Conformidade dos Funcionários com a Política de Segurança da Informação da Organização: Validação de um Modelo

Jonas Silveira
jonasrsilveira@outlook.com
FURG

Decio Dolci
dbdolci@gmail.com
FURG

Jonatas Wendland
wendlandjonatas@gmail.com
FURG

Paulo Munhoz
paulorsmunhoz@hotmail.com
FURG

Bernardo Silva
contato@bernardosilva.com.br
FURG

Resumo: Teorias comportamentais têm sido amplamente utilizadas para auxiliar na identificação das variáveis antecedentes ao cumprimento de Políticas de Segurança da Informação. Na presente pesquisa, fez-se uso do modelo proposto por Vance, Siponen e Pahnila (2012) para avaliar como o hábito influencia os processos cognitivos presentes na Teoria da Motivação a Proteção (PMT) e como os processos da PMT influenciam o cumprimento das Políticas de Segurança da Informação. Empregou-se o método de cenários hipotéticos em conjunto com uma pesquisa survey. A pesquisa foi realizada com 122 funcionários de empresas localizadas no estado do Rio Grande do Sul. Primeiramente, avaliou-se o modelo de mensuração e, após, o modelo estrutural. Os resultados demonstram a validade do modelo proposto em um novo contexto, reafirmando a importância do hábito para o cumprimento das Políticas de Segurança da Informação nas organizações.

Palavras Chave: Segurança - PMT - Motivação a Proteção - Hábito -

1. INTRODUÇÃO

Para sobreviver e competir em ambientes operacionais turbulentos como os de hoje, organizações continuam a confiar e investir em seus sistemas de informação (IFINEDO, 2014), porém os avanços técnicos na Ciência da Computação não são suficientes para produzir ambientes seguros, ao contrário, os avanços tecnológicos podem multiplicar o potencial de magnitude das violações e a velocidade na qual suas consequências são percebidas (METALIDOU *et al*, 2014). Proteger dados sensíveis se tornou vital às organizações (LOWRY *et al*, 2015).

De acordo com a pesquisa divulgada pela consultoria Ernest & Young (2016), os funcionários são a segunda maior fonte provável de ataque cibernético, citado por 56% dos respondentes. Para diminuir os riscos de possíveis perdas, organizações tem implementado Políticas de Segurança da Informação e sansões para impedir que seus funcionários cometam atividades que podem ser prejudiciais à organização (LOWRY *et al*, 2015). Paralelamente, no meio acadêmico, estudos são necessários para melhorar a nossa compreensão das questões que servem para incentivar a Segurança da Informação (IFINEDO, 2014). Uma das teorias utilizadas para colaborar com a discussão tem sido a Teoria da Motivação a Proteção (PMT, no idioma Inglês *Protection Motivation Theory*), desenvolvida por Rogers (1975). Recentes pesquisas com diferentes abordagens demonstram o uso da PMT. Investigações sobre a intenção de cumprir com Políticas de Segurança envolvendo BYOD (*Bring Your Own Device*) (RODRIGUES, 2015); a percepção de usuários sobre senhas e a conformidade com as Políticas de Segurança (MWAGWABI, MCGILL e DIXON, 2014); os fatores que afetam ou não a decisão de CEOs de melhorar ou não a Segurança da Informação de suas empresas (BARLETTE, GUNDOLF e JAOUEN, 2015), são exemplos do uso da Teoria da Motivação a Proteção na área de Segurança da Informação.

Vance, Siponen e Pahnila (2012) foram os primeiros autores a demonstrar a aplicação da Teoria da Proteção a Motivação por completo na área de Segurança da Informação. Além disso, pesquisas anteriores não haviam considerado o comportamento passado, sendo ele um componente para o desencadeamento do processo da PMT. Outro diferencial foi o uso do método de cenários hipotéticos, no qual foi apresentado uma vinheta que descrevia uma ação ou decisão relacionada com o cumprimento de Políticas de Segurança, auxiliando no preenchimento do questionário. Considerando a relevância e o pioneirismo do referido estudo, delineou-se a presente pesquisa, sendo o problema de pesquisa identificar quais os fatores que influenciam no cumprimento das Políticas de Segurança da Informação pelos indivíduos a luz da Teoria da Motivação a Proteção e da Teoria do Hábito. O objetivo geral dessa pesquisa é a validação do modelo proposto por Vance, Siponen e Pahnila (2012) em um novo contexto, tendo como objetivos específicos: (1) Elaborar cenários de não cumprimento a Políticas de Segurança em SI que correspondam a realidade dos respondentes; (2) Adaptar o questionário elaborado por Vance, Siponen e Pahnila (2012) de maneira clara ao contexto investigado nesta pesquisa; (3) Comparar os resultados obtidos com a pesquisa de Vance, Siponen e Pahnila (2012).

