem e exercerem suas responsabilidades fiduciárias e de governança (ISACA, 2012a). O critério da confiabilidade da informação garante a autoria das informações armazenadas nos Sistemas de Informação.

f) Conformidade: é o atendimento a um requisito (ISO/IEC 27000:2012, 2012a), o que significa, em um contexto de Segurança da Informação, que a informação deve ser mantida em conformidade com o regulatório a qual está sujeita em todo o ciclo de vida, ou seja, desde a sua geração até o seu descarte. A conformidade envolve aderência às leis, regulamentos e acordos contratuais e políticas externas às quais um determinado processo de negócio está sujeito. Entre os regulatórios, com os quais as organizações poderiam necessitar estar em conformidade, pode ser citada a Lei nº 12.527 (BRASIL, 2011) de acesso à informação. A conformidade, uma vez estabelecida, deve ser mantida em todo o ciclo de vida da informação, mostrando garantias de que a informação não é resultante de uma alteração indevida.

g) Irrefutabilidade: ocorre quando o remetente ou autor de uma informação não pode negar que a enviou ou que a gerou, constituindo uma forma estrita de autenticação e pode, por

exemplo, ser obtida mediante uma assinatura eletrônica (ISO/IEC 27000:2012). Desta forma, se constitui em um requisito prévio indispensável para a realização de muitas ações e serviços, como compras eletrônicas através da internet. Conhecida também como não-repúdio, garante a impossibilidade de negar a autoria em relação a uma transação anteriormente feita (ISO/IEC 27000:2012). Como, por exemplo, um documento liberado por algum órgão de governo deve ter sua autoria, sua responsabilidade técnica, autenticada de forma que não possa ser refutada.

Contudo, a ISO/IEC 27002:2005 (ABNT, 2005) indica que a Segurança da Informação é obtida a partir da colocação em prática de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Os controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde forem necessários, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos.

Não obstante, a ISO/IEC 27001 (ABNT, 2006) considera como ativo tudo que é relevante ao escopo do Sistema de Gestão de Segurança da Informação, ou seja, documentos em papel ou em softwares, hardwares, instalações, pessoas, serviços, inclusive a imagem e a reputação da organização. Segundo a norma NBR ISO/IEC 27002 (ABNT, 2005), a informação é um ativo, como qualquer outro ativo importante para os negócios, que possui valor para a organização e consequentemente necessita ser adequadamente protegida. Para a ISO/IEC 27002 (ABNT, 2005) os ativos de informação relevante são aqueles que podem materialmente afetar a entrega de um produto ou serviço devido à sua ausência ou deterioração, ou causar dano à organização através de perda de disponibilidade, integridade ou confidencialidade. A proteção desses ativos torna-se questão estratégica para as organizações, tanto pelo valor associado, quanto pelos impactos negativos que a destruição, a alteração ou a divulgação indevida ocasiona à organização.

Nesse contexto, a ISO/IEC 27002:2005 (ABNT, 2005) enfatiza que o SGSI (Sistema de Gestão de Segurança da Informação) deve ser implementado de acordo com as necessidades e porte da organização, em outras palavras uma organização simples requer um SGSI simples. O escopo e limites do SGSI precisam estar balizados pelos termos e características do negócio, da organização, da localização e dos ativos de tecnologia. Precisa incluir uma estrutura para definir objetivos e estabelecer um direcionamento global, além de abranger os princípios para as ações relacionadas à Segurança da Informação, considerando os requisitos de negócio, legais ou regulamentares. Contemplando também as obrigações de segurança contratuais e alinhamento com o contexto estratégico de gestão de risco da

organização, estabelecendo critérios em relação aos riscos que serão avaliados e por fim, definindo a abordagem de análise e avaliação de riscos da organização (ABNT, 2005).

2.1.1 Vulnerabilidade

Para Vance et al. (2012) a vulnerabilidade é a probabilidade de um incidente indesejado acontecer se não forem tomadas medidas preventivas. Já Albrechtsen e Hovden (2009) consideram os usuários de Sistemas de Informação uma vulnerabilidade quando esses usuários não estão preparados para utilizar os sistemas. Entretanto, Bulgurcu et al. (2010) afirmam que a vulnerabilidade é um estado importante que decorre de um funcionário que não segue a Política de Segurança da Informação (PSI) e para Kraemer et al. (2009), os erros humanos podem resultar em vulnerabilidades da Segurança da Informação. Segundo Warkentin e Willison (2009), as condições atuais de infraestrutura tecnológica e desenvolvimentos socioculturais contribuem para um ambiente cada vez mais turbulento e dinâmico para os Sistemas de Informação (SI) das organizações. Como esses Sistemas tornam-se cada vez mais globalizados e interligados, acabam confiando em controles automatizados e interligações via Internet, gerando vulnerabilidades crescentes nos sistemas e processos.

A vulnerabilidade na Segurança da Informação também pode ocorrer por erro humano devido à sobrecarga de trabalho, fadiga ou falta de atenção (LIGINLAL et al., 2009; ALBRECHTSEN, 2007; KRAEMER e CARAYON, 2007), que subsequentemente é explorada para fins maliciosos, com os incidentes resultantes sendo classificados como oriundos ao erro humano.

2.1.2 Percepção e Avaliação da Ameaça

A avaliação da ameaça pode abranger a gravidade percebida de uma violação de segurança (HERATH e RAO, 2009a) ou a probabilidade percebida de uma violação de segurança (HERATH e RAO, 2009b). A gravidade é o nível do impacto potencial da ameaça e o dano que ele pode causar, ou seja, a gravidade da falha de segurança e a possibilidade de evento negativo causado pela violação da segurança (VANCE et al., 2012). Herath e Rao (2009b) constataram que a percepção da gravidade da brecha da segurança não tem impacto sobre o cumprimento das normas ou políticas de segurança. Em contraponto, Workman, et al. (2008) descobriram que a severidade percebida foi significativa para o cumprimento, assim como a probabilidade da quebra de segurança. Johnston e Warkentin (2010) encontraram

indicativos que as percepções sobre a gravidade de uma ameaça influenciam negativamente nas percepções sobre a eficácia de resposta e também sobre as percepções de autoeficácia em relação à ameaça.

Segundo Liang e Xue (2010) a ameaça percebida é definida como o grau em que um indivíduo percebe uma Tecnologia da Informação mal intencionada como perigosa ou nociva. Os usuários de TI desenvolvem a percepção da ameaça, monitorando seu ambiente computacional e detectando perigos potenciais. Com base na psicologia da saúde e análise de risco, Liang e Xue (2010) propõem que a percepção da ameaça é formada por dois antecedentes: susceptibilidade percebida e a gravidade percebida.

A susceptibilidade percebida é definida por Liang e Xue (2010) como a probabilidade subjetiva de um indivíduo que uma Tecnologia da Informação mal intencionada (*malware*) vai afetá-lo negativamente, por outro lado a severidade percebida é definida como o grau em que um indivíduo percebe que consequências negativas causadas por um *malware* serão graves (LIANG e XUE, 2009). Conforme Liang e Xue (2010), estudos anteriores sobre o comportamento de proteção à saúde forneceram um embasamento teórico e empírico sobre o comportamento prudente dos pacientes, influenciado pelas percepções relativas à ameaça, que podem ser adaptados à área de Segurança da Informação. Os autores argumentam que a probabilidade percebida e as consequências negativas da gravidade de uma doença podem resultar na percepção de ameaça à saúde, o que motiva as pessoas a assumir ações de proteção à saúde.

Pesquisas de segurança de TI têm estudado a percepção a respeito da suscetibilidade e gravidade das ameaças, obtendo diversos resultados:

a) Ng et al. (2009) demonstraram que a susceptibilidade percebida afeta o comportamento dos usuários de em relação aos e-mails. Segundo os autores, quando os usuários estão conscientes da probabilidade das ameaças (suscetibilidade percebida) e da eficácia da segurança controles (benefícios percebidos), eles podem ter uma decisão consciente de realizar o comportamento apropriado. No entanto, a gravidade percebida não foi determinante no comportamento seguro dos usuários.
b) Johnston e Warkentin (2010) não conseguiram demonstrar que as percepções de susceptibilidade da ameaça influenciam negativamente as percepções de eficácia de resposta, nem que as percepções de susceptibilidade ameaça influenciam negativamente a percepção de autoeficácia. Entretanto, conseguiram demonstrar que as percepções da gravidade da ameaça influenciam negativamente as

percepções da eficácia de resposta e que as percepções da gravidade da ameaça influenciam negativamente percepções de autoeficácia.

c) Workman et al. (2008) revelam que tanto a vulnerabilidade percebida quanto a gravidade têm um efeito sobre os usuários em relação ao comportamento de Segurança da Informação.

d) Herath e Rao (2009b) sugerem que as percepções sobre a gravidade da violação, a eficácia de resposta e autoeficácia são susceptíveis a terem um efeito positivo sobre as atitudes em relação a políticas de segurança, enquanto que o custo de resposta influencia negativamente as atitudes favoráveis. Também sugerem que a influência social tem um impacto significativo sobre as intenções de cumprimento da PSI (Política de Segurança da Informação) e a disponibilidade de recursos é um fator significativo no aumento da autoeficácia que, por sua vez, é um importante preditor de intenções de conformidade com as Políticas de Segurança da Informação. Além disso, o comprometimento organizacional desempenha um duplo papel tendo impacto direto nas intenções, bem como na promoção da crença que as ações dos funcionários têm um efeito global sobre a Segurança da Informação de uma organização de (HERATH e RAO, 2009b).

Apesar da diferença entre os resultados, o consenso entre os pesquisadores é que os usuários avaliam a susceptibilidade e a gravidade de consequências negativas para determinar a ameaça à segurança que eles estão enfrentando. Assim, Liang e Xue (2010) propõem que tanto a suscetibilidade quanto a gravidade contribuem para a percepção de ameaça.

2.1.3 Malware

Segundo Lee e Larsen (2009), *malware* é um programa malicioso projetado para se transferir de forma autônoma de computador para computador, com o objetivo de extrair informações ou modificar intencionalmente os sistemas de computador sem o consentimento do proprietário ou operador. Para Lee e Larsen (2009) o *malware* evoluiu e é atualmente considerado a fonte mais comum e perigosa de ataques cibernéticos.

Para Chen et al. (2012), *malware* são softwares maliciosos que são especialmente projetados para se transferir de forma autônoma de um software para outro, com o objetivo de extrair informações ou modificar intencionalmente os sistemas de um dispositivo de Tecnologia da Informação, sem o consentimento do usuário, comprometendo a confidencialidade, integridade e disponibilidade dos sistemas de computação infectados. Segundo Shahzad et al. (2013), um *malware*, com o intuito de prolongar a sua vida útil, não

só ofusca o seu código com técnicas de criptografia, mas também recorre ao polimorfismo. Os softwares maliciosos classificados com *malware* incluem, mas não estão limitados a:

a) *Vírus*: software malicioso que se replica de forma autônoma, anexando-se a outro software do mesmo dispositivo de TIC ou de outros dispositivos, sem deixar vestígios óbvios da sua presença (WORKMAN et al., 2013).

b) *Computer worm*: software malicioso que se replica e propaga de forma autônoma para outros dispositivos de TIC de forma independente e autossuficiente, utilizando mecanismos da rede de computadores. Ao contrário de um vírus, não precisa se anexar a um programa existente, sendo utilizados, por exemplo, para instalar *backdoors* ou enviar arquivos via e-mail de forma autônoma e sem deixar vestígios claramente perceptíveis (WORKMAN et al., 2013).

c) *Trojan*: também conhecido como *horse trojan*, ou cavalo de Tróia, é um software malicioso que aparenta possuir uma função útil, mas possui funções ocultas potencialmente danosas (COLE, 2009). Age burlando os mecanismos de segurança dos dispositivos de TIC através de uma autorização legítima para a sua execução, muitas vezes fornecida pelo próprio usuário (WORKMAN et al., 2013).

d) *Bot*: processo automatizado que interage com outros serviços de uma rede de computadores e dispositivos de TIC. Frequentemente automatizam tarefas e fornecem informação ou serviços. Entretanto podem ser também um *malware* projetado para se autopropagar e infectar dispositivos de TIC, permitindo o controle remoto desse dispositivo de forma perceptível ou não, incluindo-o em uma rede denominada *botnet* (COLE, 2009). Através de uma *botnet* os hackers conseguem lançar ataques remotos sincronizados e massivos contra sites na internet, utilizando dispositivos de terceiros, sem que sejam claramente percebidos pelos usuários desses dispositivos. Além da capacidade de se autopropagar, *bots* podem incluir a capacidade de registrar as teclas digitadas pelo usuário (*keylogger, keystroke logging*), obter senhas, capturar e analisar a comunicação de rede, recolher informações financeiras, lançar ataques de negação de serviço em sites, enviar spam e instalar backdoors no dispositivo hospedeiro infectado (VACCA, 2009).

e) *Spyware*: software malicioso que é instalado secretamente ou sub-repticiamente em um sistema de informação, com o objetivo de reunir informações sobre os usuários ou organizações sem o seu conhecimento (VACCA, 2009). Uma forma popular de *spyware* utilizado na atualidade é o denominado *tracking cookie* que permite rastrear a navegação de um usuário a partir de um site onde ele se identificou primariamente (WORKMAN et al., 2013).

Alguns tipos de *malwares* podem instalar um *backdoor*, também conhecido como *back door*, produzindo uma vulnerabilidade na Segurança da Informação, que poderá ser explorada por demais hackers (COLE, 2009). O *backdoor* é uma forma irregular de acessar um Sistema de Informação, ignorando os mecanismos normais de autenticação e podem ser colocado no software pelo próprio programador do software (TIPTON e KRAUSE, 2007), ou através de uma vulnerabilidade do sistema, tal como um *vírus* ou um *worm* (VACCA, 2009). Normalmente os hackers utilizam o *backdoor* para facilitar o acesso continuo a um sistema após a segurança ter sido comprometida (VACCA, 2009).

Muitos *malwares* são instalados através de *phishing*, que é uma forma de enganar os usuários na busca de suas informações pessoais, utilizando meios enganosos (WORKMAN et al., 2013). Segundo os autores, o *phishing* começa com uma isca, normalmente uma mensagem de spam que parece ser de um banco legítimo ou empresa de comércio eletrônico. A mensagem instiga o leitor a visitar um site fraudulento, que finge ser legítimo. O site fraudulento tenta replicar ao máximo a aparência do site legítimo. Dessa forma, as vítimas são induzidas a fornecer informações pessoais valiosas (VACCA, 2009). Outra forma de *malware* envolvendo sites são os *cross-site scripting* (XSS), encontrados normalmente em aplicações web mal-intencionadas que injetam *scripts* dentro das páginas web visitadas pelos usuários (GROSSMAN et al., 2007). O *cross-site scripting (*XSS) pode executar uma programação maliciosa no navegador do usuário, enquanto o navegador está conectado a um site confiável, o que pode ocorrer se, por exemplo, um atacante consegue instalar uma propaganda infectada ou um link nesse site confiável, ou também através do envio de um e-mail (WORKMAN et al., 2013).

Segundo Chen et al. (2012), um crescimento espantoso de *malwares* ocorreu na internet na última década, com o objetivo de comprometer a confidencialidade, integridade e disponibilidade dos sistemas de computação infectados.

2.2 TEORIAS COMPORTAMENTAIS APLICADAS AO TEMA E FOCO DA PESQUISA

Apesar do uso de tecnologias que visam à garantia da Segurança da Informação pelas organizações, essas tecnologias não são suficientes para evitar brechas e por isso a área de pesquisa do comportamento de usuários relativos à segurança (*Information Security Behavior*) ganhou uma maior atenção (HERATH e RAO, 2009b). Segundo os autores, o comportamento em relação à segurança pode ser influenciado por motivações intrínsecas e extrínsecas. As pressões exercidas por normas subjetivas e comportamentos de demais colegas influenciam

nos comportamentos dos usuários na área da Segurança da Informação. Várias das abordagens comportamentais atuais, aplicadas à Segurança da Informação, recorrem a teorias de criminologia e psicologia, como, por exemplo, a teoria da dissuasão, técnicas de neutralização e sócio-cognitiva (VANCE et al., 2012). As teorias comportamentais, aplicadas à Segurança da Informação e utilizadas nessa pesquisa, e seus principais conceitos, serão sucintamente descritas a seguir. O Quadro 1 resume os principais conceitos obtidos a partir de cada teoria abrangida nesse tópico, que serão explicados posteriormente.

Quadro 1 - Conceitos utilizados provenientes de teorias e áreas de pesquisas comportamentais

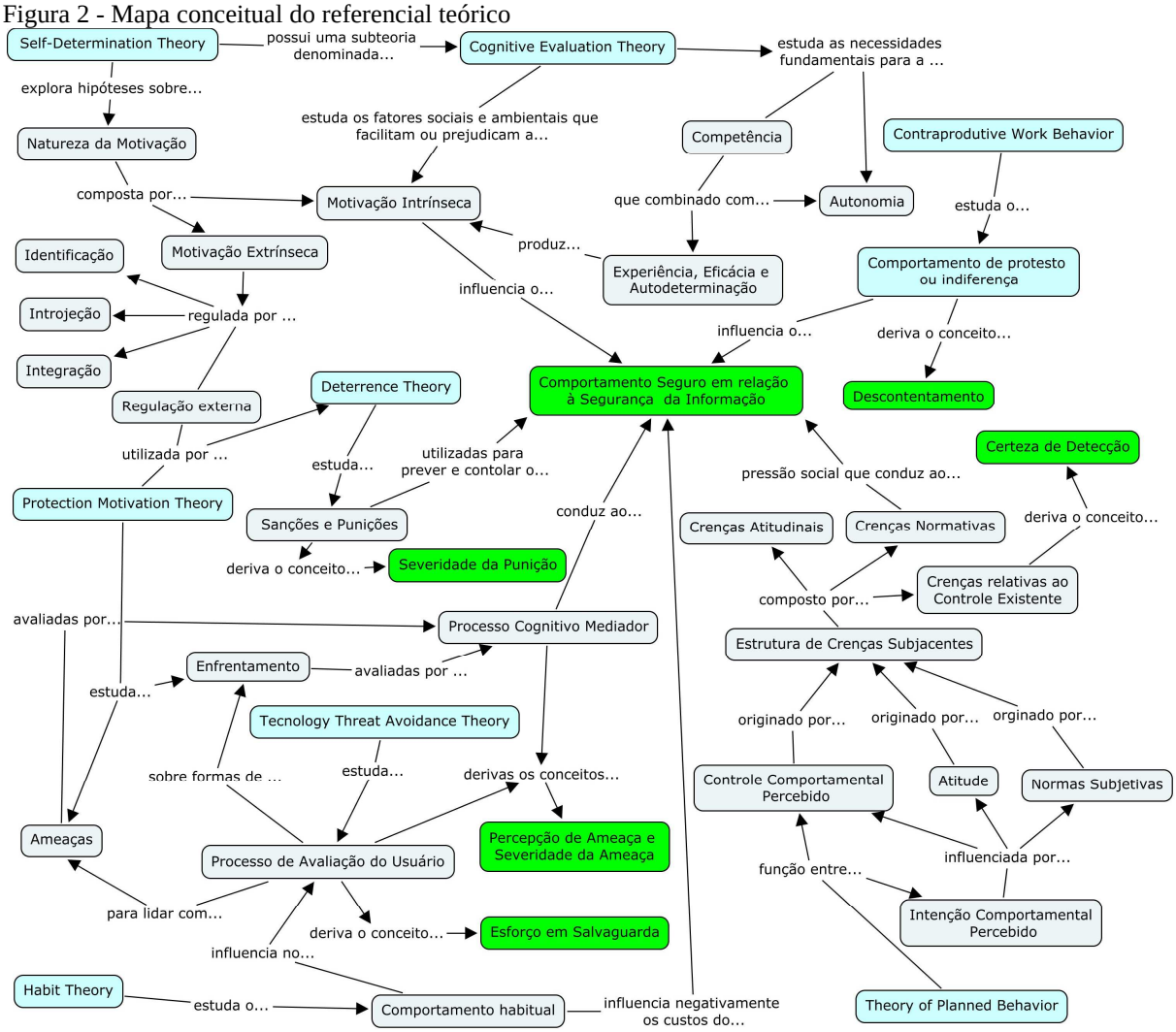
Teoria	Resumo dos conceitos aplicados à pesquisa
Self-Determination Theory	Componentes da motivação no cumprimento das orientações oriundas da Política da Segurança da Informação, que podem ser influenciados por motivadores intrínsecos e extrínsecos (BULGURCU et al., 2010; SIPONEN, 2000).
Cognitive Evaluation Theory	Recompensas intrínsecas e extrínsecas irão aumentar a probabilidade de uma resposta inadequada ao passo que a percepção da gravidade e a percepção de vulnerabilidade às ameaças diminuirá a probabilidade de tal resposta (VANCE et al. 2012).
Protect Motivation Theory	Aborda os processos, avaliação de ameaça e avaliação de enfrentamento. O primeiro refere-se ao grau em que um indivíduo se sente ameaçado, enquanto o segundo refere-se à eficácia da resposta na remoção da ameaça (HERATH e RAO, 2009b).
Deterrence Theory	O comportamento inadequado pode ser controlado pela ameaça de sanções que forem inevitáveis, severas e céleres, e tem sido utilizada para prever o comportamento dos usuários que são favoráveis ou desfavoráveis a segurança de Sistemas de Informação (D'ARCY e HERATH, 2011).
Habit Theory	O hábito de cumprir a orientação sobre Segurança da Informação, contidas no PSI, diminui a importância das recompensas pelo cumprimento e dos custos de resposta, como por exemplo, o tempo perdido para cumpri-la (VANCE et al., 2012)
Theory of Planned Behavior	O comportamento é uma função da intenção comportamental e do controle comportamental percebido. A intenção comportamental, por sua vez, é influenciada pela atitude em relação ao comportar-se, pelas normas subjetivas e pelo controle comportamental percebido. Os determinantes da intenção que seriam a atitude, as normas subjetivas e o controle comportamental percebido; são determinados pela estrutura de crenças subjacentes: crenças atitudinais, normativas e de controle (BULGURCU et al., 2010).
Tecnology Threat Avoidance Theory	Os usuários ao decidirem como lidar com ameaças de TI passam por dois processos cognitivos, avaliação da ameaça e avaliação das formas de enfrentamento da ameaça. Na avaliação da ameaça, os usuários percebem a ameaça à qual estão suscetíveis e avaliam se as consequências negativas serão severas. A percepção de ameaça leva à avaliação de enfrentamento, nos quais os usuários avaliam o grau em que a ameaça à TI pode ser evitada, tomando medidas de salvaguarda baseadas na eficácia percebida, nos custos da medida de salvaguarda e na autoeficácia da adoção da medida de salvaguarda (LIANG e XUE, 2009).
Counterproductive Work Behaviors	Comportamento intencional, por parte de um membro da organização, visto pela organização como contrário aos seus interesses legítimos, com o objetivo de causar danos em represália à injustiça ou desencadeada por condições ambientais e estressoras (GRUYS e SACKETT, 2003).

Fonte: Autor

Nos próximos tópicos serão apresentadas de uma forma mais detalhada os conceitos e teorias apresentadas no Quadro 1.

A Figura 2 apresenta um mapa de conceitos aplicados à presente pesquisa. As teorias apresentadas nesse mapa não se restringem aos conceitos apresentados. No entanto, com o intuito de simplificar o mapa conceitual, foram indicados apenas os relacionamento das Teorias e conceitos com os construtos (conceitos) do modelo teórico desta pesquisa. O detalhamento sobre cada conceito e sua referência consta no decorrer do referencial teórico desta pesquisa.

Figura 2 - Mapa conceitual do referencial teórico



Fonte: Autor

2.2.1 Teoria da Autodeterminação

A Teoria da Autodeterminação (*Self-Determination Theory* - STD), proposto por Deci e Ryan em 1985 (RYAN e DECI, 2000) explora a hipótese sobre a natureza da motivação, que pode ser aplicada à Segurança da Informação, permitindo compreender os aspectos e

componentes da motivação no cumprimento das orientações oriundas da Política da Segurança da Informação.

