

# ***ANÁLISE DA PUNIÇÃO, DETECÇÃO E COMPORTAMENTO DOS PARES COMO INFLUÊNCIAS NA INTENÇÃO DE CUMPRIMENTO DAS POLÍTICAS DE SEGURANÇA CIBERNÉTICA NAS ORGANIZAÇÕES***

Rui Dini <sup>1</sup>, Leonardo Rocha de Oliveira <sup>2</sup>.

1) Programa de Pós-Graduação em Administração (PPGAd)  
Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS),  
Brasil [ruycarlos.dini@gmail.com](mailto:ruycarlos.dini@gmail.com)

2) Programa de Pós-Graduação em Administração (PPGAd)  
Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS), Brasil

[leo.oliveira@pucrs.br](mailto:leo.oliveira@pucrs.br)

## **Resumo**

Segurança cibernética é um desafio de gestão que vem sendo enfrentado pelos mais diversos tipos de empresas do mundo todo. Contramedidas de proteção contra ataques cibernéticos de diversos tipos vem sendo adotadas por empresas, e barreiras como invasão de privacidade e perda de produtividade são questões a serem consideradas na sua adoção. Este trabalho tem o objetivo de analisar influências na intenção de cumprimento de políticas empresariais para segurança cibernética por funcionários em diferentes organizações. A revisão de literatura indica que os principais fatores de influência são (i) severidade da punição, (ii) certeza da detecção e (iii) comportamento de pares. Neste trabalho foi desenvolvida uma pesquisa quantitativa e descritiva para analisar a relação destes três fatores sobre a (iv) intenção de cumprimento das políticas de segurança nas organizações. A pesquisa foi elaborada por meio de survey com questionário de 11 questões para serem respondidas com base em escala Likert de 7 pontos. Os resultados apontam que fatores de (ii) certeza de detecção e (iii) comportamento dos pares são predecessores da (iv) intenção de cumprimento das políticas de segurança.

**Palavras chave:** Segurança Cibernética; Políticas de Segurança Cibernética, Governança de TI, Fatores Humanos em Segurança Cibernética.

## 1. Introdução

O impacto de novos desenvolvimentos tecnológicos é frequente e se reflete mundialmente sobre os mais diversos aspectos organizacionais, tais como processos de negócios, estruturas hierárquicas, desenvolvimento de novos produtos, comunicações e práticas de gestão do conhecimento [Bélanger & Crossler 2011; Liang & Xue 2010]. O valor da informação e dos serviços prestados pelos recursos de tecnologia de informação (TI) tem crescido nas atividades de negócios, acompanhando a evolução tecnológica [Sund 2007]. Esta evolução tem levado a um desafio crescente e internacional para prevenir empresas contra ataques cibernéticos em infraestruturas de TI, capazes de afetar diversos ativos organizacionais que dependem deste recurso [Batteau 2011; Glennon 2012]. Ataques cibernéticos podem ser prejudiciais em diversos aspectos internos e externos de empresas, afetando desde a produtividade de processos, até a imagem global e valor das ações em bolsas de valores [Siponen et al. 2008].

Ameaça cibernética é qualquer indicação, circunstância ou evento com potencial para causar danos em algum tipo de infraestrutura de TI e nos ativos que dependem dessa infraestrutura [Forward 2009]. Leis, regulamentos, políticas e ferramentas para a prevenção de ataques cibernéticos estão constantemente sendo desenvolvidas e aplicadas em todo o mundo [Ye; Farley & Deepak, 2006; Anderson & Agarwal 2010]. Esforços neste sentido devem ser contínuos, pois as formas de ataques cibernéticos também evoluem, acompanhando o desenvolvimento de novas tecnologias [Cetron & Davies 2009], e envolvem aspectos como [Forward 2009]: redes de computadores, virtualização de software e hardware (computação em nuvem), dispositivos de acesso (telefones, tablets, computadores pessoais), restrição de acesso aos serviços de infraestruturas de TI (Denial of Service), fatores humanos, e requisitos de segurança insuficientes. Ameaças cibernéticas também envolvem espionagem industrial e podem ter origem em qualquer país, corporação ou indivíduo, com prejuízos até mesmo em investimentos de longo prazo em pesquisa, desenvolvimento e inovação [Bulgurcu et al. 2010]. Embora a maioria dos danos causados por ataques cibernéticos tenham ocorrido em empresas privadas, aspectos de segurança nacional tampouco podem ser negligenciados [Etzioni 2011]. Por exemplo, o governo Norte Americano já anunciou que está desenvolvendo legislação para assuntos de segurança cibernética (Cybersecurity Act of 2009), o qual deve estabelecer bases para uma estratégia nacional de coibir ataques contra a segurança no uso de recursos de TI [Harknett & Stever 2009].

Apesar da magnitude das ameaças contra a segurança cibernética, a TI é um importante ativo organizacional para fornecer e manter vantagens competitivas, mas para isso precisa ser

utilizado e gerenciado de forma alinhada aos objetivos de negócios das organizações [Weill & Ross 2004]. Atualmente existe uma variedade de novos dispositivos e aplicações de TI tornando-se disponíveis diariamente, exigindo que empresas enfrentem constantes desafios para obter o máximo possível dos benefícios de seus recursos de TI, e evitando danos de ataques cibernéticos [Velani 2007].

