REVISTA DE TECNOLOGIA APLICADA (RTA)
v.8, n.1, jan-abr 2019, p.03--19
ISSN: 2237-3713

http://dx.doi.org/10.21714/2237-3713rta2019v8n1p03

Segurança da Informação: uma análise da percepção de ameaças que influenciam a Intenção de Cumprir as Políticas de Segurança da Informação por usuários de organizações do estado do Rio Grande do Sul

Information Security: an analysis of the perception of threats that affect the Intention to Comply with Information Security Policies for users of organizations in the State of Rio Grande do Sul

Jonas Rafael Silveira
Universidade Federal do Rio Grande – FURG
Programa de Pós-Graduação em Administração
jonasrsilveira@gmail.com

Décio Bittencourt Dolci
Universidade Federal do Rio Grande – FURG
Programa de Pós-Graduação em Administração
dbdolci@gmail.com

Lucas Santos Cerqueira
Universidade Federal do Rio Grande – FURG
Programa de Pós-Graduação em Administração
lucasscerqueira@gmail.com

Jonatas Wendland
Universidade Federal do Rio Grande – FURG
Programa de Pós-Graduação em Administração
wendlandjonatas@gmail.com
*

Bernardo Silva
Universidade Federal do Rio Grande – FURG
diou.bernardo@gmail.com

Resumo
Que a informação é um bem valioso na era atual para as organizações é consenso. Certamente, as políticas de segurança da informação e o esforço para adoção de práticas que neutralizem as ameaças e vulnerabilidades dos sistemas de informação têm crescido ultimamente. Este estudo busca identificar como a percepção às ameaças de Segurança da Informação influencia na Intenção de Cumprir as Políticas de Segurança da Informação (PSI) por usuários de organizações do estado do Rio Grande do Sul, a partir do modelo

* Recebido 15 december 2018; recebido revisado em 22 January 2019; aceito em 10 April 2019; publicado online 22 April 2019.

desenvolvido por Vance et al. (2012). Para isso, realizou-se uma pesquisa exploratória e de abordagem quantitativa. Pode-se perceber que tanto a Vulnerabilidade Percebida como a Eficácia da Resposta não produzem efeitos diretos significantes na Intenção de Cumprir com a PSI da organização, indicando que os usuários pesquisados não percebem a ameaça por completo nem creem na eficácia do PSI de suas organizações no seu enfrentamento.
Palavras-chave: Segurança da Informação, Teoria da Motivação a Proteção, Teoria do Hábito, Conformidade com a política de segurança da informação, Rio Grande do Sul, Metodologia de cenário.

Abstract
That information is a valuable asset in the current Era for organizations is consensus. Certainly, the information security policy and the effort to adopt practices that neutralize the threats and vulnerabilities of information systems have grown lately. This study seeks to identify how the perception of information security threats influences in order to Fulfill with information security policies for users of organizations in the State of Rio Grande do Sul, from the model developed by Vance et al. (2012). The results indicate that respondents do not realize the vulnerabilities to which they are exposed, hindering the fight against possible threats available when using the information systems of the organizations in which they work in their confrontation.
Keywords: *Information security, Protection Motivation theory, Theory of habit, Information security policy compliance, Rio Grande do Sul, Scenario methodology.*

1. Introdução

O Brasil desenvolve as suas capacidades em Segurança da Informação a fim de se adequar à nova configuração mundial, na qual o Ciberespaço ganha um papel protagonista e amplia a vulnerabilidade das informações tanto dos indivíduos como das organizações. A lei Lei nº 13.709 de agosto de 2018 é um exemplo de regulação nesse sentido. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 − Marco Civil da Internet (Lei n. 13.709, 2018). Mesmo sendo a temática Segurança da Informação bem estruturada do ponto de vista legal no Brasil, considerada atualizada se comparada a Políticas de Segurança da Informação (PSI) de organizações de outros países (Souza & Streit, 2017), ela não repercute no comportamento dos seus atores (Albuquerque & Santos, 2014).

Albuquerque e Santos (2014) evidenciaram que muitas empresas possuem PSI formalizadas, mas não possuem procedimentos que instituam a análise crítica dessas políticas com o intuito de verificar sua validade ao longo do tempo, e que o nível de satisfação com a formalização dessas políticas é baixo. Faz-se necessário, assim, conscientizar e disseminar a cultura da segurança entre todos os atores que, de alguma forma, são vulneráveis e podem ser afetados por ataques cibernéticos, como empresas, instituições governamentais e usuários em geral (Alves, Gomes-De-Souza, Chrispino, & Ogasawara, 2014).

Pesquisas recentes, como o Relatório de Ameaças à Segurança na Internet realizada pela consultoria Symantec em 2017, aponta que o Brasil é um dos países que mais sofrem com *spams*, ocupando a terceira posição, e demonstra uma nova modalidade de ataque: contra a cadeia de suprimentos das empresas (Symantec, 2018). Na área acadêmica, pesquisas já apontaram a conscientização dos usuários sobre a preocupação com suas informações no uso da plataforma *Facebook*, destacando os usuários das regiões Sul e Sudeste como os mais preocupados com a privacidade de suas informações (Britto-da-Silva, Magnagnagno, & Luciano, 2015). Esse comportamento recomendado, quando levado para dentro das organizações nas quais esses indivíduos trabalham, pode colaborar para a segurança das

informações, pois sendo as pessoas partes integrantes dos Sistemas de Informações, as chances de perda de informações seriam menores.

Foi realizada uma busca nos indexadores *Scopus*, *Scielo*, *Web Of Science* e Portal de Periódicos da CAPES, onde se encontrou poucos artigos que abordam a temática Segurança da Informação na percepção de usuários do estado do Rio Grande do Sul, sendo esses em sua maior parte dos artigos de cunho qualitativo, utilizando da técnica de estudo de caso, por exemplo.

Pela necessidade de explorar a temática da Segurança da Informação, e como os indivíduos percebem as ameaças a que estão expostos, e se esses se sentem capazes de responder corretamente às determinações das PSI nas organizações em que trabalham, se define como a problemática da pesquisa: **Como a percepção de ameaças a Segurança da Informação nas organizações influencia a intenção de cumprir as Políticas de Segurança da Informação por indivíduos que trabalham em empresas do estado do Rio Grande do Sul?**

Para isso, utilizou-se o modelo de Vance, Siponen e Pahnila (2012), desenvolvido e aplicado em uma organização finlandesa para identificar a Intenção de Cumprir com as PSI pelos indivíduos. A Finlândia é referência mundial quando se trata de Segurança da Informação, possuindo uma reputação mundial na educação de seus usuários de tecnologia, sendo esta extremamente orientada para a prática (Soceanu, Vasylenko, & Gradinaru 2016).