2. MODELO DE VANCE, SIPONEN E PAHNILA

O Modelo de Vance, Siponen e Pahnila (Figura 1) baseia-se na Teoria da Motivação à Proteção e na Teoria do Hábito. Nesta seção, apresentam-se as variáveis e as hipóteses presentes no modelo.

A Teoria da Motivação a Proteção (PMT), proposta por Rogers (1975), foi inicialmente utilizada para prever a intenção em adotar um comportamento de saúde recomendado através do perigo percebido, o qual desencadeia processos cognitivos. Configura-se em dois componentes principais: avaliação das ameaças e avaliação de enfrentamento. Dessas dimensões resultam seis variáveis latentes.

A avaliação de ameaça está relacionada com as percepções de como um indivíduo se sente ameaçado com base na avaliação dos componentes do medo (HERATH e RAO, 2009). Vulnerabilidade é a probabilidade de que um incidente indesejado possa acontecer caso não sejam tomadas medidas para impedi-lo. No contexto dessa pesquisa, vulnerabilidade da segurança de SI remete aos incidentes que os usuários percebem que podem acontecer caso não cumpram com as Políticas de Segurança da Informação. A severidade percebida diz respeito ao impacto que uma ameaça pode causar para o indivíduo. No contexto dessa pesquisa, severidade percebida refere-se ao impacto negativo que uma violação na segurança da informação pode causar para ele ou para a empresa. Os benefícios se referem a qualquer motivação intrínseca ou extrínseca para aumentar ou manter um comportamento indesejado. No contexto dessa pesquisa, benefício percebido foi conceituado como a economia de tempo que o indivíduo identifica caso não cumpra com as políticas de segurança.

A avaliação de enfrentamento centra-se nas respostas disponíveis que o indivíduo possui para lidar com a ameaça (NORMAN, BOER e SEYDEL, 2005). 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 essa pesquisa, a eficácia da resposta consiste na capacidade que o indivíduo possui em compreender a importância do cumprimento das Políticas de Segurança da Informação. A auto eficácia corresponde a capacidade do indivíduo de responder à ameaça percebida, se demonstrando como uma variável de impacto significativo sobre o indivíduo (IFINEDO, 2014). Neste estudo, auto eficácia corresponde à convicção que o indivíduo possui capacidades para cumprir com as Políticas de Segurança da Informação. O custo da resposta são os custos envolvidos no comportamento adaptativo (RODRIGUES, 2015), sendo no contexto dessa pesquisa, todos os custos envolvidos no cumprimento das Políticas de Segurança da Informação que não se refiram a tempo de trabalho.

Seguindo essas premissas, Vance, Siponen e Pahnila (2012) propõem as seguintes hipóteses:

H1. Vulnerabilidade percebida afeta positivamente a intenção de cumprir as políticas de segurança de SI.
H2. A severidade percebida 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.
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.

No que se refere à Teoria do Hábito, esta sugere que muitas ações ocorrem sem decisão consciente de agir e são realizadas porque os indivíduos estão acostumados a realizá-las; frequentemente comportamento repetido é mais controlado por estímulos situacionais do que pela tomada de decisão consciente. Assim, Vance, Siponen e Pahnila (2012), postularam que o comportamento habitual tem uma influência negativa sobre o custo da resposta e os benefícios percebidos, isto é, o custo da resposta e os benefícios percebidos diminuem com o hábito de cumprir as políticas de segurança em SI. Por outro lado, o hábito de cumprir com as políticas de segurança de SI influencia positivamente a gravidade, a auto eficácia, a eficácia da resposta e a vulnerabilidade, pois se ele possui o hábito de cumprir com essas políticas ele

percebe melhor os incidentes que podem ocorrer caso ele não as cumpra (VANCE, SIPONEN e PAHNILA, 2012). Nesse sentido, sugerem-se as seguintes hipóteses:

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.

