Revista de Gestão e Projetos - GeP
e-ISSN: 2236-0972
DOI: 10.5585/gep.v6i3.381
Data de recebimento: 28/03/2015
Data de Aceite: 15/08/2015
Organização: Comitê Científico Interinstitucional
Editor Científico: Marcos Roberto Piscopo
Avaliação: Double Blind Review pelo SEER/OJS
Revisão: Gramatical, normativa e de formatação

FATORES QUE INFLUENCIAM A PREDISPOSIÇÃO EM SEGUIR UMA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO EM UMA INSTITUIÇÃO DE ENSINO SUPERIOR

RESUMO

A informação é um recurso estratégico para as organizações. Estudos acadêmicos e pesquisas de mercado revelam que esse ativo tem seus elementos de proteção violados em maior grau por funcionários do que por ameaças externas, algo que demanda a implementação de uma Política de Segurança da Informação para assegurar sua confidencialidade, integridade e disponibilidade. Este estudo pretende investigar os motivadores extrínsecos e intrínsecos que afetam a predisposição dos estudantes a estar em conformidade com a política de segurança que venha a ser proposta pela universidade do caso. Na revisão bibliográfica foram abordadas as temáticas de Segurança da Informação e Teoria da Dissuasão em conjunto com os fatores comportamentais que influenciam a predisposição dos indivíduos. Para tanto, foi aplicado um *survey* de 18 itens em escala Likert de concordância com cinco pontos que versavam acerca dos fatores de predisposição. O método adotado consistiu nas técnicas quantitativas: análise fatorial, análise de c*lusters* e regressão logística. Na análise dos resultados, verifica-se que a que a amostra foi dividida em dois grupos: os mais predispostos e os menos predispostos a seguir uma política de segurança. Como conclusão, constata-se que a *severidade da punição* é o fator que exerce maior influência na predisposição dos usuários.

Palavras-chave: Política de Segurança da Informação; Comportamento de Segurança do Usuário; Teoria da Dissuasão.

FACTORS THAT INFLUENCE THE READINESS TO FOLLOW INFORMATION SECURITY POLICY IN A HIGHER EDUCATION INSTITUTION

ABSTRACT

Information is a strategic resource for organizations. Academic studies and market researches showed that the information has protective tools violated in higher degree by employees than by external threats, which demand implementation of Information Security Policy to ensure confidentiality, integrity and availability. This study aims to investigate extrinsic and intrinsic motivators that affect student readiness to comply with security policy which will proposed by university. In the literature review were discussed the issues of information security and deterrence theory together with behavioral factors that influence individual readiness. Therefore, was applied a survey with 18 items in Likert scale concordance, with five points, that focused in readiness factors. The research method is composed of quantitative techniques, being: factorial analysis, cluster and logistic regression. The results showed that sample was fragmented in two groups: higher readiness and smaller readiness to follow security policy. In conclusion, it evidenced that severity of punishment has the most influence on user's readiness.

Keywords: Information Security Policy; Security User Behavior; Deterrence Theory.

Larissa Mayara da Silva Damasceno[1]
Anatália Saraiva Martins Ramos[2]
Fernando Antonio de Melo Pereira[3]

[1] Mestre em Administração pela Universidade Federal do Rio Grande do Norte - UFRN. Professora da UNIFACEX e da Universidade Federal do Rio Grande do Norte - UFRN. Brasil. E-mail: **damasceno.larissa@gmail.com**
[2] Doutora em Engenharia de Produção pela Universidade Federal do Rio de Janeiro - UFRJ. Professora da Universidade Federal do Rio Grande do Norte - UFRN. Brasil. E-mail: **anatalia@ufrnet.br**
[3] Doutorando em Administração pela Faculdade de Economia, Administração e Contabilidade da Universidade de São Paulo - FEA/USP. Brasil. E-mail: **fernandopcmm@gmail.com**

1 INTRODUÇÃO

No contexto atual de hipercompetição entre as organizações, a informação passa a ser considerada um ativo estratégico assim como as pessoas e seus respectivos investimentos, devendo ser protegida com a mesma preocupação que muitos bens móveis e imóveis. A proteção dessa informação – além do uso de senhas numéricas e biométricas, *Firewall* e antivírus – costuma ser realizada por uma Política de Segurança da Informação.

A Política de Segurança da Informação é um documento que visa conscientizar os usuários de realizarem um bom uso dos recursos de TI a fim de proteger a informação da organização (D'Andrea, 2004) com a finalidade de evitar ataques e incidentes de segurança. Segundo o autor, a segurança da informação é um processo estratégico, já que ela tanto protege os ativos informacionais do mau uso como também habilita o acesso às pessoas autorizadas.

Contudo, em pesquisas de mercado aplicadas mundialmente por empresas de consultoria na área de segurança é revelado que grande parte da origem dos incidentes de segurança é interna, ou seja, a maioria deles são causados por funcionários ativos (37%) e ex-funcionários (27%). No Brasil, o percentual dos ataques causados por ex-funcionários é maior (36%) e apesar de os gestores estarem mais preocupados com o monitoramento de incidentes, os mecanismos de controle das empresas ainda estão centrados em questões bastante limitadas, como o uso adequado do *e-mail* e *internet*. Isso é perigoso se considerado o fato de que os invasores utilizam técnicas cada vez mais sofisticadas, o que fez o número de incidentes aumentar em 25% entre 2012 e 2013 (PWC, 2013; 2014).

A partir de dados dessa natureza, pode-se inferir que os usuários (ex-funcionários e colaboradores ativos) são a maior ameaça à Segurança da Informação de uma organização, considerando que são quem conhecem o ambiente da corporação e identificam facilmente as brechas nos controles internos. Albrechtsten e Hovden (2009) consideram os usuários uma vulnerabilidade quando estes não possuem habilidades e conhecimentos, provocando o uso imprudente das conexões de rede e das informações ou ao praticarem atos inseguros dentro da organização.

Para que esta política seja eficaz, além de prover a gestão e supervisão contínua dos sistemas de informação, é pertinente que o usuário tenha prontidão para aceitar e seguir os procedimentos e normas de segurança, considerando-se que, além de controles de segurança lógico e físicos, também devem ser considerados os componentes de Organização e Processos para que se tenha a segurança dos ativos informacionais em uma organização, conforme defende Von Solms (2001).

Logo, é relevante a mensuração de alguns aspectos comportamentais dos usuários que, segundo Pereira (2013), se concentram na disposição de uso da tecnologia, percepção do usuário em relação à própria performance quanto à aprendizagem, atitude do usuário, entre outros aspectos que se encontram presentes na literatura sobre o tema. Neste trabalho, será adotado o enfoque na atitude do usuário, mais precisamente os fatores motivadores intrínsecos e extrínsecos que afetam a predisposição do usuário em seguir uma política de segurança. A predisposição é sinônima do vocábulo prontidão, a qual Parasuraman (2000) refere-se como a propensão das pessoas em abraçar e utilizar novas tecnologias para realizar objetivos na vida, em casa e no trabalho. Essa prontidão pode ser vista como um estado de espírito global resultante de uma *Gestalt* de facilitadores e inibidores mentais que determinam coletivamente a predisposição de uso de uma nova tecnologia.