Vance et al. (2012) foram os primeiros autores a aplicar a Teoria da Proteção a Motivação (*Protection Motivation Theory - PMT*) por completo na área de Segurança da Informação. Pesquisas anteriores não haviam utilizado o modelo em sua totalidade (Vance et al., 2012). Além disso, pesquisas anteriores não haviam considerado o comportamento passado, sendo este um componente para o processo da PMT (Vance et al., 2012).

Outro diferencial deste estudo foi o uso do método de cenários hipotéticos, no qual foi apresentada uma vinheta que descrevia uma ação ou decisão relacionada com o cumprimento de PSI, demonstrando uma quebra de um possível ponto de uma PSI, que exporia a organização e o indivíduo a ameaças aos Sistemas de Informação, auxiliando no preenchimento do questionário.

Sendo o Brasil, especificamente o Rio Grande do Sul, um contexto diferente do local onde a pesquisa de Vance et al. (2012) foi desenvolvida, e pela ausência de estudo sobre Segurança da Informação no Rio Grande do Sul, define-se como objetivo geral desta pesquisa identificar como a percepção de ameaças pelos indivíduos influenciam no cumprimento das Políticas de Segurança da Informação pelos mesmos em organizações do estado do Rio Grande do Sul à luz do modelo de Vance et al. (2012). A pesquisa tem por objetivos específicos: (1) aplicar o modelo proposto por Vance et al. (2012) em um contexto diferente, com usuários de Sistemas da Informação que trabalhem em empresas situadas no estado do Rio Grande do Sul; (2) verificar se os cenários de quebra de Políticas de Segurança da Informação são percebidos como realistas pelos respondentes; (3) discutir através da Teoria da Motivação a Proteção e Teoria do Hábito as percepções de ameaças e a possibilidade de respostas disponíveis pelos indivíduos.

2. Referencial Teórico

A seguir será apresentado o referencial teórico utilizado para essa pesquisa. Aborda-se primeiramente as Políticas de Segurança da Informação, para após se desenvolver os aspectos referentes ao modelo utilizado nesta pesquisa, de Vance et al. (2012).

2.1. Políticas de Segurança da Informação (PSI)

A ISO/IEC 27002 (Associação Brasileira de Normas Técnicas [ABNT], 2005), uma das normas de referência internacional sobre Gestão da Segurança da Informação, define

como objetivo de uma Política de Segurança da Informação prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações pertinentes. É uma ferramenta que traduz as expectativas sobre a gestão da segurança de modo claro, específico, mensurável e normativo (Goel & Chengalur-Smith, 2010).

Para Bulgurcu, Cavusoglu e Benbasat (2010), as PSI são declarações dos papéis e responsabilidades dos empregados para proteger as tecnologias de informação (TI) e recursos de suas organizações. Cabe a PSI trazer as informações de forma clara e precisa, para bom entendimento do indivíduo, sem deixar de mencionar questões associadas às punições quando não cumpridas (Ferreira, Dolci, & Tondolo, 2016).

Um dos problemas das PSI para as empresas é o fato de ser praticamente impossível delinear e controlar todos os comportamentos de segurança (Hsu, Shih, Hung, & Lowry, 2015). Uma compreensão dos fatores que podem motivar os funcionários a cumprir com as políticas de segurança é fundamental para ajudar os gerentes a diagnosticar as deficiências em seus esforços, proporcionando-lhe maneiras para resolver os problemas comportamentais na gestão da segurança da informação (Bulgurcu et al., 2010).

Como partes desses fatores estão às ameaças às quais esses indivíduos estão expostos ao utilizarem os Sistemas de Informação nas empresas em que trabalham. Quando um indivíduo não cumpre com a determinação da PSI, expões as vulnerabilidades dos sistemas que utiliza, abrindo espaço para as ameaças do ciberespaço. Então, mesmo que a organização possua PSI bem estruturadas, é necessária a conscientização dos funcionários sobre a importância das informações para as organizações, da presença da alta gerência e a construção de uma cultura organizacional que defina as regras, metas e punições relacionadas ao cumprimento das PSI (Hu, Dinev, Hart, & Cooke, 2012).

2.2. Modelo de Vance et al. (2012)

A PMT, teoria proposta por Rogers (1975), foi inicialmente utilizada para prever a intenção em adotar um comportamento de saúde recomendado através do perigo percebido, que desencadeia processos cognitivos. Amplamente utilizada em pesquisas que buscavam identificar quais fatores determinavam o comportamento inadequado de pacientes em relação às suas doenças (Norman, Boer, & Seydel, 2005). A revisão da teoria por Maddux e Rogers (1983) possibilitou a aplicação desse modelo em diversas áreas para explicar como os indivíduos reagem à determinada ameaça percebida.

A teoria reformulada possibilitou o uso da PMT para fins mais gerais, ao incluir ao modelo a Auto Eficácia como mais uma variável. Para Jhonston e Warkentin (2010), a PMT configura-se como uma teoria estabelecida e robusta para a análise e exploração de ações ou comportamentos recomendados para evitar as consequências das ameaças. Vance et al. (2012) sugerem que a informação sobre uma ameaça provoca um processo mediador cognitivo em indivíduos que avaliam respostas positivas ou negativas. Assim, o não cumprimento das PSI pelos funcionários representa uma resposta inadequada, enquanto que o seu cumprimento é uma resposta adaptativa.

Norman et. al. (2005) colocam que a Motivação a Proteção (intenção de realizar um comportamento recomendado) resulta de dois processos de avaliação, uma é a função positiva de percepções de perigo, vulnerabilidade, eficácia da resposta e auto eficácia, e outra negativa de percepções dos benefícios associados com respostas adaptadas e os custos de resposta do comportamento adaptativo.

A avaliação de ameaça está relacionada com as percepções de como um indivíduo se sente ameaçado com base numa avaliação dos componentes do medo (Herath & Rao, 2009). Percebendo essa ameaça, as pessoas ajustarão seu comportamento de acordo com a quantidade de riscos que estão dispostas a aceitar (Barlette, Gundolf, & Jaouen, 2015).

Vulnerabilidade Percebida é a percepção da probabilidade de que um incidente indesejado possa acontecer caso não sejam tomadas medidas para impedi-lo. No contexto dessa pesquisa, Vulnerabilidade Percebida da segurança de sistemas de informação remete à percepção dos usuários de sistemas sobre o quanto eles estão expostos caso não cumpram as PSI. O Perigo Percebido diz respeito ao impacto que uma ameaça percebida pode causar para o indivíduo. No contexto desta pesquisa, o Perigo Percebido refere-se ao impacto negativo que uma violação nos sistemas de informação organizacionais pode causar para o usuário ou a organização na qual ele trabalha. Além disso, foi incluída a percepção de sanções que o mesmo pode sofrer pela organização caso não cumpra com as PSI. Pesquisas apontam a importância das sanções relacionadas ao não cumprimento de PSI (Hu et al., 2012).