De acordo com Herath e Rao (2009b) os comportamentos de segurança podem ser influenciados por motivadores intrínsecos e extrínsecos. Pressões exercidas por normas subjetivas e comportamentos de colegas influenciam o comportamento de funcionários em relação à Segurança da Informação. Segundo os autores, a motivação intrínseca e a eficácia percebida das ações de um usuário de Sistemas de Informação desempenham um papel importante nas intenções do cumprimento da política de segurança. Em relação às sanções pelo não cumprimento das normas da Segurança da Informação, Herath e Rao (2009b) sugerem que a certeza da detecção do não cumprimento é um fator significativo sobre as intenções de comportamento na área de Segurança da Informação, assim como a severidade da punição.

Segundo Ryan e Deci (2000), a motivação intrínseca é a inclinação natural para a assimilação, o domínio, o interesse espontâneo e a exploração que é tão essencial para o desenvolvimento cognitivo e social e representa a principal fonte de prazer e vitalidade ao longo da vida. Para Herath e Rao (2009b) a motivação intrínseca desempenha um papel importante nas intenções de cumprimento das normas da Segurança da Informação. No entanto, apesar do fato dos seres humanos serem dotados de tendências intrínsecas de motivação, a valorização desta propensão inerente requer condições favoráveis, assim como pode ser prontamente interrompido por condições desfavoráveis. Contudo, a teoria da motivação intrínseca não diz respeito ao que é realizado com a motivação intrínseca, mas examina as condições que provocam e a sustentam, bem como o que diminui esta propensão inata (RYAN e DECI, 2000).

Segundo Ryan e Deci (2000) a desmotivação pode resultar da falta de competência ou da falta da valorização adequada para alguma atividade. No contexto da Segurança da Informação, um indivíduo pode estar desmotivado para cumprir a segurança por receber uma sobrecarga de informação técnica para a qual não possui competência para compreender (ALBRECHTSEN e HOVDEN, 2009).

Conforme Ryan e Deci (2000) a motivação intrínseca é um tipo importante de motivação, porém não é o único tipo de motivação, ou até mesmo o único tipo autodeterminado de motivação. Muitas pessoas não são, estritamente, intrinsecamente motivadas, especialmente após a infância, quando a liberdade de ser intrinsecamente motivado é cada vez mais reduzida por pressões sociais para a realização de atividades que não são interessantes e para assumir uma variedade de novas responsabilidades.

Para Ryan e Deci (2000) a verdadeira questão sobre as práticas de motivação não intrínsecas está na forma como os indivíduos adquirem a motivação para realizá-las e como isso afeta a motivação para a persistência contínua, para a qualidade do comportamento e para o bem-estar. Sempre que uma pessoa tenta incentivar determinados comportamentos em outros, a motivação dos outros para o comportamento pode variar de falta de vontade, para cumprimento de forma passiva e posteriormente para compromisso pessoal ativo. De acordo com a SDT, essas motivações diferentes refletem diferentes graus em que o valor e a regulação do comportamento solicitado foram internalizados e integrados. A internalização refere-se às pessoas "tomarem para si" a um valor ou regulamento, e a integração refere-se à transformação adicional daquela regulação em algo do próprio indivíduo e emanado por ele (RYAN e DECI, 2000).

A motivação extrínseca refere-se ao desempenho de uma atividade a fim de alcançar algum resultado à parte e, portanto, contrasta com a motivação intrínseca, que se refere a fazer uma atividade para a satisfação inerente à própria atividade (RYAN e DECI, 2000). Ao contrário de algumas perspectivas que veem o comportamento extrinsecamente motivado como invariavelmente não autônomo, a SDT propõe que a motivação extrínseca pode variar muito em sua autonomia relativa. Por exemplo, os estudantes que fazem o dever de casa porque pessoalmente compreendem o seu valor para a carreira escolhida são motivados extrinsecamente.

2.2.2 Teoria Cognitiva de Avaliação (CET)

A Teoria da Avaliação Cognitiva, CET na sigla em inglês de *Cognitive Evaluation Theory*, foi apresentada por Deci e Ryan em 1985 (RYAN e DECI, 2000) como uma subteoria dentro da SDT (*Self-Determination Theory*) que tinha o objetivo de especificar fatores que explicam a variabilidade na motivação intrínseca. A CET é focada em fatores sociais e ambientais que facilitam ou que minam a motivação intrínseca. Segundo essa teoria, a motivação intrínseca é inerente ao ser humano e será catalisada quando os indivíduos estão em condições que conduzem em direção à sua expressão pessoal. O estudo das condições que facilitam e dificultam a motivação intrínseca é importante para a compreensão de aspectos que alienam ou libertam dos aspectos positivos da natureza humana (RYAN e DECI, 2000).

A CET estuda as necessidades fundamentais para a competência e autonomia, sendo formulada para integrar os resultados de experiências de laboratório iniciais sobre os efeitos das recompensas, opinião, e outros eventos externos sobre a motivação intrínseca (RYAN e DECI, 2000). Essa Teoria argumenta que eventos sócio-contextuais, como por exemplo,

opinião, comunicação e recompensas, conduzem para sentimentos de competência e podem aumentar a motivação intrínseca para a ação. Assim, os desafios ideais, o desejo de sentir-se eficiente e a ausência de avaliações humilhantes são conceitos que facilitam a motivação intrínseca. Estudos demonstraram que a opinião a respeito do desempenho positivo produz maior motivação intrínseca, enquanto a opinião sobre o desempenho negativo a diminuiu (RYAN e DECI, 2000).

A CET especifica ainda que o sentimento de competência não aumentará a motivação intrínseca se não forem acompanhados por um sentimento de autonomia. Assim, de acordo com a CET, além de experiência, competência e eficácia, as pessoas precisam de autodeterminação para produzir motivação intrínseca. No entanto, a maior parte da pesquisa sobre os efeitos dos eventos ambientais em motivação intrínseca se concentram na questão da autonomia versus um controle melhor, do que em relação à competência (DECI et al., 1999).

Segundo Vance et al. (2012), as recompensas intrínsecas e extrínsecas irão aumentar a probabilidade de uma resposta inadequada, ao passo que a percepção da gravidade e a percepção de vulnerabilidade às ameaças diminuirá a probabilidade de tal resposta. Recompensas indicam prazer físico ou psicológico ou aprovação dos colegas, o que aumenta a probabilidade de uma resposta adequada. Se um indivíduo percebe que a recompensa por não adotar a resposta de enfrentamento é maior do que adotá-lo ele será menos propenso a adotar a resposta de enfrentamento. Mesmo assim, para Vance et al. (2012), a recompensa é um mecanismo que estimula a conformidade e a sanção, além de ser um aspecto que desencoraja o descumprimento.

A pesquisa de Deci et al. (1999) revelou que não apenas as recompensas tangíveis, mas também ameaças, prazos, diretrizes, avaliações e metas impostas diminuem a motivação intrínseca. Por outro lado, o reconhecimento pelos indivíduos de suas escolhas e dos sentimentos e oportunidades geradas por elas foram aspectos que aumentaram a motivação intrínseca, porque forneceram um maior sentimento de autonomia (DECI e RYAN, 1999).

De acordo com a SDT, a motivação extrínseca é regulada por quatro conceitos resumidos a seguir:

a) A regulação externa, que garante que os comportamentos são satisfeitos pela aplicação de uma demanda externa, incluindo controles e incentivos, tal como as recompensas, que influenciam os funcionários dispostos a seguir as orientações da Política de Segurança da Informação (VANCE et al., 2012);
b) A introjeção, que ocorre quando as pessoas se sentem pressionadas a executar ações apenas para evitar a ansiedade ou manter o seu ego (RYAN e DECI, 2000),

Nesse sentido, pode estar associado com o clima social de uma organização, pois o clima social relaciona-se com a cultura de segurança em geral, que inclui comportamentos demonstrados pela diretoria e colaboradores (LEACH, 2003). Tais comportamentos, como por exemplo, práticas de gestão, práticas de supervisão de superiores diretos e práticas de socialização de colega de trabalho, também podem motivar um indivíduo a cumprir a Política de Segurança da Informação (CHAN et al., 2005);

c) A identificação, que ocorre quando um indivíduo se identifica com a importância individual de um comportamento (RYAN e DECI, 2000).
d) A integração, que é a forma mais autônoma de regulação extrínseca, ela ocorre através da introspecção dos regulamentos, sendo assimilada conjuntamente com a hierarquia dos valores e necessidades (RYAN e DECI, 2000).

Dentre as teorias que utilizam a regulação externa, e que foram aplicadas em pesquisas na área da Segurança da Informação na última década, encontram-se a *Deterrence Theory* (WILLISON e WARKENTIN, 2013) e a PMT (*Protect Motivation Theory*)(VANCE et al., 2012), que são apresentada a seguir.

2.2.3 Teoria da Dissuasão

De acordo com D'Arcy e Herath (2011), a Teoria da Dissuasão (*Deterrence Theory*) é uma das teorias mais amplamente aplicada em Sistemas de Informação no âmbito comportamental relativos à segurança. Com base na visão da escolha racional do comportamento humano, a teoria prevê que o comportamento inadequado pode ser controlado pela ameaça de sanções que forem inevitáveis, severas e céleres, e tem sido utilizada para prever o comportamento dos usuários que são favoráveis ou desfavoráveis a segurança de Sistemas de Informação.

Segundo Bulgurcu et al. (2010) sanções são penalidades tangíveis ou intangíveis, como rebaixamentos, perda de reputação, reprimendas, penalizações monetárias ou não monetárias, ou menções desfavoráveis em relatórios de avaliação oral ou escrita, que ocorrem quando o empregado não cumpre as exigências da PSI (Política de Segurança da Informação). Herath e Rao (2009b) surpreenderam-se ao descobrir que nem as sanções e tampouco as recompensas têm um impacto significativo sobre o cumprimento das normas ou políticas de segurança, sendo mais importante a certeza da detecção. A menor ênfase na severidade da sanção coincide com a SDT (RYAN e DECI, 2000) e com o estudo de Bulgurcu et al. (2010), o qual conclui que as crenças relativas à autoeficácia e as crenças normativas tem um efeito

mais significativo sobre a intenção de cumprimento, quando comparado à severidade das sanções. Para Puhakainen e Siponen (2010), um objetivo chave nos treinamentos em Segurança da Informação para os funcionários de uma organização deve ser a comunicação das sanções que podem ocorrer em caso de descumprimento da política de segurança, bem como a revisão dessas políticas de segurança.

Em geral, a dissuasão é definida como o efeito preventivo que a punição ou ameaça tem em potenciais infratores (SIPONEN e VANCE, 2010). A Teoria da Dissuasão é baseada na certeza de detecção, severidade da punição e a rapidez da punição, como fatores que afetam a decisão de um indivíduo a respeito da segurança, impedindo-o de se expor a ameaças (HERATH e RAO, 2009b). Um dos conceitos da Teoria da Dissuasão envolve dissuadir usuários que estejam em não conformidade com obrigações relativas à segurança, forçando-os a cumprir as condições impostas (HERATH e RAO, 2009a). Nesse sentido, D'Arcy e Hovav (2009) estudaram as contramedidas que impedem o mau uso de Sistemas de Informação, considerando quatro fatores: o conhecimento das políticas de segurança, o monitoramento, os softwares de prevenção e o treinamento; e concluíram que esses fatores evitam o mau uso e promovem comportamentos de segurança compatíveis com os níveis atuais e desejáveis de segurança nas organizações.

Harrington (1996) descobriu que os códigos de ética são considerados como um tipo de sanção formal e que dentro de uma organização não afetam o julgamentos dos empregados ou intenções de cometer abusos relativos a Sistemas de Informação. No entanto, há códigos de ética genéricos que afetavam os empregados e que foram considerados na negação de responsabilidade. Da mesma forma, segundo Harrington (1996), códigos de ética específicos da área de Sistemas de Informação não afetam o julgamento ou intenções, exceto no caso de sabotagem de computadores, ou um tipo grave de abuso de computador. Assim, os efeitos dos códigos de ética foram considerados esporádicos e fracos.

Herath e Rao (2009b) ao testarem os efeitos de dissuasão, descobriram que a certeza da detecção tem um impacto positivo sobre as intenções de conformidade com a política de segurança. Se os funcionários percebem que há alta probabilidade de serem pegos ao violar as políticas de segurança, eles serão mais propensos a seguir as políticas de segurança. Para Herath e Rao (2009b) é provável que a existência e a visibilidade de mecanismos de detecção sejam mais importantes que a severidade da sanção imposta.

O colaborador de uma organização precisa não apenas ser influenciada por um ambiente propício de Segurança da Informação, mas também deve possuir as habilidades para

executar as ações necessárias (CHAN et al., 2005), por isso ter habilidades de trabalho apropriadas é um requisito necessário para cumprir as determinações (SIPONEN, 2000).

2.2.4 Teoria da Motivação para a Proteção

A Teoria da Motivação para a Proteção, ou PMT na sigla em inglês para *Protect Motivation Theory*, tem sido utilizado por diversos estudos para examinar o comportamento de segurança compatível (HERATH e RAO, 2009b; VANCE et al., 2012). A PMT evoluiu a partir da avaliação cognitiva de dois processos, avaliação de ameaça e avaliação de enfrentamento. O primeiro refere-se ao grau em que um indivíduo se sente ameaçado, enquanto o segundo refere-se eficácia da resposta na remoção da ameaça (HERATH e RAO, 2009b).

Segundo Vance et al. (2012) a PMT explica as motivações das reações dos usuários aos avisos sobre ameaças ou comportamentos perigosos, denominados apelos ao medo. Na interpretação de tais avisos, as pessoas usam um processo cognitivo de comparar a suas possíveis reações à ameaça.

A PMT inclui três fatores que explicam como as ameaças são percebidas e avaliadas, que são:

a) As recompensas ou benefícios, que correspondem a qualquer motivação intrínseca ou extrínseca para aumentar ou manter um comportamento indesejado;
b) A gravidade, que equivale à magnitude da ameaça;
c) A vulnerabilidade, que se refere à percepção de suscetibilidade da ameaça (NG et al., 2009).

Conforme Vance et al. (2012) a PMT também inclui três fatores que explicam a capacidade do indivíduo de lidar com a ameaça, chamadas avaliações de enfrentamento, que são:

a) A eficácia de resposta, que corresponde à crença dos benefícios percebidos a partir da ação de enfrentamento e da eliminação da ameaça;
b) O custo de resposta para o indivíduo na implementação do comportamento protetor;
c) A autoeficácia, na medida em que o indivíduo acredita que é possível implementar um comportamento de proteção.

A PMT sugere que a informação sobre uma ameaça provoca um processo cognitivo mediador que avalia as possíveis respostas positivas ou negativas. Por exemplo, se os usuários não percebem um *spyware* como uma ameaça, eles podem optar por não instalar um *anti-*

spyware, embora o considerem eficaz para combater spyware e fácil de utilizar (LIANG e XUE, 2009). Portanto a percepção da ameaça é crucial para o comportamento do usuário em termos de Segurança da Informação.

2.2.5 Tecnology Threat Avoidance Theory (TTAT)

Segundo Liang e Xue (2009) a TTAT explica os comportamentos individuais dos usuários de TI na tentativa de evitar as ameaças de Tecnologias de Informação maliciosas (*malware*). Os autores articulam que evitar e adotar são dois fenômenos qualitativamente diferentes e afirmam que as teorias de aceitação de tecnologias fornecem uma valiosa, mas incompleta, compreensão do comportamento dos usuários de TI ao evitar uma ameaça.

Segundo a TTAT os usuários ao decidirem como lidar com ameaças de TI passam por dois processos cognitivos: a avaliação da ameaça e a avaliação das formas de enfrentamento da ameaça. Na avaliação da ameaça, os usuários percebem a ameaça à qual estão suscetíveis e avaliam se as consequências negativas serão severas. A percepção de ameaça leva à avaliação de enfrentamento, na qual os usuários avaliam o grau em que a ameaça à TI pode ser evitada, tomando medidas de salvaguarda baseadas na eficácia percebida, nos custos da medida de salvaguarda e na autoeficácia da adoção da medida de salvaguarda. A TTAT propõe que os usuários são motivados a evitar *malwares* quando percebem uma ameaça e acreditam que a ameaça é evitável através de medidas de salvaguarda. Por outro lado, se os usuários acreditam que a ameaça não pode ser totalmente evitada tomando as medidas de salvaguarda, optam pelo enfrentamento focado na emoção (LIANG e XU, 2009).

2.2.6 Teoria do Hábito

Segundo Vance et al. (2012) a Teoria do Hábito (*Habit Theory*) sugere que muitas ações ocorrem sem a decisão consciente de agir e são realizadas porque os indivíduos estão acostumados a realizá-las. O comportamento frequentemente repetido é controlado mais por estímulos situacionais do que pela tomada consciente de decisão. Além disso, propõe que o início de um novo padrão de comportamento exige uma decisão consciente e que o novo comportamento irá gradualmente se tornar automático.

Vance et al. (2012) defende que o comportamento habitual para cumprir as normas das políticas de segurança tem uma influência negativa no custo de resposta e recompensas, pois praticar o hábito de cumprir a Política de Segurança da Informação diminui tanto as recompensas pelo cumprimento, quanto os custos de resposta, como por exemplo, o tempo

perdido para cumpri-la. Por sua vez, praticar o hábito de cumprir a Política de Segurança da Informação terá uma influência positiva sobre a mitigação da gravidade, a autoeficácia, a eficácia de resposta e a vulnerabilidade.

2.2.7 Theory of Planned Behavior (TPB)

De acordo com Venkatesh et al. (2003) a Teoria do Comportamento Planejado (*Theory of Planned Behavior* - TPB) é uma extensão do TRA, adicionando o conceito de controle comportamental percebido. Na TPB o controle comportamental percebido é um determinante adicional da intenção do comportamento. Ajzen (1991) apresentou uma revisão de vários estudos que utilizaram com sucesso a TPB para prever a intenção do comportamento em uma ampla variedade de situações. A TPB tem sido aplicada com sucesso na compreensão da aceitação individual e uso de diferentes tecnologias. A TPB foi proposta por Ajzen como uma extensão à Teoria da Ac□ão Racional (FISHBEIN e AJZEN, 1975) para situações em que os indivíduos não têm controle completo sobre o seu comportamento.

A TPB acrescenta um condicionante da intenção comportamental e da atitude em relação ao comportamento, que é o controle comportamental percebido. O controle comportamental percebido reflete as percepções do indivíduo sobre os limites internos ou externos ao comportar-se, podendo ser definido mais formalmente como a facilidade ou dificuldade percebida por um indivíduo em se comportar de determinada maneira (AJZEN, 1991).

Na TPB, o comportamento é uma função da intenção comportamental e do controle comportamental percebido. A intenção comportamental é influenciada pelos seguintes aspectos: a atitude em relação ao comportamento, as normas subjetivas e o controle comportamental percebido. Segundo a TPB, os determinantes da intenção são: a atitude, as normas subjetivas e o controle comportamental percebido; que são originados pela estrutura de crenças subjacentes, que por sua vez, são compostas por: crenças atitudinais, crenças normativas e crenças relativas ao controle existente (BULGURCU et al., 2010). Workman et al. (2008), argumenta que Ajzen combinou na teoria do comportamento planejado, o lócus de controle e a autoeficácia em um único conceito e denominou de controle comportamental percebido.

Bulgurcu et al. (2010) resumem as crenças normativas com a pressão social percebida pelo usuário a respeito da conformidade com os requisitos da Política de Segurança da Informação, sendo a pressão social ocasionada pela expectativa de comportamento de pessoas consideradas importantes para o usuário, como executivos, colegas e gerentes. Em sua

pesquisa demonstraram que a intenção do empregado de cumprir com o PSI (Política de Segurança da Informação) é significativamente influenciada pela atitude, pelas crenças normativas e pela autoeficácia para cumpri-la. As crenças nos resultados afetam significativamente as crenças sobre avaliação global das consequências e essas, por sua vez, afetam de forma significativa a atitude de um funcionário. Além disso, a Conscientização da Segurança da Informação, ou ISA na sigla em inglês para *Information Security Awareness*, afeta positivamente tanto a atitude quanto as crenças de resultado.

Com base na TPB, Bulgurcu et al. (2010) identificaram os antecedentes de cumprimento da Política de Segurança da Informação (PSI) de uma organização, investigando os fatores que impulsionam racionalmente um funcionário a cumprir os requisitos do PSI e argumentam que, junto com a crença normativa e autoeficácia, a atitude de um funcionário para o cumprimento determina a intenção de cumprir com o PSI, sendo que a atitude é influenciada pelo benefício de conformidade, custos de conformidade e custo de não-conformidade. Segundos autores, estes benefícios e custos são crenças sobre a avaliação global das consequências do cumprimento ou descumprimento das orientações da PSI, e sugerem que essas crenças são moldadas por crenças resultantes dos eventos consecutivos a conformidade ou não-conformidade. Para os autores, o benefício do cumprimento é moldado por benefício intrínseco à segurança dos recursos e as recompensas, enquanto que o custo de conformidade é moldado pelo impedimento do trabalho. O custo do descumprimento é formado pelo custo intrínseco, pela vulnerabilidade dos recursos e pelas sanções. Os autores investigaram também o impacto da conscientização da Segurança da Informação em crenças resultantes e na atitude de um funcionário em acordo com o PSI. Os resultados mostraram que a intenção do empregado de cumprir as orientações sobre Segurança da Informação abrangidas no PSI é significativamente influenciada pela atitude, crenças normativas e autoeficácia em cumpri-la. As crenças nos resultados afetam significativamente as crenças sobre avaliação global de consequências e elas, por sua vez, afetam de forma significativa a atitude de um funcionário. Além disso, a Conscientização em Segurança da Informação afeta positivamente tanto a atitude quanto as crenças de resultados (BULGURCU et al., 2010).

2.2.8 Comportamento Contraproducente no Trabalho

Gruys e Sackett (2003) combinam várias pesquisas para sintetizar o Comportamento Contraproducente no Trabalho, CWB na sigla em inglês para *Counterproductive Work Behaviors*, como qualquer comportamento intencional por parte de um membro da organização visto pela organização como contrário aos seus interesses legítimos. Para os

autores, o foco do CWB é o comportamento em si e não nos resultados ou consequências desse comportamento e somente os comportamentos intencionais estão incluídos nesta definição, pois as ações acidentais que podem causar danos não fazem parte do conceito do CWB. A definição engloba comportamento que é destinado a outros funcionários ou a organização, pois os dois tipos de ações podem ter consequências graves sobre a organização. O foco do CWB não inclui pessoas de fora da organização, como por exemplo, clientes ou ex-funcionários.

Conforme Gruys e Sackett (2003) o domínio do CWB é bastante amplo, sendo que no início dos anos 1980 foi realizada uma quantidade considerável de pesquisas sobre comportamentos individuais contraproducentes no local de trabalho, tais como o roubo do empregado, furto, sabotagem, desempenho lento e desleixado, atrasos e absenteísmo.

Para Spector et al. (2006) o Comportamento Contraproducente no Trabalho consiste em atos intencionais por parte dos funcionários com o objetivo de causar danos às organizações ou a suas partes interessadas, podendo incluir desde violência física contra as pessoas, bem como as formas mais brandas de comportamento agressivo, como agressão verbal e atos voltados à organização como a destruição, uso indevido de propriedade organizacional, ou propositalmente fazer o trabalho incorretamente e não notificar superiores sobre erros e problemas de trabalho. Com base na combinação de vários estudos Spector et al. (2006) resumem que a agressão é desencadeada por condições ambientais e estressoras, incluindo frustração com alguma situação, sentimento de injustiça e insultos; e sugerem que um ato de vingança é uma possível resposta a determinadas situações que envolvam obstrução de metas, violações de regras, normas, promessas não cumpridas, ou ataques ao poder e status. Todas essas situações que podem desencadear raiva, sentimento de violação e de desamparo que, conforme a intensidade, podem produzir um ato de vingança. Entretanto a vingança não é sempre uma reação imediata e impulsiva a uma situação, mas envolve uma complexa interação de cognição e emoção ao longo do tempo (SPECTOR et al. 2006).