Diante das ameaças de ataques cibernéticos, o comportamento da força de trabalho tem papel fundamental para a manutenção de um ambiente seguro. Apesar das organizações manterem esforços para alcançar altos níveis de proteção por meio da implantação de dispositivos técnicos e regulatórios para segurança cibernética, observa-se que é comum encontrar funcionários que não seguem as práticas e procedimentos indicados [Herath & Rao 2009b]. O objetivo destes dispositivos é influenciar e conduzir os funcionários a atuar com ações consideradas adequadas para cada tipo de situação [Herath & Rao, 2009a]. O uso destes dispositivos deve ser regulado e gerenciado de forma diferente em cada organização, seguindo políticas ou regras para o comportamento que podem ser específicas para cada tipo de trabalho e perfil profissional [Herath & Rao 2009a; Vaast 2007]. Contemplar o comportamento dos funcionários relativo ao cumprimento das políticas de segurança é necessidade básica para melhorar a efetividade de práticas e procedimentos de segurança [Herath & Rao 2009b]. Como a intenção dos empregados em seguir as políticas empresariais não é geralmente voluntária, especialmente as de segurança cibernética, mecanismos de detecção e de punição são utilizados como forma de reforçar a importância do cumprimento das políticas e garantir um ambiente de TI seguro [Herath & Rao 2009a].

Este artigo tem como objetivo analisar as influências na intenção de cumprimento de políticas organizacionais para segurança cibernética. Para isso foi revisada a literatura e identificados três fatores que representam essa influência, que são: (i) de severidade da punição, (ii) certeza da detecção, (iii) comportamento dos pares e, (iv) Intenção de Cumprimento das Políticas de Segurança. Mais detalhes sobre o trabalho estão presentes nos itens a seguir, sendo que a introdução situa o assunto abordado no trabalho no contexto das organizações. No segundo item é apresentada a fundamentação teórica, abrangendo temas como segurança cibernética e suas influências na intenção de cumprimento das políticas de segurança das organizações. O terceiro item apresenta o método utilizado para desenvolver a etapa da pesquisa e justificar as atividades adotadas no desenvolvimento do trabalho. O item quatro apresenta os resultados da pesquisa com discussão sobre os motivos das relações apontadas para as variáveis e fatores de análise quanto ao contexto das organizações. Ao final são apresentadas as considerações finais, juntamente com as limitações e sugestões para futuros trabalhos.

## **2. Segurança Cibernética**

Com um histórico recente que combina com a evolução no uso da TI, a segurança cibernética é uma área de conhecimento que afeta tanto organizações quanto pessoas. A informação é considerada um ativo para as organizações e algo de muito valor para as pessoas, e por isso necessita de proteção contra os mais diversos tipos de ameaças [Bulgurcu et al. 2010]. No mundo empresarial, informações compartilhadas e/ou armazenadas em meios eletrônicos estão expostas a inúmeros fatores que, mesmo sem intenção, oferecem risco de serem violadas. Podem ser exploradas as vulnerabilidades dos dados, informações e sistemas em uma organização, de forma que seus ativos de negócios fiquem expostos a ameaças de terceiros. Entre os alvos dessas ameaças estão o hardware, o software, os dados e as comunicações no ambiente interno e com o externo das empresas [Harknett & Stever 2009]. A diversidade de alvos que podem ser atacados contribui para a importância de práticas e procedimentos de segurança cibernética [Wilson et al. 1992].

Segurança cibernética diz respeito à proteção dos ativos da informação contra exposição não-autorizada, seja ocasional ou mal-intencionada, causando modificação, destruição ou indisponibilidade [Ward & Smith 2002]. Do ponto de vista organizacional, se pode dizer que segurança cibernética é a proteção de recursos de TI contra as mais variadas ameaças, buscando garantir a manutenção da competitividade, diminuir riscos de operação, maximizar o retorno sobre os investimentos ou proporcionar oportunidades de negócio [ABNT 2005]. A Segurança cibernética possui três atributos fundamentais quando relacionados à proteção dos ativos de informação, que são [ABNT 2001]:

- **Confidencialidade:** garantia de que o acesso à informação seja feito somente por pessoal autorizado, assim como em relação ao grau de sigilo do conteúdo;
- **Integridade:** certeza de que a informação está correta e não foi alterada, seja de forma accidental ou intencional, bem como no seu processamento;
- **Disponibilidade:** garantia de que o pessoal autorizado tenha acesso à informação e aos recursos associados no momento em que se torna necessária.

Outros dois atributos de segurança cibernética também foram identificados na revisão de literatura e podem ser considerados como determinantes para a proteção das trocas de dados e informações, que são [Sêmola 2003]:

- **Legalidade:** garantia de que a informação está de acordo com as leis;

- Autenticidade: garantia da identidade dos elementos envolvidos em um determinado processo de comunicação eletrônica, garantindo a identidade de quem gerou, enviou e recebeu a informação transmitida.

Para garantir que a segurança cibernética não seja violada é necessário que as empresas possuam regras claras indicando sobre o comportamento das pessoas envolvidas nos processos de trocas de dados e informações. Segurança cibernética deve seguir um processo com adoção de diferentes tipos de dispositivos e controles, incluindo políticas, entendimento da legislação, procedimentos operacionais, estruturas organizacionais e requisitos para adoção de sistemas e equipamentos de TI [ABNT 2005]. Segurança cibernética está relacionada ao comportamento das pessoas perante as regras das empresas e da sociedade. Mais detalhes sobre formas para garantir o cumprimento e penalizar sobre violações são apresentadas nos itens a seguir.