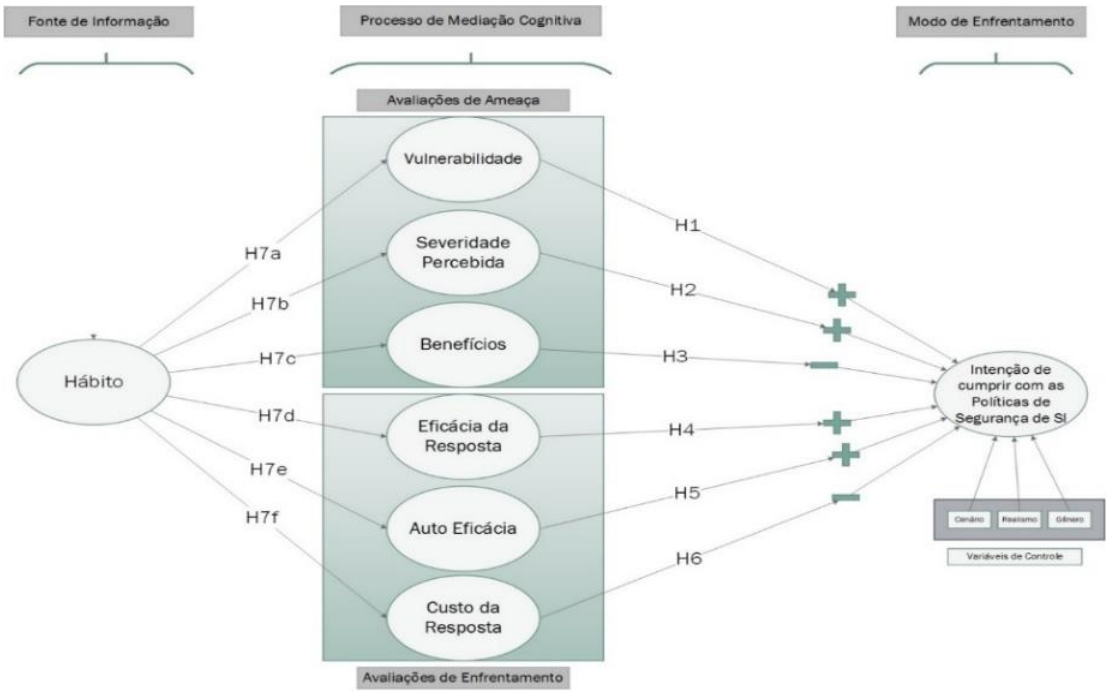

Figura 1: Modelo do estudo de Vance, Siponen e Pahnila (2012)

3. METODOLOGIA

Além do método de cenários hipotéticos, foi utilizado o método *survey*. O instrumento de coleta de dados foi estruturado em duas partes. De acordo com o que evidenciaram De Albuquerque Junior e Dos Santos (2014), muitas empresas possuem políticas de segurança formalizadas, mas não possuem procedimentos que instituam a análise crítica dessas políticas com o intuito de verificar sua validade ao longo do tempo. Também foi verificado que o nível de satisfação com a formalização dessas políticas é baixo. Sendo assim, foram utilizadas duas perguntas de filtro que abordavam o nível de implementação da política de segurança dentro das organizações dos respondentes, sendo essas questões extraídas dos estudos de Ferreira, Dolci e Tondolo (2016). Já a segunda parte continha o cenário que evidenciava uma quebra de uma possível Política de Segurança da Informação de uma empresa, sendo utilizados quatro cenários, baseados no estudo de Vance, Siponen e Pahnila (2012), adaptados para a realidade dos possíveis respondentes e atualizados de acordo com as ameaças mais comuns a que esses indivíduos estão sujeitos.

Tabela 1: Cenários hipotéticos

Cenário Proposto	**Descrição Cenário**
Compartilhando documentos sigilosos	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	Flavia 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. Flavia 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 causados por ele. Rodrigo perde o pen drive, 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.

A segunda parte também continha as questões sobre informações gerais como gênero, idade, cidade, e as questões relacionadas aos constructos do modelo, sendo essas 34 questões fechadas e estruturadas em escala Likert de 7 pontos, variando de 1 (discordo totalmente) a 7 (concordo totalmente). 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 se determinou a técnica bola de neve, sendo o link para a pesquisa compartilhado via e-mail e redes sociais, com a solicitação que fosse compartilhado com outras pessoas. É válido observar que a coleta de dados de Vance, Siponen e Pahnila (2012) ocorreu com funcionários de uma única organização, diferentemente da presente pesquisa.

4. ANÁLISE E RESULTADOS

A análise dos dados foi realizada em duas etapas: primeiramente, realizou-se a purificação dos dados empregando o software estatístico 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. 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, três foram removidos pelo excesso

de questões não respondidas, restando ao final um total de 122 respondentes. A caracterização da amostra encontra-se na tabela 2.