Os Benefícios Percebidos se referem a qualquer motivação intrínseca ou extrínseca para aumentar ou manter um comportamento indesejado. No contexto desta pesquisa, Benefício Percebido foi conceituado como a percepção de economia de tempo no trabalho que indivíduo teria ao não cumprir com as normativas relativas à Segurança da Informação. Seguindo essas premissas, Vance et al. (2012) propuseram as seguintes hipóteses:

- H1. Vulnerabilidade percebida afeta positivamente a intenção de cumprir as políticas de segurança de SI.
- H2. O perigo percebido afeta positivamente a intenção de cumprir as políticas de segurança em SI.
- H3. Benefícios afetam negativamente a intenção de cumprir as políticas de segurança de SI.

A avaliação de enfrentamento centra-se nas respostas disponíveis que o indivíduo possui para lidar com a ameaça (Norman et al., 2005), resultando em maior motivação de proteção se o indivíduo perceber que o método de enfrentamento sugerido é significativo e simples de empregar (Sommestad, Karlzén, & Hallberg, 2015). A Eficácia da Resposta refere-se à crença que um indivíduo possui sobre a eficácia de um determinado comportamento em relação a minimizar uma ameaça (Johnston & Warkentin, 2010). Para esta pesquisa, a Eficácia da Resposta consiste na capacidade que o indivíduo possui de compreender a importância do cumprimento das PSI como forma de combater as ameaças no uso dos sistemas.

A Auto Eficácia corresponde à capacidade do indivíduo de responder à ameaça percebida, demonstrando-se como uma variável de impacto significativo sobre o indivíduo (Ifinedo, 2014). Neste estudo, Auto Eficácia corresponde à convicção do indivíduo de que possui as capacidades necessárias para cumprir com as PSI determinadas pelas organizações. O Custo da Resposta refere-se aos custos envolvidos no comportamento adaptativo (Rodrigues, 2015), sendo considerada nesta pesquisa a necessidade de investimentos de esforços, que vão além do tempo no trabalho direcionado para o cumprimento das PSI, o que se determina como os custos envolvidos para cumprir com as PSI.

Seguindo essas premissas, Vance et al. (2012) propõem as seguintes hipóteses:

- H4. A eficácia da resposta afeta positivamente a intenção de cumprir as políticas de segurança de SI.
- H5. A auto eficácia afeta positivamente a intenção de cumprir as políticas de segurança de SI
- H6. O custo da resposta afeta negativamente a intenção para o cumprimento das políticas de segurança de SI.

O Hábito refere-se não apenas a comportamentos repetidos, mas a comportamentos que, quando repetidos, são percebidos como mais vantajosos para o indivíduo, tornando esses comportamentos frequentemente habituais (Verplanken & Orbell, 2003). Decisões e comportamentos que são novos ou ocorrem em situações que não são familiares são mais fortemente influenciados pelo inconsciente (Martin & Zafar, 2015). Como as pistas

situacionais estão intimamente relacionadas ao comportamento habitual, à consciência das ameaças desencadeia o processo, no caso desse modelo, o processo cognitivo da PMT, o que leva à intenção de cumprir com as PSI (Vance et al., 2012).

Isso demonstra a importância do Hábito de cumprir com as PSI para a percepção das ameaças disponíveis ao utilizar os Sistemas de Informação. Sendo assim, o comportamento habitual tem uma influência negativa sobre o Custo da Resposta e os Benefícios Percebidos, isto é, o hábito de cumprir com as normativas referentes à Segurança da Informação consequentemente diminuiria a percepção de desvantagens, como a perda de tempo para executar as tarefas do dia-a-dia e para realizar outras atividades dentro da organização.

Por outro lado, o Hábito de cumprir as PSI influenciaria positivamente o Perigo Percebido, a Auto Eficácia, a Eficácia da Resposta e a Vulnerabilidade Percebida, pois quanto mais esse hábito fosse rotineiro, maior seria a percepção desses indivíduos sobre as vulnerabilidades envolvidas ao usar os sistemas organizacionais, maior a percepção do perigo disponível no uso desses sistemas, maior a noção de capacidade para responder a essas ameaças, e maior a percepção da efetividade dessas ações estabelecidas pela PSI para a segurança dos sistemas das organizações. Sendo assim, postula-se:

- H7a. O hábito influencia positivamente a vulnerabilidade.
- H7b. O hábito influencia positivamente a severidade percebida.
- H7c. O hábito influencia negativamente os benefícios.
- H7d. O hábito influencia positivamente a eficácia da resposta.
- H7e. O hábito influencia positivamente a auto eficácia.
- H7f. O hábito influencia negativamente o custo da resposta.

3. Metodologia

Esta pesquisa caracteriza-se de caráter exploratório, pois busca identificar em organizações no Rio Grande do Sul, que possui poucos estudos realizados sobre Segurança da Informação, a aplicação do Modelo de Vance et al. (2012). Pretende, também, apresentar mais familiaridade sobre o assunto e buscar o refinamento das ideias (Gil, 2002), na perspectiva de analisar os aspectos influenciadores no comportamento recomendado no modelo nas práticas de Segurança da Informação dos usuários nas organizações.

É uma pesquisa de abordagem quantitativa, e a amostragem é não probabilística por conveniência, onde se utilizou o método para a coleta dos dados bola de neve. Com o objetivo de identificar quais os fatores que influenciam no cumprimento das PSI em usuários de sistemas que trabalhem em organizações no estado do Rio Grande do Sul, foram utilizados os mesmos métodos do modelo de referência, entre eles o método de cenários hipotéticos, sendo esse amplamente utilizado para pesquisas que buscam avaliar o comportamento social e ético (Vance et al., 2012).

3.1. Desenvolvimento do instrumento

O instrumento foi estruturado em duas partes. A primeira parte continha duas perguntas de filtragem que abordam o nível de implementação da política de segurança dentro das organizações dos respondentes. Tais questões foram extraídas dos estudos de Ferreira et al. (2016), a saber:

Quadro 1 – Perguntas de filtro

Questão	Orientação sobre a Questão
É política da empresa em que trabalho comunicar aos funcionários ações aceitáveis e inaceitáveis visando à segurança da informação da organização.	Relacionado ao uso de senhas, acesso a determinados sites etc.
A empresa em que trabalho tem definidas as consequências do não cumprimento das normas quanto à segurança da informação.	Como por exemplo, advertência verbal, escrita, suspensão ou até desligamento.

Fonte: Elaboração a partir de Ferreira et al. (2016).

Passando pelas duas questões, o respondente recebia o acesso à segunda parte do questionário, que continha um cenário que evidenciava uma quebra em uma possível política de segurança da informação, sendo esses cenários baseados nos desenvolvidos por Vance et al. (2012). Os cenários foram discutidos e validados por especialistas na área de TI, buscando-se atualizá-los e adaptá-los a uma realidade mais próxima à dos respondentes. O Quadro 2 demonstra os cenários de possíveis quebras de PSI utilizados.