### **3. Intenção de Cumprimento das Políticas de Segurança da Informação**

A revisão de literatura indica a existência de diversos dispositivos técnicos e regulatórios para garantir a segurança cibernética das organizações. Exemplos de dispositivos tecnológicos são firewall, antivírus, leitoras de cartões, leitores biométricos e senhas, cuja utilização permite acesso a ativos organizacionais. Dispositivos regulatórios são leis, regras, regulamentos e manuais de procedimentos, os quais estão ligados a direcionar o comportamento dos funcionários, dentro e fora do ambiente de trabalho [Kankanhalli et al. 2003]. Apesar da quantidade de dispositivos de segurança, a relação destes com o papel das pessoas envolvidas no cumprimento das regras e políticas organizacionais para segurança cibernética é pouco abordada na literatura [Pahnila et al. 2004; Herath & Rao 2009a]. Essa relação é necessária, pois somente a formalização de uma política de segurança cibernética não garante que usuários e funcionários venham a cumprir com as práticas e procedimentos nela indicados [Herath & Rao 2009a].

A revisão de literatura permitiu identificar alguns fatores que podem influenciar na intenção de cumprimento das políticas de segurança cibernética por parte das pessoas envolvidas nas organizações. Por exemplo, a confiança é um fator que está envolvido na intenção de cumprimento das políticas de segurança informacionais das organizações [Trcek et al. 2007]. O conceito de confiança tem sido utilizado em relações econômicas e sociais onde a incerteza, a delegação de autoridade e o medo do oportunismo são presenças constantes [Cho 2006; Trcek et al. 2007]. Com origem em estudos da sociologia, a confiança em segurança cibernética demonstra o sentimento dos colaboradores em relação às crenças de que as políticas

organizacionais são capazes de influenciar na forma de comportamento em relação às atividades de trabalho nas organizações [Cho 2006].

Conhecimento e conscientização dos colaboradores quanto a necessidades em seguir regras e aceitar punições é também um fator que apresenta impacto sobre os resultados da aplicação de políticas e práticas de segurança cibernética [Goodhue & Straub 1991; Leonard et al. 2004; Lacey 2009]. Este fator está relacionado com a familiaridade e conscientização sobre a necessidade de mudanças de atitudes das pessoas, proporcionando um ambiente de trabalho capaz de motivar e tornar as pessoas mais receptivas a treinamentos e práticas de gestão de segurança [Chan et al. 2005; Albertin & Pinochet 2010].

Para analisar a efetividade da conscientização em adotar as práticas de segurança cibernética é necessário o entendimento por parte das pessoas sobre os danos e punições associadas aos resultados pessoais e organizacionais [Shaw et al. 2009; Lacey 2009]. Portanto, o resultado do comportamento dos funcionários em relação à segurança cibernética impacta no comportamento em relação a adoção de dispositivos de segurança (Vance et al. 2012). Ou seja, pessoas informadas e conscientes sobre os possíveis danos causados por ameaças cibernéticas e sobre a real possibilidade de sua ocorrência se tornam mais suscetíveis a se submeter às alterações causadas por dispositivos de segurança no ambiente de trabalho [Pahnila et al. 2007; Ng et al. 2009]. Conforme Kruger e Kearney [2006], a conscientização cria e mantém um comportamento positivo do funcionário, fazendo com que ele perceba a relevância do assunto em questão, facilitando a adoção de práticas de gestão de segurança cibernética.

Pressões sociais também representam um fator de influência na adoção de práticas de segurança cibernética [Lacey 2009]. Este fator considera aspectos que motivam o comportamento de um indivíduo pela possibilidade de ganhar aprovação de demais indivíduos influentes no ambiente. Também conhecido como comportamento entre pares, este fator está relacionado ao comportamento de um indivíduo inserido dentro de um grupo, onde o grupo exerce pressões sociais, de modo que o indivíduo siga o mesmo comportamento [Vaast 2007]. A lealdade dos profissionais com a organização em que trabalha também é apontada como influência no comportamento entre pares, que no caso de segurança cibernética contempla aspectos como experiência profissional com TI, nível de escolaridade e posição na hierarquia funcional como aspectos que impactam no comportamento das pessoas nas organizações [Albrechtsen & Hovden 2009].

Outro fator identificado na literatura com influência no comportamento perante práticas de segurança cibernética se refere ao uso de penalidades e pressões em caso de descumprimento

nas organizações [Lee et al. 2004; Herath & Rao 2009a]. As penalidades envolvem aspectos referentes ao grau de severidade e também quanto ao grau de certeza de que o colaborador será detectado em caso de descumprimento [D'arcy et al. 2008; Herath & Rao 2009a].

A revisão de literatura também apresenta uma série de escalas para avaliação de aspectos humanos e comportamentais em relação a práticas de segurança cibernética [Leonard et al. 2004; Chan et al. 2005; Cho 2006; Trcek et al. 2007; Pahnla et al. 2007; Ng et al. 2009; Lacey 2009]. Para este artigo foi adotada a escala sugerida por Herath e Rao [2009a], a qual considera quatro fatores, que são: (i) severidade da punição, (ii) certeza da detecção, (iii) comportamento entre pares e, (iv) intenção de cumprimento das políticas de segurança. As variáveis mensuráveis que representam cada fator e detalhes sobre a construção do questionário estão descritas no item a seguir. No Apêndice A está a versão final do questionário usado para entrevistas.