Entende-se que um dos problemas mais comuns enfrentados para a implementação bem-sucedida de práticas e procedimentos de segurança da informação é o elemento humano (Datt, 2012; Herath & Rao, 2009; Furnell, Pahnila, Siponen & Mahmood, 2007; Furnell & Thompson, 2009) e apresenta a maior carência de cuidados por parte das empresas (Silva, Netto & Silveira, 2007). Esse fato aliado à não-conformidade com as políticas instituídas pela organização não só compromete a integridade do sistema, como também custa uma quantidade significativa de recursos financeiros devido à perda de informação ou o tempo que é dispendido para corrigir os problemas causados pelo mau uso da TI por parte do usuário (PWC, 2013).

Acerca da temática de Segurança da informação a nível nacional, nota-se a predominância de trabalhos que discutem normas, procedimentos e uso de tecnologias sob aspectos técnicos de forma completa, mas não tratam de forma satisfatória o fator humano envolvido nessas questões. Isso elucida o fato de que a abordagem social é incipiente em trabalhos com a temática de segurança da informação (Albuquerque Junior & Santos, 2013; 2014a; 2014b). Já em estudos internacionais, nota-se uma melhor abordagem com enfoque no usuário (Furnel *et al*, 2007; Furnell & Thomsom, 2009; Thomsom & Nierkek, 2012), porém a literatura crítica acerca de seus comportamentos em relação ao cumprimento das políticas de segurança ainda está em sua infância (Heralth & Rao, 2009).

O presente estudo tem como objetivo investigar a predisposição do usuário individual em seguir a Política de Segurança da Informação que

poderia ser proposta pela Instituição de Ensino Superior (IES) em que estuda.

Em termos de relevância prática, este trabalho poderá auxiliar as organizações na elaboração de PSI eficazes a partir do maior cumprimento espontâneo por parte dos usuários. Ao considerar o ponto em que, no estabelecimento desse documento, Herath and Rao (2009) lembram que as organizações podem se deparar com um grande desafio devido à natureza relativamente arbitrária de adesão a essas políticas. Tendo em vista que a adesão com menor arbitrariedade poderia permitir que boas práticas sejam incorporadas à cultura e estratégias da organização.

Deste ponto em diante, o presente artigo se encontra definido nas seguintes seções: Problema de Pesquisa e Objetivo; Revisão Bibliográfica, em que se discute temas relacionados à Segurança da Informação; Modelo de Pesquisa e Hipóteses do Estudo; Análise e Discussão dos Resultados; Conclusão e Referências.

2 REVISÃO BIBLIOGRÁFICA

Nesta seção, serão apresentadas e discutidas temáticas referentes à Segurança da Informação e Política de segurança bem como as teorias comportamentais que visam responder ao problema e objetivo de pesquisa, retratados no item anterior.

2.1 A Segurança da Informação e a Política de Segurança da Informação no ambiente organizacional

A *Segurança da Informação* é um conceito amplo e concerne à proteção da informação em suas propriedades (confidencialidade, integridade e disponibilidade) e em seus aspectos (autenticidade, legalidade etc), evitando que as vulnerabilidades dos ativos relacionados sejam exploradas por ameaças que possam trazer consequências negativas para os negócios. Em outras palavras, ela deve existir para trabalhar contra o mau uso acidental ou intencional da informação por pessoas dentro ou fora da organização (Von Solms, 2001; Gualberto, 2003; Mattord & Whitman, 2004; Baltzan & Phillips, 2012).

Quanto à *Política de Segurança da Informação* (PSI), trata-se de um documento em que constam declarações de diretrizes gerais de metas a serem alcançadas em relação à segurança dos recursos de informações corporativas (Gaston, 1996 *Apud* Doherty & Fulford, 2006) que são exibidas de forma compreensível, prática, útil e com uma abordagem apelativa voltada diretamente aos usuários, convencendo-os da necessidade de usar de forma segura os recursos de informação (Höne & Eloff, 2002).

A segurança da informação alcançou uma posição de destaque na agenda de muitas organizações, pois deixou de ser um mero detalhe administrativo ou de orçamento e passou a ser considerada como tema estratégico em função impacto que pode provocar diretamente no objetivo de negócio, desempenho e transparência na prestação de contas para os *stakeholders* (D'Andrea, 2004), constituindo-se como um dos elementos-chave para a existência de boas práticas de governança corporativa.

Logo, para o desenvolvimento de uma cultura de segurança na implementação de uma PSI, é necessária a compreensão do comportamento humano quanto às atitudes favoráveis e desfavoráveis em relação a um objeto (a predisposição em seguir a política). No próximo tópico serão abordados os pressupostos de uma teoria da psicologia que justifica a razão para tais atitudes individuais (Mattord & Whitman, 2004; Marciano, 2006; Gaunt, 1998).

2.2 A influência da componente atitude nos sentimentos e condutas do indivíduo

O conceito de 'atitude' é oriundo da psicologia, engloba a avaliação de uma realidade social e retrata "sentimentos pró ou contra pessoas ou objetos com quem entramos em contato" (Rodrigues, Asmar & Jabloski, 2012, p.160). Esses sentimentos costumam se referir a fatos onde é impossível determinar qual seria a posição 'correta' ou 'verdadeira'.

Essas atitudes sociais se manifestam a partir de três componentes claramente discerníveis: (a) o componente cognitivo; (b) o componente afetivo e (c) o componente comportamental. (Albeson; Ajezen & Allport; 1988; 1935 *apud* Monteiro & Vala, 2004). Smith e Mackie (1997) clarificam os componentes anteriormente mencionados como, respectivamente, a tradução em: crenças sobre as características positivas e negativas do objeto; sentimentos e emoções sobre o objeto; e, informação sobre ações passadas e presentes que dizem respeito ao mesmo.

Para Newcomb, Turner e Converse (1965 *apud* Rodrigues *et al.*, 2012), as atitudes do ser humano são propiciadoras de um estado de prontidão que, se ativado por uma motivação específica, resultará num determinado comportamento. Com isso, pode-se afirmar que o comportamento é uma resultante de múltiplas atitudes.

Correlacionado essa temática ao objeto de estudo em questão, pode-se inferir que algumas atividades extrínsecas que poderiam influenciar na aceitação das normas estão relacionadas ao processo de comunicação da política de segurança, treinamento e conscientização. Essa política tem a finalidade de auxiliar os funcionários a

compreenderem seus papéis e responsabilidades, bem como dizer as práticas que são intoleráveis. Sobre esse fato, Furnell e Thompson (2009) apontam que as organizações não podem verdadeiramente proteger seus ativos sem garantir que os funcionários tenham a compreensão desses papéis e também estejam suficientemente aptos a realizá-los.

Ao alinhar essas considerações sobre a origem das atitudes ao objetivo da pesquisa, alerta-se para o fato que este estudo visa identificar aspectos de conduta do indivíduo a partir do seu grau de concordância com afirmações retiradas de modelos teóricos sobre o tema, pois eles trazem a teoria da dissuasão como uma influenciadora nos fatores motivacionais que impulsionam as atitudes favoráveis (ou não) dos indivíduos em seguir uma política de segurança e serão abordados na próxima seção.