Para Kelloway et al. (2010) o comportamento contraproducente no trabalho, por definição, viola as normas e orientações organizacionais, ameaçando o bem-estar dos membros e da própria organização. Segundo os autores, esse comportamento contraproducente pode ser visto como uma forma de protesto, onde membros da organização tentam expressar o descontentamento ou tentam compensar algo que julgam injusto dentro da organização.

2.2.9 Comportamento Seguro em Relação à Segurança da Informação

Segundo Ng et al. (2009), o dano devido a incidentes de Segurança da Informação está motivando as organizações a adotar mecanismos de proteção, que vão além dos controles tecnológicos, pois a segurança do computador também depende do comportamento seguro do indivíduo. Conforme os autores, os estudos sobre o comportamento seguro estudam a prática de segurança no computador e abordam como comportamento de usuários, que podem ser modificado para praticar contramedidas de segurança. Um dos componentes mais importantes do comportamento de segurança individual é a gestão eficaz do risco. A gestão de riscos requer a identificação de ameaças e determinação da probabilidade e impacto das ameaças. Isto é similar aos conceitos de susceptibilidade percebida e gravidade percebida no modelo de crenças em saúde, pois a orientação geral sobre a saúde é análoga à orientação geral de um indivíduo ou predisposição para a segurança (NG et al., 2009). Aplicando esta ideia a área da Segurança da Informação, o comportamento seguro é mapeado para a "segurança - consciência" de um indivíduo em relação às orientações de segurança em geral (NG et al., 2009), que no contexto organizacional deveriam estar presentes em Políticas da Segurança da Informação e em processos de conscientização dos colaboradores (PUHAKAINEN e SIPONEN, 2010).

Segundo Puhakainen e Siponen (2010), os documentos de políticas de segurança são chamados por vários nomes em diferentes organizações. Além disso, vários tipos de documentos de políticas de segurança podem existir em níveis diferentes em uma mesma organização, tais como documentos de alto nível, abrangendo estratégias de segurança, e outros mais granulares, como as orientações (*guidelines*) de nível operacional. Assim como ocorreu na pesquisa de Puhakainen e Siponen (2010), nesta pesquisa será utilizado o termo orientação (*guideline*) para se referir a Política de Segurança da Informação, por ser mais amplo e mais familiar a uma maior gama de respondentes.

Para Anderson e Agarwal (2010) a segurança dos sistemas de informação tem sido abordada a partir de várias perspectivas, incluindo a concepção técnica de mecanismos de segurança e tratamentos mais sócio-técnicos do tema, a maioria das pesquisas abordando o lado humano do problema de segurança foi realizada dentro das organizações, com o objetivo de entender o comportamento do funcionário. Os estudos realizados com os funcionários e usuários domésticos sugerem que comportamentos preventivos são influenciados por dois processos, chamados de avaliação da ameaça e avaliação de enfrentamento, que são princípios fundamentais na *Protection Motivation Theory* (PMT). Conforme os autores, um indivíduo

que está ciente das ameaças de segurança produz crenças sobre a severidade percebida e a probabilidade da ameaça, que então são avaliadas em contraponto às crenças formadas sobre o potencial da eficácia da resposta.

Para Anderson e Agarwal (2010), vários estudos mostram que a avaliação da ameaça e da forma de enfrentamento influenciam no comportamento de segurança no local de trabalho e no uso pessoal. No entanto, há influência da avaliação da ameaça em relação ao cumprimento das orientações das Políticas de Segurança, pois os estudos realizados no local de trabalho indicam as recompensas e as sanções, como potencias influenciadores do comportamento seguro. Todavia, esses fatores são menos relevantes para usuários domésticos, porque não estão sujeitos a esforços de conscientização, nem são propensos a ser monitorados em termos de comportamento de segurança em suas próprias casas. De acordo com os autores, vários estudos realizados em um ambiente de trabalho recomendam a promoção de uma cultura de segurança através da construção de um contrato psicológico dos colaboradores com a organização e indicam que os trabalhadores com maior fidelidade à organização tendem a apresentar uma maior conformidade com as políticas de segurança. Estes resultados sugerem que os indivíduos são suscetíveis a serem influenciados pela forma como eles se sentem intimamente ligados aos objetos nos quais eles são convidados, voluntariamente, a proteger com medidas preventivas (ANDERSON e AGARWAL, 2010).

Conforme Herath e Rao (2009b), a motivação intrínseca e a eficácia das ações percebidas pelos próprios usuários também desempenham um papel importante nas intenções de cumprir as orientações da Política da Segurança da Informação (PSI). Não obstante, as sanções e a certeza da detecção do não cumprimento da política, bem como a severidade e a celeridade da punição tem efeito significativo sobre as intenções de manter um comportamento seguro e em conformidade com a Segurança da Informação.

A identificação com a conformidade de segurança inclui condições que facilitam a formação de recursos, disponibilidade de recursos e visibilidade (HERATH e RAO, 2009b), onde:

a) A visibilidade envolve o uso de campanhas sobre Segurança da Informação, incluindo cartazes e anúncios que enviem uma mensagem convincente sobre a importância da conformidade de segurança (ALBRECHTSEN e HOVDEN, 2009);
b) A disponibilidade de recursos trata de assegurar que os recursos, tais como as políticas de segurança, são de fácil acesso (HERATH e RAO, 2009b).

Para Siponen e Vance (2010), é importante educar os funcionários para que internalizem que a conformidade com as orientações da Política de Segurança da Informação

é parte integrante do seu trabalho e qualquer negligência com essa conformidade deve ser vista como uma negligência das responsabilidades do seu trabalho, justificando que apesar das políticas de segurança exigirem um esforço extra, é importante realizar este esforço extra.

Da Veiga e Ellof (2010) complementam afirmando que caso os funcionários considerem difícil compreender algum item da política de Segurança da Informação ou considerá-lo não aplicável à sua unidade de negócio, podem não cumpri-lo, como consequência podem introduzir ameaças tanto intencionais como não intencionais ao ambiente.

Ng et al. (2009) reforçam que o sucesso da Segurança da Informação depende do comportamento eficaz dos usuários. Os funcionários de uma organização desempenham um papel essencial na prevenção e detecção de incidentes de segurança. Embora os administradores de sistemas sejam responsáveis pela configuração de firewalls e servidores de forma segura, os usuários são responsáveis por práticas de segurança, tais como o uso de senhas apropriadas, porém para que resulte em uma segurança eficaz, os usuários precisam tomar decisões conscientes sobre o cumprimento das Políticas de Segurança da organização.

Segundo Albrechtsen (2007), os usuários afirmam estarem motivados para exercer o seu trabalho levando em conta a Segurança da Informação, mas na prática não realizam muitas ações de segurança individual e os requisitos documentados de comportamento, bem como as campanhas de sensibilização, em geral, têm pouco efeito sobre o comportamento do usuário ou sobre sua consciência.

Em termos de comportamentos intrínsecos em conformidade com a segurança, estes se relacionam com a personalidade de um indivíduo, suas habilidades (WORKMAN et al. 2008) e os bons hábitos (VANCE et al., 2012). Um bom hábito, por exemplo, poderia ser não escrever a senha em algum papel como forma de lembrete, ou não compartilhar a senha com algum colega.

A competência dos usuários no que tange à Segurança da Informação está relacionada às suas habilidades (WORKMAN et al. 2008) e a conhecimentos para estarem condizentes com os controles de segurança. Dessa forma, é mais provável a adoção e internalização de uma meta quando se tem a competência para alcançar esse objetivo (RYAN e DECI, 2000).

Herath e Rao (2009b) descobriram que as crenças normativas, avaliação de ameaças, autoeficácia, a eficácia da resposta, visibilidade e impedimentos foram fatores que contribuíram para o comportamento em conformidade com a Política de Segurança da Informação. Estas variáveis ajudam a predizer se um usuário pode violar informações de segurança do sistema, mas também explicam por que um usuário pode ter uma propensão para

ignorar as medidas de segurança. Não obstante, a personalidade de um indivíduo engloba valores ou atitudes, bem como um padrão próprio de conduta (RYAN e DECI, 2000), esses valores e atitudes incluem aspectos como compromisso, obediência e autorreprovação (D'ARCY e HERATH, 2011).

D'Arcy e Hovav (2009) descobriram que o conhecimento das políticas de segurança, programas de conscientização, monitoramento e a percepção de sanções formais, reduzem a intenção de abusos na área de Segurança da Informação.

Segundo Herath e Rao (2009a), quando os funcionários acreditam que o cumprimento de políticas é um obstáculo ao seu do dia-a-dia, eles são menos propensos a ter pontos de vista favoráveis às políticas de segurança. No entanto, a eficácia percebida das ações dos funcionários desempenha um papel em comportamentos relacionados com a informação e o cumprimento da política de segurança, pois se os funcionários percebem que os comportamentos em conformidade com a política da Segurança da Informação têm um impacto favorável sobre a organização ou beneficiam a organização, eles são mais propensos a ter atitudes mais positivas em relação às políticas de segurança (BULGURCU et al., 2010).

Além disso, segundo Herath e Rao (2009b), a disponibilidade de recursos pode melhorar significativamente a capacidade dos funcionários para realizar as ações necessárias à segurança. Essa capacidade tem um efeito sobre as atitudes e intenções de política de segurança para cumprir com as políticas. Assim, torna-se provável que funcionários com alta autoeficácia tenham atitudes favoráveis e maiores intenções de conformidade.

Com base nos conceitos apresentados no decorrer desse capítulo foi elaborado um modelo teórico que visa determinar um conjunto de relações de interdependências e as respectivas hipóteses de pesquisas, ambos são apresentados no capítulo seguinte.

3 MODELO TEÓRICO E HIPÓTESES DE PESQUISA

As hipóteses de pesquisa e o modelo teórico, apresentados a seguir, foram embasados na revisão de literatura realizada na etapa anterior e que consta no capítulo anterior. A partir do refinamento dos conceitos apresentados foram selecionados aqueles que poderiam operacionalizar a presente pesquisa e a partir desse ponto definiu-se um conjunto de hipóteses que estão relacionadas à percepção humana. Esses conceitos foram combinados de forma sintética a partir das definições de cada um dos autores já apresentadas no referencial teórico, essas sínteses são apresentadas a seguir, junto a sua respectiva hipótese.

Segundo Ng et al. (2009), a percepção sobre riscos e danos em Segurança da Informação e sua possibilidade de ocorrência, depende da capacidade de mensuração e abrange a percepção sobre a suscetibilidade da ameaça e a severidade da ameaça, pois quando um indivíduo percebe uma maior susceptibilidade a incidentes de segurança, será provável que apresente um maior nível de comportamento de segurança. Com base nesses conceitos foi formulada a seguinte hipótese:

H1: A percepção de suscetibilidade da ameaça à Segurança da Informação influencia positivamente o comportamento seguro em relação à Segurança da Informação.

Workman, et al. (2008) descobriram que a severidade percebida foi significativa para o cumprimento das orientações da Política da Segurança da Informação, assim como a probabilidade da quebra de segurança. Para Liang e Xue (2009) a severidade percebida é definida como o grau em que um indivíduo percebe que consequências negativas causadas por *malwares* serão graves. Conforme Ng et al. (2009), quando os usuários estão cientes da suscetibilidade e da severidade de ameaças podem tomar decisões conscientes para exercer um comportamento preventivo adequado. Considerando esses conceitos e foi criada a seguinte hipótese:

H2: A percepção de severidade da ameaça à Segurança da Informação influencia positivamente o comportamento seguro em relação à Segurança da Informação.

Herath e Rao (2009b), em sua pesquisa sobre os efeitos da dissuasão, descobriram que a certeza da detecção tem um impacto positivo sobre as intenções de conformidade com as orientações da Política de Segurança. Quando os funcionários percebem uma alta probabilidade de serem identificados violando as orientações, eles serão mais propensos a seguir as orientações. Esse conceito produziu a seguinte hipótese:

H3: A percepção da certeza de detecção por não seguir as orientações sobre Segurança da Informação influencia positivamente o comportamento seguro em relação à Segurança da Informação.

As sanções são definidas como punições, materiais ou imateriais como rebaixamentos, perda de reputação, reprimendas, penalizações monetárias ou não monetárias e menção pessoal desfavorável, oral ou escrita, em relatórios de avaliação incorridos por um empregado ao descumprir as exigências das orientações mencionadas na Política de Segurança da Informação (BULGURCU et al., 2010). A percepção dessas sanções referentes ao não cumprimento das normas sobre a Segurança da Informação influência o usuário a um comportamento responsável perante a Segurança da Informação, conforme a certeza da detecção do não cumprimento das normas de segurança, a severidade e a celeridade da punição (HERATH e RAO, 2009a; HERATH e RAO, 2009b). A partir da combinação desses conceitos foi criada a seguinte hipótese:

H4: A percepção de severidade da punição por não seguir as orientações sobre Segurança da Informação influencia positivamente o comportamento seguro em relação à Segurança da Informação.

De acordo com Liang e Xue, 2009 o esforço de salvaguarda refere-se aos esforços físicos e cognitivos – tais como tempo, dinheiro, inconveniência e compreensão – necessários à ação de salvaguarda. Esses esforços tendem a criar barreiras ao comportamento e reduzem a motivação do Comportamento Seguro em relação à Segurança da Informação, devido à análise de custo-benefício. Liang e Xue (2010) citam como exemplo o comportamento das pessoas em relação à saúde, quando comparam os custos e benefícios de um determinado comportamento saudável antes de decidir praticá-lo, não sendo susceptíveis a adotar o comportamento preconizado pelos profissionais da saúde, se o custo for considerado alto em comparação aos malefícios e benefícios. Dessa forma, a motivação do usuário para evitar a ameaça de TI pode ser atenuada pelo custo potencial do uso da salvaguarda (Liang e Xue, 2010). De acordo com esses conceitos foi elaborada a seguinte hipótese:

H5: A percepção de esforço em salvaguarda em seguir as orientações sobre Segurança da Informação influencia negativamente o comportamento seguro em relação à Segurança da Informação.

Há a possibilidade da ocorrência de brechas na Segurança da Informação por falta de motivação para seguir às orientações de segurança (KELLOWAY et al., 2010), devido ao descontentamento com a organização ou colegas (WILLISON e WARKENTIN, 2013;

SPECTOR et al., 2006), ou como forma de protesto devido a uma situação insatisfatória (SPECTOR et al., 2006). De acordo com essa possibilidade é formulada a seguinte hipótese:

H6: O contentamento com colegas, superiores ou organização Informação influencia positivamente o Comportamento Seguro em relação à Segurança da Informação.

As hipóteses apresentadas representam uma síntese das relações destacadas no referencial teórico a respeito das percepções do usuário sobre Segurança da Informação e sobre o Contentamento.

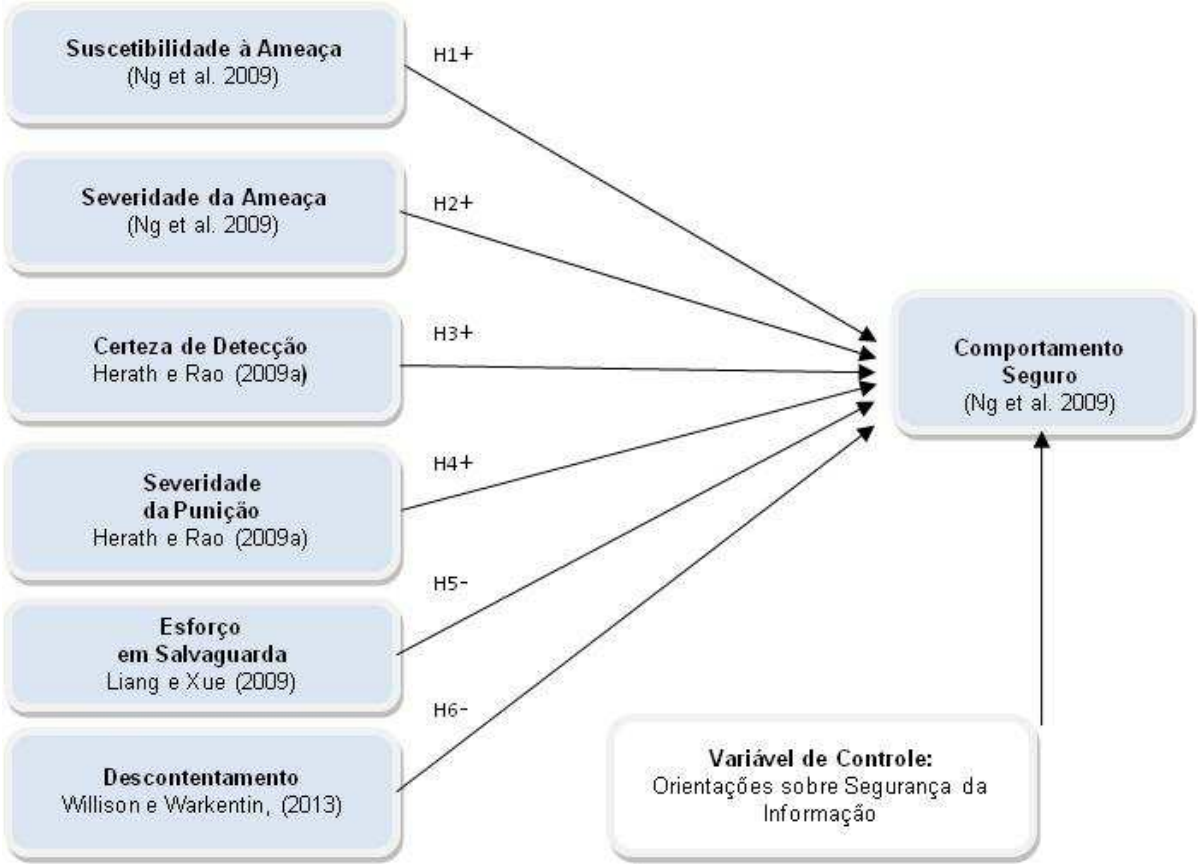
O instrumento de pesquisa produzido a partir do presente trabalhou utilizou as questões da pesquisa de Ng et al. (2009) para mensurar o Comportamento Seguro. Para esses autores, o Comportamento Seguro de um indivíduo é inerente à consciência sobre as orientações de Segurança da Informação em geral e é o produto de práticas de segurança guiadas pelas orientações. Puhakainen e Siponen (2010) complementam, indicando que no contexto organizacional essas orientações devem constar em Políticas da Segurança da Informação e em processos de conscientização dos colaboradores (PUHAKAINEN e SIPONEN, 2010). Analogamente à pesquisa Puhakainen e Siponen (2010), na presente pesquisa será utilizado o termo orientação (*guideline*) para se referir a Política de Segurança da Informação, por ser mais amplo e mais familiar a um maior número de respondentes. Contudo, dentre os vários aspectos do comportamento seguro, essa pesquisa restringe-se a mensuração do Comportamento Seguro em SEGINF com relação a alguns procedimentos realizados ao trabalhar com e-mails, similarmente à pesquisa Ng et al. (2009).

A partir do referencial teórico desta pesquisa e de suas hipóteses definiu-se um modelo teórico preliminar que serviu como base para o desenvolvimento, demonstrado na Figura 3. Esse modelo teórico apresenta os construtos Suscetibilidade à Ameaça, Severidade da Ameaça, Certeza de Detecção e Severidade da Punição como variáveis independentes e indutores positivos, influenciando positivamente a variável dependente denominada Comportamento Seguro. Por outro lado, os construtos Esforço de Salvaguarda e Descontentamento são variáveis independentes, apresentadas como indutores negativos, que podem influenciar negativamente a variável Comportamento Seguro.

O item Variável de Controle apresentado no modelo teórico indica que a análise dos dados será realizada sobre a amostra de respondentes que receberam alguma orientação, verbal ou escrita, sobre a Segurança da Informação, proveniente da organização na qual trabalhavam no momento da coleta. Essa seleção permite que obter as percepções de respondentes que já possuem algum esclarecimento sobre as ameaças à Segurança da Informação, como por exemplo, o nível de controle e monitoramento e as punições em não

seguir as orientações recebidas. Também permite comparar os resultados como o grupo de respondentes que não recebeu esse mesmo tipo de orientação.

Figura 3- Modelo teórico preliminar



Fonte: Autor

Foi utilizado termo orientação (*guideline*) para se referir a Política de Segurança da Informação, por ser mais amplo e mais familiar a uma maior gama de respondentes, similarmente ao ocorrido na pesquisa de Puhakainen e Siponen (2010). Segundo Puhakainen e Siponen (2010), os documentos de políticas de segurança são chamados por vários nomes em diferentes organizações. Além disso, vários tipos de documentos de políticas de segurança podem existir em níveis diferentes em uma mesma organização, desde estratégias de segurança até orientações (*guidelines*) de nível operacional.

O modelo teórico suas hipóteses, apresentados na Figura 3, nortearam o restante da pesquisa. A validação deste modelo está descrita no capítulo a seguir, juntamente com os procedimentos utilizados para atingir os objetivos propostos.

Conforme orientações recebidas no decorrer da etapa da Validação de Face e Conteúdo do Instrumento de Pesquisa, descrita no próximo capítulo, as questões relativas ao Descontentamento foram alteradas para questionar o contentamento do funcionário, com a

organização, colegas e superiores. Dessa forma, o modelo foi alterado, a versão final consta no capítulo de resultados.

4 MÉTODO DE PESQUISA

Neste capítulo é apresentado o método de pesquisa utilizado para alcançar os objetivos propostos anteriormente. Será apresentada a estratégia adotada e o desenho de pesquisa, bem como o detalhamento das técnicas de coleta de dados e a condução da análise dos dados.

4.1 CARACTERIZAÇÃO DA PESQUISA

A pesquisa realizada utilizou dados quantitativos, tipo *survey*, transversal, com caráter exploratório (PINSONNEAULT e KRAEMER, 1993), utilizando um questionário autoadministrado como instrumento para a coleta de dados.

Na presente pesquisa optou-se por uma pesquisa tipo *survey* por ser uma das formas de coletar dados ou informações por intermédio de um questionário, no qual podem ser obtidas as particularidades, ações ou opiniões de um determinado grupo de pessoas que representam a população-alvo da pesquisa (PINSONNEAULT e KRAEMER, 1993). O questionário tem a função de mensurar um determinado número de aspectos dos conceitos, através uma série regras e convenções (HAIR et al., 2005). No entanto, para realizar as medições é preciso o desenvolvimento de instrumentos pesquisa adequados ao que se deseja medir (MALHOTRA, 2012). Dessa maneira, os questionários são compostos de itens os quais mantêm conceitos a ser operacionalizado e uma forma que permita a sua mensuração (MALHOTRA, 2012).

A *survey* neste estudo tem o objetivo de validar o conjunto de fatores e itens a ser avaliados pelos usuários de recursos de TI para o trabalho. Tais itens foram selecionados com base na revisão da literatura. Segundo Pinsonneault e Kraemer (1993), a pesquisa *survey* pode ser descrita como a obtenção de dados ou informações sobre características, ações ou opiniões de um determinado grupo de pessoas, indicado como representante de uma população alvo, por meio de um instrumento, normalmente um questionário. Como principais características do método de pesquisa *survey* podem ser citadas: a) O interesse em produzir descrições quantitativas de uma população; b) Utiliza um instrumento pré-definido.

Em relação ao período de coleta, segundo HAIR et al. (2005), em estudos transversais os dados são coletados em um único ponto no tempo e resumidos estatisticamente, por outro lado em estudos longitudinais são coletados em diversos pontos no tempo, com os dados representando uma série temporal, sendo que a maioria das pesquisas tipo *survey* é transversal (HAIR et al. 2005).