Quadro 2 – Cenários hipotéticos

Cenário Proposto	Descrição do Cenário
Utilizando aplicativos piratas	Paulo trabalha editando documentos importantes para sua empresa. Ele precisa editar um documento importante, mas a versão do seu aplicativo está muito antiga, o que está dificultando seu trabalho. A Política de Segurança da Informação proíbe o uso de aplicativos não instalados pela TI da empresa. Paulo consegue uma versão pirata do aplicativo e instala no computador.
Não relatar vírus no computador	Flávia deseja baixar uma música no computador da empresa. Ela acessa vários sites pouco confiáveis, e acaba baixando um vírus no computador, sendo alertada através do antivírus. A política de segurança da empresa determina que casos de infecção por vírus devem ser relatados ao suporte de TI. Flávia não informa o pessoal do suporte de TI sobre o ocorrido, e tenta resolver o problema sozinha.
Utilizando mídias portáteis	Rodrigo tem acesso a importantes informações da empresa em que trabalha. A empresa solicita que Rodrigo faça uma viagem de negócios, mas ele precisa analisar algumas dessas informações com urgência. Rodrigo resolve levar alguns documentos importantes em um pendrive. A política de segurança responsabiliza o usuário por perdas de informação causadas por ele. Rodrigo perde o pendrive, e não conta a ninguém.
Compartilhamento de senhas	Claudia possui acesso ao sistema de compras da empresa através de uma senha de uso pessoal. Cláudia está no meio de uma viagem de negócios, impossibilitada de acessar o sistema, mas seus colegas precisam liberar um processo para a próxima etapa, e sem a liberação do usuário de Claudia o processo não pode ocorrer. A política de segurança da empresa proíbe o compartilhamento de senhas. Claudia compartilha a sua senha com seus colegas.

Fonte: Elaboração própria.

A segunda parte também continha as questões sobre informações gerais como gênero, idade, cidade, e as questões relacionadas aos constructos, sendo essas 34 questões fechadas

estruturadas em escala Likert de 7 pontos, variando de 1 (discordo totalmente) a 7 (concordo totalmente), diferentemente da pesquisa de Vance et al. (2012), na qual se utilizou uma escala Likert de 11 pontos.

Escalas com maiores números geralmente são indicadas quando os entrevistados dominam o assunto objeto de estudo (Dalmoro & Vieira, 2013). Então, determinou-se a diminuição dos pontos da escala por não se conhecer o nível de implementação de PSI nas organizações que os respondentes trabalham. As questões foram traduzidas por uma nativa da língua inglesa e adaptadas para uma linguagem mais informal, a fim de auxiliar os respondentes.

3.2. Coleta dos dados

A coleta foi realizada através da ferramenta Google Forms, utilizando-se quatro formulários, um para cada cenário. Para o funcionamento da pesquisa, foi criado um código que redirecionava os possíveis respondentes para os formulários, objetivando manter uma equidade no número de respostas por cenário. A coleta ocorreu entre outubro e novembro de 2016 e como método de amostragem determinou-se a técnica bola de neve, sendo o *link* para a pesquisa compartilhado via e-mail e redes sociais, com a solicitação para que esse *link* fosse compartilhado com outras pessoas.

O total de indivíduos que se disponibilizaram a responder a pesquisa foi de 186. Destes, 125 passaram pelas perguntas de filtragem. Também foi verificada a frequência de respostas em branco nas questões, tendo sido considerado quatro o número máximo permitido para compor as respostas utilizadas na análise dos modelos. Desses 125 respondentes, três foram removidos pelo excesso de questões não respondidas, restando ao final um total de 122 respondentes.

Dos 12 respondentes, 61 (50,4%) são do gênero feminino e 60 (49,6%) do masculino. A maior parte dos respondentes, 63 (52,1%) possui entre 25 e 40 anos. Da cidade dos respondentes, 74 (60,3%) são da cidade de Rio Grande, 21 (17,2 %) da cidade de Santa Cruz do Sul e o restante de demais cidades do estado. Sobre a escolaridade, 58 indivíduos (47,9%) possuem Ensino Superior Incompleto e 33 (27,3%) Ensino Superior Completo. Referente ao tipo de empresa que o respondente exerce suas atividades, 91 (74,6%) trabalham em empresas privadas e 31 (25,4%) em organizações públicas.

4. Análise e Resultados

A análise dos dados foi realizada em duas etapas: primeiramente, realizou-se a avaliação da percepção da realidade dos cenários pelos respondentes empregando o *software* estatístico *Statistical Package for the Social Sciences* (SPSS) da IBM; na segunda etapa fez-se uso de modelagem de equações estruturais (MEE), mais especificamente utilizando o *software* estatístico *SmartPLS* 3, sendo verificada e avaliada a relação entre as variáveis do modelo. Assim, foram avaliados o modelo de mensuração e o modelo estrutural.

4.1. Avaliação dos cenários

Primeiramente, antes de se iniciar as análises relativas ao modelo de mensuração, avaliou-se a percepção da realidade dos cenários de quebra de PSI pelos respondentes. De modo geral, os respondentes consideraram os cenários realistas, com uma média geral de 5,58 com desvio padrão de 1,407.

Tabela 1 – Realismo dos cenários

Cenário	Média	Número de casos	Desvio padrão	Mínimo	Máximo
Não relatar vírus no computador	5,35	34	1,475	1	7
Compartilhamento de senhas	5,70	30	1,418	2	7
Utilizando aplicativos piratas	5,32	31	1,492	3	7
Utilizando mídias portáteis	6,08	25	1,115	3	7
Total	**5,58**	**120**	**1,412**	**1**	**7**

Fonte: Elaboração própria.

Foi realizado um teste ANOVA para verificar se probabilidade de que diferenças em médias ao longo de diversos grupos ocorrem apenas devido a erro amostral (Hair, Black, Babin, Anderson, & Tatham 2009), por conta do uso de quatro formulários diferentes para a realização da pesquisa. O teste ANOVA não apontou diferença significativa entre as respostas dos formulários, com o valor de significância de 0,153, o que reforça a credibilidade do método de cenários hipotéticos.

4.2. Análise do modelo

Utilizando o *software* estatístico *SmartPLS3*, primeiramente se fez a avaliação do modelo de mensuração, e após a avaliação do modelo estrutural. Através da Análise Fatorial Confirmatória, avaliamos a confiabilidade dos itens, dentro de seus respectivos constructos. Nessa análise, foram excluídas as questões Q22-VP e Q11-CR, por estarem abaixo da carga fatorial recomendada em uma pesquisa exploratória (Hulland, 1999).