2.3 A Teoria da dissuasão e os fatores motivacionais intrínsecos e extrínsecos

Apesar de haver pouca literatura acerca de fatores que afetam o comportamento do usuário nas questões de segurança da informação, um estudo que merece destaque é o de Heralth e Rao (2009), cujo modelo teórico avalia a relativa importância de três mecanismos de incentivo para o encorajamento de comportamento de segurança nas organizações, que estão nas seguintes dimensões: (1) punições; (2) pressões sociais e (3) eficácia percebida. Nesse estudo, as punições e pressões sociais constituem fatores motivacionais extrínsecos (que ajudam a promover a política de segurança na organização). Já a eficácia percebida, constitui um fator motivacional intrínseco.

Os fatores motivacionais intrínsecos movem a pessoa para a ação, pois são motivos baseados em necessidades internas e a gratificação da pessoa é pela ação em si, sem que sejam necessários benefícios externos como impulsionadores ao indivíduo (Appel-Silva, Wendt & Argimon, 2010). Portanto, constitui-se no desejo de ocupar-se de uma atividade porque gosta dela e a julga interessante, e não por causa de recompensas ou pressões externas (Aronson, Wilson & Arket; 2002).

No modelo proposto por Herath e Rao (2009), para dar prosseguimento a uma política de segurança, a *eficácia percebida* entra como um fator motivacional intrínseco do usuário em seguir a PSI, sendo definido no Quadro 1. Já os fatores motivacionais são considerados extrínsecos quando a pessoa é movida por condições externas a ela, sejam benefícios ou punições, mas que a ação por si só não a satisfaça (Appel-Silva *et al.*,, 2010); tratando-se de uma recompensa contingente de fatores externos (Herath & Rao, 2009) como, por exemplo, as pressões sociais (Aronson *et al.*, 2002).

As *punições* e *pressões sociais* são consideradas pelo modelo teórico de Herath e Rao (2009) como fatores motivacionais extrínsecos. Os efeitos da punição são criados por dois mecanismos: a "severidade da punição" (*severity of penalty*) e "certeza de detecção" (*Certainty of detection*). Já as *pressões sociais* são divididas em dois grupos: *crenças normativas* e *comportamento dos pares*, também definidos na Figura 1.

FATOR	DEFINIÇÃO	AUTORES
Eficácia percebida	Percepção do indivíduo de que suas ações individuais podem contribuir para a organização.	Herath e Rao (2009); Venkatesh *et al.* (2012)
Severidade da punição	A medida que a punição aumenta, o indivíduo se sentirá menos inclinado a praticar um ato transgressivo.	Herath e Rao (2009)
Certeza de Detecção	Percepção do indivíduo de que está sendo observado ou monitorado.	Herath e Rao (2009); Darcy *et al.*, (2009)
Comprometimento moral	Inibições morais individuais que efetivamente impedem a realização de comportamentos que contrariam ao que é aceitável.	Darcy *et al.*, (2009)

Comportamento dos pares	Percepção do indivíduo com relação ao comportamento e as ações de seus pares.	Herath e Rao (2009)
Intenção de conformidade	Predisposição do usuário em seguir a Política de Segurança proposta pela organização.	Herath e Rao (2009)

Figura 1 - Fatores, definições, variáveis e origens
Fonte: elaborado pelos autores, 2015.

Darcy, Hovav e Galletta (2009) incluem em seu modelo de pesquisa uma motivação intrínseca não contemplada no estudo de Herath e Rao (2009), denominada de "comprometimento moral", que compreende uma das três dimensões (normativo, moral e instrumental) do conceito de comprometimento organizacional amplamente difundido por Meyer e Allen (1991).

Este artigo acadêmico contempla o contexto de predisposição de adesão à uma política, onde a dimensão de comprometimento adotada é o moral, que é resultado das pressões normativas, originadas dos objetivos e interesses organizacionais, que internalizam e orientam atitudes e ações dos indivíduos no trabalho. Nesses termos, o comprometimento moral do indivíduo é fruto de um sentimento de obrigação (Meyer & Allen, 1991) e influencia positivamente seu grau de cooperação no trabalho, condicionando sua avaliação e formas de proceder (Maciel & Camargo, 2011).

Para Darcy *et al.* (2009), num contexto de uso abusivo dos recursos de SI, a certeza de detecção é mais um elemento mais dissuasor para os indivíduos com fortes inibições morais enquanto que a severidade da punição é o elemento mais dissuasivo para as pessoas com menor comprometimento moral.

Nesta pesquisa, optou-se por adotar a aplicação de um instrumento em que foram mesclados os modelos teóricos de Herath e Rao (2009) e o de Darcy *et al.* (2009), considerando-se que o contexto existente ainda é o de uma política não existente e, quando for aplicada, o contexto de comprometimento moral poderia influenciar na intenção de cumprir tais normas.

No embasamento teórico de ambos os trabalhos tomados como referência, são adotadas versões modificada/estendida da "Teoria da Dissuasão" para o contexto de segurança da informação com o intento de avançar na compreensão do processo subjacente em que as medidas de segurança afetam os usuários nas intenções de mau uso dos sistemas de informação, cujos resultados também têm importantes implicações para a prática de gestão de segurança.

Segundo Viapiana (2006), o núcleo central da "Teoria da Dissuasão" é a de que o comportamento criminoso das pessoas pode ser refreado pela estrutura de sanções que podem ser legais (propostas por normas e regulamentos) ou extralegais (formação moral e religiosa, nível educacional e vínculos comunitários). Essa teoria aponta para a existência de fatores/elementos que afetariam o uso mal-intencionado dos recursos de TI nas organizações. Ela sugere que a ameaça de punição percebida influencia o comportamento individual do usuário através da certeza e severidade dessa punição. Portanto, certos controles organizacionais podem servir como mecanismos de dissuasão a partir do aumento da ameaça de punição pelo abuso no uso dos recursos de TI (Darcy *et al.*, 2009; Herath & Rao, 2009). Ou seja, a pessoa passaria a seguir a política essencialmente pelo "medo" de sofrer punições de natureza normativa ou moral.

Esses constructos que acabaram de ser explanados serviram como "pano de fundo" para a elaboração do modelo e hipóteses desta pesquisa, que será exibida na seção a seguir.

3 MODELO DE PESQUISA E HIPÓTESES DE ESTUDO

Neste estudo foi elaborado um instrumento de pesquisa baseado nos modelos propostos por Herath e Rao (2009) e Darcy *et al.* (2009) com a finalidade de verificar a obediência às regras de Segurança da Informação dentre o público ingressante no ambiente universitário e que, num futuro breve, atuará no mercado de trabalho. O significado de cada construto pode ser visto no quadro 1 da seção 2.3 deste trabalho e a representação gráfica do modelo adotado para a elaboração do instrumento pode ser vista na Figura 2.