Tabela 2: Características da amostra

Características		**Absoluta (n)**	**Relativa %**
Gênero			
	Feminino	60	49,2
	Masculino	62	50,8
Idade			
	18 a 24	42	34,4
	25 a 40	63	51,6
	41 a 60	15	12,3
	Acima de 60	2	1,6
Cidade			
	Rio Grande	74	60,7
	São José do Norte	21	17,2
	Porto Alegre	3	2,5
	Pelotas	2	1,6
	Alegrete	2	1,6
	Outro	14	11,3
	Não informaram	4	3,3
Escolaridade			
	Ensino Médio	10	8,2
	Ensino Superior Incompleto	58	47,5
	Ensino Superior Completo	33	27
	Pós Graduação	21	17,2
Tipo de Empresa			
	Pública	31	25,4
	Privada	91	74,6
Setor da Empresa			
	Serviço	50	41
	Indústria	19	15,6
	Educação	28	23
	Comércio	21	17,2
	Agropecuária	1	0,8
	Não informaram	3	2,5

4.1 MODELO DE MENSURAÇÃO

Considerando a avaliação do modelo de mensuração, constatou-se que as cargas fatoriais dos itens estão maiores em seus respectivos constructos (Tabela 1). Foram removidas do modelo as questões Q07-AE, Q19-AE, Q22-VP, Q27-CR, por não terem se mostrado relevantes junto ao modelo. Das questões que permaneceram, apenas duas não apresentaram carga fatorial superior a 0,60, sendo elas a Q11-CR e Q31-IC. Mesmo não tendo respeitado esse critério de validade convergente, optou-se por manter essas questões no modelo por adicionarem mais confiabilidade à sua variável latente. Os resultados estão na tabela 3.

Tabela 3: Cargas fatoriais dos itens nos constructos

Constructo	Item	1	2	3	4	5	6	7	8
Auto Eficácia (1)	Q17-AE	**0,750**	-0,166	-0,054	0,363	0,354	0,396	0,411	0,287
	Q29-AE	**0,858**	0,453	-0,294	0,422	0,514	0,454	0,355	0,350
	Q34-AE	**0,637**	0,072	0,022	0,507	0,508	0,007	0,281	0,291
Benefícios (2)	Q06-BN	-0,209	**0,748**	0,301	-0,013	-0,127	-0,502	-0,137	-0,101
	Q12-BN	-0,209	**0,885**	0,381	0,056	-0,127	-0,590	-0,177	-0,180
	Q25-BN	-0,316	**0,817**	0,544	-0,085	-0,239	-0,524	-0,115	-0,153
	Q20-BN	-0,195	**0,715**	0,501	0,029	-0,197	-0,487	-0,076	-0,037
Custo da resposta (3)	Q05-CR	-0,063	0,333	**0,722**	-0,060	-0,088	-0,317	-0,044	-0,032
	Q11-CR	-0,017	0,347	**0,575**	0,080	-0,002	-0,267	0,090	0,032
	Q26-CR	-0,239	0,483	**0,843**	-0,155	-0,241	-0,406	-0,102	-0,060
Eficácia da resposta (4)	Q08-ER	0,443	0,020	-0,091	**0,805**	0,602	0,141	0,524	0,605
	Q16-ER	0,377	-0,066	-0,112	**0,788**	0,495	0,051	0,449	0,632
	Q30-ER	0,430	-0,021	-0,047	**0,705**	0,418	0,125	0,441	0,370
	Q32-ER	0,452	0,054	-0,023	**0,749**	0,442	0,011	0,342	0,439
Hábito (5)	Q01-HB	0,346	-0,299	-0,153	0,330	**0,644**	0,172	0,301	0,249
	Q10-HB	0,476	-0,157	-0,126	0,610	**0,791**	0,288	0,610	0,479
	Q23-HB	0,472	-0,133	-0,115	0,422	**0,762**	0,255	0,367	0,427
	Q28-HB	0,522	-0,118	-0,174	0,563	**0,824**	0,165	0,468	0,402
Intenção (6)	Q02-IC*	0,402	-0,525	-0,281	0,043	0,221	**0,817**	0,336	0,155
	Q14-IC*	0,072	-0,492	-0,506	0,005	0,101	**0,629**	0,019	0,167
	Q21-IC*	0,433	-0,614	-0,337	0,112	0,319	**0,899**	0,354	0,271
	Q31-IC*	0,264	-0,284	-0,321	0,208	0,195	**0,574**	0,254	0,122
Severidade (7)	Q03-SP	0,368	-0,123	-0,031	0,474	0,539	0,301	**0,887**	0,526
	Q04-SP	0,406	-0,187	-0,048	0,481	0,506	0,332	**0,876**	0,619
	Q13-SP	0,415	-0,147	-0,055	0,525	0,449	0,260	**0,746**	0,615
	Q33-SP	0,372	-0,083	-0,042	0,493	0,499	0,248	**0,853**	0,585
Vulnerabilidade (8)	Q09-VP	0,292	-0,066	0,050	0,506	0,359	0,163	0,548	**0,796**
	Q15-VP	0,368	-0,161	-0,060	0,629	0,509	0,199	0,518	**0,824**
	Q24-VP	0,348	-0,134	-0,071	0,544	0,408	0,249	0,660	**0,860**