Tabela 2 – Cargas fatoriais dos itens nos constructos

Constructo	Questão	AE	BP	CR	ER	HCPSI	ICPSI	PP	VP
Auto Eficácia (AE)	**Q29AE**	**0,798**	-0,463	-0,349	0,429	0,525	0,456	0,362	0,357
	Q34AE	**0,712**	0,018	0,026	0,589	0,557	0,045	0,328	0,344
	Q17AE	**0,689**	-0,169	-0,119	0,376	0,388	0,398	0,414	0,287
	Q19AE	**0,686**	-0,062	-0,029	0,709	0,465	0,043	0,386	0,515
Benefícios Percebidos (BP)	**Q12BP**	-0,155	**0,875**	0,383	0,042	-0,136	-0,586	-0,186	-0,168
	Q25BP	-0,289	**0,831**	0,616	-0,115	-0,246	-0,533	-0,117	-0,164
	Q20BP	-0,228	**0,759**	0,597	-0,065	-0,281	-0,518	-0,144	-0,071
	Q06BP	-0,190	**0,733**	0,296	0,006	-0,156	-0,505	-0,158	-0,095
Custo de Resposta (CR)	**Q26CR**	-0,200	0,537	**0,913**	-0,137	-0,220	-0,444	-0,102	-0,104
	Q27CR	-0,199	0,485	**0,805**	-0,064	-0,190	-0,368	-0,037	0,079
	Q05CR	-0,028	0,369	**0,617**	-0,043	-0,067	-0,349	-0,062	0,003
Eficácia da Resposta (ER)	**Q08ER**	0,562	-0,054	-0,094	**0,810**	0,583	0,159	0,586	0,606
	Q16ER	0,505	-0,076	-0,105	**0,801**	0,491	0,036	0,473	0,618
	Q32ER	0,625	0,030	-0,036	**0,798**	0,488	0,070	0,419	0,547
	Q30ER	0,524	-0,029	-0,111	**0,753**	0,466	0,138	0,441	0,398
Hábito de Cumprir (HCPSI)	**Q23HB**	0,615	-0,156	-0,133	0,539	**0,862**	0,256	0,533	0,473
	Q28HB	0,528	-0,198	-0,186	0,530	**0,813**	0,184	0,446	0,367
	Q10HB	0,533	-0,183	-0,195	0,593	**0,803**	0,302	0,614	0,509
	Q01HB	0,407	-0,320	-0,153	0,326	**0,658**	0,174	0,307	0,257

(continua)

Tabela 2 – Cargas fatoriais dos itens nos constructos (continuação)

Constructo	Questão	AE	BP	CR	ER	HCPSI	ICPSI	PP	VP
Intenção de Cumprir (ICPSI)	**Q21ICPSI**	0,384	-0,622	-0,373	0,121	0,306	**0,896**	0,363	0,268
	Q02ICPSI	0,315	-0,519	-0,280	0,037	0,249	**0,820**	0,337	0,174
	Q14ICPSI	0,062	-0,510	-0,512	0,040	0,095	**0,639**	0,038	0,124
	Q31ICPSI	0,265	-0,304	-0,386	0,238	0,210	**0,594**	0,250	0,136
Perigo Percebido (PP)	**Q03PP**	0,397	-0,140	-0,078	0,511	0,562	0,303	**0,889**	0,539
	Q04PP	0,451	-0,206	-0,092	0,515	0,521	0,334	**0,878**	0,631
	Q33PP	0,435	-0,103	-0,026	0,516	0,533	0,256	**0,853**	0,607
	Q13PP	0,465	-0,197	-0,101	0,559	0,505	0,296	**0,796**	0,714
Vulnerabilidade Percebida (VP)	**Q24VP**	0,426	-0,141	-0,013	0,531	0,400	0,244	0,673	**0,863**
	Q15VP	0,495	-0,172	-0,075	0,690	0,526	0,177	0,577	**0,831**
	Q09VP	0,331	-0,069	0,061	0,487	0,375	0,199	0,583	**0,826**

Fonte: Elaboração própria.

Na avaliação das cargas fatoriais, verificou-se a validade convergente através da AVE (*Average Variance Expected*) Variância Média Esperada. A AVE do constructo Auto Eficácia estava abaixo do recomendado (0,5), então se optou por remover a questão Q07-AE para um melhor ajuste do constructo. Assim, se alcançou o valor mínimo esperado para todos os constructos na AVE. Nessa análise também verificamos a confiabilidade das escalas utilizadas, a qual se deu através da verificação dos valores da confiabilidade composta (*Composite Reliability* - CR), a qual todos os constructos atenderam o mínimo esperado de 0,7, e do Alfa de Crombach com todos os constructos com o coeficiente próximos e acima de 0,7, mais que o esperado em estudos exploratórios (Hulland, 1999).

Tabela 3 – Validade convergente e confiabilidade das escalas

Constructo	α	αA	CR	AVE
Auto Eficácia	0,698	0,715	0,813	0,522
Benefícios Percebidos	0,812	0,816	0,877	0,642
Custo de Resposta	0,680	0,724	0,828	0,621
Eficácia da Resposta	0,801	0,808	0,870	0,626
Hábito de Cumprir	0,795	0,818	0,866	0,621
Intenção de Cumprir	0,731	0,787	0,831	0,559
Perigo Percebido	0,876	0,878	0,915	0,731
Vulnerabilidade Percebida	0,793	0,802	0,878	0,705

Fonte: Elaboração própria.
Nota. α – Alfa de Crombach, **α**A – Alfa de Crombach Ajustado, CR - Confiabilidade Composta, AVE - Avaliação da Validade Convergente.

Na análise da validade discriminante, utilizamos o critério de cargas cruzadas (Fornell-Larcker), onde se espera que cada item seja maior que suas cargas cruzadas e a AVE, na qual a raiz quadrada da AVE é maior que as correlações entre os constructos do modelo. Os critérios da validade discriminante também foram atendidos.

Tabela 4 – Validez discriminante

	AE	BP	CR	ER	HCPSI	ICPSI	PP	VP
AE (1)	**0,723**							
BP (2)	-0,269	**0,801**						
CR (3)	-0,191	0,595	**0,788**					
ER (4)	0,701	-0,042	-0,110	**0,791**				
HCPSI (5)	0,668	-0,257	-0,211	0,646	**0,788**			
ICPSI (6)	0,359	-0,669	-0,493	0,131	0,297	**0,748**		
PP (7)	0,510	-0,189	-0,087	0,613	0,621	0,348	**0,855**	
VP (9)	0,505	-0,157	-0,018	0,690	0,525	0,244	0,726	**0,840**

Fonte: Elaboração própria.