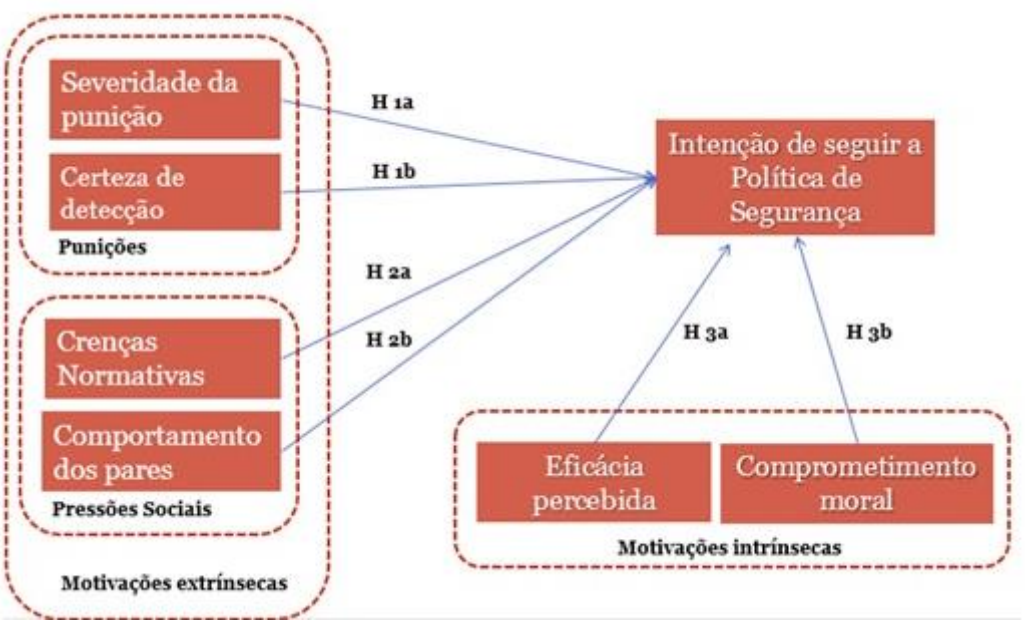

Figura 2 - Modelo de pesquisa com os fatores motivacionais intrínsecos e extrínsecos que identificam a predisposição em seguir uma Política de Segurança da Informação.
Nota. Fonte: Elaborado pelos autores, 2015.

Os autores citados formularam hipóteses de que as pressões sociais exercidas pelas normas subjetivas (expectativa percebida) e normas descritivas (observância) influenciariam positivamente na intenção de seguir uma PSI. Sendo assim, com a finalidade de aumentar o poder preditivo do modelo apresentado nesta pesquisa, também foi acrescentado em conjunto com a eficácia percebida pelo empregado (fator motivacional intrínseco) quanto às suas ações, se o comprometimento moral — variável presente no estudo de D'Arcy *et al.* (2009) – também teria um efeito positivo no cumprimento de políticas de segurança da informação caso sejam implementadas. Com base nesses conceitos, foram formuladas as seguintes hipóteses:

Hipótese 1a*: O aumento da severidade da punição contribui na formação de grupos distintos de intenção de seguir a Política de Segurança da Informação da organização.*

Essa hipótese foi delineada por Herath e Rao (2009) por defenderem que a certeza de punição contra os empregados é um importante aspecto de dissuasão para que elas sejam cumpridas, já que a punição funcionaria como um esforço para controlar comportamentos antissociais.

Hipótese 1b: *O aumento da certeza de detecção da punição contribui na formação de grupos distintos de intenção de seguir a Política de Segurança da Informação da organização.*

Num contexto de segurança da informação, fazer cumprir com punições só é possível quando a organização for hábil para detectar a falta de bom comportamento do empregado. Logo, é pertinente que se lancem mecanismos de monitoramento e detecção de descumprimento de regras de segurança como uma forma de ter certeza que os empregados estão agindo em conformidade com a política de segurança.

Hipótese 2a: *As crenças normativas contribuem na formação de grupos distintos de cumprimento com as políticas de segurança da informação.*

O comportamento de segurança da informação é executado como uma forma de atender às expectativas do que outros (colegas e especificamente a alta administração) efetivamente esperam.

Hipótese 2b: *O comportamento dos pares contribui na formação de grupos distintos de intenção em seguir a Política de Segurança da Informação da organização.*

As normas subjetivas incentivam o comportamento individual através da possibilidade de obtenção da aprovação dos outros. Portanto, o comportamento individual é motivado pela observação daquilo que normalmente é típico ou normal para se fazer, havendo um enfoque na expectativa de que os outros indiretamente realizem o mesmo comportamento.

Hipótese 3a: *A eficácia percebida do comportamento de segurança do empregado contribui na formação de grupos distintos de intenção em seguir a Política de Segurança da Informação da organização.*

Os empregados podem se engajar em atividades que são benéficas para a organização porque eles se sentem comprometidos e acreditam que suas ações individuais farão a diferença quanto à proteção dos ativos de informação pela organização.

Hipótese 3b: *O alto comprometimento moral contribui na formação de grupos distintos de intenção em seguir a Política de Segurança da Informação.*

Quem tem um comprometimento moral maior costuma "fazer o que é certo". Segundo D'Arcy *et al.* (2009), as pessoas que têm esse comportamento procuram seguir as regras por medo de "serem pegas" descumprindo/desobedecendo as ordens. Assim, quem teria um comprometimento moral maior poderia estar mais predisposta a seguir uma política de segurança da informação. Do outro lado, aqueles que não teriam um comprometimento moral tão alto só cumpririam as políticas caso percebessem um alto grau de severidade nas punições aplicadas contra quem descumprisse o que estaria disposto no documento.

Com o conhecimento do modelo de pesquisa e possíveis hipóteses formuladas, será possível explanar com maior clareza o método de pesquisa, a ser apresentado na próxima seção.

4 MÉTODO DE PESQUISA

Esta pesquisa tem um caráter exploratório e descritivo, utilizando uma abordagem quantitativa para responder ao objetivo proposto. Acerca do público escolhido, verificou-se que tanto em estudos nacionais como internacionais sobre segurança da informação são investigados somente os gestores de TI e/ou empregados de organizações, já acostumado (e adaptado) a seguir normas, regras e procedimentos. Já o estudante universitário é ignorado, embora ele também use de forma bastante ativa os dispositivos de TI e tenha expectativa de ingressar em breve nessas mesmas organizações. A razão para tal fato pode estar atrelada à permanência temporária na Instituição de Ensino Superior (que também tem ativos informacionais e estratégicos a proteger). Porém, essa temporariedade não o exime da responsabilidade para com o uso correto de recursos de TI que são concedidos para a realização de atividades de ensino e extensão.

As faixas etárias predominantes nesse estudo compreendem até os 20 anos (53,45%) e entre 21 e 25 anos (21,99%). São representantes das chamadas geração Z e Y, respectivamente. A geração Y foi a primeira que nasceu com TV, computador e comunicação rápida, realizada por dispositivos tecnológicos como *smartphones* (Loiola, 2009). Já a geração Z, compreende os jovens que nasceram na segunda metade da década de 90, período que coincide com a forte expansão *internet* e não chegaram a conhecer um mundo sem ela. A pesquisa do Instituto Brasileiro de Geografia e Estatística (IBGE), sobre o uso de Internet no Brasil em 2011, revela que 66,4% dos jovens dessa faixa etária acessam a internet (IBGE, 2011).