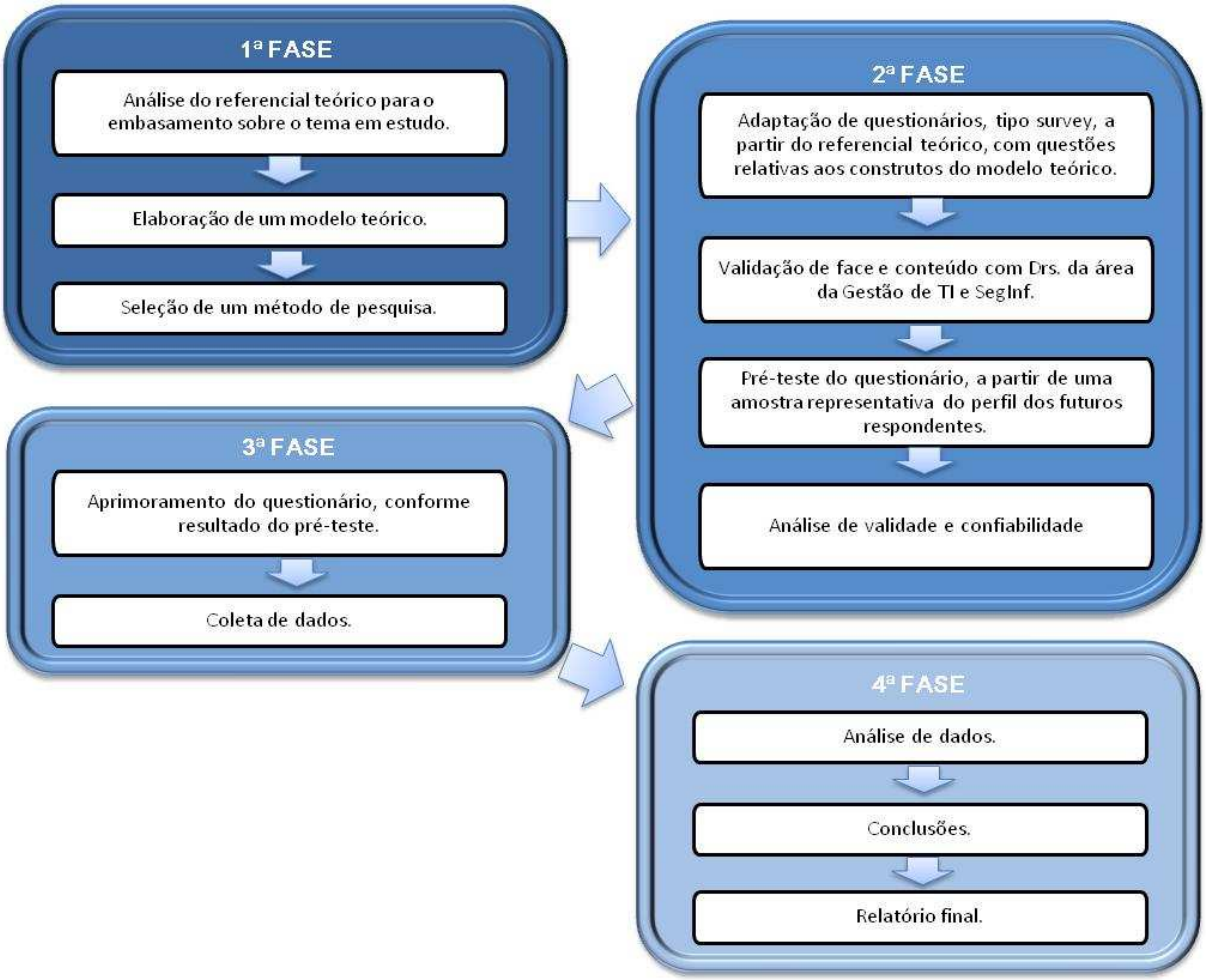
Pinsonneault & Kraemer (1993) classificam os propósitos da pesquisa *survey* em: a) explanatória: com o objetivo de testar uma teoria e suas relações causais, estabelecendo as relações causais e questionando o motivo dessas relações; b) exploratória: que objetiva

identificar os conceitos iniciais sobre um assunto, dando ênfase na determinação de quais conceitos devem ser medidos e como devem ser medidos, buscando descobrir novas possibilidades e dimensões da população de interesse; c) descritiva: buscam identificar quais situações, eventos, atitudes ou opiniões estão presentes em uma população; descreve a distribuição de algum fenômeno na população ou entre os subgrupos da população e compara essas distribuições. Neste tipo de *survey* a hipótese não é causal, mas tem o propósito de verificar se a percepção dos fatos está ou não de acordo com a realidade.

A presente pesquisa tem propósito exploratório no que tange a disposição dos construtos no modelo teórico e suas inter-relações, pois cria um novo modelo teórico a partir da junção de quatro pesquisas atuais, também pode ser considerada exploratória pelo ineditismo da adaptação, combinação e ordem das questões no instrumento de pesquisa, relacionadas aos construtos dessas quatro pesquisas, bem como em seu contexto de aplicação.

O método utilizado para atingir os objetivos propostos por este estudo compreende: a) análise do referencial teórico para o embasamento sobre o tema em estudo; b) elaboração de um modelo teórico; c) adaptação do questionário, tipo *survey*, a partir das questões provenientes dos construtos do modelo teórico; d) validação do questionário por cinco Drs. da área de Gestão de TI e Segurança da Informação; e) pré-teste do questionário, a partir de uma pequena amostra representativa do perfil dos futuros respondentes; f) correção do questionário, conforme resultado do pré-teste; g) coleta de dados; h) análise de dados; i) conclusões e j) relatório final; conforme demonstrado na Figura 4.

Figura 4 - Desenho de pesquisa com as fases e etapas da pesquisa



Fonte: Autor

Conforme o desenho de pesquisa, ilustrado da Figura 4, serão descritos a seguir os procedimentos realizados na 2ª fase da pesquisa que possibilitaram a criação de um instrumento de pesquisa tipo *survey* com o objetivo de realizar a coleta de dados.

4.2 POPULAÇÃO E AMOSTRA

A população desta pesquisa é composta por usuários de Sistemas de Informação em ambiente organizacional, em organizações de qualquer porte, setor ou ramo de atividade. Entretanto, os respondentes precisavam ter recebido orientações sobre Segurança da Informação de forma escrita ou oral, por parte da organização onde trabalhavam no momento do preenchimento do questionário.

Considerando a possibilidade da coleta por meio eletrônico, foi optado por não restringir geograficamente a abrangência da coleta. Dessa forma, a população da presente pesquisa não pôde ser determinada.

O processo de amostragem foi o não probabilístico por conveniência (HAIR et al., 2005).

4.3 ELABORAÇÃO E VALIDAÇÃO DO INSTRUMENTO DE PESQUISA

De acordo com Malhotra (2012) o questionário deve ter os seguintes objetivos: a) deve transformar a informação em uma pergunta que os entrevistados saibam responder; b) deve motivar o entrevistado a responder, ou seja, o questionário não pode ser cansativo; c) deve mitigar o erro do respondente.

No questionário foram utilizadas 15 questões para identificar as características sócio-demográficas do respondente e de controle, que foram agrupadas em dois blocos, questões relativas ao respondente e questões sobre a organização onde o respondente trabalha. Foi priorizado o uso questões com resposta objetiva, para facilitar a resposta e diminuir o tempo total de preenchimento do questionário, conforme instrumentos originais, que constavam como fonte do modelo teórico.

Segundo Hair et al.(2005), a escala um instrumento de mensuração que pode ser distinto ou contínuo, cuja precisão está associada com o termo validade, enquanto que a coerência está ligada ao termo confiabilidade, uma pesquisa tipo *survey* será considerada confiável se sua aplicação repetida resultar em escores coerentes. Conforme os autores o desenvolvimento de escalas envolve:

a) Definição do conceito (construto) ou conceitos a serem medidos, incluindo relacionamento entre conceitos e referencial teórico sobre o(s) conceito(s);
b) Identificação dos componentes do conceito;
c) Especificação de indicadores mensuráveis que representem os componentes do conceito;
d) Seleção das escalas adequadas para mensurar os indicadores;
e) Combinação de itens em uma escala composta que, por sua vez, serve como um meio de mensurar o conceito;
f) Administração do instrumento (escala) a uma amostra e avaliação da compreensão do respondente;
g) Avaliação da confiabilidade e da validade;
h) Revisão do instrumento, se necessário.

Todos esses procedimentos foram utilizados na presente pesquisa, os resultados constam nos tópicos apresentados a seguir. Os procedimentos identificados anteriormente de “a” a “d” foram realizados de 12/09/2012 a 18/07/2013 e contaram com o apoio de diversos

Drs. da linha de pesquisa da Gestão da Informação do PPGAd da PUCRS, neste período vários modelos teóricos alternativos foram cogitados.

Em relação à construção de uma de uma escala confiável e válida, Hinkin (2008) indica as seguintes etapas:

1. Geração do questionário, tipo *survey*, podendo ser oriundo de duas formas distintas:
    a. Forma dedutiva: o conjunto de itens é derivado da teoria, o que requer entendimento dos fenômenos a ser investigados e através da revisão literatura deve-se obter a definição teórica dos construtos sob mensuração, que é o caso da pesquisa em questão, como aspecto negativo consome tempo, mas com aspecto positivo assegura a validade da escala;
    b. Forma indutiva: ocorre quando o construto não possui dimensões facilmente identificáveis. Nesse caso deve ser desenvolvidas escala através de exemplos dos respondentes. Essa forma é útil em pesquisas exploratórias, quando há construtos abstratos, porém não há garantias da mensuração;

    Ainda nessa etapa é realizado o desenvolvimento do item do questionário, utilizando uma linguagem familiar, clara, objetiva, com uma única informação a ser mensurada, sem viés e sem ser tendencioso.

    Após a criação deve ocorrer a avaliação da validade de conteúdo, abrangendo os seguintes passos: a) pré-teste, para validar consistência conceitual; b) validação dos itens versus as definições de construtos, utilizando a opinião de leigos ou entrevistados. Caso a escala se replique entre as várias amostras haverá maior garantia de consistência.
2. Realizar a administração do questionário, ou seja, a coleta dos dados, cuidando para que o tamanho da amostra respeite a seguinte regra: para cada item do questionário deve ser obtidas respostas de quatro respondentes.
3. Redução inicial, utilizando, por exemplo, o software SPSS, no qual devem ser realizadas as seguintes atividades:
    a. Análise fatorial, permitindo reduzir o número de variáveis observadas. A variância deverá ser retirada caso seja menor que 0,4, porém com parcimônia;
4. Avaliação da consistência interna, utilizando coeficiente alfa de Cronbach.
5. Análise fatorial, na qual deve ser utilizada a matriz de variância-covariância;

6. Validação Convergente e Discriminante;
7. A etapa final abrange a replicação dos passos anteriores, que pode ocorrer em caso de acréscimo de escalas, que nesse caso deverão ser submetida a um novo pré-teste, com uma nova amostra.

Todas as etapas mencionadas acima foram utilizadas no desenvolvimento da escala da presente pesquisa e os resultados serão apresentados nos tópicos a seguir.

4.3.1 Validação de Face e Conteúdo do Instrumento de Pesquisa

Seguindo o recomendado por Hoppen et al. (1996) foram realizados pré-testes e um conjunto de validações prévias, necessários quando é utilizado um instrumento de medida adaptado de outras pesquisas. A primeira parte da validação do instrumento, foi realizada através da validação de face e conteúdo, envolveu cinco Drs. da área de Gestão de TI e Segurança da Informação da PUCRS e UFRGS, ligados a linha de pesquisa de Administração da Informação. Como resultado da validação de face e conteúdo, algumas perguntas foram alteradas em termos de conteúdo e ordem, a mudança mais significativa foi a alteração das questões relativas ao construto Descontentamento (WILLISON e WARKENTIN, 2013), que foram invertidas, e desde a versão de pré-teste questionam sobre o contentamento do respondente, com a organização, colegas e superiores, como pode ser observado no Quadro 2. Portanto, após a validação de face e conteúdo do instrumento de pesquisa passou a validar o descontentamento pelo viés da falta de contentamento.

As questões de confirmação dos construtos que possuíam originalmente esse tipo de questão, forma distribuídas dentre as demais questões de forma aleatória, conforme orientações obtidas, durante a validação de face conteúdo.

O Quadro 2 apresenta as origens das questões agrupadas pelos construtos do modelo teórico e suas respectivas fontes e também permite identificar a variável associada a cada questão. No questionário aplicado à amostra de pré-teste as questões foram reordenadas, seguindo as orientações recebidas durante a etapa de validação de face e conteúdo do instrumento de pesquisa. O questionário final utilizado na coleta final consta no Apêndice A. Algumas questões apresentadas no Quadro 2 foram adaptadas a partir de sugestões realizadas na etapa de validação de face e conteúdo, essas questões estão identificadas como “adaptado de”, demais itens que foram apenas traduzidos para o português, constam apenas como “traduzido de”. A tradução das questões também foi submetida à validação de face e conteúdo.

O questionário final possui notas explicativas dos termos utilizados em cada questão, conforme pode ser verificado no Apêndice A.

Quadro 2 - Questões preliminares do pré-teste ordenadas provisoriamente por construto.

Construto	Questão	Fonte
Suscetibilidade à ameaça	SUS1: As chances de receber um anexo de e-mail com um *malware* são altas. (Discordo Plenamente ... Concordo Plenamente) SUS2: Há uma boa possibilidade de que eu receba um anexo de e-mail com um *malware*. (Discordo Plenamente ... Concordo Plenamente) SUS3: Eu estou suscetível a receber um anexo de e-mail com *malware*. (Discordo Plenamente ... Concordo Plenamente)	**Traduzido de Ng et al. 2009**
Severidade da ameaça	SEV1: Ter o computador infectado por um *malware* como resultado de abrir um anexo de e-mail suspeito é um problema sério para mim. (Discordo Plenamente ... Concordo Plenamente) SEV2: A perda de dados da organização, como resultado de abrir um anexo de e-mail suspeito, é um problema sério para mim. (Discordo Plenamente ... Concordo Plenamente) SEV3: Se o meu computador está infectado por um *malware*, como resultado de abrir um anexo de e-mail suspeito, meu trabalho será afetado negativamente. (Discordo Plenamente ... Concordo Plenamente)	**Traduzido e adaptado de Ng et al. 2009** Nas questões originais era utilizado o termo "vírus" o termo foi atualizado para "*malware*", conforme orientação recebida durante a etapa de validação de face e conteúdo. A explicação sobre o termo *malware* foi acrescida ao instrumento de pesquisa. A versão final do instrumento consta no Apêndice A.
Certeza de Detecção	DETCERT1: Na organização onde trabalho o uso do computador é monitorado. (Discordo Plenamente ... Concordo Plenamente) DETCERT2: Na organização onde trabalho o uso inadequado do computador certamente seria detectado. (Discordo Plenamente ... Concordo Plenamente)	**Traduzido de Herath e Rao (2009a)**
Severidade da Punição	A organização onde trabalho ... PUNSEV1: repreende funcionários que não seguem as orientações sobre segurança da informação. (Discordo Plenamente ... Concordo Plenamente) PUNSEV2: demite funcionários que fazem uso inadequado do computador. (Discordo Plenamente ... Concordo Plenamente) PUNSEV3: se eu fosse pego usando inadequadamente o computador, seria severamente punido. (Discordo Plenamente ... Concordo Plenamente)	**Traduzido de Herath e Rao (2009a)**
Esforço em Salvaguarda	PSC1: Na organização onde você trabalha, o seu computador possui um anti-spyware? ❍ Sim. ❍ Não. ❍ Não sei Caso tenha respondido Não ou Não sei na questão anterior, defina seu grau de concordância com as afirmações abaixo. Escolhendo um valor entre 1 e 5 (1 = Discordo	**Adaptado de Liang e Xue (2010)** A questão PSC1 não existia no instrumento de pesquisa original, foi acrescida conforme orientação recebida durante na etapa de validação de face e conteúdo. As questões originais PSC2,

	Totalmente, 5= Concordo Totalmente): PSC2: Eu não sei como conseguir um software anti-spyware. (Discordo Plenamente ... Concordo Plenamente) PSC3: O software anti-spyware pode causar problemas para outros programas no meu computador . (Discordo Plenamente ... Concordo Plenamente) PSC4: A instalação de um software anti-spyware é muito complicada. (Discordo Plenamente ... Concordo Plenamente).	PSC3 e PSC4, presumiam a ausência de um anti-spyware no computador do respondente. Caso fosse utilizada essa mesma pressuposição, seria necessário limitar os respondentes a essa condição, o que poderia limitar muito o número de respondentes.
Descontentamento	Considerando à organização onde você trabalha ... DESC1: Estou muito contente com os meus colegas de trabalho. (Discordo Plenamente ... Concordo Plenamente) DESC2: Estou muito contente com os meus superiores. (Discordo Plenamente ... Concordo Plenamente) DESC3: Estou muito contente com a organização onde trabalho. (Discordo Plenamente ... Concordo Plenamente)	**Adaptado do artigo de Willison e Warkentin (2013)** As questões foram criadas a partir do referencial teórico. O viés da questão mudou de descontentamento para contentamento, de vido às orientações recebidas durante na etapa de validação de face e conteúdo.
Comportamento Seguro	BEH1: Antes de ler um e-mail, verifico primeiro se o assunto e o remetente fazem sentido. (Discordo Plenamente ... Concordo Plenamente) BEH2: Antes de abrir um anexo de um e-mail, verifico primeiro se o nome do arquivo anexado faz sentido. (Discordo Plenamente ... Concordo Plenamente) BEH3: Eu tenho cautela ao receber um anexo de e-mail, pois pode conter um *malware*. (Discordo Plenamente ... Concordo Plenamente) BEH4: Eu não abro anexos de e-mail se o conteúdo do e-mail parece suspeito. (Discordo Plenamente ... Concordo Plenamente).	**Ng et al. 2009**

Fonte: Autor

O Quadro 3 apresenta as demais questões sócio-demográficas, que permitiram a identificação do perfil do respondente e posteriores análises estatísticas descritivas.

Quadro 3 - Questões de identificação do respondente.

Item de Questionário	Questão	Fonte
Dados demográficos	Qual das opções abaixo melhor representa seu nível de escolaridade: ❍ Ensino fundamental (1o. grau) ❍ Ensino médio (2o. grau) ❍ Ensino superior ❍ Especialização/MBA ❍ Mestrado/Doutorado Gênero: ❍ Feminino	**Adaptado dos artigos** **Bulgurcu et al. (2010)** **Malhotra (2012)** **Siponen (2000)** **Ng et al. (2009)** Nesse item foi apenas utilizado o conceito de coleta de dados demográficos para identificação dos respondentes.

	❍ Masculino Qual a sua idade? _____ Quantos anos experiência de profissional você tem (total de anos)? _____ Qual das opções abaixo melhor representa seu área de formação: ❍ Administração ❍ Informática ❍ Direito ❍ Engenharia ❍ Outra: _____ Você já trabalhou ou trabalha atualmente na área de Informática ou Tecnologia da Informação? ❍ Sim. Quantos anos: _____ ❍ Não Qual o número aproximado de pessoas que trabalham na organização onde você trabalha atualmente?_____ Qual o seu cargo/função atual? _____ Quantos anos de experiência profissional você tem (total de anos)? _____anos. Qual o segmento de atuação da organização onde você trabalha? ❍ Indústria ❍ Comércio ❍ Serviços ❍ Governo ❍ Outro:	
Dados demográficos	EXP1) Algum dispositivo de TI que você utilizou (computador, smartphone, notebook, laptop, etc.), profissionalmente ou pessoalmente, já foi infectado por um *malware*? ❍ Sim. ❍ Não. ❍ Não sei.	**Autor**
Variável de Controle	ORI1: A organização na qual você trabalha fornece orientações sobre Segurança da Informação, verbais ou escritas? ❍ Sim, mas não são esclarecidas as razões de cada item apontado na orientação. ❍ Sim, e as razões de cada item apontado na orientação são esclarecidas. ❍ Não. ORI2: Caso tenha respondido alguma opção com Sim na questão anterior, as orientações ocorreram: ❍ Periodicamente, a cada ____ meses. ❍ Uma única vez.	**Adaptado de Ng et al. 2009.** Nesse item foi apenas utilizado o conceito de variável de controle, como filtro para a amostragem.

Fonte: Autor

Foi utilizado uma escala do tipo Likert com variação de cinco categorias, de 1 (discordo plenamente) a 5 (concordo plenamente), com base nos instrumentos utilizados nas três pesquisas originas utilizadas como referência para o modelo teórico. Segundo Malhotra (2012), a escala do tipo Likert é uma escala balanceada de comparações, que possui o mesmo número de categorias favoráveis e desfavoráveis. A utilização de um número impar de categorias impedirá a reação neutra ou indiferente de algum dos respondentes, além disso, é uma escala na qual os respondentes são forçados a emitir uma opinião, pois não haverá a categoria "sem opinião".

Após a elaboração do questionário foi aplicado um pré-teste, com uma amostra do perfil dos respondentes a fim de identificar e eliminar potenciais erros (MALHOTRA, 2012). Os resultados obtidos com a versão preliminar do instrumento de pesquisa constam no tópico sobre o pré-teste do instrumento e os resultados obtidos com a versão final do instrumento de pesquisa constam no capítulo da análise dados.

5 RESULTADOS

No decorrer desse capítulo são expostos os resultados obtidos pela análise quantitativa dos dados coletados através do instrumento de pesquisa, que foi aprimorado por intermédio dos procedimentos a seguir. O instrumento de pesquisa utilizado na coleta final consta no Apêndice A.

Considerando que dentre os objetivo constava a elaboração de instrumento de pesquisa, as análise que validam esse instrumento constam entre os resultados da pesquisa. Dessa forma, os procedimentos metodológicos utilizados para a análise dos dados seguiram os seguintes critérios e etapas: a) Pré-teste do Instrumento de pesquisa; b) Análise Descritiva da Amostra; c) Análise Descritiva Univariada e a verificação da normalidade dos dados; d) Análise de Confiabilidade do Instrumento de Pesquisa; e) Análise de Regressão Linear Múltipla e f) Modelagem pelos Mínimos Quadrados Parciais.

5.1 PRÉ-TESTE

O objetivo do pré-teste é identificar e eliminar os potenciais problemas, permitindo o aperfeiçoamento do instrumento de pesquisa, testando o conteúdo das questões, enunciados, sequência, formato, layout, dificuldade das perguntas e instruções (MALHOTRA, 2012).

A etapa de pré-teste foi conduzida no período entre 15/08/2013 e 07/10/2013 e teve por objetivos: a) validar novamente a face e conteúdo do instrumento, pelos respondentes com o mesmo perfil da amostra final; b) analisar a confiabilidade interna das variáveis propostas; c) refinar o instrumento de pesquisa.

5.1.1 Amostragem e Coleta de Dados na Etapa de Pré-teste

A segunda parte da validação do instrumento foi realizada a partir da aplicação do instrumento em uma amostra de 229 de alunos de cursos de graduação Gestão de TI e Administração de Empresas da PUCRS, escolhidas ao acaso, que estavam cursando disciplinas do 6º e 7º semestre de cursos de Negócios e Gestão Estratégica em Tecnologia da Informação da PUCRS. Foi utilizada uma amostra não probabilística por conveniência (HAIR et al., 2005) na coleta de pré-teste. A coleta foi realizada através de um questionário autoadministrado com 36 questões, sendo 21 questões que participaram da Análise Fatorial no Pré-teste e 15 questões sócio-demográficas e de controle que permitiram a identificação do perfil do respondente, através de análises estatísticas descritivas.

Devido ao tamanho da amostra para o pré-teste, não foi considerado necessário imputar médias em questões não respondidas, optando-se por desconsiderar todas as questões

do respectivo respondente que não completou o questionário na íntegra, excluindo da base utilizada na análise. Após as exclusões dos questionários incompletos restaram 216 respondentes válidos.

Entretanto, após aplicar o filtro pela variável de controle EXP1, mantendo na amostra somente os respondentes que receberam alguma orientação sobre Segurança da Informação de forma oral ou escrita, remanesceu 135 respondentes válidos na amostra de pré-teste.