#### **4. Método**

Este trabalho foi desenvolvido como uma pesquisa quantitativa e confirmatória, com a utilização de questionários distribuídos como survey eletrônica para resposta por profissionais que atuam em empresas do parque de tecnologia da PUCRS (Tecnopucrs). O questionário foi adaptado de Herath e Rao [2009a] e traduzido para o português e adaptado de forma a representar a realidade brasileira. A validação da tradução e capacidade do instrumento em representar o objetivo do estudo foi realizada com entrevistas em profundidades com três especialistas da área de segurança cibernética. Nestas entrevistas foi buscada a convergência das opiniões, sendo que os resultados da primeira entrevista foram considerados para a segunda e assim respectivamente. Após a validação com especialistas, o instrumento foi validado com um grupo de 12 profissionais que representam o público alvo das entrevistas. Nesta validação foi revisado o tempo de aplicação, entendimento das questões e do objetivo geral de avaliação. Todas as questões do instrumento foram respondidas com base em escala Likert de sete pontos e a versão final encontra-se no Apêndice A do trabalho.

Nesta primeira etapa foram entrevistados profissionais que trabalham em empresas de tecnologia, mas com diferentes perfis de formação, cargo e tempo de serviço. Neste primeiro momento o intuito foi de contemplar o maior número de respondentes. No total foram respondidos 53 questionários, porém apenas 41 foram validados após a sanitização da amostra. A aplicação do questionário foi feita com distribuição do material em formato impresso para posterior coleta na recepção do parque tecnológico.



Propondo verificar as relações entre os fatores de (i) severidade da punição, (ii) certeza da detecção e (iii) comportamento dos pares, com a intenção de cumprimento das políticas de segurança cibernética por parte dos colaboradores, análises estatísticas descritivas e de correlação foram desenvolvidas. Todas as análises estatísticas foram realizadas com o uso do SPSS (versão 11) e os resultados preliminares realizados com base na geração de gráficos de histograma com distribuição normal indicaram que os dados coletados na pesquisa foram considerados paramétricos [Hair Jr. et al. 2005]. Mais detalhes sobre os resultados das análises quantitativas estão apresentados no item a seguir.

## 5. Resultados

A versão final do instrumento de pesquisa encontra-se no Apêndice A deste trabalho e apresenta 11 questões distribuídas em 4 fatores, seguidas de questões sobre o perfil do respondente e da empresa para a qual trabalha. As análises do perfil dos respondentes foram realizadas sobre o total de 41 respostas válidas e a média de tempo de experiência profissional foi de 13,92 anos e a de atuação na empresa atual foi de 7,36 anos. As Figuras 1a e 1b descrevem o ramo de atuação da empresa e cargo dos entrevistados.

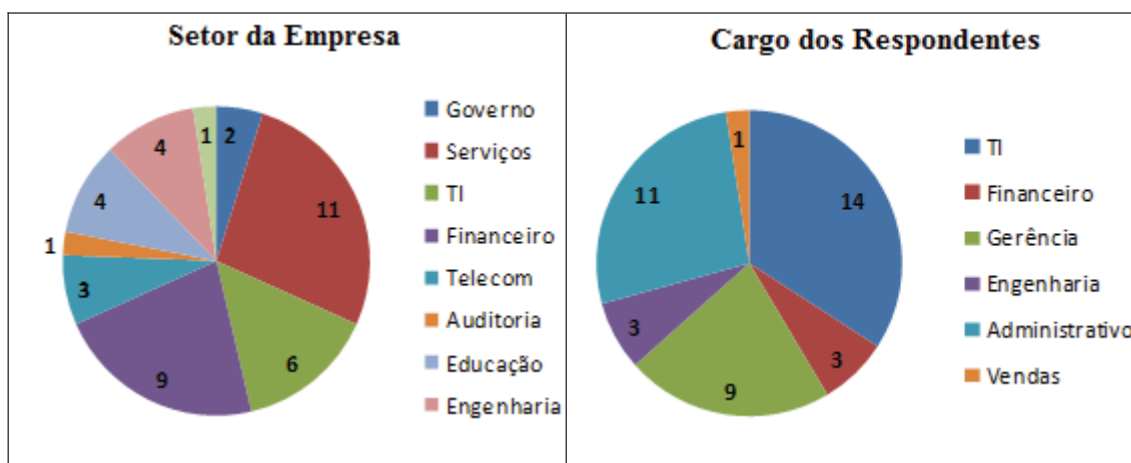


Figura 1a: Setor de atuação da empresa

Figura 1b: Cargo dos respondentes

A análise descritiva das 11 questões do instrumento está presente na Tabela 1 e contém resultados sobre a média, mediana, moda, desvio padrão, valor mínimo e máximo de cada uma das questões. Estes resultados indicam sobre as variáveis que obtiveram maior e menor média na avaliação geral e dentro de cada fator de análise. Na dimensão (i) severidade da punição, a maior média foi do item Q1 (A organização pune quem quebra regras de segurança cibernética) e a menor foi do item Q3 (Se eu fosse pego violando políticas de segurança cibernética, eu seria severamente punido). Para o fator (ii) certeza da detecção, a maior média foi de Q4 (O uso de recursos de TI é monitorado pela empresa para identificar violações de políticas). No (iii) comportamento dos pares, a Q8 (Acredito que os outros concordam que as políticas ajudam a proteger a empresa contra violações de segurança cibernética) obteve a maior média e Q7 (Estou certo de que os outros concordam com as políticas de segurança da empresa), a pior. Em relação à (iv) intenção de cumprimento das políticas de segurança, a maior média foi do item



Q11 (Acredito que as políticas de segurança da empresa são úteis para proteger a organização) e a menor foi de Q9 (Estou propenso a seguir as políticas de segurança da empresa).