A geração Z é autônoma, autodidata, não gosta de hierarquia nem de horários pouco flexíveis e é incipiente na maturidade para cumprir regras, algo que desafia as organizações para que se adaptem e apliquem novas práticas para atrair e reter profissionais (Mendonça, 2015). Dessa forma, os estudantes universitários são os sujeitos que integram o rol de respondentes da pesquisa com o intento de procurar responder a esses desafios.

Para a coleta dos dados, foi realizada uma pesquisa de campo, utilizando-se da técnica de aplicação de questionário impresso sob a forma de *survey* com os alunos da organização em estudo a fim de compreender seu funcionamento e orientar a elaboração futura de Política de Segurança da Informação.

A população compreende os alunos regularmente matriculados em uma instituição de ensino superior (IES), mais especificamente, uma universidade pública do Nordeste. A amostra é constituída de alunos do primeiro ano (1º e 2º período) de um Centro de Ciências Sociais Aplicadas, compreendendo os cursos de graduação em: Administração, Biblioteconomia, Ciências Contábeis, Ciências Econômicas, Direito, Pedagogia, Serviço Social e Turismo.

Hair; Black; Babin; Anderson e Tatham (2009) preconizam que, para a aplicação das técnicas de regressão, é necessária a quantidade mínima de 20 observações para cada variável estudada. Nesta pesquisa, existem 18 variáveis que buscam investigar a predisposição, o que implicaria na obtenção de 360 observações. Este estudo contém 391 observações, o que ultrapassa o mínimo recomendado para a aplicação das técnicas utilizadas.

Foi conduzido um pré-teste para validação do conteúdo do instrumento. Foram coletados 30 questionários tendo como respondentes o público-alvo da pesquisa. Neste momento, foram inclusas perguntas abertas com o objetivo de obter *feedback* acerca da compreensão que os respondentes tinham em relação aos itens avaliados.

Na análise de dados quantitativos do pré-teste, foi realizado primeiramente uma análise de dados faltantes (*missing values*). O método de substituição que melhor se adequou foi a substituição pela mediana, sendo também adotado este método para a amostra final.

Por fim, foi executada a identificação de observações atípicas. Como o número de observações no pré-teste era pequeno, a avaliação foi feita por análise gráfica (*box-plot*). Nenhuma observação apresentou recorrência em avaliações extremas. Na amostra completa é adotada a substituição pelo método de forçar os desvios padronizados a uma amplitude de -3 a 3. Esse método garante a perda de influência indesejada dos *outliers*, ao mesmo tempo que mantém a observação na amostra e não modifica significativamente a variabilidade dos dados.

5 ANÁLISE E DISCUSSÃO DOS RESULTADOS

No trabalho optou-se por avaliar as variáveis de forma descritiva, mais precisamente, a média e a mediana, medidas de tendência central que possibilitam compreender a opinião dos indivíduos a respeito de cada item. A média posiciona a opinião da maioria em escala de 1 a 5 do tipo Likert e a mediana indica em que nível da escala as opiniões são divididas em 50%. O desvio padrão indica quanto às opiniões variam em torno da média, indicando se há uma convergência de opiniões que sustentam a afirmação de que a maioria tem de fato, a opinião apontada. As variáveis utilizadas podem ser consultadas na tabela 1.

Os resultados apontam que as variáveis 2 e 3 possuem as maiores médias (4,12; 4,00), dentre as variáveis independentes, indicando nível de concordância alto das afirmações avaliadas. As variáveis 16, 17 e 18 também evidenciam alto grau de concordância (4,07; 4,18; 4,06) com médias ultrapassando 4. Nota-se que as variáveis que possuem maior média, também são aquelas que possuem menor desvio (abaixo de 0,1). Esse resultado indica baixo coeficiente de variação, ou seja, há uma convergência de opiniões dos entrevistados em relação a esses itens, aumentando a precisão das estimativas das médias. Dessa forma, sendo os itens 2 e 3 referentes ao constructo eficácia percebida e os itens 16, 17 e 18 referentes ao constructo *intenção de seguir as políticas de segurança da Universidade*, é possível afirmar que há um sentimento positivo no que concerne aos alunos entenderem seus papéis em seguir as políticas de segurança e em de fato, cumpri-las.

Porém, o fator que mede *comprometimento moral*, representado pelas variáveis 10, 11 e 12 tem médias destoantes das demais (1,92; 1,64 e 2,24) respectivamente, indicando baixa concordância às afirmações que definem o comprometimento moral do aluno em seguir as políticas de segurança da instituição.

5.1 Análise fatorial exploratória

A análise fatorial exploratória (AFE) é uma técnica exploratória de dados que foi utilizada com o objetivo de redução e busca de explicação do fenômeno de forma sintética e de fácil compreensão. Marôco (2007, p.361) destaca que ao utilizar a AFE busca-se "descobrir e analisar a estrutura de um conjunto de variáveis inter-relacionadas de modo a construir uma escala de medida para fatores (intrínsecos) que de alguma forma controlam as variáveis originais". Dessa forma, 15 variáveis quantitativas podem ser reduzidas em construtos, mantendo o poder de explicação em níveis desejáveis.

O modelo do estudo conta com cinco fatores, sendo possíveis sintomas da predisposição em seguir as políticas de segurança. A AFE permite indicar se as variáveis preconizadas realmente fazem parte do construto designado e se as variáveis contribuem para caracterizar o construto a partir da inspeção da matriz de correlações.

A operacionalização dos cálculos inicia com a formação da matriz de correlações das variáveis do estudo. Essas p variáveis podem ser explicadas (esperançosamente) por um conjunto reduzido de fatores (Maroco, 2007). Em seguida, decide-se o uso do método de extração. Para o estudo, foram testados os dois métodos mais comuns: componentes principais e máxima verossimilhança. O primeiro une as variáveis em fatores comuns que devem explicar a maior proporção da variância, o segundo estima matrizes até o número de variáveis utilizadas, buscando convergir uma matriz estimada a matriz observada (Hair *et al.* 2009). Nesse caso, o método de componentes principais se mostrou mais adequado por oferecer uma solução fatorial melhor interpretável.

Outra decisão a ser tomada é o método de rotação. Foram testados o método Varimax e o método Kappa. O primeiro consiste em um método ortogonal, que rotaciona o eixo de rotação para buscar uma solução melhor interpretável, atribuindo média 0 e variância 1 nos fatores, enquanto que o segundo consiste em um método oblíquo, assumindo as correlações entre os fatores. O resultado no uso dos dois métodos não gerou diferenças significativas devido à baixa correlação entre os fatores encontrados (Maroco, 2007). A seguir, na Tabela 1, os resultados da análise fatorial são apresentados, com os pesos fatoriais e comunalidades das variáveis.