5.1.2 Análise de Confiabilidade do Instrumento de Pesquisa no Pré-teste

Para a validação da confiabilidade do instrumento de pesquisa na fase de pré-teste foi utilizado o alfa de Cronbach, através do software SPSS Statistics versão 20.0.2. Segundo Malhotra (2012), o Alfa de Cronbach é um dos testes mais usados para verificar a coerência interna de um conjunto de variáveis, determinando assim a confiabilidade de uma medida. Nessa etapa de validação também foi realizada uma análise multivariada através da Análise Fatorial das diferentes variáveis, visando verificar a estrutura dos fatores que compõem as escalas, com uso da análise de componente principal e rotação varimax (HAIR et al., 2009). Tais procedimentos permitiram uma depuração das escalas, possibilitando o uso de uma estrutura mais consistente no instrumento de pesquisa.

5.1.3 Refinamento do Instrumento de Pesquisa no Pré-teste

Através da Análise Fatorial e do índice de Alfa de Cronbach foi identificada a necessidade de retirada das questões BEH4, PUNSEV1 e SEV2, descritas anteriormente no Quadro 2, pois na análise de confiabilidade interna de cada construto do modelo obteve-se índices abaixo de 0,6, enquanto foram mantidas essas questões. A Tabela 1 demonstra o Alfa de Cronbach de cada construto após a retirada dessas questões.

Tabela 1 - Alfa de Cronbach dos construtos na coleta do pré-teste

Construto	Variáveis / Questões	Alfa de Cronbach
Suscetibilidade à ameaça (SUS)	SUS1, SUS2 e SUS3	0,878
Contentamento (DESC)	DESC1, DESC2 e DESC3	0,798
Comportamento Seguro (BEH)	BEH1, BEH2 e BEH3	0,746
Severidade da Punição (PUNSEV)	PUNSEV2 e PUNSEV2	0,691
Certeza de Detecção (DETCERT)	DETCERT1 e DETCERT2	0,687
Severidade da Ameaça (SEV)	SEV1 e SEV3	0,630
Esforço em Salvaguarda (PSC)	PSC2, PSC3 e PSC4 (questões opcionais)	0,604

Fonte: Autor

Conforme Hair et al. (2005) valores a partir de 0,6 para o Alfa de Cronbach são aceitáveis para pesquisa exploratórias, quando são definidos novos instrumentos de pesquisa, como é o caso desta pesquisa.

Através da Análise Fatorial na fase de pré-teste foi percebido a baixa comunalidade da variável BEH4, conforme demonstrado na Tabela 2. A comunalidade representa a quantidade de variância em uma única variável, que pode ser explicada pelos fatores extraídos através de uma Análise Fatorial (HAIR et al., 2005).

Tabela 2 - Comunalidade das variáveis dependentes no pré-teste

Variável	Comunalidade
BEH1	0,631
BEH3	0,592
BEH2	0,698
BEH4	0,172
Método de Extração: *Principal Component Analysis*.	

Fonte: Autor

Após a retirada das questões BEH4, PUNSEV1 e SEV2 foi obtido o alfa de 0,670, para todas variáveis obrigatórias que mensuravam os construtos do modelo, mostrando-se bastante satisfatório para pesquisas do tipo exploratória ou descritiva, nas quais a coerência interna tende a ser menor (MALHOTRA, 2012).

A comunalidade das demais variáveis dependentes apresentaram resultados satisfatórios. As comunalidades foram extraídas pelo método *Principal Component Analysis*. Nenhuma variável dependente apresentou índice abaixo de 0,5. Segundo Malhotra (2012), quando a comunalidade está abaixo de 0,5 a variável não fornece explicação suficiente para o que está mensurando, sendo necessário obter amostras maiores.

Durante a Análise Fatorial na fase de pré-teste foi verificado o índice de Kaiser-Meyer-Olkin (KMO) que sinaliza a adequação da amostra. Pequenos valores no KMO indicam que a análise fatorial pode ser inapropriada (MALHOTRA, 2012), são indicados valores acima 0,6 para o índice KMO (MALHOTRA, 2012). No entanto, devido ao baixo número de respondentes para as variáveis PSC2, PSC3 e PSC4 — 54 respondentes — o KMO ficou abaixo de 0,6, conforme demonstrado no Quadro 4. No questionário da pesquisa original (LIANG E XUE, 2010) estas questões eram obrigatórias, pois os pesquisadores selecionaram respondentes que não possuíam spyware em suas estações de trabalho, algo fundamental para a percepção mensurada por essas questões. Entretanto, durante a validação de face e conteúdo foi indicada a necessidade de tornar essas questões opcionais, através da criação da questão PSC1. Cogitou-se, durante essa indicação, que a aplicação deste mesmo critério de seleção de respondentes, conjuntamente ao critério já estabelecido — orientação sobre SEGINF (Segurança da Informação) — poderia dificultar a obtenção de uma amostra adequada à pesquisa.

Ao não incluir as variáveis PSC2, PSC3 e PSC4 na Análise Fatorial do pré-teste o índice KMO obteve o valor de 0,700 para as os construtos (fatores) independentes, como apresentado no Quadro 5.

O Quadro 6 demonstra que foi obtido valor 0,687 para o índice KMO do construto (fator) dependente, composto pelas variáveis BEH1, BEH2 e BEH3.

Os resultados dos testes de esfericidade apresentados nos Quadros 4, 5 e 6 indicam que os resultados são válidos ($p<0,001$).

Quadro 4 - Resultado do teste de KMO e Bartlett dos fatores independentes no pré-teste com variáveis PSC

KMO and Bartlett's Test		
Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		0,557
Bartlett's Test of Sphericity	*Approx. Chi-Square*	261,328
	df	105
	Sig.	,000

Fonte: Autor

Quadro 5 - Resultado do teste de KMO e Bartlett dos fatores independentes no pré-teste sem variáveis PSC

KMO and Bartlett's Test		
Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		0,700
Bartlett's Test of Sphericity	*Approx. Chi-Square*	817,859
	df	66
	Sig.	0,000

Fonte: Autor

Quadro 6 - Resultado do teste de KMO e Bartlett do fator dependente (BEH) no pré-teste

KMO and Bartlett's Test		
Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		*0,687*
Bartlett's Test of Sphericity	*Approx. Chi-Square*	90,444
	df	3
	Sig.	0,000

Fonte: Autor

A Tabela 3 demonstra o total da variância explicada dessa análise. A Tabela 4 demonstra o resultado da Análise Fatorial com os dados coletados no pré-teste após a retirada das questões BEH4, PUNSEV1, SEV2, PSC2, PSC3 e PSC4.

Tabela 3 - Total da variância explicada pelos fatores independentes no pré-teste

Fatores	*Extraction Sums of Squared Loadings*			*Rotation Sums of Squared Loadings*		
	Total	% da Variância	Acumulado %	Total	% da Variância	% Acumulado
1	2,995	24,960	24,960	2,445	20,371	20,371
2	2,367	19,728	44,689	2,193	18,279	38,650
3	1,778	14,814	59,502	1,590	13,246	51,896
4	1,253	10,442	69,944	1,519	12,659	64,555
5	0,831	6,921	76,865	1,477	12,310	76,865
Método de Extração: *Principal Component Analysis.*						

Fonte: Autor

Tabela 4 - Matriz de componentes rotacionados das variáveis independentes no pré-teste

Variáveis	Fatores				
	1 (SUS)	2 (DESC)	3 (PUNSEV)	4 (DECERT)	5 (SEV)
SUS2	**0,895**	0,002	-0,068	-0,103	0,061
SUS1	**0,890**	-0,184	-0,031	-0,056	0,076
SUS3	**0,882**	0,075	-0,015	-0,001	0,103
DESC3	0,033	**0,885**	0,052	0,125	-0,019
DESC2	-0,009	**0,824**	-0,005	0,183	0,075
DESC1	-0,102	**0,798**	0,045	-0,030	-0,024
PUNSEV3	-0,039	0,125	**0,852**	0,138	0,120
PUNSEV2	-0,049	-0,049	**0,847**	0,215	-0,067
DECERT1	0,007	0,103	0,124	**0,894**	0,068
DECERT2	-0,180	0,157	0,300	**0,750**	0,055
SEV1	0,155	-0,019	-0,092	-0,042	**0,856**
SEV3	0,048	0,040	0,150	0,160	**0,832**

Observação: *Rotation converged in 5 iterations.*

Método de Extração: *Principal Component Analysis.*

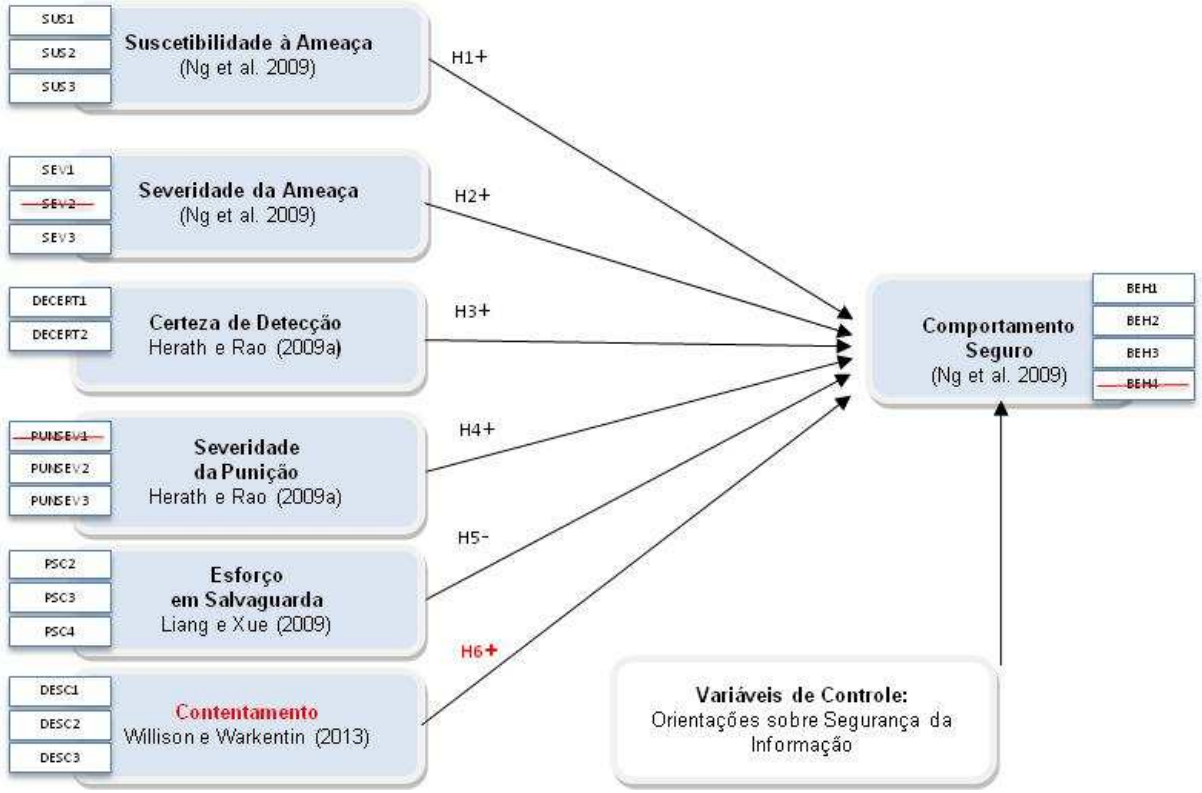
Método de Rotação: *Varimax with Kaiser Normalization*

Fonte: Autor

Nessa etapa também foi optado por manter as questões PSC2, PSC3 e PSC4 no questionário (instrumento de pesquisa) para a coleta final, apesar do baixo número de respondentes que as preencheram durante a coleta do pré-teste. Entretanto, as questões BEH4, PUNSEV1, SEV2 foram retirados do questionário antes da coleta final.

O resultado dos processos de validação apresentados anteriormente está sumarizado na Figura 5. As variáveis (questões) estão ao lado dos respectivos construtos e os itens tachados indicam as questões que foram eliminadas no instrumento de pesquisa final, antes de realizar a coleta final. A Figura 4 também demonstra a mudança do construto Descontentamento para Contentamento, como resultado da Análise de Face e Conteúdo.

Figura 5- Resumo das alterações após validações



Fonte: Autor

5.2 COLETA DE DADOS FINAL

Após a adaptação do questionário, na fase de pré-teste, foi realizada coleta de dados de forma presencial, através de um formulário impresso, e paralelamente por intermédio de uma *survey* eletrônica, publicada em www.pucrs.qualitrics.com, cujo link foi distribuído via e-mail. A versão final impressa do instrumento de pesquisa consta no Apêndice A.

5.2.1 Amostragem na Coleta de Dados Final

A coleta final iniciou através de formulário impresso em 21/10/2013 e no modo online em 04/11/2013, sendo que ambas encerraram em 02/12/2013. Na versão impressa foram entregues 106 formulários a respondentes em turmas da pós-graduação da PUCRS e UFRGS -— incluindo cursos de especialização, mestrado e doutorado da área de administração — obtendo 83 respondentes válidos, com o questionário preenchido completamente e sem erros no preenchimento. O tempo médio de preenchimento foi de 14 minutos.

Nessa pesquisa foi utilizada uma amostra não probabilística por conveniência (HAIR et al., 2005). Foram escolhidos, ao acaso, turmas dos cursos da PUCRS e UFRGS. A coleta foi realizada através de um questionário autoadministrado com 33 questões, sendo 18 questões que participaram da Análise Fatorial e mais 15 questões sócio-demográficas e de

controle, que permitiram a identificação do perfil do respondente, através de análises estatísticas descritivas. Na versão eletrônica foram repassados 114 convites por e-mail, indicando o site onde estava hospedado o questionário eletrônico, obtendo 88 respondentes válidos, com o questionário preenchido completamente e sem erros no preenchimento. Foi solicitado a alguns respondentes que receberam convites por e-mail que repassassem o convite a demais colegas da organização e demais contatos pessoais.

Não foram considerados válidos os respondentes que não completaram totalmente o questionário, ou cometeram lapsos em relação à experiência profissional em comparação à idade.

Depois de finalizada a coleta foi estabelecido um filtro na base dados, selecionando apenas respondentes que já haviam recebido alguma orientação sobre Segurança da Informação da organização onde trabalhavam. Foi escolhido o termo “orientação”, com base na pesquisa de Puhakainen e Siponen (2010), por ser mais amplo e mais familiar a uma maior gama de respondentes. O filtro aplicado foi identificado no modelo teórico como variável de controle, a exemplo da pesquisa de Ng et al. (2009), também foram retirados *outliers* durante a análise dos dados. Essa filtragem resultou em 54 respondentes que preencheram o questionário eletrônico e em 58 respondentes que preencheram o questionário em papel.

Dessa forma dos 171 respondentes válidos, 112 receberam alguma orientação sobre SEGINF e foram utilizados na análise final dos dados. Ao considerar 112 respondentes e 15 questões na análise de dados final, o índice de respondentes por questão foi de 7,46.

5.2.2 Teste de diferenças entre as amostras finais online e em papel

Conforme indicado por Hair et al. (2005) foi realizado o Teste T através do software SPSS Statistics versão 20.0.2, para averiguar se haviam diferenças entre as respostas das amostras coletadas em papel, em comparação as respostas obtidas pela *survey* online.

Em ambos as amostras foi realizada uma análise de estatística descritiva para as dimensões (valores médios, diferenças de médias e desvio padrão), aplicação do teste de igualdade de médias, através teste t *Student* bicaudal, além da determinação do intervalo de confiança de 95% (MALHOTRA, 2012) e teste de Levene para igualdade das variâncias (DANCEY e READ, 2006). As diferenças apresentadas entre as duas amostras não foram significativas, exceto paras as variáveis PSC2, PSC3 e PSC4, que foram desconsideradas posteriormente, devido ao baixo número de respondentes. Essas três questões eram opcionais, e também obtiveram em um índice de Alfa de Cronbach muito baixo no pré-teste e na amostra final.

5.3 ANÁLISE DESCRITIVA DA AMOSTRA

A seguir é apresentada a caracterização da amostra, conforme a análise descritiva. Os respondentes foram caracterizados com base no cargo, tempo trabalhado na organização, tempo em que vêm utilizando recursos pessoais de TI para o trabalho, tempo na atual posição na organização e sua formação. A amostra foi formada por respondentes que são usuários de Sistemas de Informação em ambiente organizacional, que tenham recebido orientações sobre Segurança da Informação de forma escrita ou oral, por parte da organização onde trabalham ou estudam atualmente.

A amostra da pesquisa foi composta por 112 respondentes. A seguir são apresentadas e analisadas, com o auxílio de tabelas, as características desses participantes. O porte da organização foi mensurado pelo nº de funcionários na organização onde o respondente estava trabalhando, o resultado consta na Tabela 5. Essa informação visa identificar se os respondentes que atuavam em organizações de grande porte recebiam orientações sobre Segurança da Informação mais frequentemente do que em organizações menores, conforme demonstrado na Figura 6.

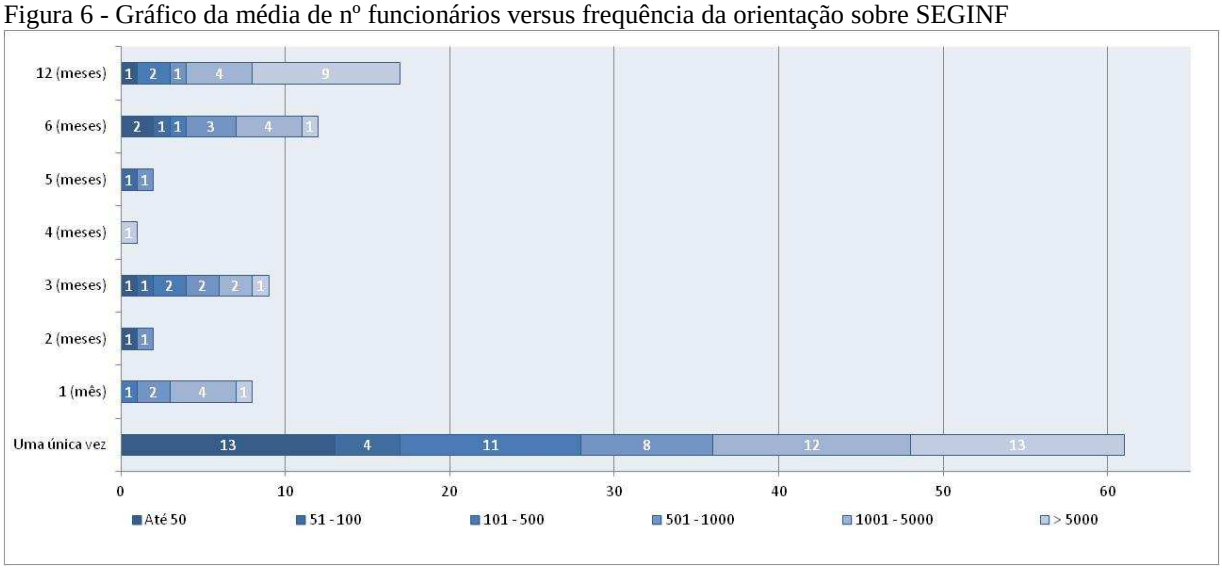
Tabela 5 - Perfil parcial dos respondentes

		N º de Funcionários da Organização	Anos de Experiência Profissional	Idade
Média		13754,26	14,75	34,55
Mediana		1000,00	13,00	32,50
Moda		1000	20	25
Desvio Padrão		40601,406	9,889	9,985
Variância		1648474165,563	97,797	99,691
Percentil	25	200,00	7,00	27,00
	50	1000,00	13,00	32,50
	75	5000,00	20,00	40,00

Fonte: Autor

A variância apresentou um alto valor na Tabela 5, devido a grande heterogeneidade do número de funcionários na organização onde o respondente estava trabalhando, com o valor mínimo de três funcionários e o máximo de 310.000 funcionários.

Figura 6 - Gráfico da média de nº funcionários versus frequência da orientação sobre SEGINF



Fonte: Autor

Como pode ser percebido na Figura 6, nove respondentes que trabalhavam em organizações com mais de 5.000 funcionários informaram que recebiam orientações com uma frequência de 12 meses, em contrapartida, 13 respondentes que trabalhavam em organizações com até 50 pessoas receberam orientações uma única vez.

A Tabela 6 identifica o segmento de atuação da organização onde o respondente estava trabalhando, com destaque para o segmento de serviços.

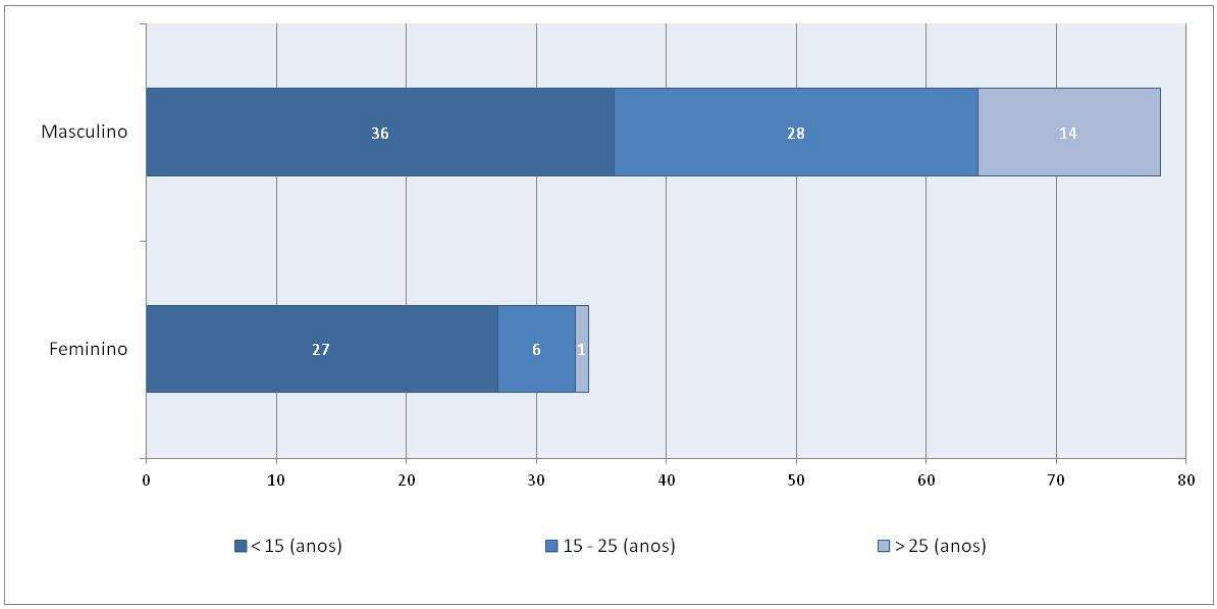
Tabela 6 - Segmento da organização onde o respondente trabalha

Segmento da organização	Frequência	Percentual
Indústria	18	16,1%
Comércio	9	8,0%
Serviços	54	48,2%
Governo	14	12,5%
Outros	17	15,2%
Total	112	100,0%

Fonte: Autor

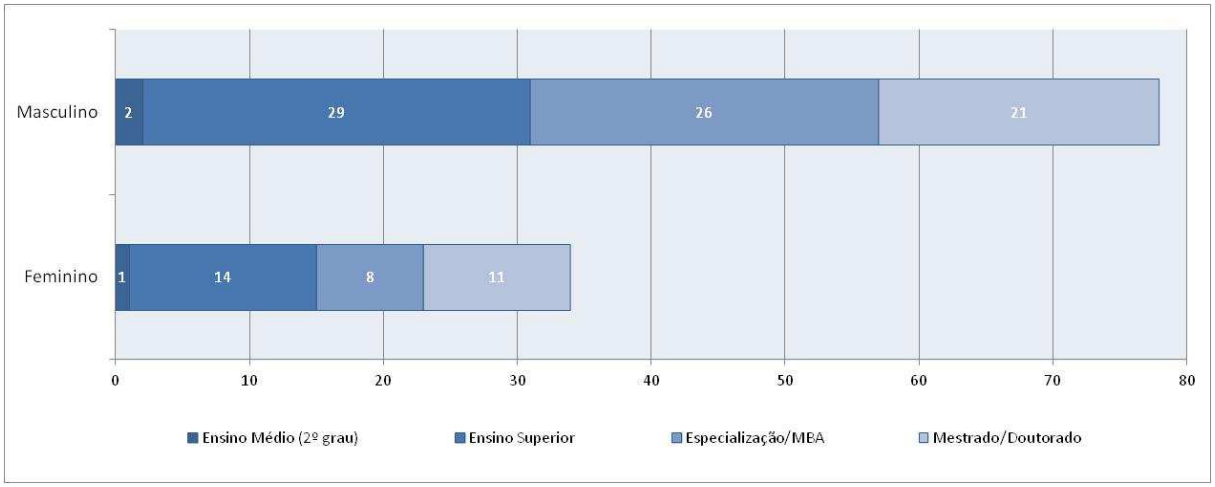
A Figura 7 e 8 expõem dados demográficos dos respondentes como gênero e área de formação e os respectivos cruzamentos dessas informações, demonstrando que os respondentes possuem uma média alta de experiência profissional e também tem um alto nível de escolaridade, possivelmente motivado pelo tipo da amostragem.