	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11
Média	5,05	4,32	4,10	5,61	4,63	4,37	4,29	4,66	5,41	5,44	6,10
Mediana	5,00	4,00	4,00	6,00	5,00	5,00	5,00	5,00	6,00	6,00	7,00
Moda	6,00	7,00	4,00	6,00	5,00	5,00	5,00	6,00	6,00	6,00	7,00
Desvio Padrão	1,75	2,10	1,87	1,36	1,53	1,46	1,40	1,80	1,20	1,21	1,34
Mínimo	1,00	1,00	1,00	2,00	1,00	1,00	1,00	1,00	2,00	2,00	2,00
Máximo	7,00	7,00	7,00	7,00	7,00	7,00	7,00	7,00	7,00	7,00	7,00

Tabela 1: Análise descritiva das variáveis

As relações entre dos fatores (i) severidade da punição, (ii) certeza da detecção e (iii) comportamento dos pares com a (iv) intenção comportamental de cumprir com as políticas de segurança cibernética foram realizadas com base nas análises de correlação de Pearson. Os resultados das análises estão indicados nas Tabelas 3, 4 e 5. Cabe destacar que as correlações podem ser positivas e negativas. Uma correlação positiva significa que, quando um fator X varia em um sentido, o fator Y varia no mesmo sentido, ou seja, com o aumento de X ocorre o aumento de Y. Correlação negativa significa quando um fator X varia em tal sentido, um fator Y varia no sentido contrário. Por exemplo, com o aumento de X ocorre a diminuição de Y [Hair Jr. et al. 2005).

A interpretação dos resultados da Tabela 2 está apresentada a seguir e considera apenas as correlações significantes ao nível de 0,01:

Q1 x Q2: Correlação positiva com associação alta, ou seja, os dois itens podem fazer parte do mesmo fator (i) severidade da punição e podem ter seus resultados como precedentes da (iv) intenção de cumprimento das políticas de segurança;

Q1 x Q3: Correlação positiva com associação moderada, ou seja, os dois itens podem fazer parte do mesmo fator (i) severidade da punição e podem ser precedentes da (iv) intenção de cumprimento das políticas de segurança;

Q1 x Q9: Correlação positiva com associação moderada, ou seja, organizações que punem empregados que quebram regras de segurança cibernética possuem a propensão de que seus funcionários atendam as diretrizes previstas nas políticas de segurança;

		Q1	Q2	Q3	Q9	Q10	Q11
Q1	Correlação	1	,765 <sup>***</sup>	,581 <sup>***</sup>	,418 <sup>***</sup>	,382 <sup>***</sup>	,319 <sup>***</sup>
	Significância		,000	,000	,006	,014	,042
Q2	Correlação	,765 <sup>***</sup>	1	,488 <sup>***</sup>	,204 <sup>***</sup>	,171 <sup>***</sup>	,344 <sup>***</sup>
	Significância	,000		,001	,202	,286	,028
Q3	Correlação	,581 <sup>***</sup>	,488 <sup>***</sup>	1	,404 <sup>***</sup>	,391 <sup>***</sup>	,196 <sup>***</sup>
	Significância	,000	,001		,009	,011	,219
Q9	Correlação	,418 <sup>***</sup>	,204 <sup>***</sup>	,404 <sup>***</sup>	1	,957 <sup>***</sup>	,518 <sup>***</sup>
	Significância	,006	,202	,009		,000	,001
Q10	Correlação	,382 <sup>***</sup>	,171 <sup>***</sup>	,391 <sup>***</sup>	,957 <sup>***</sup>	1	,593 <sup>***</sup>
	Significância	,014	,286	,011	,000		,000
Q11	Correlação	,319 <sup>***</sup>	,344 <sup>***</sup>	,196 <sup>***</sup>	,518 <sup>***</sup>	,593 <sup>***</sup>	1
	Significância	,042	,028	,219	,001	,000	

Tabela 2: Correlação entre os fatores (i) e (iv)

\*\*. Correlação é significativa no nível de 0.01.

\*. Correlação é significativa no nível de 0.05.

Q2 x Q3: Correlação positiva com associação moderada, ou seja, os dois itens podem pertencer ao mesmo fator (i) e podem ser precedentes da (iv) intenção de cumprimento das políticas de segurança;

Q3 x Q9: Correlação positiva com associação pequena, isto é, se eu for pego violando as políticas de segurança e souber que vou ser severamente punido, estou mais propenso a seguir as políticas de segurança da empresa;

Q9 x Q10: Correlação positiva com associação muito forte, ou seja, os dois itens podem ser relacionados em conjunto num mesmo fator (i) e podem ser sucessores do fator (iv);

Q9 x Q11: Correlação positiva com associação moderada, ou seja, os dois itens podem ser relacionados em conjunto no fator (i) e podem ser sucessores do fator (iv);

Q10 x Q11: Correlação positiva com associação moderada, ou seja, os dois itens podem ser relacionados em conjunto no fator (i) e sucessores do fator (iv).

A Tabela 3 apresenta os resultados das correlações para os fatores (ii) certeza da detecção e (iv) intenção de cumprimento das políticas de segurança, considerando apenas com nível de significância de 0,01.