Tabela 1 - Fatores encontrados pelo estudo

FATORES	**Comunalidade**	**Carga fatorial**
Fator 1: Eficácia percebida α = 0,779		
01. Cada estudante poderia fazer sua parte quando se trata de proteger os sistemas de informação da Universidade.	0,580	0,741
02. Se eu seguir a Política de Segurança da Universidade, poderia contribuir na proteção os sistemas de informação da universidade.	0,748	0,859
03. Eu acredito que seguir a Política de Segurança da Informação da Universidade poderia ser algo útil para mim.	0,599	0,698
Fator 2: Severidade de punição α = 0,790		
04. A Universidade deveria punir os alunos que não seguem as orientações de Segurança da Informação.	0,700	0,819
05. A Universidade deveria expulsar os alunos que descumprissem as regras de segurança repetidamente.	0,736	0,851
06. Se eu fosse pego violando as regras de Segurança da Informação da Universidade, deveria ser severamente punido.	0,723	0,837
Fator 3: Comprometimento moral α = 0,710		
10. Se eu receber um e-mail com piadas e gostar, não vejo problema em encaminhá-lo pela caixa postal do SIGAA para meus colegas de classe.	0,574	0,720
11. Se eu tivesse a oportunidade de acessar um sistema de informação restrito, não vejo problema em utilizar alguma informação desse sistema para obter algum benefício pessoal.	0,599	0,737
12. Se a Universidade não tiver como comprar a licença de um software para instalar nos laboratórios de informática, não vejo problema em baixar uma cópia pirata caso precisasse usá-lo.	0,587	0,667
Fator 4: Certeza de detecção		
08. Se eu fosse pego violando as políticas de segurança da Universidade, certamente eu seria punido.	0,585	0,656
09. Eu acredito que a Universidade conduz inspeções periódicas para detectar o uso de programas não autorizados em seus computadores.	0,814	0,897

Nota. Fonte: dados da pesquisa, 2015.

Os resultados da fatorial indicam a formação de quatro fatores e não cinco como preconizados na revisão teórica. O fator *comportamento dos pares* possuía variáveis que violavam os pressupostos da AFE e não eram significantes. Dessa forma, foram descartadas da análise fatorial. O fator 4 teve uma variável descartada por violar o pressuposto de comunalidade e apresentar baixa carga fatorial. Apesar de o fator ser formado por apenas duas variáveis, entende-se que o constructo *Certeza de Detecção*, originalmente formado por duas variáveis, foi bem captado. A variável apresenta cargas fatoriais próximas de 0 nos demais fatores e sua manutenção valida a manutenção do fator, já que, se fosse representado apenas pela variável 9, não haveria representatividade do mínimo de itens exigido em um fator (Maroco, 2007; Hair *et al.* 2009).

As variáveis mantidas na análise foram aquelas que obtiveram comunalidades acima de 0,5. A comunalidade é uma medida que representa a probabilidade de variância de cada variável explicada pelos fatores comuns após a extração. O valor de 0,5 refere-se a 50%, ou seja, espera-se que cada variável contribua para o modelo fatorial mais do que o mínimo que uma variável ao acaso contribuiria.

Já os pesos fatoriais ou cargas fatoriais correspondem às correlações entre os fatores e as variáveis. Era esperado que uma variável possuísse alta carga em 1 fator e baixa carga nos demais. Esse

índice também foi utilizado como eliminatório para a manutenção das variáveis no modelo fatorial.

Uma medida de confiabilidade do fator formado e comumente utilizado na AFE é o Alpha de Crombach (α). Para os fatores 1, 2 e 3 o índice ultrapassou 0,7, sendo considerado como uma boa confiabilidade, segundo Hair *et al.* (2009). Para o fator 4, o α não representaria adequadamente a confiabilidade do fator, visto que é sensível a premissa de medida forte (fator formado por, pelo menos, três itens). No entanto, devido à representatividade das variáveis na % cumulativa de variância, foi decidido manter o fator. A seguir, na Tabela 2, encontra-se resumida a avaliação dos resultados do modelo completo.

Tabela 2 - Variância explicada do modelo fatorial

Componente	Somas de extração de carregamentos ao quadrado			Somas rotativas de carregamentos ao quadrado		
	Total	% de variância	% cumulativa	Total	% de variância	% cumulativa
1	2,726	24,781	24,781	2,485	22,593	22,593
2	1,897	17,246	42,027	1,896	17,239	39,833
3	1,374	12,487	54,514	1,532	13,924	53,757
4	1,073	9,753	64,267	1,156	10,510	64,267

Nota. Método de extração: componentes principais
Método de rotação: Varimax com normalização de Kaiser
Medida de Kaiser Meyer Olkin: 0,755
Teste de Esfericidade de Bartlett: 799,888 Sig: 0,000
Fonte: dados da pesquisa, 2015.

O resultado da avaliação global do modelo fatorial dá o valor do KMO = 0,75, sendo considerado aceitável e o teste de Bartlett com p valor menor que 0,05. Dessa forma, concluímos que as correlações simples e as correlações parciais indicam homogeneidade das variáveis e que as correlações entre as variáveis são elevadas o suficiente para que a AFE tenha utilidade na estimação dos fatores.

A Tabela 2 mostra que o poder de explicação do modelo atingiu 64,26% com quatro fatores que obtiveram autovalor acima de 1 (um). Observando o gráfico de sedimentação, a solução com cinco fatores atingia 74% de poder de explicação, no entanto continha dois fatores com apenas uma variável, que violariam o pressuposto de medida forte. O fator 1: *eficácia percebida* é o que mais contribui para a solução fatorial, com 22,59% de variância. Em seguida vem o fator *severidade de punição* (17,23%). O fator que menos contribui é o 4: *certeza de detecção* (10,51), que contribui com 13,92% de variância, levando em consideração que é formado apenas pela variável 9 (Eu acredito que a Universidade conduz inspeções periódicas para detectar o uso de programas não autorizados em seus computadores).

A AFE também foi utilizada como primeiro passo das técnicas de dependência utilizadas no estudo. A AFE entrega como produto os escores fatoriais, que consistem em uma quantificação padronizada pela distribuição normal dos fatores encontrados, englobando as informações das variáveis observáveis que compõem cada fator (Hair *et al.* 2009).

5.2 Cluster hierárquico e cluster k-means

A análise de conglomerados ou cluster foi utilizada com o objetivo de formar a variável dependente, sendo agrupados os casos de acordo com as dissimilaridades que indiquem a formação de subgrupos em relação à predisposição em seguir as políticas de segurança da IES pesquisada.

A forma de aglomeração utilizada é a de menor distância ou *single linkage*. "Este método tende a maximizar a conectividade entre clusters e tem tendência para criar um menor número de clusters do que o método da máxima distância ou complete linkage" (Maroco, 2007, p. 428). O planejamento de aglomeração indica possíveis soluções ideais de clusterização a partir das medidas de distância euclidiana. "Essa medida de dissemelhança métrica mede o comprimento da reta que une duas observações num espaço p-dimensional. Para p variáveis, a distância euclidiana entre os casos é dado" (Maroco, 2007, p. 420). Quanto maior a distância euclidiana, maior é a dissemelhança entre dois casos. Dessa forma, identificamos, nas últimas distâncias calculadas, aquelas com maior grau de dissemelhança.