Outra análise realizada foi a da confiabilidade das escalas utilizadas, a qual se deu através da verificação dos valores da confiabilidade composta (*Composite Reliability* - CR), sendo que todos os constructos apresentaram cargas maiores do que o limite mínimo de 0,70. A avaliação da validade convergente também foi positiva, com todos os constructos ultrapassando o valor mínimo de 0,50 para a AVE (*Average Variance Expected*). A validade discriminante também foi confirmada, com todos os itens com a carga fatorial maior em suas cargas cruzadas. A tabela 4 demonstra os resultados obtidos e a tabela 4 compara os resultados obtidos com os da pesquisa de Vance, Siponen e Pahnila (2012).

Tabela 4: Variância compartilhada, correlações e confiabilidade dos constructos

Constructo	**CR**	**AVE**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Auto eficácia (1)	0,796	0,568	**0,754**							
Benefícios (2)	0,871	0,630	-0,293	**0,794**						
Custo (3)	0,761	0,520	-0,177	0,544	**0,721**					
Eficácia (4)	0,847	0,582	0,555	-0,004	-0,093	**0,763**				
Hábito (5)	0,847	0,581	0,602	-0,217	-0,184	0,652	**0,762**			
Intenção (6)	0,826	0,550	0,416	-0,664	-0,466	0,112	0,292	**0,742**		
Severidade (7)	0,907	0,710	0,462	-0,161	-0,052	0,583	0,593	0,340	**0,842**	
Vulnerabilidade (8)	0,866	0,684	0,411	-0,152	-0,039	0,683	0,523	0,248	0,693	**0,827**

Notas:
CR - Confiabilidade Composta;
AVE - Avaliação da Validade Convergente.

Tabela 5: Comparação entre os resultados

Constructo	**Estudo**	**CR**	**AVE**	**VD**
Auto eficácia (1)	Vance *at al* (2012)	0.820	0.600	**0.770**
	Neste estudo	0.796	0.568	**0.754**
Benefícios (2)	Vance *at al* (2012)	0.870	0.690	**0.83**
	Neste estudo	0.871	0.630	**0.794**
Custo (3)	Vance *at al* (2012)	0.800	0.570	**0.760**
	Neste estudo	0.761	0.520	**0.721**
Eficácia (4)	Vance *at al* (2012)	0.860	0.680	**0.830**
	Neste estudo	0.847	0.582	**0.763**
Hábito (5)	Vance *at al* (2012)	0.860	0.550	**0.740**
	Neste estudo	0.847	0.581	**0.762**
Intenção (6)	Vance *at al* (2012)	0.960	0.930	**0.960**
	Neste estudo	0.826	0.550	**0.742**
Severidade (7)	Vance *at al* (2012)	0.850	0.740	**0.860**
	Neste estudo	0.907	0.710	**0.842**
Vulnerabilidade (8)	Vance *at al* (2012)	0.850	0.740	**0.860**
	Neste estudo	0.866	0.684	**0.827**

Notas
CR - Confiabilidade Composta
AVE - Avaliação da Validade Convergente
VD - Validade Discriminante

4.2 MODELO ESTRUTURAL

O modelo estrutural tem por objetivo avaliar o relacionamento preditivo ou causal entre os constructos do modelo. 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 (R2), que indica o quanto as variáveis exógenas conseguem explicar a variação da variável endógena. Ainda foi analisado o grau de associação entre as variáveis. A técnica de *bootstrapping* foi utilizada para avaliar a consistência do modelo em geral, utilizando 500 amostras. Apenas a relação entre a variável Vulnerabilidade Percebida e Intenção de Cumprir não se encontrou dentro do intervalo de confiança determinado. Severidade Percebida, Eficácia da Resposta e Custo da

Resposta com a Intenção em um intervalo de confiança de 95%, a relação dos Benefícios e da Auto Eficácia com a Intenção no intervalo de confiança de 99%. Assim como no estudo de Vance, Siponen e Pahnila (2012), o Hábito demonstrou ter grande impacto sobre os constructos da PMT.