		Q4	Q5	Q9	Q10	Q11
Q4	Correlação	1	,483 <sup>***</sup>	,331 <sup>**</sup>	,352 <sup>**</sup>	,352 <sup>**</sup>
	Significância		,001	,035	,024	,024
Q5	Correlação	,483 <sup>***</sup>	1	,655 <sup>***</sup>	,632 <sup>***</sup>	,275 <sup>*</sup>
	Significância	,001		,000	,000	,082
Q9	Correlação	,331 <sup>**</sup>	,655 <sup>***</sup>	1	,957 <sup>***</sup>	,518 <sup>***</sup>
	Significância	,035	,000		,000	,001
Q10	Correlação	,352 <sup>**</sup>	,632 <sup>***</sup>	,957 <sup>***</sup>	1	,593 <sup>***</sup>
	Significância	,024	,000	,000		,000
Q11	Correlação	,352 <sup>**</sup>	,275 <sup>*</sup>	,518 <sup>***</sup>	,593 <sup>***</sup>	1
	Significância	,024	,082	,001	,000	

Tabela 3: Análise de correlação entre os fatores (ii) e (iv)

\*\*. Correlação é significativa no nível de 0.01.

\*. Correlação é significativa no nível de 0.05.

Q4 x Q5: Correlação positiva com associação moderada, ou seja, os dois itens podem ser relacionados no mesmo fator (ii) certeza da detecção e podem ser precedentes da (iv) intenção de cumprimento das políticas de segurança;

Q5 x Q9: Correlação positiva com associação moderada, isto é, se eu violar as políticas de segurança e provavelmente ser pego, estarei mais propenso a seguir as políticas de segurança cibernética;

Q5 x Q10: Correlação positiva com associação moderada, ou seja, se eu violar as políticas de segurança e possivelmente ser pego, certamente seguirei as políticas de segurança.

A Tabela 4 apresenta os resultados das correlações para os fatores (iii) comportamento dos pares e (iv) intenção de cumprimento das políticas de segurança, considerando apenas relações com nível de significância de 0,01:

Q6 x Q7: Correlação positiva com associação muito forte, ou seja, os dois itens podem fazer parte do mesmo fator (iii) comportamento dos pares e podem ser precedentes da (iv) intenção de cumprimento das políticas de segurança;

Q6 x Q8: Correlação positiva com associação alta, isto é, os dois itens podem fazer parte do mesmo fator (iii) e podem ser precedentes do fator (iv);

Q7 x Q8: Correlação positiva com associação alta, ou seja, os dois itens podem fazer parte de uma mesma dimensão (Comportamento dos Pares) e podem ser precedentes da Intenção de Cumprimento das Políticas de Segurança;

		Q6	Q7	Q8	Q9	Q10	Q11
Q6	Correlação	1	,923 <sup>**</sup>	,819 <sup>**</sup>	,380 <sup>*</sup>	,389 <sup>*</sup>	,275
	Significância		,000	,000	,014	,012	,082
Q7	Correlação	,923 <sup>**</sup>	1	,845 <sup>**</sup>	,401 <sup>**</sup>	,381 <sup>*</sup>	,305
	Significância	,000		,000	,009	,014	,053
Q8	Correlação	,819 <sup>**</sup>	,845 <sup>**</sup>	1	,483 <sup>**</sup>	,498 <sup>**</sup>	,274
	Significância	,000	,000		,001	,001	,083
Q9	Correlação	,380 <sup>*</sup>	,401 <sup>**</sup>	,483 <sup>**</sup>	1	,957 <sup>**</sup>	,518 <sup>**</sup>
	Significância	,014	,009	,001		,000	,001
Q10	Correlação	,389 <sup>*</sup>	,381 <sup>*</sup>	,498 <sup>**</sup>	,957 <sup>**</sup>	1	,593 <sup>**</sup>
	Significância	,012	,014	,001	,000		,000
Q11	Correlação	,275	,305	,274	,518 <sup>**</sup>	,593 <sup>**</sup>	1
	Significância	,082	,053	,083	,001	,000	

Tabela 4: Análise de correlação entre os fatores (iii) e (iv)

\*\* . Correlação é significativa no nível de 0.01.

\* . Correlação é significativa no nível de 0.05.

Q7 x Q9: Correlação positiva com associação pequena, indicando que estar certo de que os outros funcionários concordem com as políticas de segurança da empresa faz com que eu seja mais propenso a seguir as políticas de segurança;

Q8 x Q9: Correlação positiva com associação moderada, indicando que acreditar que os demais funcionários concordam que as políticas ajudam a proteger a empresa contra violações de segurança aumenta também a propensão de seguir as políticas de segurança;

Q8 x Q10: Correlação positiva com associação moderada, indicando que acreditar que os demais funcionários concordam que as políticas ajudam a proteger a empresa contra violações de segurança faz com que eu tenha mais certeza de que seguirei as políticas de segurança organizacional.

A análise geral de todas as correlações significativas destaca algumas relações importantes, as quais estão marcadas em negrito no texto acima. Dois itens do fator (i) Severidade da Punição (Q1 e Q3), um do (ii) certeza da detecção (Q5) e dois do (iii) comportamento dos pares (Q7 e Q8) tiveram relação mais forte especificamente com um dos itens (Q9) do fator (iv) intenção de cumprimento das políticas de segurança cibernética (Q9). Da mesma forma, somente os itens Q5 do fator (ii) e Q8 do fator (iii) indicaram provável relação com o item Q10 do fator (iv). Nenhum dos itens indicaram relação com o item Q11 do fator (iv).

Das correlações em destaque, somente o item Q5 (Se eu violasse as políticas de segurança, eu provavelmente seria pego) do fator (iv) e o item Q8 (Acredito que os demais empregados

concordam que as políticas ajudam a proteger a empresa contra violações de segurança) do fator (iii) foram correlacionados com dois itens do fator (iv), que são (Q9) Propensão de seguir as políticas e (Q10) Certeza de que seguirá as políticas. Isto mostra a relevância destas duas questões (Q5 e Q8) com a intenção de cumprir com as políticas de Segurança da Informação e abre caminho para novas pesquisas sobre o assunto.