Após assegurar a qualidade do modelo, realizamos novamente o *bootstrapping*, para obter os valores relacionados ao modelo estrutural, medindo a correlações entre os constructos através do teste *t Student*. Para isso foi estimado a aceitação de um coeficiente entre 1,96 até 2,56 para as ligações entre os constructos, representando uma significância estatística de $p < 0,05$ para testar as hipóteses, também acima de 2,56 representando uma significância estatística de $p < 0,01$. Também foi calculado o coeficiente de determinação (R^2), que indica o quanto as variáveis independentes explicam a variância da variável dependente. A técnica de *bootstrapping* foi utilizada para avaliar a consistência do modelo em geral, utilizando 500 amostras. Como a pesquisa foi realizada em diferentes organizações, incluímos como variável de controle o tipo de empresa (pública ou privada) para verificar se haviam diferenças significativas nas respostas.

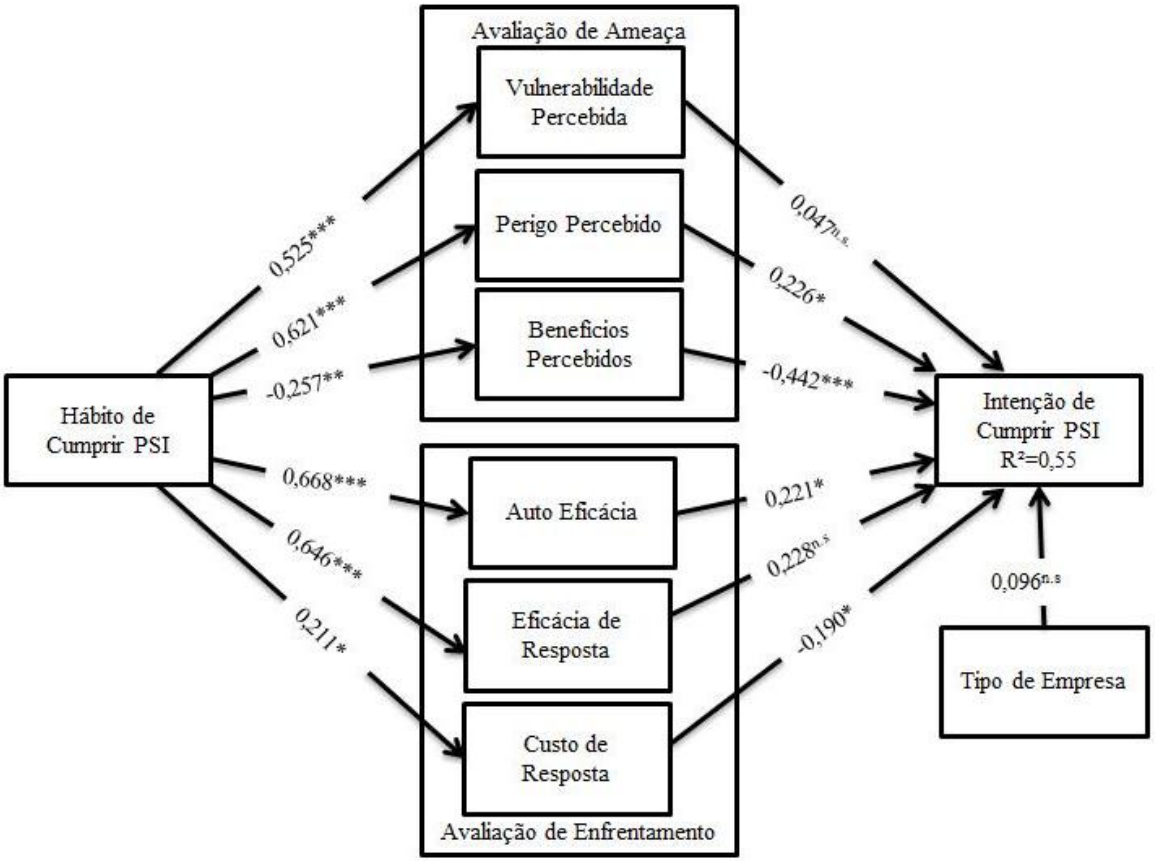
Com o teste do coeficiente de determinação, os constructos da PMT em conjunto são capazes de explicar 55% da variância presente na Intenção de Cumprir com as PSI. Na análise do coeficiente de caminho, onde os valores sempre serão entre +1 e -1, em que o sinal indica a direção positiva ou negativa da correlação entre as variáveis, e a magnitude do valor indica a força da correlação. Referente à variável de controle, o Tipo de Empresa (Pública ou Privada) não influenciou na Intenção de Cumprir com as PSI (β 0,096; $p > 0,05$).

Nos resultados referentes à Avaliação da Ameaça, a Vulnerabilidade Percebida não obteve um efeito significante na Intenção de Cumprir (β 0,047; $p > 0,05$), não suportando H1. O Perigo Percebido influenciou a Intenção de Cumprir com as PSI (β 0,226; $p < 0,05$) validando H2 e os Benefícios influenciaram negativamente a Intenção de Cumprir com as PSI (β -0,442; $p < 0,000$), validando H3.

Referente à Avaliação de Enfrentamento, a Eficácia da Resposta não teve influência significativa sobre a Intenção de Cumprir com as PSI, não suportando H4 (β -0,228; $p > 0,05$). A Auto Eficácia demonstrou impactar na Intenção de Cumprir com as PSI (β 0,221; $p < 0,05$), suportando a H5, o Custo da Resposta influenciou negativamente na Intenção de Cumprir com as PSI, validando a H6 (β -0,190; $p < 0,05$).

O Hábito demonstrou influenciar todos os constructos da PMT, influenciando a Vulnerabilidade Percebida (β 0,525; $p < 0,000$), o Perigo Percebido (β 0,621; $p < 0,000$), a Eficácia da Resposta (β 0,646; $p < 0,000$) e a Auto Eficácia (β 0,668; $p < 0,000$) positivamente, e os Benefícios (β -0,257; $p < 0,01$) e o Custo de Resposta (β -0,211; $p < 0,05$) negativamente. Todos os resultados estão dentro do esperado, validando H7a, H7b, H7c, H7d e H7f.

Figura 1 – Modelo de pesquisa e resultados



Nota. *** – p < 0,001, ** – p < 0,01, * – p < 0,05, e $^{n.s}$ – Não significante.
Fonte: Elaboração própria.

4.3. Discussão dos resultados

Os resultados deste estudo podem ser avaliados e discutidos sobre diferentes perspectivas. O estudo contribui para o avanço do conhecimento sobre como indivíduos que trabalham em organizações no estado do Rio Grande do Sul compreendem as ameaças a que estão sujeitos usando os componentes de SI das organizações nas quais trabalham.

Na Avaliação dos cenários, pode-se perceber através da análise descritiva, que mesmo que todos os cenários tenham uma boa percepção como realistas pelos respondentes, alguns obtiveram um reconhecimento maior, se destacando o uso de mídias portáteis, como no exemplo do cenário um pen drive e o compartilhamento de senhas de uso exclusivo entre os usuários de um mesmo sistema. Com esses resultados, acreditamos que esses aspectos necessitam de investigações mais profundas.