Figura 7 - Perfil dos respondentes: gênero versus experiência profissional



Fonte: Autor

Figura 8 - Perfil dos respondentes: gênero versus escolaridade



Fonte: Autor

A Tabela 7 exibe dados relativos à área de formação, com a maioria dos respondentes possuindo formação na área de Administração e Informática.

Tabela 7 - Área de formação dos respondentes

Área de formação	Frequência	Percentual
Administração	51	45,5%
Informática	45	40,2%
Direito	1	0,9%
Engenharia	4	3,6%
Outra	11	9,8%
Total	112	100,0%

Fonte: Autor

Com objetivo de fornecer subsídios para a análise dos resultados foram questionadas informações relativas à experiência prévia com *malwares* e a experiência profissional do respondente na área de informática, com os resultados descritos nas Tabelas 8 e 9.

Tabela 8 - Respondentes que trabalham ou já trabalharam na área de informática

Você já trabalhou ou trabalha atualmente na área de Informática ou Tecnologia da Informação?	Frequência	Percentual
Sim	78	69,6%
Não	34	30,4%
Total	112	100,0%

Fonte: Autor

Tabela 9 - Experiência prévia com *malware*

Algum dispositivo de TI que você utilizou (computador, smartphone, notebook, laptop, etc.), profissionalmente ou pessoalmente, já foi infectado por um *malware*?	Frequência	Percentual
Sim	83	62,9%
Não	40	30,3%
Não sei.	9	6,8%
Total	132	100,0%

Fonte: Autor

5.3.1 Análise Descritiva Univariada

A Análise Descritiva Univariada que considera cada uma das variáveis individualmente, foi realizada através da caracterização da amostra, através da frequência simples e percentuais; e itens das escalas de mensuração, incluindo medidas de tendência central (média e desvio padrão), conforme demonstrado na Tabela 10. Através da Análise Univariada é possível verificar o padrão médio das respostas obtidas para cada uma das variáveis observáveis do modelo de mensuração.

A normalidade dos dados coletados foi verificada juntamente com a Análise Descritiva Univariada. A normalidade é a suposição mais fundamental no âmbito da inferência estatística dentro do escopo da análise multivariada e considera a forma de distribuição dos dados em sua correspondência à distribuição normal como base de referência dos métodos estatísticos (HAIR et al., 2009).

A verificação da normalidade foi realizada pela análise de simetria e de curtose. A assimetria mensura a distribuição simétrica, em uma distribuição simétrica média, mediana e a moda estão na mesma localização. A curtose é a medida do pico de uma distribuição (HAIR et al., 2005). Segundo Kline (2011), valores de assimetria acima de 3 podem ser descritos como extremamente assimétricas e valores de curtose acima de 10 podem sugerir um problema. Na análise não foi encontrado nenhum item com valores superiores aos limites, conforme Tabela 10, confirmando a suposição de normalidade em relação à distribuição dos dados amostrais.

Tabela 10 - Análise estatística descritiva da amostra

Variáveis	N	Média	Desvio Padrão	Variância	Assimetria		Curtose	
					Valor (*statistic*)	Erro Padrão (*std. error*)	Valor (*statistic*)	Erro Padrão (*std. error*)
BEH1	112	4,73	0,520	0,270	-1,816	0,228	2,499	0,453
BEH2	112	4,55	0,655	0,430	-1,179	0,228	0,212	0,453
BEH3	112	4,16	1,087	1,181	-1,012	0,228	-0,379	0,453
DETCERT1	112	3,96	1,150	1,322	-1,034	0,228	0,347	0,453
DETCERT2	112	3,58	1,144	1,309	-0,403	0,228	-0,654	0,453
DESC1	112	4,03	0,765	0,585	-0,292	0,228	-0,574	0,453
DESC2	112	3,76	0,942	0,887	-0,551	0,228	-0,210	0,453
DESC3	112	3,93	0,824	0,680	-0,455	0,228	0,248	0,453

PUNSEV2	112	2,92	1,253	1,570	0,154	0,228	-0,911	0,453
PUNSEV3	112	3,26	1,214	1,473	-0,051	0,228	-1,053	0,453
SEV1	112	4,10	1,280	1,639	-1,210	0,228	0,164	0,453
SEV3	112	3,88	1,129	1,275	-0,724	0,228	-0,444	0,453
SUS1	112	2,85	1,261	1,589	0,319	0,228	-1,032	0,453
SUS2	112	3,02	1,388	1,928	0,070	0,228	-1,281	0,453
SUS3	112	3,12	1,327	1,761	0,089	0,228	-1,272	0,453

Fonte: Autor

5.4 ANÁLISE DE CONFIABILIDADE DO INSTRUMENTO DE PESQUISA

A etapa de análise preliminar dos dados e preparação da base dos dados para estudos envolveu uma análise cuidadosa, que levou a resultados mais apurados e diretamente ligados as características dos dados e relações das variáveis, o que permite uma melhor eliminação de alguns “ruídos” presentes nos dados brutos da pesquisa (HAIR et al., 2009). Conforme Hair et al. (2005) os primeiros passos envolvendo a análise de dados quantitativos deve envolver a verificação de *missing data* (não-resposta), *outliers*, análise da normalidade dos dados, a verificação da multicolinearidade e o cálculo da homoscedasticidade.

Previamente antes da digitação dos dados, os questionários foram conferidos pelo pesquisador, com o objetivo de verificar se todos se encontravam com preenchimento compreensível e adequado. Após esta etapa, foi realizada a análise dos *missing values*, que ocorre com frequência em questionários autoadministrados (HAIR et al., 2005). Foram identificados 18 respondentes com erros de preenchimento nas questões de confirmação, através do indicador de resíduo *Cook Distance* (HAIR et al., 2009) e do *Anomalous Cases* do SPPS, que identificou 4 respondentes em relação às questões de confirmação do construto Severidade da Ameaça.

A confiabilidade das escalas foi aferida pelo coeficiente de Alpha de Cronbach. A ferramenta utilizada nas análises foi o SPSS Statistics 20.0. Foi obtido um Alpha de Cronbach de **0,767** para o conjunto de todas as 15 variáveis obrigatórias, que mensuravam os construtos dos modelos. O Alpha de Cronbach de cada grupo de questões, referentes a cada construto do modelo teórico, constam na Tabela 11.

Tabela 11 - Alfa de Cronbach dos construtos na coleta oficial

Construto	Variáveis / Questões	Alfa de Cronbach
Suscetibilidade à ameaça (SUS)	SUS1, SUS2 e SUS3	0,857
Contentamento (DESC)	DESC1, DESC2 e DESC3	0,819
Severidade da Punição (PUNSEV)	PUNSEV2 e PUNSEV2	0,852
Comportamento Seguro (BEH)	BEH1, BEH2 e BEH3	0,725
Certeza de Detecção (DETCERT)	DETCERT1 e DETCERT2	0,684
Severidade da Ameaça (SEV)	SEV1 e SEV3	0,615
Esforço em Salvaguarda (PSC)	PSC2, PSC3 e PSC4 (questões opcionais)	0,591

Fonte: Autor

Segundo Hair et al. (2005) valores a partir de 0,6 para o Alfa de Cronbach são aceitáveis para pesquisa exploratórias, quando são definidos novos instrumentos de pesquisa, como é o caso dessa pesquisa, na qual está sendo criado um novo modelo teórico e um novo questionário a partir da evolução de questionários já existentes e bem conceituados.

As questões opcionais das variáveis PSC2, PSC3, PSC4 obtiveram o um índice muito baixo de Alfa de Cronbach, devido ao baixo número de respondentes que preencheram essas questões (N=35). Dessa forma, essas variáveis e o respectivo construto “Esforço em Salvaguarda” (LIANG e XUE, 2010) que elas mensuram, não foram utilizadas no restante da pesquisa, acarretando na ausência de suporte a hipótese H5. Nessa decisão também foram considerados demais índices estatísticos, como a diferença no Teste *T* e a falta de convergência para o respectivo fator na Análise Fatorial Convergente.

5.5 ANÁLISE FATORIAL CONVERGENTE

Com o objetivo de ampliar a consistência e o potencial de generalização dos resultados foi elaborada uma Análise Fatorial Convergente, que analisa o padrão de correlações existentes entre as variáveis e utiliza esses padrões de correlações para convergir (agrupar) suas variáveis em fatores, com uma rotação Varimax. Para Hair et al. (2009), este método de rotação dos fatores é o mais comumente usado, sendo considerado o melhor em comparação a outros tipos de rotação, por gerar uma estrutura fatorial simplificada.

O fator dependente no modelo teórico (BEH) foi obtido a partir de três variáveis dependentes (BEH1, BEH2 e BEH3). As cargas fatoriais das variáveis desse fator são demonstradas na Tabela 12.

Tabela 12 - Matriz de componentes rotacionados das variáveis dependentes

Variáveis	Fator Dependente (BEH)
BEH2	0,860
BEH1	0,809
BEH3	0,741
Método de Extração: *Principal Component Analysis.*	

Fonte: Autor

Os cinco fatores independentes que foram obtidos pela Análise Fatorial a partir das variáveis independente do modelo teórico constam na tabela 13. A Tabela 14 demonstra que 79,371% da foi variância explicada por esses fatores.

Tabela 13 - Matriz de componentes rotacionados das variáveis independentes

Variáveis	Fatores				
	1 (SUS)	2 (DESC)	3 (PUNSEV)	4 (DECERT)	5 (SEV)
SUS1	**0,894**	-0,031	-0,148	0,080	0,146
SUS2	**0,868**	-0,085	-0,092	-0,003	0,060
SUS3	**0,854**	0,056	-0,003	-0,081	0,046
DESC1	0,015	**0,875**	0,023	0,054	-0,106
DESC2	-0,102	**0,861**	-0,133	-0,095	0,115
DESC3	0,029	**0,819**	0,168	0,091	0,175
PUNSEV3	-0,083	0,025	**0,899**	0,108	0,203
PUNSEV2	-0,142	0,011	**0,890**	0,208	0,111
DETCERT1	0,077	-0,105	0,121	**0,900**	0,002
DETCERT2	-0,121	0,212	0,220	**0,774**	0,285
SEV1	0,223	-0,005	0,052	0,153	**0,821**
SEV3	0,022	0,152	0,282	0,052	**0,792**
Observação: *Rotation converged in 5 iterations.* Método de Extração: *Principal Component Analysis.* Método de Rotação: *Varimax with Kaiser Normalization*					

Fonte: Autor

Tabela 14 - Total da variância explicada pelos fatores independentes

Fatores	*Extraction Sums of Squared Loadings*			*Rotation Sums of Squared Loadings*		
	Total	% da Variância	Acumulado %	Total	% da Variância	% Acumulado
1	2,962	24,683	24,683	2,393	19,940	19,940
2	2,536	21,135	45,818	2,268	18,904	38,844
3	2,114	17,618	63,436	1,821	15,177	54,021
4	1,062	8,849	72,285	1,523	12,693	66,713
5	0,850	7,086	79,371	1,519	12,658	79,371
Método de extração: *Principal Component Analysis.*						

Fonte: Autor

Durante a Análise Fatorial foi verificado o índice de Kaiser-Meyer-Olkin (KMO) que sinaliza a adequação da amostra. Pequenos valores no KMO indicam que a análise fatorial pode ser inapropriada (MALHOTRA, 2012). Segundo Malhotra (2012) é indicado valores superiores 0,6 para o índice KMO. O índice KMO obtido foi 0,677 para as os construtos (fatores) independentes e 0,646 para os construtos (fatores) dependentes, sendo que teste de esfericidade indica que o resultado é válido (p<0,001), conforme apresentados no campo *Sig.* nos Quadros 7 e 8.

Quadro 7 - Resultado do teste de KMO e Bartlett dos fatores independentes

KMO and Bartlett's Test		
Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		0,677
Bartlett's Test of Sphericity	*Approx. Chi-Square*	*541,121*
	df	*66*
	Sig.	*0,000*

Fonte: Autor

Quadro 8 - Resultado do teste de KMO e Bartlett do fator dependente (BEH)

KMO and Bartlett's Test		
Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		*0,646*
Bartlett's Test of Sphericity	*Approx. Chi-Square*	*72.185*
	df	*3*
	Sig.	*0,000*

Fonte: Autor

A comunalidade representa a quantidade de variância em uma única variável, que é explicada pelos fatores extraídos através de uma Análise Fatorial (HAIR et al., 2005). Na Análise Fatorial Convergente as comunalidades apresentaram resultados satisfatórios, conforme Tabela 15. As comunalidades foram extraídas pelo método *Principal Component Analysis*, sendo que nenhuma variável indicou índice abaixo de 0,5. Segundo Malhotra (2012), quando a comunalidade está abaixo de 0,5 não fornece explicação suficiente para o que está mensurando, necessitando amostras maiores.

Tabela 15 - Comunalidades das variáveis dependentes e independentes

Comunalidades das variáveis independentes		**Comunalidades das variáveis dependentes**	
Variável	Extração	Variável	Extração
DETCERT1	0,841	BEH1	0,654
DETCERT2	0,788	BEH2	0,739
DESC1	0,780	BEH3	0,548
DESC2	0,793		
DESC3	0,738		
PUNSEV2	0,868		
PUNSEV3	0,868		
SEV1	0,750		
SEV3	0,733		
SUS1	0,850		
SUS2	0,773		
SUS3	0,742		

Fonte: Autor

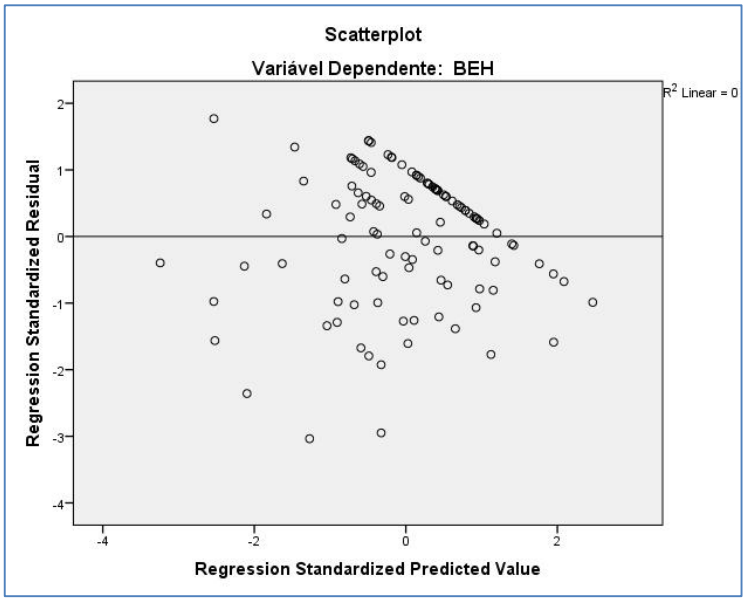
Hair et al. (2009) sugerem que o nível de significância de 0,001 seja estabelecido para identificar observações atípicas multivariadas, verificáveis através da analise dos índices de multicolinearidade e homoscedasticidade dos dados.

A multicolinearidade significa a existência de uma perfeita relação linear entre algumas variáveis explicativas de um modelo, já a homoscedasticidade dos dados se refere à suposição de que as variáveis dependentes exibem níveis iguais de variância entre as variáveis preditoras (HAIR et al., 2009). A multicolinearidade foi verificada através do cálculo de

valores de tolerância e do fator de inflação da variância (FIV) (MALHOTRA, 2012), calculado através da regressão linear. O FIV mede o quanto a variância dos coeficientes de regressão está afetada por problemas de multicolinearidade (HAIR et al., 2009), a tolerância, por sua vez, é a quantidade de variância em uma variável independente que não é explicada pelas outras variáveis independentes. Segundo Hair et al. (2009), quando o FIV é 1 significa que a tolerância é 1 e por isso não existe multicolinearidade.

A homoscedasticidade foi verificada através do diagrama de dispersão, apresentado na Figura 9.

Figura 9 - *Scatterplots* bivariado para avaliação homoscedasticidade



Fonte: Autor

O teste de homoscedasticidade dos dados se refere à suposição de que as variáveis dependentes exibem níveis iguais de variância entre as variáveis preditoras (HAIR et al., 2009). Pode ser analisada através de diagramas de dispersão, em que uma relação homoscedástica entre os pontos de dados para duas variáveis exibirá igual dispersão em todos os valores dos dados. Caso exista uma dispersão desigual, as previsões serão melhores em alguns níveis da variável dependente do que em outros, tornando futuros testes de hipóteses acentuadamente conservadores ou sensíveis (HAIR et al., 2005). Na análise dos diagramas de dispersão houve dispersão simétrica dos valores dos dados, indicando existir homoscedasticidade, conforme Figura 9. A linearidade foi avaliada pela inspeção de *scatterplots* bivariado, demonstrando que a relação entre duas variáveis representa uma função linear, ou seja, variações em uma variável produzirão variações linear e constante na variável relacionada. Sendo verificado através da verificação gráfica dos *scatterplots*, todas as

dimensões do modelo estudado apresentaram relações lineares, não surgindo relações curvilíneas (quadráticas ou cúbicas).

5.6 ANÁLISE DE REGRESSÃO LINEAR MÚLTIPLA

Para confirmar as relações entre os construtos, a partir dos fatores da Análise Fatorial, foi realizada uma Análise de Regressão Linear Múltipla entre os fatores independentes e o fator dependente.

Segundo Malhotra (2012) a análise de regressão é um procedimento estatístico para analisar relações associativas entre uma variável dependente métrica e uma ou mais variáveis independentes. Trata-se de um procedimento poderoso e flexível para a análise de relações associativas entre uma variável dependente métrica e uma ou mais variáveis independentes, e pode ser utilizada para: a) determinar se as variáveis independentes explicam uma variação significativa na variável dependente; b) determinar quanto da variação na variável dependente pode ser explicado pelas variáveis independentes; c) determinar a estrutura ou a forma da relação; d) predizer os valores da variável dependente e e) controlar outras variáveis independentes a partir da avaliação das contribuições de uma variável ou um conjunto de variáveis específicas.

Conforme Malhotra (2012), análise de regressão múltipla, ou apenas regressão múltipla, envolve uma única variável dependente e duas ou mais variáveis independente. A análise de regressão, segundo Hair et al. (2005), é uma das técnicas estatísticas mais amplamente utilizada para mensurar relações lineares entre duas ou mais variáveis e permite indicar se existe relação entre duas variáveis e a força dessa relação, é frequentemente empregada com o objetivo de prever o impacto de uma variável X em outra variável Y (HAIR et al., 2005). Em outras palavras, o procedimento tenta estimar os valores de Y, que é variável dependente, a partir de mudanças nos valores de X, que é a variável independente (DANCEY e REIDY, 2006; HAIR et al., 2005).

A função geral que identifica esse comportamento consta no Quadro 9 (DANCEY e REIDY, 2006; HAIR et al., 2005):

Quadro 9 - Função da Regressão Linear

$Y = a + bX$

Fonte: Dancey e Reidy (2006)

Onde: Y é um valor da variável a ser prevista; X é um valor da variável preditora de Y; *a* é o ponto onde a linha intercepta o eixo Y quando X é 0; *b* é a inclinação da linha, ou a respectiva mudança em Y para qualquer mudança correspondente em uma unidade de X.

A Análise de Regressão foi utilizada para predizer o Comportamento Seguro a partir da Suscetibilidade à Ameaça (SUS), Severidade da Ameaça (SEV), Certeza de Detecção (DETCERT), Severidade da Punição (PUNSEV) e o Contentamento (DESC).

O principal resultado da regressão linear é o R2, denominado coeficiente de correlação ao quadrado, ou coeficiente de determinação, que indica o percentual de variação total da variável dependente, a partir das variáveis independentes, dentro de um modelo de regressão (HAIR et al., 2009). Se o modelo de regressão prevê perfeitamente a variável dependente, o valor de R^2 será igual a 1,0 (HAIR et al., 2009).

O coeficiente de correlação ao quadrado obtido pelo modelo teórico final da pesquisa foi 0,413, conforme Tabela 16, indicando que os construtos (fatores) mensurados pelo modelo final explicam 41,3% do Comportamento Seguro dos usuários respondentes desta pesquisa. O software utilizado nesta análise foi o SPPS Statistics versão 20.0.2.

Tabela 16 - Coeficiente de correlação do modelo teórico final da pesquisa

R	*R Square*	*Adjusted R Square*	*Std. Error of the Estimate*	*Change Statistics*				
				R Square Change	*F Change*	*df1*	*df2*	*Sig. F Change*
0,643	0,413	0,386	0,78389390	0,413	14,928	5	106	0,000
Fatores Preditores (variáveis): SEV (SEV1 e SEV3), DETCERT (DETCERT1 e DETCERT2), PUNSEV(PUNSEV1, PUNSEV2 e PUNSEV3), DESC (DESC1, DESC2e DESC3), SUS (SUS1,SUS2 e SUS3)								
Fator dependente (variáveis): BEH (BEH1, BEH2 e BEH3)								

Fonte: Autor

A pesquisa de Herath e Rao (2009a), que foi utilizada como origem para as questões dos construtos Certeza de Detecção (DETCERT) e Severidade da Punição (PUNSEV) alcançou um R2 muito próximo desse (0,42). Para Hair et al. (2005) um coeficiente de correlação que esteja na faixa de valores de $\pm 0{,}41$ a $\pm 0{,}7$ tem uma força de associação moderada.

Na Tabela 16 o R representa o *r* de Pearson, denotando uma correlação de 0,643 (DANCEY e REIDY, 2006). O *Std. Error of the Estimate* é o erro padrão estimado, segundo Hair et al. (2009) trata-se da raiz quadrada da soma dos quadrados dos erros individuais

dividida pelo número de graus de liberdade e representa uma estimativa do desvio-padrão dos valores reais dependentes em torno da reta de regressão.

Na Tabela 17 são apresentados os coeficientes de regressão padronizado *Beta*, indicando o impacto da associação entre a variável dependente e a variável independente e reflete a importância da variável independente sobre a dependente (HAIR et al., 2009). O resumo das associações suportadas ou não suportadas que dão suporte as hipóteses, consta no modelo final da pesquisa, que é demonstrado na Figura 10.