## **6. Considerações Finais**

O trabalho analisa a influência de fatores como (i) severidade da punição, (ii) certeza da detecção e (iii) comportamento dos pares em relação à (iv) intenção comportamental dos funcionários de cumprir com as políticas de Segurança Cibernética nas organizações. Utilizando a escala desenvolvida por Herath e Rao (2009b) a pesquisa buscou identificar essas relações em empresas de tecnologia do parque universitário da PUCRS. Portanto, a escala e as análises de correlação usadas no trabalho contribuem para o entendimento sobre a aplicação de políticas de segurança cibernética nas organizações. Ainda, os resultados das empresas do Tecnopuc podem ser replicados para as mais diversas empresas e setores do mercado.

Os resultados das respostas confirmam alguns aspectos indicados na revisão de literatura, tal como dos funcionários tenderem a não levar a sério as políticas de segurança cibernética. A literatura também indica que a melhor forma para garantir a segurança é com o uso de dispositivos regulatórios acompanhados de conscientização e treinamento para os funcionários. Estes aspectos confirmam as principais descobertas deste estudo e mostra que a (ii) certeza da detecção e o (iii) comportamento dos pares são fatores com influência para garantir a intenção em aderir às políticas de segurança por parte dos empregados.

Como limitações do trabalho, ressalta-se que as análises estatísticas utilizadas, apesar de indicadas como adequadas para este tipo de estudo, podem ser melhoradas com uso de modelagem de equações estruturais, mas para isso seria necessário um volume de respostas bastante superior. Portanto, como pesquisas futuras, sugere-se o estudo específico da relação entre (ii) certeza da detecção e o (iii) comportamento dos pares com a (iv) intenção de cumprimento das políticas de segurança cibernética, bem como a utilização de técnicas de modelagem de equações estruturais na pesquisa para identificar o impacto de cada um dos itens sobre o fator (iv).

## 7. Referências

ABNT. NBR ISO/IEC 17799: Tecnologia da informação - Código de prática para a gestão de segurança da informação. Rio de Janeiro, 2001.

ABNT. NBR ISO/IEC 27002: Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão de segurança da informação. Rio de Janeiro, 2005.

Albertin, A. L.; Pinochet, L. H. C., *Política de segurança de informações: Uma visão organizacional para a sua formulação*, Elsevier, São Paulo, 2010.

Albrechtsen, E.; Hovden, J., *The information security digital divide between information security managers and users*, *Computers & Management*, 28 (2009), 476-490.

Anderson, A. L.; Agarwal, R. "Practicing safe computing: a multimethod empirical examination of home computer user security behavioral intentions." *MIS Quarterly, Special Issue*, 34, 3 (2010), 613-643.

Batteau, A. W., "Creating a culture of enterprise cybersecurity", *International Journal of Business Anthropology*, 2, 2 (2001).

Bélanger, F.; Crossler, R. E., "Privacy in the digital age: a review of information privacy research in information systems", *MIS Quarterly*, 35 (2011), 1017-1041.

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

Cetron, M.; Davies, O. Ten critical trends for cybersecurity. World Future Society, USA, Bethesda, Sep/Oct. Pp. 40 – 49, 2009.

Chan, M., Woon, I., Kankanhalli, A., "Perceptions of information security at the Workplace: Linking information security Climate to Compliant Behavior", *Journal of Information Privacy and Security*, 1, 3 (2005), 18-41.

Cho, V., "A study of the roles of trusts and risks in information-oriented online legal services

D'arcy, J.; Hovav, A.; Galletta, D., "User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach", *Information Systems Research, Articles in Advance*, 2008, 1-20.

Etzioni, A., *Cybersecurity in the private sector. Issues in Science and Technology*, <http://www.issues.org/28.1/etzioni.html>, (Maio de 2013), 2011.

Forward. *Managing emerging threats in ICT Infrastructures*. Seventh Framework Program. White book: Emerging ICT threats. <http://www.ict-forward.eu/media/publications/forward-d2.1.x.pdf>, (Maio de 2013), 2009.

Glennon, M. J., “State-level cyber security,” *Policy Review*, Feb/Mar., 171 (2012), 85 – 102.

Goodhue, D. L.; Straub, D. W., “Security concerns of system users: A study of perceptions of the adequacy of security”, *Information & Management*, 20, 1 (1991), 13-27.

Hair JR., J. F.; Babin, B.; Money, A. H.; Samouel, P., *Fundamentos de métodos de pesquisa em administração*, Bookman, Porto Alegre, 2005.

Harknett, R.; Stever, J., “The New Policy World of Cybersecurity”, *Public Administration Review*, N. Roberts, Ed., 2011, 455-460.

Herath, T.; Rao, H. R., “Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness”, *Decision Support Systems*, 47 (2009), 154-165.

Herath, T.; Rao, H. R., “Protection motivation and deterrence: A framework for security policy compliance in organizations”, *European Journal of Information Systems*, 18 (2009b), 106-125.

Kankanhalli, A., Teo, H. H., Tan B.C.Y; Wei, K.K., “An Integrative Study of Information Systems Security Effectiveness”, *International Journal of Information Management*, 23, 2 (2003), 139-154.

Kruger, H. A.; Kearney, W. D., “A prototype for assessing information security awareness”, *Computers & Security*, 25, 4 (2006), 289-296.

Lacey, D. *Managing the human factor in information security: How to win over staff and influence business managers*. West Sussex: John Wiley and Sons, 2009.