O constructo Hábito demonstrou ter grande impacto nos constructos da PMT, com todas as hipóteses validadas (H7a, H7b, H7c, H7d e H7f). Isso está de acordo com outras pesquisas, que colocam o Hábito como fator importante para a intenção de cumprir com as normativas relacionadas à Segurança da Informação dentro das organizações (Vance et al., 2012; Pahnila, Siponen, & Mahmood, 2007), reafirmando a importância da frequência no cumprimento das PSI para o fortalecimento dos hábitos relacionados à Segurança da Informação.

A Vulnerabilidade Percebida não demonstrou influenciar a Intenção de Cumprir com as PSI. Este resultado vai contra o determinado pela PMT, não suportando H1. Outros estudos já encontram esse resultado (Vance et al., 2012; Bauer & Bernroider, 2015; Hamus & Wu, 2016). Isto é um problema, pois se o usuário de sistema dentro de uma organização não se sente vulnerável a usar o mesmo, existe a necessidade de desenvolver nesse indivíduo a

consciência sobre as ameaças disponíveis. Parte disso se estabelece através de treinamentos, por exemplo.

O constructo Perigo Percebido demonstrou ter influência sobre a Intenção de Cumprir com as PSI, validando H2. É importante salientar esse resultado, pois as sanções disponíveis aos indivíduos caso não cumpram com as PSI determinadas pelas suas organizações são percebidas como significantes, e influenciam positivamente na intenção de cumprir com as normativas. Mesmo assim, reafirmamos que somente sanções não são suficientes para evitar esse comportamento não recomendado, sendo necessário levar em conta os outros aspectos relacionados à Segurança da Informação (Hu et al., 2012).

O constructo Benefícios Percebidos, assim como o definido pela PMT, influenciou negativamente a Intenção de Cumprir com as PSI, suportando H3. Podemos supor que, ao não cumprir com as PSI nas organizações, os usuários acreditam estar ganhando um tempo que seria perdido ao cumprir com as normativas. Neste ponto, com relação às variáveis utilizadas para avaliar a ameaça, é válido destacar que a magnitude do benefício percebido é praticamente o dobro da do perigo percebido, ou seja, demonstra a importância da primeira para o não cumprimento de PSI no contexto investigado. Fica clara a necessidade de estabelecer dentro das organizações a centralidade da temática Segurança da Informação.

Os resultados referentes à Auto Eficácia ficaram dentro do determinado pela PMT, com o constructo influenciando positivamente na Intenção de Cumprir com as PSI. Se esse usuário está acostumado com uso das mais variadas tecnologias, cumprir com as determinações das PSI não é uma tarefa complicada, o que justifica o resultado. O Custo de Resposta influenciou negativamente na Intenção de Cumprir as PSI, validando H6. Sendo assim, observa-se um custo associado ao cumprir com as normativas especificadas nas PSI das organizações nas quais os respondentes trabalham, sendo estes considerados inconvenientes e trabalhosos. Isso reflete a possível falta de conscientização dos respondentes quanto à importância dessas políticas.

O constructo Eficácia da Resposta não demonstrou influência sobre a Intenção de Cumprir com as PSI, não validando H4. Esse resultado demonstra que esses indivíduos não percebem a efetividade em cumprir com as PSI. Isto pode estar relacionado à maneira que cada organização dispõe de sua PSI para esse funcionário. Assim, o resultado revela que no contexto estudado os indivíduos em suas organizações ainda não acreditam na importância do comportamento que exige cumprimento das PSI como forma de combater as ameaças no uso dos sistemas.

Sommestad et al. (2015) evidenciaram através de uma Meta-Análise com estudos que utilizaram a PMT, que o poder de explicação dela é maior quando a ameaça é em relação a segurança do indivíduo, e não a organização na qual ele se encontra. Isso se apoia em outro estudo, no qual Warkentin, Johnston, Walden e Straub (2016) colocam que, mesmo que uma ameaça seja percebida por um usuário em seu ambiente profissional, ela certamente não terá o mesmo impacto que uma ameaça a nível pessoal. Por isso as organizações possuem a necessidade de não apenas impor normativas, mas desenvolver em seus colaboradores a preocupação relacionada ao uso correto das tecnologias disponíveis, a fim de evitar problemas com Segurança da Informação. Isso só é possível com a presença da Alta Gerência, pois as PSI são ferramentas de defesa dos recursos da empresa. A presença da gestão da segurança da informação a partir do envolvimento da Alta Gerência é que converge em processos efetivos, incluindo as PSI (Ferreira et al., 2016).

5. Considerações Finais

Com a consolidação do paradigma tecnológico atual, com seu alto grau de penetrabilidade nas diversas atividades humanas, em que praticamente a maioria das atividades prescinde ou perpassa por alguma solução tecnológica, a adoção de práticas de

segurança da informação torna-se, por evidência, essencial para que as organizações fiquem menos vulneráveis a ataques externos, seja de vírus ou *hackers*, perda ou violação de dados, instabilidades na rede e no sistema de informação e dentre outros problemas, cujas consequências podem afetá-las estrategicamente.

Desta forma, identificar como a percepção de ameaças influenciam os usuários na Intenção de Cumprir com as PSI faz-se necessário em um contexto de constantes evoluções tecnológicas, em que a busca por proteger os sistemas organizacionais tornou-se parte incessável no mundo globalizado. Os resultados apontam que, de maneira geral, para os respondentes, mesmo aqueles que trabalham em empresas que possuem normas de segurança estabelecidas quanto ao uso dos Sistemas de Informação com a finalidade de proteger os ativos organizacionais, as vulnerabilidades a que as organizações estão sujeitas não são perceptíveis por esses usuários, mas mesmo assim, eles percebem como importantes os problemas envolvidos no não cumprimento das PSI, como as sanções, por exemplo.

Do ponto de vista prático, isso dificulta o combate às ameaças do mundo cibernético pelas organizações, pois o usuário torna-se um vetor de possíveis problemas relacionados à Segurança da Informação. Contudo, há de se considerar que o usuário não pode ser responsabilizado totalmente pelas ameaças em virtude das suas práticas. Tendo em vista que, dialeticamente, o usuário é ao mesmo tempo o responsável pela adoção das práticas e estabelecimento da cultura de segurança e àquele mais suscetível a ameaças, já que usam os mais variados sistemas e dispositivos tecnológicos na organização. Se existe a possibilidade de portas a serem abertas, através de e-mail, por exemplo, para ataques de vírus, a organização deve estabelecer políticas de bloqueios de site, infraestrutura interna para comunicação dos usuários, alguns filtros, treinamento e acompanhamento das ações para evitar consequências custosas.