Os resultados indicam duas soluções possíveis, com dois clusters e com sete clusters. A regra de decisão é escolher o número de clusters baseado no objeto de estudo e na capacidade de

interpretação da solução. Nesse caso, buscamos a identificação de possíveis grupos com opiniões divergentes em relação às variáveis quantitativas que são possíveis influenciadoras da predisposição em seguir as políticas de segurança da Universidade pesquisada. Ao comparar as médias das variáveis quantitativas por cluster, a solução com sete fatores apresentou diferenças pouco significantes, enquanto que a solução com dois clusters conseguiu diferenciar um grupo com menor predisposição e outro com mais predisposição.

Ao decidir utilizar dois clusters, o cluster não-hierárquico é conduzido calculando centróides ou médias próximas entre os casos até obter convergência adequada. Três variáveis não obtiveram níveis de significância abaixo de 0,05, evidenciando que não contribuem para a discriminação dos casos. Ao todo, 12 variáveis no teste de comparação de médias obtiveram níveis de significância adequados.

Observando o teste F, pode-se ranquear as variáveis que melhor discriminam os grupos, ou seja, cujas médias são mais diferentes comparando os dois clusters. As variáveis do constructo *severidade de punição* são aquelas que mais contribuem para diferenciar os grupos. Após obter convergência com 391 casos válidos, tem-se a presença de 188 casos no primeiro cluster e 203 no segundo cluster. Observando as médias dos clusters, percebe-se que no cluster 1 há a predominância de indivíduos com menor predisposição, pois apresentam menores médias nos constructos *eficácia percebida*, *severidade da punição* e *certeza de detecção*.

Sintetizando os resultados do *cluster*, foram encontrados dois grupos com opiniões divergentes em relação a determinados itens que compõem possíveis influenciadoras da intenção em seguir as políticas de segurança da Universidade investigada. Não foi encontrado nenhum grupo que poderia ser caracterizado como de baixa intenção ou predisposição negativa ou nula. Esses resultados corroboram a predominância das médias das variáveis nos pontos 4 e 5 da escala, que correspondem a concordância das afirmações com direção positiva para a intenção.

5.3 Modelo logístico

A regressão logística binária foi utilizada com o objetivo de gerar um modelo de previsão capaz de diferenciar grupos em níveis de predisposição a seguir políticas de segurança de instituições de ensino superior. A variável de agrupamento gerada no cluster k-means é utilizada como variável dependente, por ser a variável que distingue dois níveis de predisposição. Os escores fatoriais gerados na análise fatorial exploratória atuam como variáveis independentes. Dessa forma, é testado um modelo de previsão de predisposição a seguir políticas de segurança baseado na percepção dos indivíduos em relação às características que sendo praticadas levam ao atendimento das políticas de segurança.

Foi utilizado o método *stepwise*, com o uso de quatro fatores, onde se tem a convergência em quatro etapas. Os primeiros referem-se aos passos do cálculo da estatística -2LL, que mostra o quanto o modelo se destaca do método do acaso. Os coeficientes de Omnibus na última etapa são utilizados para verificar uma taxa de *improvement* ou melhoria na capacidade preditiva do modelo.

Pelo método do acaso, como mostrado na Tabela 3, temos uma porcentagem global de 51,9%. Esse resultado se refere a representatividade de indivíduos em cada grupo na amostra. A estatística de verossimilhança ou -2LL reduziu a partir do final da etapa 1 de 233,12 para 179,959 na etapa em que os quatro fatores estão presentes. O R quadrado de Cox & Snell e o R quadrado Nagelkerke indicam bom poder de explicação do modelo, sendo respectivamente 60,3% e 80,5%.

O resultado da estatística -2LL no teste de Hosmer e Lemeshow indica que o *improvement* foi significante. O modelo também foi significante nas etapas 1 e 3. O resultado na etapa 2 indica que o fator 2 é o que menos contribui no modelo de previsão.

Tabela 3 - Resumo do modelo

Teste de coeficiente de modelo Omnibus			**Porcentagem pelo método do acaso**	
Qui-quadrado	df	Sig.	51,9%	
361,507	4	0,000		
Testes de poder de explicação do modelo				
Verossimilhança de log -2	R quadrado de Cox e Snell		R quadrado de Nagelkerke	
179,959	0,603		0,805	
Teste de Hosmer e Lemeshow				
	Etapa 1	Etapa 2	Etapa 3	Etapa 4
Qui-quadrado	8,049	18,875	8,715	10,644
Sig.	0,429	0,016	0,367	0,223

Nota. Fonte: dados da pesquisa, 2015.

A partir dos resultados de qualidade de ajustamento e poder de explicação, o modelo na etapa 4 é o que melhor converge. O teste de Wald testa a hipótese nula de que o coeficiente logístico é zero. Na etapa 4, temos que todos os coeficientes são significantemente diferentes de 0. A estatística de Wald é maior para o fator 1, valor que pode ser atribuído ao maior desvio padrão do fator em relação aos demais. O fator 1 também apresenta o maior expoente, indicando que a *eficácia percebida* apresenta maior impacto na desigualdade (para a previsão) na mudança de uma unidade, mantendo as outras constantes. O fator 3 – *comprometimento moral*, é o único que apresenta coeficiente logístico negativo, isso indica que quanto menor o valor associado ao fator, maior a tendência do indivíduo de fazer parte do grupo dos predispostos a seguir as políticas de segurança da Universidade pesquisada.

A tabela 4, referente à classificação final, indica o poder de previsibilidade do modelo a partir do número de acertos dos indivíduos em cada grupo. Dessa forma, na etapa 4 é obtido o maior número de acertos, confirmando os resultados da estatística de Wald, que considerou todos os fatores significantes. No cluster 1, o modelo conseguiu acertar 166 indivíduos e no cluster 2 acertou 183. O modelo consegue prever os indivíduos que são menos e mais predispostos a seguir as políticas de segurança da Universidade com 88,3% e 90,1% respectivamente.

Tabela 4 - Tabela de classificação final

	Observado		**Previsto**		
			Número de caso de cluster		**Porcentagem correta**
			1	2	
Etapa 4	Número de caso de cluster	1	166	22	88,3
		2	20	183	90,1
	Porcentagem global				89,3

Nota. Fonte: dados da pesquisa, 2015.

Com esses resultados, pode-se afirmar o modelo tem capacidade de previsão de 89,3%. Levando em consideração a tabela de classificação ao acaso, o modelo conseguiu incrementar em 37,4%, sendo 89,3 – 51,9.

A partir de tais considerações, na próxima seção, será apresentada as últimas considerações desta pesquisa.

6 CONSIDERAÇÕES FINAIS

Este estudo analisa o papel das punições, comprometimento moral e eficácia percebida como fatores motivadores sobre os comportamentos do indivíduo na segurança da informação de uma IES. Embora tenham sido considerados somente fatores motivacionais extrínsecos e intrínsecos positivos, esse estudo procurou avaliar a influência de vários mecanismos de incentivo na intenção do usuário quanto ao cumprimento de uma Política de Segurança da Informação.