Tabela 17 - Impacto da associação entre as variáveis independentes e a dependente

Fatores	*Unstandardized Coefficients*		*Standardized Coefficients*	*t*	*Sig.*	*Correlations*			*Collinearity Statistics*	
	B	*Std. Error*	*Beta*			*Zero-order*	*Partial*	*Part*	*Tolerance*	*VIF*
SUS	0,362	0,074	**0,362**	40,860	**0,000**	0,362	00,427	00,362	1,000	1,000
DESC	0,443	0,074	**0,443**	50,950	**0,000**	0,443	0,500	0,443	1,000	1,000
PUNSEV	0,018	0,074	0,018	0,247	0,806	0,018	0,024	0,018	1,000	1,000
DETCERT	0,155	0,074	**0,155**	20,087	**0,039**	0,155	0,199	0,155	1,000	1,000
SEV	0,249	0,074	**0,249**	30,347	**0,001**	0,249	0,309	0,249	1,000	1,000
Fator dependente: BEH										

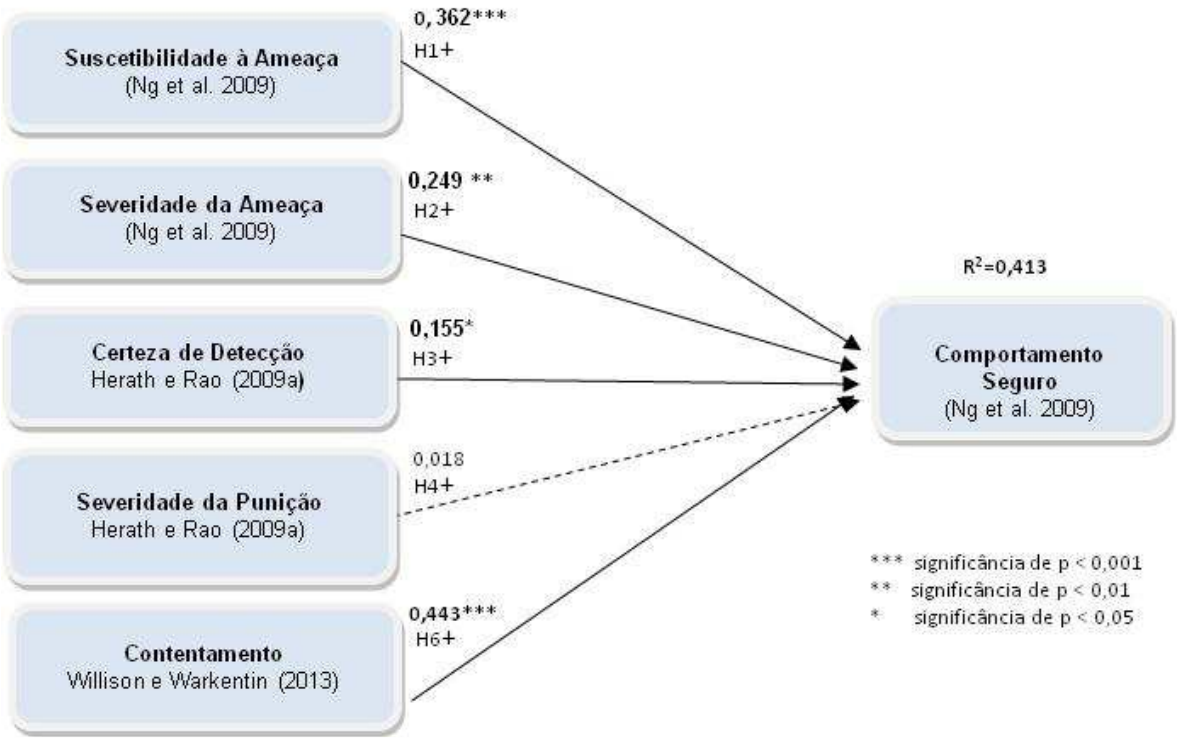
Fonte: Autor

A coluna *Sig*. da Tabela 17 indica o grau de significância estatística do coeficiente de regressão indicada por *Beta*, nessa coluna estão destacadas em negrito as associações que possuem significância estatística.

O VIF (Fator de Inflação da Variância) com valor 1,0 indica que não há multicolinariedade (HAIR et al., 2009).

A Figura 10 sumariza os resultados obtidos na Análise de Regressão Linear Múltipla.

Figura 10 - Regressão linear do modelo final



Fonte: Autor

A Figura 10 apresenta o modelo final da pesquisa, no qual os construtos Suscetibilidade à Ameaça, Severidade da Ameaça, Certeza de Detecção e Severidade da Punição são apresentados como variáveis independentes e indutores positivos, influenciando positivamente a variável dependente denominada Comportamento Seguro. Por outro lado, o construto Esforço de Salvaguarda é uma variável independente, apresentada como indutor negativo, que pode influenciar negativamente a variável Comportamento Seguro.

O construto Contentamento originou-se do construto Descontentamento, o termo foi alterado após as orientações da etapa de validação de face e conteúdo do instrumento de pesquisa. Este construto é uma variável independente e indutora positiva da variável dependente Comportamento Seguro.

Na Figura 10 as linhas tracejadas indicam as hipóteses não suportadas e as linhas contínuas as hipóteses suportadas, nas quais os índices de associação entre a variável independente e a dependente fornecem suporte à hipótese. Os asteriscos indicam a significância estatística.

5.7 MODELAGEM DE CAMINHO PELOS MÍNIMOS QUADRADOS PARCIAIS

Para confirmar os resultados obtidos na regressão linear foram utilizados técnicas de Modelagem de Caminho pelos Mínimos Quadrados Parciais. Conforme Henseler et al. (2009)

os Mínimos Quadrados Parciais (PLS na sigla em inglês) são uma família de algoritmos, que se estendem desde a análise de componentes principais até a análise de correlação canônica. O método foi desenvolvido para a análise de dados de alta dimensão em um ambiente com pouca estrutura e passou por várias ampliações e modificações. Para Kline (2011), esta técnica é basicamente uma extensão da técnica de correlação, mas que explicitamente distingue entre os indicadores e os fatores, permitindo a estimativa dos efeitos diretos e indiretos entre os fatores. Semelhante à correlação, os indicadores no PLS são ponderados de modo a maximizar a previsão. Os métodos de estimação do PLS fazem menos exigências de dados em comparação ao MEE (Modelagem de Equações Estruturais), consequentemente, o PLS pode ser aplicado em pequenas amostras, tornando mais fáceis a análise de modelos complexos com muitos indicadores, em comparação ao MEE (KLINE, 2011). Ainda conforme Kline (2011), no PLS são avaliados os valores de cargas fatoriais, coeficientes de trilha, e as estatísticas de regressão. As cargas fatoriais dos construtos são a correlação de cada variável com o fator do construto.

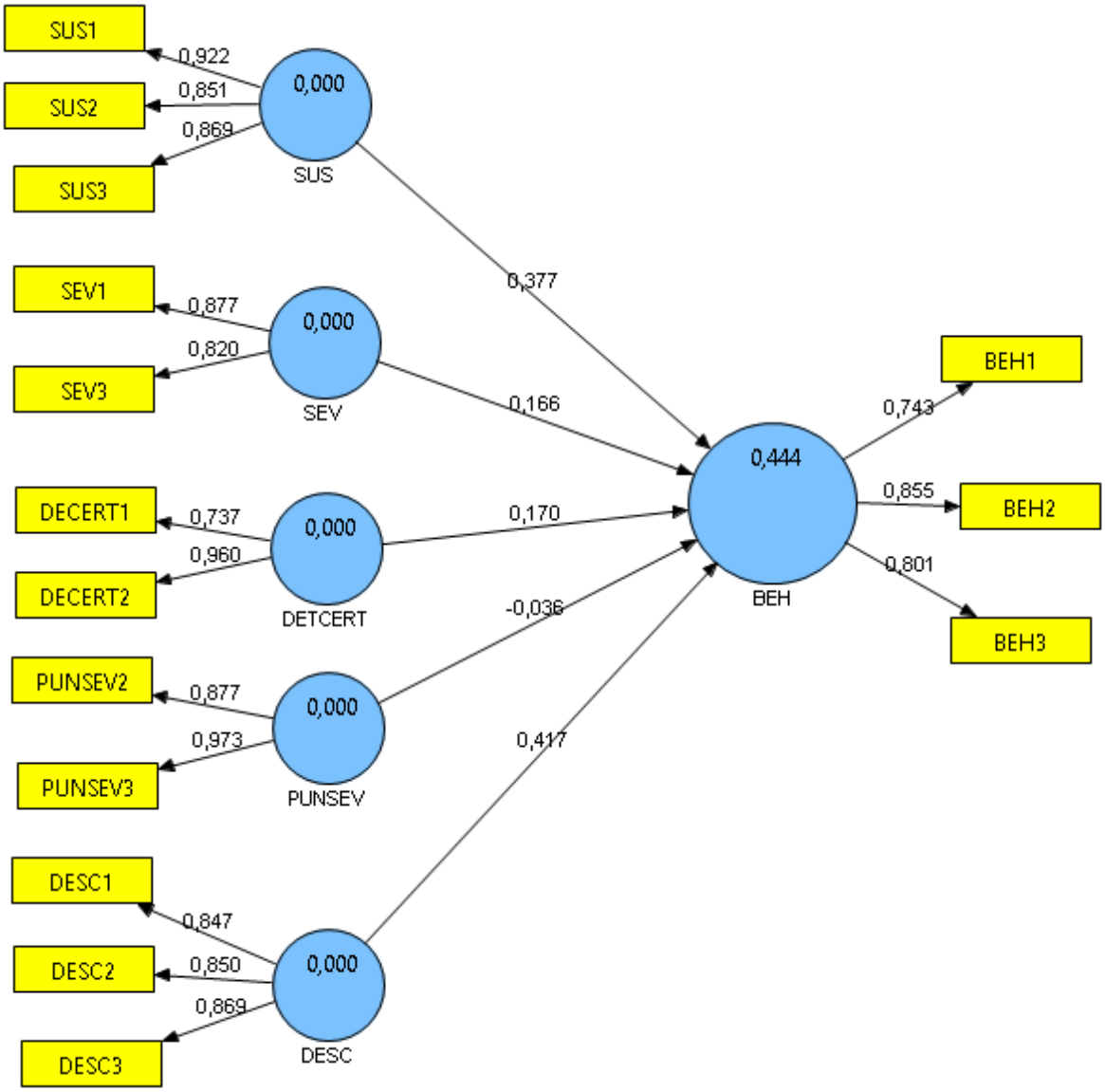
5.7.1 Etapas da Modelagem pelos Mínimos Quadrados Parciais

Conforme Goodhue et al. (2012) a regressão e o PLS têm três etapas: 1) determinar os coeficientes de ponderação para as variáveis de um construto; 2) usando os coeficientes de ponderação calcular os escores dos construtos compostos e através dos mínimos quadrados ordinários calcular estimativas do caminho; e 3) determinar a significância estatística do caminho estimado. Na regressão, o primeiro passo é normalmente realizado dando pesos iguais para todos os indicadores. Então os escores compostos são determinados e cada construto composto dependente e os seus preditores são analisados separadamente. A regressão utiliza os mínimos quadrados ordinários (álgebra linear) no cálculo da solução para os valores de caminho, que minimiza o quadrado das diferenças, entre o previsto e as pontuações reais para cada construto dependente. Não há iteração envolvida. A solução de regressão inclui estimativas do desvio padrão de cada caminho estimado, a partir do qual a significância estatística pode ser determinada, utilizando a teoria de distribuição normal (GOODHUE et al., 2012). No PLS, ao contrário da regressão que utiliza pesos iguais, há iterações através de um processo de busca pelos melhores pesos indicadores para cada construto, de modo que o R^2 dos construtos dependentes é maximizado. O segundo passo no PLS, assim como em uma regressão, é utilizar os pesos indicadores para calcular uma pontuação, que então é utilizada nos mínimos quadrados para determinar as estimativas finais do caminho. O terceiro passo no PLS determinar os desvios padrões daquele caminho

estimado como *bootstrapping*. Assim, o PLS e a regressão usam médias ponderadas de valores dos indicadores para desenvolver construir escores de construtos, e ambos utilizam mínimos quadrados para determinar os valores de caminho. A diferença fundamental entre os dois em termos de valores de caminho é que a regressão usa pontuações dos indicadores igualmente ponderadas, enquanto que PLS tem um processo destinado a otimizar os pesos (GOODHUE et al., 2012).

Conforme a Figura 11, o coeficiente de correlação R2, obtido pelo modelo calculado no software SmartPLS versão 2.0, foi 0,444.

Figura 11 - Análise de caminho para o Comportamento Seguro e seus coeficientes.



Fonte: Autor

O nível de significância foi calculado pelo algoritmo de *Bootstrapping*, com 5000 iterações de 112 casos, ou seja, o mesmo número de casos da amostra final (HAIR et al., 2013). O resultado é demonstrado na Tabela 18.

Segundo Hair et al. (2013), o número de interações de *bootstrap* deve ser maior que o número de observações válidas da amostra, geralmente, 5.000 iterações (amostras) de *bootstrap* são recomendadas. O número de casos do *bootstrapping* deve ser tão grande quanto o número de observações válidas no conjunto de dados da amostra original. A rotina de *bootsrap* fornece o erro padrão de um coeficiente estimado. Esta informação permite que seja determinado o valor de *p* empiricamente. Os valores e referência de *t* para um teste bicaudal são de 1,65 ($p = 0,10$), 1,96 ($p = 0,05$), ou 2,57 ($p = 0,01$).

Tabela 18 - Nível de significância pelo algoritmo de *Boostrapping*

	***Original Sample* (O)**	***Sample Mean* (M)**	***Standard Deviation* (STDEV)**	***Standard Error* (STERR)**	***T Statistics* (|O/STERR|)**
DESC -> BEH	0,416958	0,417115	0,062620	0,062620	6,658543**
DETCERT -> BEH	0,170367	0,169256	0,073178	0,073178	2,328130*
PUNSEV -> BEH	-0,035623	-0,024507	0,081394	0,081394	0,437662
SEV -> BEH	0,165529	0,167457	0,077485	0,077485	2,136253*
SUS -> BEH	0,376766	0,380539	0,063110	0,063110	5,969973**
Observação: ** equivalente à significância bicaudal p < 0,01 (HAIR et al., 2013). * equivalente à significância bicaudal p < 0,05 (HAIR et al., 2013).					

Fonte: Autor

5.7.2 Validade Convergente e Discriminante

Os valores da Média da Variância Extraída, ou *Average Variance Extracted* (AVE) em inglês, que são relativos à validade convergente, estão bem acima do nível mínimo requerido de 0,50 (HAIR et al., 2013), conforme demonstrando na Tabela 19. Os valores da Média da Variância Extraída foram calculadas pelo software SmartPLS versão 2.0.

Tabela 19 - Validade e confiabilidade convergente do modelo

Construto	AVE	*Composite Reliability*	*R Square*	Alpha de Cronbach	Comunalidade	Redundância
BEH	**0,6416**	0,8426	0,4436	0,7253	0,6416	0,0368
DETCERT	**0,7329**	0,8436		0,684	0,7329	
DESC	**0,7319**	0,8912		0,8185	0,7319	
PUNSEV	**0,8581**	0,9235		0,8522	0,8581	
SEV	**0,7208**	0,8376		0,6152	0,7208	
SUS	**0,776**	0,9121		0,8574	0,776	

Fonte: Autor

A validade convergente do modelo também foi avaliada através do SmartPLS versão 2.0, extraindo o fator e cargas significativas de todos os itens. Estes resultados, apresentados na Tabela 20, indicam que o fator de carga de cada variável em seu respectivo fator (construto) foi significativo e maior do que nos demais fatores.

Tabela 20 - Cargas significativas das variáveis do modelo

Variáveis	Construtos					
	BEH	DESC	DETCERT	PUNSEV	SEV	SUS
BEH1	0,742990	0,314727	0,111166	0,050939	0,193047	0,223113
BEH2	0,854574	0,448898	0,235647	0,030361	0,283170	0,299992
BEH3	0,801480	0,329076	0,253980	0,052235	0,368086	0,402844
DESC1	0,363092	0,847038	0,137294	0,029689	0,027848	-0,024371
DESC2	0,350543	0,850478	0,026638	-0,063750	0,112093	-0,078359
DESC3	0,448829	0,868944	0,239754	0,200701	0,253243	0,012271
DECERT1	0,116817	-0,058043	0,737077	0,253077	0,168604	0,053648
DECERT2	0,283565	0,235673	0,960464	0,381645	0,368622	-0,094226
PUNSEV2	0,029754	0,059147	0,413997	0,877408	0,276768	-0,206271
PUNSEV3	0,061649	0,081556	0,336904	0,972827	0,362358	-0,149110
SEV1	0,334283	0,077550	0,286529	0,235811	0,877427	0,279808
SEV3	0,279876	0,213234	0,304983	0,381676	0,819581	0,079425
SUS1	0,383137	-0,035175	0,008414	-0,198749	0,235202	0,921930
SUS2	0,260745	-0,095522	-0,078231	-0,181259	0,165686	0,850692
SUS3	0,380642	0,027219	-0,090628	-0,099495	0,176704	0,868513

Fonte: Autor

A validade discriminante demonstra o grau em que um construto mostra-se verdadeiramente distinto dos demais. Segundo HAIR et al. (2009), para que a validade discriminante seja identificada, todas as estimativas quadráticas das correlações devem ser estatisticamente significativas, com coeficientes menores que as estimativas das variâncias extraídas. A Tabela 21 demonstra esses resultados.

Tabela 21 - Validade discriminante do modelo

Construto	BEH	DETCERT	DESC	PUNSEV	SEV	SUS
BEH	**0,8009**					
DETCERT	0,2624	**0,8560**				
DESC	0,4581	0,1675	**0,8555**			
PUNSEV	0,0544	0,3844	0,0789	**0,9263**		
SEV	0,3636	0,3466	0,1638	0,3552	**0,8489**	
SUS	0,3971	-0,0571	-0,0309	-0,1781	0,2215	**0,8809**

Fonte: Autor

Os valores da linha diagonal da tabela, em negrito, representam a raiz quadrada das médias das variâncias extraídas dos construtos, enquanto que os demais valores expressam o coeficiente de correlação, calculados pelo software SmartPLS versão 2.0. Na Tabela 21 os valores em negrito são superiores aos demais valores da correlação entre os construtos da linha e coluna correspondentes, confirmando a validade discriminante dos construtos analisados.

Conforme pode ser observado, através das tabelas 18, 19, 20 e 21, as hipóteses suportadas e não suportadas na regressão linear foram confirmadas através da Modelagem pelos Mínimos Quadrados Parciais.

6 CONSIDERAÇÕES FINAIS

Neste capítulo são apresentadas as considerações finais acerca dos fatores que influenciam o Comportamento Seguro em relação à Segurança da informação, que foram mensurados através da presente pesquisa. As principais conclusões do trabalho estão descritas na Seção 6.1 e as contribuições para a pesquisa científica na área de Segurança da informação constam na Seção 6.2. Além disso, a Seção 6.3 apresenta as contribuições gerenciais e na Seção 6.4 são abordadas as limitações do trabalho e sugestões de pesquisas futuras.

6.1 CONCLUSÃO

Os resultados do estudo mostram que as percepções de Susceptibilidade à Ameaça, de Severidade da Ameaça e o Contentamento são determinantes do Comportamento Seguro, no que tange aos cuidados em relação à *malwares* em e-mails, fornecendo suporte às hipóteses H1, H2 e H6 e parcialmente à hipótese H3. Além disso, demonstram que os principais efeitos da percepção de Severidade da Punição não são significativos, sem fornecer suporte à hipótese H4 nessa pesquisa. Esses resultados são resumidos no Quadro 10.

Quadro 10 - Hipóteses suportadas pelo resultado da pesquisa

H1	A percepção de suscetibilidade da ameaça à Segurança da Informação influencia positivamente o comportamento seguro em relação à Segurança da Informação.	Suportada.
H2	A percepção de severidade da ameaça à Segurança da Informação influencia positivamente o comportamento seguro em relação à Segurança da Informação.	Suportada.
H3	A percepção da certeza de detecção por não seguir as orientações sobre Segurança da Informação influencia positivamente o comportamento seguro em relação à Segurança da Informação.	Suportada parcialmente.
H4	A percepção de severidade da punição por não seguir as orientações sobre Segurança da Informação influencia positivamente o comportamento seguro em relação à Segurança da Informação.	Não suportada.
H5	A percepção de esforço em salvaguarda em seguir as orientações sobre Segurança da Informação influencia negativamente o comportamento seguro em relação à Segurança da Informação.	Não suportada.
H6	O contentamento com colegas, superiores ou organização Informação influencia positivamente o comportamento seguro em relação à Segurança da Informação.	Suportada.

Fonte: Autor

Em relação à hipótese H5, segundo Herath e Rao (2009a), a Segurança da Informação ocasiona um maior número de procedimentos e tarefas a serem realizadas, acarretando em um maior esforço potencial para a realização das ações adicionais e que podem ser percebidos equivocadamente como um empecilho despropositado, o que pode dificultar as ações dos usuários em prol de um comportamento seguro. Na presente pesquisa não foi possível determinar a percepção de Esforço em Salvaguarda, com base nas questões de Liang e Xue (2009), por serem opcionais e se basearem na obtenção de um *antispyware*, algo que na opinião da maioria dos respondentes (72%) já estava instalado e não precisava ser obtido, impossibilitando a mensuração e a o consequente suporte à hipótese H5.

Ainda em relação às hipóteses H3 e H4, as correlações da Certeza da Detecção e da Severidade da Punição com o Comportamento Seguro são menores do que na pesquisa oriunda desses construtos (HERATH e RAO, 2009a). Isso pode indicar que os respondentes não consideraram, no contexto desta pesquisa, a Certeza da Detecção e principalmente a Severidade da Punição como fortes fatores indutores a um Comportamento Seguro. Entretanto, podem ocorrer efeitos de contingência, ou seja, o efeito desses fatores, isoladamente, pode não ser eficaz em indicar a prática de Comportamento Seguro, mas a combinação desses fatores pode levar a um Comportamento Seguro com relação à Segurança da Informação (SEGINF). Em outras palavras, a Severidade Punição não se apresentou como sendo significativa por conta própria, mas pode operar junto com outros fatores para predizer o Comportamento Seguro em relação à SEGINF em pesquisas futuras. Por outro lado, a baixa percepção sobre a Certeza de Detecção condiz com a baixa da Severidade Punição, pois o usuário que não considera que será pego, ao contrariar as orientações sobre Segurança da Informação, pode considerar que não será punido.

A hipótese H6, sobre o Descontentamento com a organização, colegas e superiores, que após a validação de face e conteúdo do instrumento de pesquisa, passou a avaliar o contentamento, teve um efeito significativo, com um papel importante na influência do Comportamento Seguro, sendo o fator mais significativo a predizer o Comportamento Seguro no contexto dessa pesquisa.

Os resultados também indicam que a orientação de uma pessoa sobre Segurança da Informação é significativa na determinação do Comportamento Seguro. Durante a regressão linear tornou-se perceptível que a orientação sobre Segurança da Informação é uma variável de controle importante, influenciando o coeficiente de correlação, pois ao realizar a regressão linear dos fatores do modelo com todos os 171 respondentes e desconsiderando o filtro de

Orientação sobre SEGINF, as correlações obtiveram valores menores, conforme demonstrados nas Tabelas 22 e 23. Isso pode indicar que esforços organizacionais, tais como programas de conscientização, são significativos no desencadeamento do Comportamento Seguro. Todavia, não exclui outras formas de estímulos para esse comportamento, como a experiência individual ou outras formas de comunicações externas à organização, que não são mensuradas por essa pesquisa.

Tabela 22 - Coeficiente de correlação obtido sem a variável de controle

R	*R Square*	*Adjusted R Square*	*Std. Error of the Estimate*	*Change Statistics*				
				R Square Change	*F Change*	*df1*	*df2*	*Sig. F Change*
0,492	0,242	0,219	0,88387127	0,242	10.521	5	165	0,000
Fatores Preditores (variáveis): SEV (SEV1 e SEV3), DETCERT (DETCERT1 e DETCERT2), PUNSEV(PUNSEV1, PUNSEV2 e PUNSEV3), DESC (DESC1, DESC2e DESC3), SUS (SUS1,SUS2 e SUS3)								
Fator dependente (variáveis): BEH (BEH1, BEH2 e BEH3)								

Fonte: Autor

Tabela 23 - Coeficiente de correlação entre fatores sem a variável de controle

Fatores	*Unstandardized Coefficients*		*Standardized Coefficients*	*t*	*Sig.*	*Correlations*			*Collinearity Statistics*	
	B	*Std. Error*	*Beta*			*Zero-order*	*Partial*	*Part*	*Tolerance*	*VIF*
SUS	0,263	0,068	0,263	3,883	0,000	0,263	0,289	0,263	1,000	1,000
DESC	0,283	0,068	0,283	4,180	0,000	0,283	0,309	0,283	1,000	1,000
PUNSEV	-0,034	0,068	-0,034	-0,495	0,621	-0,034	-0,039	-0,034	1,000	1,000
DETCERT	0,231	0,068	0,231	3,403	0,001	0,231	0,256	0,231	1,000	1,000
SEV	0,194	0,068	0,194	2,869	0,005	0,194	0,218	0,194	1,000	1,000
Fator dependente: BEH										

Fonte: Autor

Dessa forma, os resultados demonstram a importância das orientações periódicas sobre Segurança da Informação, que enfoquem especialmente na segurança de ativos de informação da organização. A divulgação de medidas de dissuasão, com ênfase na monitoria exercida pela organização, e de exemplos de repreensão de comportamento inadequados também devem ser considerados no âmbito dessas conscientizações (SIPONEN e VANCE, 2010).