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. O valor é maior do que o encontrado na pesquisa de Vance, Siponen e Pahnila (2012) o que indica que o modelo possui um grau de confiabilidade importante mesmo em um diferente contexto. Na análise do coeficiente de caminho, na qual 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, a Vulnerabilidade Percebida assim como na análise obtida por Vance, Siponen e Pahnila (2012) não obteve um efeito significante na Intenção de Cumprir (β 0,064; $p > 0,05$), não suportando H1. A Severidade Percebida afetou positivamente a Intenção de Cumprir com as políticas de segurança (β 0,231; $p < 0,05$) e os Benefícios afetaram negativamente a Intenção de Cumprir (β -0,44; $p < 0,01$), validando H3.

Também como nos resultados encontrados em 2012, a Eficácia da resposta não teve o impacto positivo esperado, mas sim um impacto negativo sobre a Intenção, não suportando H4 (β -0,22; $p < 0,05$). A Auto Eficácia demonstrou impactar na Intenção, assim como encontrado por Vance (β 0,24; $p < 0,01$), suportando a H5, o Custo da resposta impactou negativamente na Intenção, validando a H6 (β -0,19; $p < 0,01$). Todas essas interações em conjunto com os resultados obtidos na pesquisa de 2012 são demonstradas na Figura 2:

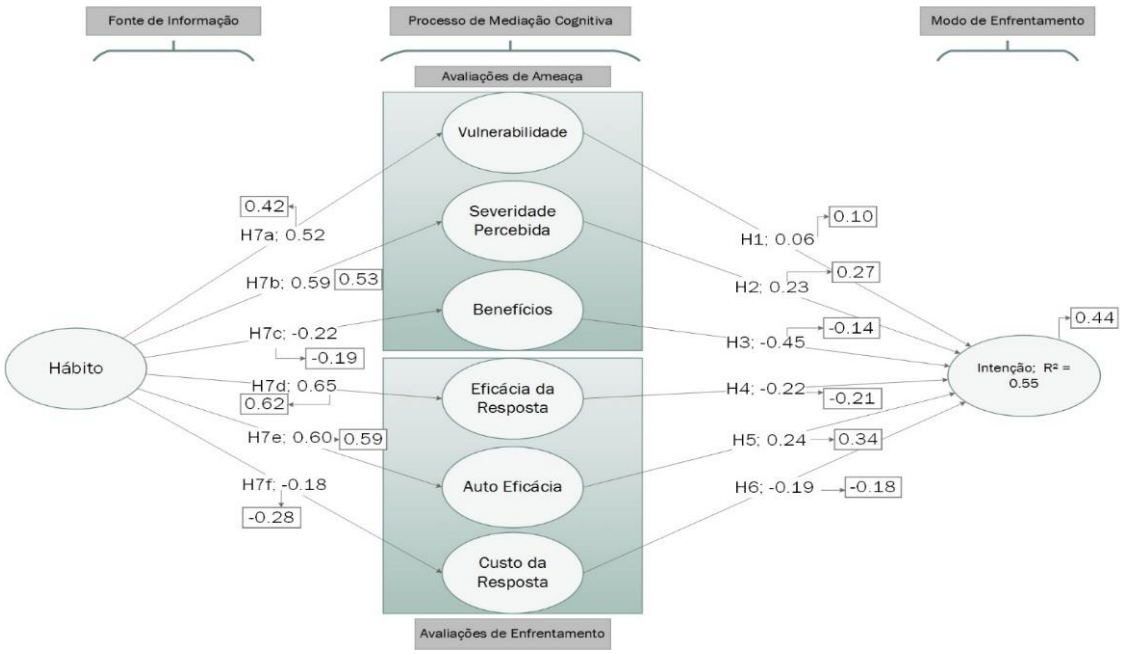

Figura 2: Resultados da correlação entre os constructos e comparação entre os estudos.

5. CONSIDERAÇÕES FINAIS

A validação do modelo proposto por Vance, Siponen e Pahnila (2012) em um novo contexto pode ser considerada satisfatória, sendo os resultados obtidos semelhantes em vários aspectos. Os cenários elaborados foram considerados realistas pelos respondentes, refletindo a importância do método de cenários hipotéticos para o resultado da pesquisa. O questionário foi adaptado de maneira clara ao contexto investigado na pesquisa, com a inclusão de novas questões para os constructos que podem ser utilizadas em futuros estudos para melhor averiguação. As variáveis se comportaram de maneira semelhante, sendo os resultados das

hipóteses os mesmos. Como principais limitações do estudo podem-se colocar a seleção da amostra pelo método bola de neve, sendo necessária a confirmação desses resultados em organizações que possuem as políticas de segurança determinadas claramente, através da formalização. 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 e relações entre empresa e empregado.