Referente ao modelo utilizado, o mesmo cumpriu com suas expectativas, auxiliando a responder o questionamento inicial, em partes graças ao uso da Teoria da Motivação à Proteção e a Teoria do Hábito, já estabelecidas na literatura. Os cenários hipotéticos foram considerados realistas pelos respondentes, retratando em partes possíveis quebras de PSI nas organizações que os respondentes trabalham, demonstrando não só a importância do método, mas a necessidade de se aprofundar o estudo sobre alguns desses comportamentos não recomendados, como o compartilhamento de senhas e o uso de dispositivos portáteis. Além do diferente contexto, deve-se levar em conta o fato desse estudo ter uma amostra formada por usuários de diferentes organizações. Pode-se colocar que outras variáveis também podem influenciar no comportamento dos indivíduos, e que não foram consideradas nesse modelo, como os aspectos físicos do ambiente de trabalho, as normas sociais, a satisfação com o trabalho e relações entre empresa e empregado.

O estudo é uma importante contribuição para as pesquisas em segurança da informação, pela ausência de estudos já referida anteriormente, pela validação de um modelo criado em um país referência em segurança da informação e pela natureza da pesquisa com a aplicação em usuários de organizações diversas no Rio Grande do Sul e que possuem normas de segurança da informação, muitas vezes diferentes, e estão imersas em culturas organizacionais difusas. É evidente que a amostra não probabilística com 121 respondentes é uma limitação do artigo, mas não inviabiliza as suas contribuições para o campo.

Referências

Albuquerque, A. E., Jr., & Santos, E. M. (2014). Adoção de medidas de segurança da informação: um modelo de análise para institutos de pesquisa públicos. *Revista Brasileira de Administração Científica, 5*(2), 46-59.

Alves, V., Gomes-De-Souza, C., Chrispino, Á., & Ogasawara, E. (2014). Segurança da informação e políticas públicas no Brasil. *Anais Simpósio de Excelência em Gestão e Tecnologia*, Brasil, 11.

Associação Brasileira de Normas Técnicas (2005). *NBR ISO/IEC 27002:2005: Tecnologia da Informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação*. Rio de Janeiro: Autor.

Barlette, Y., Gundolf, K., & Jaouen, A. (2015, May). Toward a better understanding of SMB CEOs' information security behavior: insights from threat or coping appraisal. *Journal of Intelligence Studies in Business, 5*(1).

Bauer, S., & Bernroider, E. W. (2015, August). The effects of awareness programs on information security in banks: the roles of protection motivation and monitoring. *International Conference on Human Aspects of Information Security, Privacy, and Trust* (pp. 154-164). New York: Springer, Cham.

Britto-da-Silva, V. R., Magnagnagno, O. A., & Luciano, E. M. (2015). Preocupação com a privacidade na internet: uma pesquisa exploratória no cenário brasileiro. *Anais do Encontro de Administração da Informação*, Brasil, 5.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, *34*(3), 523-548.

Dalmoro, M., & Vieira, K. M. (2014). Dilemas na construção de escalas Tipo Likert: o número de itens e a disposição influenciam nos resultados? *Revista gestão organizacional, 6*(3).

Ferreira, M. R., Dolci, D. B., & Tondolo, V. A. G. (2016). Uma proposta de diagnóstico e autoavaliação da gestão da segurança da informação. *Encontro da ANPAD*, Costa do Sauípe, BA, Brasil, 40.

Gil, A. C. (2002). *Como elaborar projetos de pesquisa* (4a ed.). São Paulo: Atlas.

Goel, S., & Chengalur-Smith, I. N. (2010). Metrics for characterizing the form of security policies. *The Journal of Strategic Information Systems, 19*(4), 281-295.

Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L. (2009). *Análise multivariada de dados*. Porto Alegre: Bookman.

Hanus, B., & Wu, Y. A. (2016). Impact of users' security awareness on desktop security behavior: a protection motivation theory perspective. *Information Systems Management*, *33*(1), 2-16.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106-125.

Hsu, J. S. C., Shih, S. P., Hung, Y. W., & Lowry, P. B. (2015). The role of extra-role behaviors and social controls in information security policy effectiveness. *Information Systems Research*, *26*(2), 282-300.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: the critical role of top management and organizational culture. *Decision Sciences*, *43*(4), 615-660.

Hulland, J. (1999). Use of partial least squares (PLS) in strategic management research: a review of four recent studies. *Strategic management journal*, *20(*2), 195-204.

Ifinedo, P. (2014). Information systems security policy compliance: an empirical study of the effects of socialisation, influence, and cognition. *Information & Management*, *51*(1), 69-79.

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: an empirical study. *MIS quarterly*, 549-566.

Lei n. 13.709, de 14 de Agosto de 2018 (2018). Dispõe sobre a proteção de dados pessoais e altera a Lei n. 12.965, de 23 de Abril De 2014 (Marco Civil da Internet). Recuperado em 10 novembro, 2018, de http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: a revised theory of fear appeals and attitude change. *Journal of experimental social psychology*, *19*(5), 469-479.

Martin, N., & Zafar, H. (2015). Information security: modeling the unconscious mind. *Americas Conference on Information Systems*, Puerto Rico, 21.

Norman, P., Boer, H., & Seydel, E. R. (2005). Protection motivation theory. *Predicting health behaviour*, *81*, 126.

Pahnila, S., Siponen, M., & Mahmood, A. (2007, January). Employees' behavior towards IS security policy compliance. *Annual Hawaii International Conference on System Sciences*, Havaii, USA, 40.

Rodrigues, G. C. (2015). *BYOD como política de segurança em uma empresa: uma análise à luz da PMT*. Dissertação de Mestrado, Universidade Federal do Rio Grande do Norte, Natal, RN, Brasil.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. *The journal of psychology*, *91*(1), 93-114.

Soceanu, A., Vasylenko, M., & Gradinaru, A. (2016). Teaching/researching practically oriented ICT security topics using green mobility solutions within a virtual campus. *Proceedings International Multi-Conference on Complexity, Informatics and Cybernetics*: *IMCIC*, 7.

Sommestad, T., Karlzén, H., & Hallberg, J. (2015). A meta-analysis of studies on protection motivation theory and information security behaviour. *International Journal of Information Security and Privacy (IJISP)*, *9*(1), 26-46.

Souza, A. F., Jr., & Streit, R. E. (2017). Segurança cibernética: política brasileira e a experiência internacional. *Revista do Serviço Público, 68*(1), 107-130.

Symantec (2017). *Internet security threat report*. Recuperado em: Acesso em: 10 novembro, 2018, de https://www.symantec.com/pt/br/security-center/threat-report.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: insights from habit and protection motivation theory. *Information & Management, 49*(3-4), 190-198.

Verplanken, B., & Orbell, S. (2003). Reflections on past behavior: a self-report index of habit strength 1. *Journal of applied social psychology*, *33*(6), 1313-1330.

Warkentin, M., Johnston, A. C., Walden, E., & Straub, D. W. (2016). Neural correlates of protection motivation for secure IT behaviors: an fMRI examination. *Journal of the Association for Information Systems, 17*(3), 194.