Lee, S. M.; Lee, S.; Yoo, S., “An integrative model of computer abuse based on social control and general deterrence theories”, *Information & Management*, 41 (2004), 707-718.

Leonard, L. N. K.; Cronan, T. P.; Kreie, J., “What influences IT ethical behavior intentions: planned behavior, reasoned action, perceived importance, or individual characteristics?”, *Information & Management*, 42 (2004), 143–158.

Liang, H.; Xue, Y., “Avoidance of Information Technology Threats: A Theoretical Perspective”, *MIS Quarterly*, 33, 1 (2009), 71-90.



- Ng, B.; Kankanhalli A.; Xu Y., “Studying users' computer security behavior: A health belief perspective”, *Decision Support Systems*, 46, 4 (2009), 815-825.
- Pahnila, S.; Siponen, M.; Mahmood, A., *Which Factors Explain Employees' Adherence to Information Security Policies? An Empirical Study*. Proceedings of the Eleventh Pacific Asia Conference on Information Systems, July 4-6, Auckland, New Zeland, 2007.
- Pahnila, S.; Siponen, M.; Mahmood, A., *Which factors explain employees' adherence to information security policies? An empirical stud*, Proceedings of the Eleventh Pacific Asia Conference on Information Systems, Auckland, New Zealand, 2007.
- Sêmola, M., *Gestão da segurança da informação: Uma visão executiva*, Elsevier, Rio de Janeiro, 2003.
- Shaw, R. S.; Chen, C. C.; Harris, A. L.; Huang, H., “The impact of information richness on information security awareness training effectiveness”, *Computers & Education*, 52 (2009), 92-100.
- Siponen, M., “A conceptual foundation for organizational information security awareness”, *Information Management & Computer Security*, 8, 1 (2000), 31-41.
- Siponen, M.; Willison, R.; Baskerville, R., *Power and practice in information systems security research*. In: Proceedings of the Twenty Ninth International Conference on Information Systems, Paris, 2008.
- Sund, C., “Towards an international road-map for cybersecurity”, *Online Information Review*, Emerald Group Publishing Limited, 31, 5 (2007), 566-582.
- Trcek, D.; Trobec, R.; Pavesic, N.; Tasic, J. F., “Information systems security and human behavior”, *Behavior & Information Technology*, 26, 2 (2007), 113–118.
- Vaast, E., “Danger is in the eye of the beholders: Social representations of information systems security in healthcare”, *Journal of Strategic Information Systems*, 16 (2007), 130-152.
- Vance, A.; Siponen, M.; Pahnila, S., “Motivating IS security compliance: Insights from habit and protection motivation theory”, *Information & Management*, 49 (2012), 190-198.
- Velani, K. H., *Strategic Security Management: A Risk Assessment Guide for Decision Makers*, Elsevier, 2007.
- Ward, P.; Smith, C. L., “The development of access control policies for information technology systems”, *Computers & Security*, 21, 4 (2002), 356-371.

Weill, P.; Ross, J. W. IT Governance: how top performers manage IT decision rights for superior results”, Harvard Business School Press, Massachusetts, 2004.

Wilson, J. L.; Turban, E.; Zviran, M., “Information systems security: A managerial perspective”, *International Journal of Information Management*, 12 (1992), 105-119.

Ye, N.; Farley, T.; Deepak, L. An attack-norm separation approach for detecting cyber attacks, *Information Systems Frontiers*, 8, 3, (2006), 163-177.

## Apêndice A - Instrumento de Pesquisa



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



**Prezado(a) Senhor(a),**

Esta é uma pesquisa sobre Segurança da Informação e todas as respostas, nome dos respondentes e empresas envolvidas são confidenciais e não serão divulgadas.

Agradecemos a sua participação.

1 - Discordo Totalmente

7 - Concordo Totalmente

Dimensões	Questões	1	2	3	4	5	6	7
Severidade da Punição	<b>Q1</b> - A organização pune empregados que quebram regras de Segurança da Informação							
	<b>Q2</b> - Minha organização demite empregados que repetidamente quebram regras de Segurança da Informação							
	<b>Q3</b> - Se eu fosse pego violando as políticas de Segurança da Informação, eu seria severamente punido							
Certeza da Detecção	<b>Q4</b> - O uso de recursos de TI é monitorado pela empresa para identificar violações de políticas da organização							
	<b>Q5</b> - Se eu violasse as políticas de segurança da organização, eu provavelmente seria pego							
Comportamento dos Pares	<b>Q6</b> - Eu acredito que os demais empregados concordam com as políticas de segurança para o uso de TI da organização							
	<b>Q7</b> - Eu estou certo de que os demais empregados concordam com as políticas de segurança de TI da organização							
	<b>Q8</b> - Acredito que os demais empregados concordam que as políticas ajudam a proteger a empresa contra violações de segurança nos recursos de TI							
Intenção de Cumprimento das Políticas de Segurança	<b>Q9</b> - Eu estou propenso a seguir as políticas de segurança de TI da empresa							
	<b>Q10</b> - Estou certo de que seguirei as políticas de segurança organizacional							
	<b>Q11</b> - Acredito que as políticas da empresa para segurança de TI são úteis para proteger a organização							

**As questões a seguir devem identificar o perfil do respondente:**

Qual o setor de atuação de sua empresa?

Qual o seu tempo total de experiência profissional?

Qual o seu tempo de atuação na empresa?

Qual a sua área de atuação na empresa?

Agradeceríamos também se pudesse oferecer comentários ou sugestões sobre o questionário.