Mesmo que as teorias comportamentais não sejam capazes de explicar o comportamento humano em todos os contextos, por conta da complexidade da mente humana, o seu uso em pesquisas da área de Segurança da Informação pode auxiliar os gestores a compreender de alguma maneira, como as expectativas, como a percepção desses indivíduos sobre o ambiente de trabalho, interfere nas suas ações dentro das organizações, e tendo melhor conhecimento disso, os gestores podem criar e coordenar ações que podem ser direcionadas para atenuar comportamentos que possam ser prejudiciais às empresas.

6. REFERÊNCIAS

BARLETTE, Yves; GUNDOLF, Katherine; JAOUEN, Annabelle. Toward a better understanding of SMB CEOs' Information Security Behavior: Insights from Threat or Coping appraisal. **Journal of Intelligence Studies in Business**, v. 5, n. 1, 2015.

BULGURCU, Burcu; CAVUSOGLU, Hasan; BENBASAT, Izak. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. **MIS quarterly**, v. 34, n. 3, p. 523-548, 2010.

DE ALBUQUERQUE JUNIOR, Antonio Eduardo; DOS SANTOS, Ernani Marques. Adoção de medidas de Segurança da Informação: um modelo de análise para institutos de pesquisa públicos. **Revista Brasileira de Administração Científica**, v. 5, n. 2, p. 46-59, 2014.

ERNEST & YOUNG. Pesquisa Global sobre Segurança da Informação 2015. **Ernest e Young**, 2016. Disponível em http://www.ey.com/br/pt/services/giss_2015>. Acesso em 06 de mar. 2017.

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

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, 2009.

IFINEDO, Princely. Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. **Information & Management**, v. 51, n. 1, p. 69-79, 2014.

JOHNSTON, Allen C.; WARKENTIN, Merrill. Fear appeals and information security behaviors: an empirical study. **MIS quarterly**, p. 549-566, 2010.

LOWRY, Paul Benjamin et al. Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organisational information security policies: An empirical study of the influence of counterfactual reasoning and organisational trust. **Information Systems Journal**, v. 25, n. 3, p. 193-273, 2015.

METALIDOU, Efthymia et al. Human factor and information security in higher education. **Journal of Systems and Information Technology**, v. 16, n. 3, p. 210-221, 2014.

MWAGWABI, Florence; MCGILL, Tanya; DIXON, Matthew. Improving compliance with password guidelines: How user perceptions of passwords and security threats affect compliance with guidelines. In: **System Sciences (HICSS), 47th Hawaii International Conference on**. IEEE, 2014. p. 3188-3197, 2014.

NORMAN, Paul; BOER, Henk; SEYDEL, Erwin R. Protection motivation theory. In: M. Conner & P. Norman (Eds.), Predicting Health Behaviour: Research and Practice with Social Cognition Models. **Open University Press**, Maidenhead, p. 81-126, 2005.

ROGERS, Ronald W. A protection motivation theory of fear appeals and attitude change1. **The journal of psychology**, v. 91, n. 1, p. 93-114, 1975.

RODRIGUES, Geórgia Cristiane. BYOD como política de segurança em uma empresa: uma análise à luz da PMT, 2015.

VANCE, Anthony; SIPONEN, Mikko; PAHNILA, Seppo. Motivating IS security compliance: insights from habit and protection motivation theory. **Information & Management**, v. 49, n. 3, p. 190-198, 2012.

ANEXO I - QUESTÕES

Tabela 1: Questões primeira parte

Questões	Observações
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.