Os programas de conscientização de segurança devem treinar os usuários sobre os objetivos e os controles de segurança, sejam eles, técnicos, físicos ou normativos. Possibilitando aos usuários compreender os benefícios dos controles e como reduzir o risco de ameaças à segurança. Segundo Ng et al. (2009), quando os usuários estão cientes da suscetibilidade e da severidade das ameaças podem tomar decisões conscientes para exercer um comportamento preventivo adequado. Dessa forma, as orientações de conscientização sobre Segurança da Informação precisam ser elaboradas para destacar a Severidade da Ameaça e a Suscetibilidade da Ameaça e devem se concentrar em educar os usuários sobre a possibilidade e os danos das ameaças, possibilitando que o usuário entenda a necessidade de segurança, o seu papel e a sua responsabilidade na proteção de dados organizacionais e outros ativos de informação.

6.2 CONTRIBUIÇÕES TEÓRICAS

A presente pesquisa revelou fatores que influenciam o Comportamento Seguro em relação a e-mail, através da aplicação de um modelo teórico que combinou três pesquisas atuais na área de Segurança da Informação, resultando em um novo Instrumento de Pesquisa. Algo pouco usual em pesquisas nessa área devido ao risco e ao esforço requerido na criação de uma nova escala.

O instrumento de pesquisa resultante deste trabalho foi embasado em pesquisas de periódicos bem conceituados e utilizou amplos, sólidos e reiterados métodos de validação, possibilitando doravante a utilização em novos contextos de aplicações e outrossim em novas pesquisas explanatórias ou descritivas.

No âmbito acadêmico, esse estudo ajudou a reduzir a lacuna na compreensão do Comportamento Seguro do Computador de um usuário no contexto de uma organização e possibilitou combinar conceitos provenientes das teorias *Protect Motivation Theory*, *Deterrence Theory*, *Self-Determination Theory* e *Tecnology Threat Avoidance Theory*, dentre outras, alcançando um considerável sucesso e dando impulso para pesquisas futuras nesta área. Em particular, o construto sobre o contentamento é novo na área da Segurança da Informação (SEGINF), sendo mais incomum ainda em pesquisas quantitativas dessa área, assim como os demais construtos, que são relativamente novos na área de Segurança da Informação.

Embora haja uma abundância de orientações práticas, sugeridas por profissionais, sobre como melhorar o comportamento do usuário, a eficácia dessas orientações ainda precisa continuar sendo pesquisada. O presente estudo operacionalizou e estendeu um modelo

original e incomum, com construtos atuais, no qual foram desenvolvidas e validadas questões que poderão ser utilizadas para medir esses mesmos construtos em novos modelos aplicados ao contexto da Segurança da Informação.

6.3 CONTRIBUIÇÕES GERENCIAIS

O estudo realizado fornece uma gama de implicações gerenciais, aplicáveis as organizações que fornecem treinamento e orientações sobre Segurança Informação. Não obstante, aborda alguns pontos, mais abrangentes, que devem ser considerados pelas organizações na busca de uma maior segurança, sendo destacado o papel da falta de orientação para o a Segurança da Informação e nesse sentido lança um alerta sobre o risco da falta de orientação. Abrange também implicações para os profissionais que elaboram orientações ou programas de conscientização para a Segurança da Informação. Em particular, a importância da Severidade Percebida e da Susceptibilidade Percebida deve ser destacada na formulação do conteúdo de orientações de conscientização sobre a Segurança da Informação nas organizações e o descontentamento do usuário em relação à organização, colegas ou superiores, é um fator a ser considerado nos programas de conscientização.

Segundo Bulgurcu et al. (2010) o fortalecimento da Segurança da Informação depende dos funcionários ao cumprirem as orientações – regras e regulamentos – relativas à Segurança da Informação. Para Puhakainen e Siponen (2010) os funcionários que não estão em conformidade com as orientações da política de Segurança da Informação são um risco sério para suas empresas. As graves consequências das brechas e vulnerabilidades da Segurança da Informação e suas implicações para os funcionários e para a organização devem ser enfatizadas nas orientações sobre segurança, permitindo aos funcionários entenderem a gravidade e servindo como um impulsionador para a prática de um Comportamento Seguro. Conforme Ng et al. (2009), as orientações sobre segurança fornecidas aos funcionários podem ser ainda mais eficazes quando são explicadas a possibilidade e gravidade dos danos aos ativos informacionais da organização. Ao enfatizar a gravidade dos incidentes de segurança, os funcionários serão motivados para a prática de um comportamento adequado as orientações, desde que não estejam descontentes com a organização, superiores ou colegas (WILLISON e WARKENTIN, 2013).

6.4 LIMITAÇÕES DO ESTUDO E SUGESTÕES PARA PESQUISAS FUTURAS

A Segurança da Informação de uma organização não pode ser negligenciada e é claro que somente soluções de tecnologia não são suficientes (NG et al., 2009). O comportamento dos funcionários desempenha um papel importante em evitar vulnerabilidades e brechas na

Segurança da Informação e isso exige mais pesquisas para estudar os fatores que influenciam a decisão do indivíduo para a prática do Comportamento Seguro em relação à Segurança da Informação.

Neste estudo, apenas a prática da Segurança da Informação com relação a e-mails foi mensurada, o que limita a generalização dos resultados para outras práticas que a comprometa, tais como falta de atualizações de softwares, acesso a hiperlinks suspeitos, empréstimo de senhas, ou o uso de senhas fracas, entre outras. Estudos futuros sobre outras práticas de segurança podem ajudar a descobrir as relações causais comuns que podem fortalecer um Comportamento Seguro, ou provocar brechas e vulnerabilidades à Segurança da Informação.

Devido ao coeficiente de correlação R^2 estar relativamente baixo, com os fatores independentes predizendo 41,3% do Comportamento Seguro, há grande possibilidade que demais fatores precisem ser agregados ao modelo, sendo mais um aspecto a ser explorado em pesquisas futuras.

Outra limitação é o tamanho da amostra. Pesquisas futuras poderiam replicar este estudo com uma amostra maior. Também seria útil comparar os resultados obtidos com os entrevistados que não tiverem incidentes prévios com *malwares* em relação aos que já tiveram.

REFERÊNCIAS

ABNT, **NBR ISO/IEC 27001**- Tecnologia da informação – Técnicas de segurança – Sistema de Gestão de Segurança da Informação – Requisitos. Rio de Janeiro: Associação Brasileira de Normas Técnicas, 2006.

_____, **NBR ISO/IEC 27002** - Tecnologia da informação – Técnicas de segurança - Código de prática para a gestão da Segurança da Informação. Rio de Janeiro: Associação Brasileira de Normas Técnicas, 2005.

ALBRECHTSEN, E. A qualitative study of users' view on information security. **Computers & Security**, v. 26, n. 4, p. 276-289, 2007.

ALBRECHTSEN, E.; HOVDEN, J. The information security digital divide between information security managers and users. **Computers & Security**, v. 28, n. 6, p. 476-490, 2009.

AJZEN, I. The Theory of Planned Behavior. **Organizational Behavior and Human Decision Processes**, v. 50, n. 2, p. 179-211, 1991.

BANG, Y., LEE, D. J., BAE, Y. S., AHN, J. H.. Improving information security management: An analysis of ID–password usage and a new login vulnerability measure. **International Journal of Information Management**, 2012.

BRASIL. LEI Nº 12.527, DE 18 DE NOVEMBRO DE 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5o, no inciso II do § 3o do art. 37 e no § 2o do art. 216 da Constituição Federal; altera a Lei no 8.112, de 11 de dezembro de 1990; revoga a Lei no 11.111, de 5 de maio de 2005, e dispositivos da Lei no 8.159, de 8 de janeiro de 1991; e dá outras providências.

BULGURCU, B.; CAVUSOGLU, H.; BENBASAT, I.. Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. **MIS Quaterly**, v. 34, n. 3, p. 523-548, 2010.

CHAN, M.; WOON, I.; KANKANHALLI, A. Perceptions of information security in the workplace: linking information security climate to compliant behavior. **Journal of information privacy and security**, v. 1, n. 3, p. 18-41, 2005.

CHEN, Z., ROUSSOPOULOS, M., LIANG, Z., ZHANG, Y., CHEN, Z., A. Delis. Malware characteristics and threats on the internet ecosystem**. Journal of Systems and Software**, v. 85, n. 7, p. 1650-1672, 2012.

COLE, E. **Network Security Bible**, 2 ed., John Wiley & Sons, 2009.

D'ARCY, J.; HERATH, T. A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. **European Journal of Information Systems**, v. 20, n. 6, p. 643-658, 2011.

D'ARCY, J.; HOVAV, A. Does one size fit all? Examining the differential effects of IS security countermeasures. **Journal of Business Ethics**, v. 89, p. 59-71, 2009.

DA VEIGA, A.; ELOFF, J. H. P. A framework and assessment instrument for information security culture. **Computers & Security**, v. 29, n. 2, p. 196-207, 2010.

DECI, E. L.; KOESTNER, R.; RYAN, R. M. A meta-analytic review of experiments examining the effects of extrinsic rewards on intrinsic motivation. **Psychological bulletin**, v. 125, n. 6, p. 627, 1999.

FISCHBEIN, M.; AZJEN, I. **Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research**, Reading: Addison-Wesley, p.480, 1975.

GOODHUE, D. L.; LEWIS, W.; THOMPSON, R. 2012. Does PLS Have Advantages for Small Sample Size or Non-Normal Data? **MIS Quarterly,** v.36, n. 3, p.981-1001, 2012.

GROSSMAN J.; HANSEN, R.; PETKOV, P; RAGER, A.; FOGIE S. **XSS Attacks: Cross Site Scripting Exploits and Defense**, Syngress Publishing, 2007.

GRUYS, M. L.; SACKETT, P. R. Investigating the dimensionality of counterproductive work behavior. **International Journal of Selection and Assessment**, v. 11, n. 1, p. 30-42, 2003.

HAIR, J. F.; ANDERSON, R. E.; TATHAM, R. L.; BLACK, W. C. **Análise multivariada de dados**. 6. ed. Porto Alegre: Bookman, 2009.

HAIR Jr., J. F.; BABIN, B., MONEY, A. H., & SAMOUEL, P. **Fundamentos de Métodos de Pesquisa em Administração**. 7 ed. Porto Alegre: Bookman, cap. 6 e 7, 2005.

HAIR JR, J. F.; HULT, G. T. M.; RINGLE, C.; SARSTEDT, M.. **A primer on partial least squares structural equation modeling (PLS-SEM)**. SAGE Publications, Incorporated, 2013.

HARRINGTON, S. J. The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions. **MIS Quaterly**, v. 20, n. 3, p. 257-278, 1996.

HENSELER, J.; RINGLE, C.; SINKOVICS, R.. The use of partial least squares path modeling in international marketing. **Advances in International Marketing (AIM),** v. 20, p. 277-320, 2009.

HERATH, Tejaswini; RAO, H. R. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. **Decision Support Systems**, v. 47, n. 2, p. 154-165, 2009a.

HERATH, Tejaswini; RAO, H. Raghav. Protection motivation and deterrence: a framework for security policy compliance in organisations. **European Journal of Information Systems**, v. 18, n. 2, p. 106-125, 2009b.

HINKIN, T. R. A brief tutorial on the development of measures for use in survey questionnaires. **Organizational Research Methods**. v. 1, n. 1, p. 104–121, 2008.

ISACA. COBIT 5 Control Objective for Information and Related Technology. Rollign Meadows (EUA), 2012a.

_____. COBIT 5 for Security Information. Rollign Meadows (EUA), 2012b.

JOHNSTON, B. A. C.; WARKENTIN, M. Fear Appeals and Information Security Behaviors: an Empirical Study. **MIS Quaterly**. v. 34, n. 3, p. 549-566, 2010.

KRAEMER, S.; CARAYON, P.; CLEM, J. Human and organizational factors in computer and information security: Pathways to vulnerabilities. **Computers & Security**, v. 28, n. 7, p. 509-520, 2009.

KRAEMER, S.; CARAYON, P. Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. **Applied Ergonomics**, v. 38, n. 2, p. 143-154, 2007.

KELLOWAY, E. K.; FRANCIS, L.; PROSSER, M.; CAMERON, J. E. Counterproductive work behavior as protest. **Human Resource Management Review**, v.20, n.1, p.18-25, 2010.

KING, N. J.; RAJA, V. T. Protecting the privacy and security of sensitive customer data in the cloud. **Computer Law & Security Review**, v. 28, n. 3, p. 308–319, 2012

KLINE, R. B. **Principals and Practice of Structural Equation Modeling**. 3a ed. New York: Guilford, 2011

LEE, Y.; LARSEN, K. R. Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software. **European Journal of Information Systems**, v. 18, n. 2, p. 177-187, 2009.

LEACH, J. Improving user security behaviour. **Computers & Security**, v. 22, n. 8, p. 685-692, 2003.

LIANG, H.; XUE, Y. Avoidance of Information Technology Threats: A Theoretical Perspective, **MIS Quaterly**. v. 33, n. 1, p. 71-90, 2009.

LIANG, H; XUE, Y. Understanding security behaviors in personal computer usage: a threat avoidance perspective. **Journal of the Association for Information Systems**, v. 11, n. 7, p. 394-413, 2010.

LIGINLAL, D.; SIM, I.; KHANSA, L. How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management. **Computers & Security**.v.28, p.215-228, 2009.

MALHOTRA, N. K. **Pesquisa de Marketing** - Uma Orientação Aplicada. 6 ed. Porto Alegre: Bookman, 2012.

MILLSON, M. R. Refining The Npd/Innovation Path To Product Market Success With Partial Least Squares Path Analysis. **International Journal of Innovation Management**, v. 17, n. 02, 2013.

NG, B.; KANKANHALLI, A.; XU, Y. Studying users' computer security behavior: A health belief perspective. **Decision Support Systems**, v. 46, n. 4, p. 815, 2009.

PINSONNEAULT, A.; KRAEMER K. L. **Journal of Management Information Systems**. v. 10, n. 2, p. 75-105, 1993.

PUHAKAINEN, P.; SIPONEN, M. Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study. **MIS Quaterly**, v. 34, n. 4, p.757–778, 2010.

RYAN, R. M.; DECI, E. L. Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being. **American Psychologist**, v. 55, n. 1, p. 68-78, 2000.

SHAHZAD, F.; SHAHZAD, M.; FAROOQ, M. In-execution dynamic malware analysis and detection by mining information in process control blocks of Linux {OS}. **Information Sciences**, v. 231, n. 0, p. 45-63, 2013.

SÊMOLA, M. **Gestão da segurança da informação: uma visão executiva**. Campus, 2003.

SIPONEN, M. T. A conceptual foundation for organizational information security awareness. **Information Management & Computer Security**, v. 8, n. 1, p. 31-41, 2000.

SIPONEN, M. T.; VANCE, A. Neutralization: new insights into the problem of employee information systems security policy violations. **MIS Quarterly**, v. 34, n. 3, p. 487, 2010.

SON, J. Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. **Information & Management**, v. 48, n. 7, p. 296-302, 2011.

SPECTOR, P. E.; FOX, S.; PENNEY, L. M.; Bruursema, K.; Goh, A.; Kessler, S. (2006). The dimensionality of counterproductivity: Are all counterproductive behaviors created equal? **Journal of Vocational Behavior**, v. 68, n. 3, p. 446-460, 2006.

VACCA, J. R. **Computer and information security handbook**. Morgan Kaufmann, 2009.

VANCE, A.; SIPONEN, M.; PAHNILA, S. Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. **Information & Management**, 2012.

TIPTON, H. F.; KRAUSE, M. **Information security management handbook**. 6 ed., vol. 1, Auerbach Publications. 2007.

VENKATESH, W; MORRIS, M. G.; DAVIS, G. B.; DAVIS, F. D. User acceptance of Information Technology: toward a unified view. **MIS Quaterly**, v. 27, n. 3, p. 425-478, set. 2003.

WILLIAMS, P. A. Information Security Governance. **Information Security Technical Report**, Vol. 6, no. 3 pp. 60-70, 2001.

WARKENTIN, M.; WILLISON, R. Behavioral and policy issues in information systems security: the insider threat. **European Journal of Information Systems**, v. 18, n. 2, p. 101-105, 2009.

WILLISON, R.; WARKENTIN, M. Beyond deterrence: An expanded view of employee computer abuse. **MIS Quarterly**, v. 37, n. 1, p. 1-20, 2013.

WORKMAN, M.; BOMMER, W. H.; STRAUB, D. Security lapses and the omission of information security measures: A threat control model and empirical test. **Computers in Human Behavior**, v. 24, n. 6, p. 2799-2816, 2008.

WORKMAN, M.; PHELPS, D. C.; GATHEGI, J. N. **Information Security for Managers**. Jones and Bartlett Publishers. 2013.

APÊNDICE A – VERSÃO FINAL DO INSTRUMENTO DE PESQUISA

Pesquisa sobre aspectos comportamentais em relação à Segurança da Informação

Este questionário é parte integrante da pesquisa acadêmica realizada por Rodrigo Hickmann Klein (rodrigo.hickmann@acad.pucrs.br), no âmbito do Programa de Mestrado Acadêmico da PUCRS, sob a orientação da Profa. Drª Edimara Mezzomo Luciano (eluciano@pucrs.br). Os dados serão usados apenas de forma consolidada, não permitindo a sua identificação ou da organização na qual você trabalha. Não há respostas certas ou erradas, responda de acordo com a sua percepção. Suas respostas são muito importantes para a área de Segurança da Informação e contribuirão para um ambiente mais seguro através da divulgação dos resultados. Desde já agradecemos a sua colaboração.

Observação: O termo "orientação sobre Segurança da Informação" refere-se às regras, normas e recomendações determinadas às pessoas que trabalham em uma organização de qualquer tipo, que tenham sido determinadas de forma verbal ou escrita, com relação ao uso do computador, *smartphone*, *tablet*, internet dentro da organização ou sobre informações da organização.

A organização na qual você trabalha fornece orientações sobre Segurança da Informação, verbais ou escritas?

- ❍ Sim, mas não são esclarecidas as razões de cada item apontado na orientação.
- ❍ Sim, e as razões de cada item apontado na orientação são esclarecidas.
- ❍ Não.

Caso tenha respondido alguma opção com **Sim** na questão anterior, as orientações ocorreram:

- ❍ Periodicamente, a cada ____ meses.
- ❍ Uma única vez.

Algum dispositivo de TI que você utilizou (computador, smartphone, notebook, laptop, etc.), profissionalmente ou pessoalmente, já foi infectado por um *malware*?

Observação: *malwares* são softwares maliciosos que visam danificar softwares, explorar vulnerabilidades, ou extrair informações do usuário, como por exemplo: vírus, cavalos de Tróia (*trojan*), *worms*, *spyware*, *bots*, etc.

- ❍ Sim.
- ❍ Não.
- ❍ Não sei.

Considerando a organização na qual você trabalha, defina seu **grau de concordância** com as afirmações abaixo, optando por um valor entre 1 e 5 (1 = Discordo Totalmente, 5= Concordo Totalmente):

	Discordo Totalmente 1	2	3	4	Concordo Totalmente 5
Há uma boa possibilidade de que eu receba um anexo de e-mail com um *malware*.	❍	❍	❍	❍	❍
Ter o computador infectado por um *malware* como resultado de abrir um anexo de e-mail suspeito é um problema sério para mim.	❍	❍	❍	❍	❍
Na organização onde trabalho o uso inadequado do computador certamente seria detectado.	❍	❍	❍	❍	❍
Eu estou suscetível a receber um anexo de e-mail com *malware*.	❍	❍	❍	❍	❍

	Discordo Totalmente 1	2	3	4	Concordo Totalmente 5
Na organização onde trabalho o uso do computador é monitorado.	❍	❍	❍	❍	❍
Se o meu computador está infectado por um *malware*, como resultado de abrir um anexo de e-mail suspeito, meu trabalho será afetado negativamente.	❍	❍	❍	❍	❍
Estou muito contente com os meus colegas de trabalho.	❍	❍	❍	❍	❍
Antes de ler um e-mail, verifico primeiro se o assunto e o remetente fazem sentido.	❍	❍	❍	❍	❍
As chances de receber um anexo de e-mail com um *malware* são altas.	❍	❍	❍	❍	❍
Eu tenho cautela ao receber um anexo de e-mail, pois pode conter um *malware*.	❍	❍	❍	❍	❍
Estou muito contente com os meus superiores.	❍	❍	❍	❍	❍
Antes de abrir um anexo de um e-mail, verifico primeiro se o nome do arquivo anexado faz sentido.	❍	❍	❍	❍	❍
A organização onde trabalho demite funcionários que fazem uso inadequado do computador.	❍	❍	❍	❍	❍
Estou muito contente com a organização onde trabalho.	❍	❍	❍	❍	❍
Na organização onde trabalho, se eu fosse pego utilizando inadequadamente o computador, eu seria punido severamente.	❍	❍	❍	❍	❍

Na organização onde você trabalha, o seu computador possui um anti-spyware?

Observação: *anti-spyware* é um software que retira ou bloqueia *spywares* em um computador. *Spyware* é um tipo de *malware* que é instalado secretamente em um computador, com o objetivo de reunir informações sobre os usuários ou organizações sem o seu conhecimento.

❍ Sim.
❍ Não.
❍ Não sei.

Caso tenha respondido **Não** ou **Não sei** na questão anterior, defina seu **grau de concordância** com as afirmações abaixo. Escolhendo um valor entre 1 e 5 (1 = Discordo Totalmente, 5= Concordo Totalmente):

	Discordo Totalmente 1	2	3	4	Concordo Totalmente 5
Eu não sei como conseguir um software anti-*spyware*.	❍	❍	❍	❍	❍
O software anti-*spyware* pode causar problemas para outros programas no meu computador.	❍	❍	❍	❍	❍
A instalação de um software anti-*spyware* é muito complicada.	❍	❍	❍	❍	❍

Qual das opções abaixo melhor representa seu nível de escolaridade:
- ❍ Ensino fundamental (1^o grau).
- ❍ Ensino médio (2^o grau).
- ❍ Ensino superior.
- ❍ Especialização/MBA.
- ❍ Mestrado/Doutorado.

Gênero:
- ❍ Feminino.
- ❍ Masculino.

Qual a sua idade?_____ anos.

Qual das opções abaixo melhor representa sua área de formação:
- ❍ Administração.
- ❍ Informática.
- ❍ Direito.
- ❍ Engenharia.
- ❍ Outra: _____.

Você já trabalhou ou trabalha atualmente na área de Informática ou Tecnologia da Informação?
- ❍ Sim. Quantos anos? _____ anos.
- ❍ Não.

Qual o número aproximado de pessoas que trabalham na organização onde você trabalha atualmente?
_____ pessoas.

Qual o seu cargo/função atual? _____.

Quantos anos de experiência profissional você tem (total de anos)? _____ anos.

Qual o segmento de atuação da organização onde você trabalha?
- ❍ Indústria
- ❍ Comércio
- ❍ Serviços
- ❍ Governo
- ❍ Outro: _____.