Tabela 2: Questões segunda

Constructo	**Abreviação**	**Questões**	**Fonte**
Hábito	Q01-HB	Cumprir com as políticas de segurança da informação é algo que faço automaticamente.	Adaptada de Vance et al (2012)
	Q28-HB	Cumprir com as políticas de segurança da informação é algo que faço sem ter que lembrar conscientemente de fazer.	Adaptada de Vance et al (2012)
	Q10-HB	Cumprir com as políticas de segurança da informação é algo que pertence a minha rotina (diária, semanal, mensal).	Adaptada de Vance et al (2012)
	Q23-HB	Cumprir com as políticas de segurança é algo que eu começo a fazer antes de perceber que estou fazendo.	Adaptada de Vance et al (2012)
Intenção (r)	Q02-IC	Há grandes chances de eu fazer o que [o personagem do cenário] fez no cenário descrito.	Adaptada de Vance et al (2012)
	Q21-IC	Eu agiria da mesma forma como [o personagem do cenário agiu] se eu estivesse na mesma situação.	Adaptada de Vance et al (2012)
	Q14-IC	Eu também não preferiria cumprir com os requisitos da política de segurança da informação da minha organização.	Adaptada de Palvia, Lowry (2013)
	Q31-IC	Eu também não tentaria seguir a política de segurança da organização.	Adaptada de Ifinedo (2014)
Severidade	QO4-SP	Uma quebra de segurança da informação em minha organização seria um problema sério para mim.	Adaptada de Vance et al (2012)
	Q13-SP	Se eu fizesse o que [o personagem do cenário] fez, haveriam sérios problemas de segurança da informação para minha organização.	Adaptada de Vance et al (2012)
	Q03-SP	Se eu fizesse o que [o personagem do cenário] fez, eu enfrentaria sérios problemas.	Adaptada de Vance et al (2012)
	Q33-SP	Eu poderia sofrer severas punições caso eu não cumprisse com as políticas de segurança.	Adaptada de Cheng (2013)
Vulnerabilidade	Q09-VP	Eu poderia ser submetido a uma ameaça de segurança da informação se eu fizesse o que [o personagem do cenário] fez.	Adaptada de Vance et al (2012)
	Q24-VP	Minha organização poderia ser submetida a uma ameaça de segurança da informação se eu fiz o que [o personagem do cenário] fez.	Adaptada de Vance et al (2012)

	Q15-VP	Um problema de segurança da informação pode ocorrer se eu fizer o que [o personagem do cenário] fez.	Adaptada de Vance et al (2012)
	Q22-VP (n)	As informações da minha organização e seu sistemas de informação são vulneráveis a ameaças de segurança.	Adaptada de Sommestad (2014)
Eficácia da resposta	Q16-ER	Cumprir com as políticas de segurança da informação em nossa organização mantem as violações dos sistemas de informação baixas.	Adaptada de Vance et al (2012)
	Q30-ER	Se eu cumprir com as políticas de segurança da informação, as violações aos sistemas de informação serão escassas.	Adaptada de Vance et al (2012)
	Q08-ER	Cumprir cuidadosamente com as políticas de segurança ajuda a evitar problemas de segurança nos sistemas de informação.	Adaptada de Vance et al (2012)
	Q32-ER	Ter políticas de segurança de informações em nos sa organização ajuda a reduzir as brechas para violações de segurança da informação.	Adaptada de Sommestad (2014)
Auto eficácia	Q34-AE	Eu posso cumprir com as políticas de segurança da informação por mim mesmo.	Adaptada de Vance et al (2012)
	Q17-AE	Seria difícil para mim, agir do modo que [o personagem do cenário] fez.	Adaptada de Vance et al (2012)
	Q29-AE	Seria fácil para mim fazer o oposto do que [o personagem do cenário] fez.	Adaptada de Vance et al (2012)
	Q07-AE (n)	Eu seria capaz de seguir a maioria das políticas de segurança mesmo sem ter ninguém por perto para me ajudar	Adaptada de Sommestad (2014)
	Q19-AE (n)	Eu tenho as habilidades necessárias para cumprir com os procedimentos de segurança da informação da minha organização.	Adaptada de Ifinedo (2014)
Realismo Percebido	Q18-RP	O cenário descreve uma possível ação de um funcionário.	Adaptada de Vance et al (2012)
Custo da resposta	Q05-CR	Cumprir com as políticas de segurança atrapalha meu trabalho.	Adaptada de Vance et al (2012)
	Q26-CR	Há muitos inconvenientes com o cumprimento de políticas de segurança da informação.	Adaptada de Vance et al (2012)
	Q11-CR	Cumprir com as políticas de segurança exigiria um investimento considerável de-esforços além de tempo.	Adaptada de Vance et al (2012)
	Q27-CR (n)	É trabalhoso cumprir com o procedimento padrão de segurança para proteger as informações da empresa.	Adaptada de Chou, Chou (2016)
Benefícios	Q06-BN	Se eu fizesse o que [o personagem do cenário] fez, eu pouparia tempo.	Adaptada de Vance et al (2012)
	Q12-BN	Se eu fizesse o que [o personagem do cenário] fez, eu pouparia tempo de trabalho.	Adaptada de Vance et al (2012)
	Q25-BN	Não cumprir com as políticas de segurança da informação economiza tempo de trabalho.	Adaptada de Vance et al (2012)
	Q20-BN	Se eu não cumprir com as políticas de segurança da informação terei mais tempo para outras atividades.	Nova

Notas:
n - não utilizada no modelo
r - questão reversa