Baseando-se nas inferências realizadas na discussão dos resultados e parágrafos anteriores, as hipóteses do estudo que serviram para a construção do modelo de pesquisa se encontram destacadas na Figura 3.

Figura 3 - Hipóteses do estudo

Hipótese da pesquisa	Status
H1a: *O aumento da severidade da punição contribui na formação de grupos distintos de intenção de seguir a Política de Segurança da Informação da organização.*	Suportada
H1b: *O aumento da certeza de detecção da punição contribui na formação de grupos distintos de intenção de seguir a Política de Segurança da Informação da organização.*	Suportada
H2a: *As crenças normativas contribuem na formação de grupos distintos de cumprimento com as políticas de segurança da informação.*	Não Suportada
H2b: *O comportamento dos pares contribui na formação de grupos distintos de intenção em seguir a Política de Segurança da Informação da organização.*	Não Suportada
H3a: *A eficácia percebida do comportamento de segurança do empregado contribui na formação de grupos distintos de intenção em seguir a Política de Segurança da Informação da organização.*	Suportada
H3b: *O alto comprometimento moral contribui na formação de grupos distintos de intenção em seguir a Política de Segurança da Informação.*	Suportada

Nota. Fonte: elaborado pelos autores, 2015.

As hipóteses estatísticas referentes à *severidade da punição* e *certeza de detecção* foram suportadas porque são fatores que possuem maior contribuição no poder de explicação na variância acumulada aferida pela AFE e por estarem presentes no modelo logístico. A *severidade da punição* apresentou maior grau de contribuição, exercendo influência significativa na formação dos *Cluster*s discriminando os respondentes em dois grupos (os mais predispostos e o menos predispostos a seguir a PSI) apontando um forte indício de que essa variável possui efeito dissuasor para o cumprimento da PSI na organização pelo usuário. Já a *certeza de detecção* é o segundo fator que mais contribui para a explicação do modelo, mais precisamente na medição das diferenças de opiniões entre grupos no *Cluster* não-hierárquico. Isso indica que a pessoa se sentirá mais inclinada a seguir uma política ao saber que é monitorada e, por consequência, haver a possibilidade de punição em caso de comportamento abusivo.

As hipóteses que versavam sobre *comportamento dos pares* e *crenças normativas* não foram suportadas e nem inclusas nas técnicas de análise multivariada. Na primeira, as variáveis desse constructo foram retiradas por revelarem baixas comunalidades e cargas fatoriais na AFE. Já na segunda, as variáveis apresentaram baixa variabilidade no pré-teste, então optou-se pela remoção das questões referentes a esse constructo.

Como estudos futuros, sugere-se estender a aplicação do instrumento em outras IES a fim de verificar o comportamento de segurança dos usuários de uma forma mais ampla, incluindo servidores, técnicos e/ou funcionários na amostra de estudos futuros para que sejam clarificados os fatores cujas variáveis não convergiram de forma plena como preconizado na teoria e possam permitir o incremento na explicação dos modelos de regressão linear múltipla.

Outra recomendação seria replicar a pesquisa com usuários que sejam empregados de organizações a fim de investigar qual é o contexto brasileiro em relação ao cumprimento de normas de segurança e também verificar se emergirão os fatores que não resultaram significantes neste estudo, tais como “comportamento dos pares” e “crenças normativas".

Como implicações práticas, esse estudo proporciona à IES pesquisada e a outras

organizações a possibilidade elaborar uma PSI que contemple todos os perfis de usuários (professores, alunos e servidores) no âmbito de uma universidade. Os resultados revelaram grupos com maior e menor predisposição em seguir as regras, algo que permitirá o planejamento e execução de ações de conscientização e treinamento mais eficiente naquele(s) grupo(s) que se configure(m) menos predisposto(s) a seguir uma política de segurança de informação na organização.

REFERÊNCIAS

Albreschstsen, E. Hovden, J (2009). The information security digital divide between managers and users. *Computers & Security***.** 28(6), 476-490. Retrieved in October 2, 2014, from http://www.sciencedirect.com/science/article/pii/S0167404809000029.

Albuquerque Junior, A. E.; Santos, E. M. (2014a, setembro). Análise das publicações brasileiras sobre segurança da informação sob a ótica social em periódicos científicos *entre 2004 e 2013*. *Encontro Anual da Associação Nacional de Pós-Graduação em Administração*, Rio de Janeiro, RJ, Brasil, 38.

Albuquerque Junior, A. E.; Santos, E. M. (2014b, maio) Produção científica sobre segurança da informação em eventos científicos brasileiros. *International Conference on Information Systems and Technology Management*, São Paulo, SP, Brasil, 11.

Albuquerque Junior, A. E.; Santos, E. M. (2013, setembro). Produção científica sobre segurança da informação em anais de eventos da ANPAD. *Encontro de Administração da Informação*, Bento Gonçalves, RS, 4.

Appel-silva, M.; Welter, G.; Argimon, I. L. (2010). A teoria da autodeterminação e as influências socioculturais sobre a identidade. *Psicol. rev.* (Belo Horizonte). 16(2),351-369. Recuperado em 04 novembro, 2013, de http://pepsic.bvsalud.org/scielo.php?script=sci_arttext&pid=S1677-11682010000200008&lng=pt&nrm=iso

Aronson, E.; Wilson, T. D.; Arket, R. M. (2002). *Psicologia Social* (3ª ed.). Rio de Janeiro: LTC.

Baltzan, P.; Phillips, A. (2012). *Sistemas de Informação***.** McGraw Hill: Porto Alegre, 2012.

D'Andrea, E. R. P. (2004) *Segurança da Informação: uma visão estratégica para as organizações*. (Albertin, A. L.; Moura, R. M.,org.). (Tecnologia de Informação). São Paulo, Atlas,

Datt, F. Empresas se armam para combater fraudes.(2012) *Assurance Journal***.** (Publicação do Departamento Marketing da Ernst & Young Terco). 17, 14-25.Recuperado em 14 novembro, 2013 de http://www.ey.com.br/Publication/vwLUAssets/Assurance_17_PDF/$FILE/Assurance.journal_n.17_Julho_Agosto.pdf

D'arcy, J.; Hovav, A.; Galletta, D (2009). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. *Information Systems Research***.** 20 (19), 79-88. Mar. Retrivied in November 8, 2013, from http://pubsonline.informs.org/doi/abs/10.1287/isre.1070.0160.

Doherty, N. F.; Fulford, H. Aligning the information security policy with the strategic information systems plan. *Computers & Security*,*(*25),55-63, 2005. Retrieved in November 2, 2013, fromhttp://ac.els-cdn.com/S0167404805001720/1-s2.0-S0167404805001720-main.pdf?_tid=4e1be27a-4442-11e3-b442-00000aacb35d&acdnat=1383453914

Furnell, S; Thomson; K. L. (2009). From culture to disobedience: recognizing the varying user acceptance of IT security. *Computer Fraud & Security*. (2), 5-10. Retrieved in April 9, 2013, from http://www.sciencedirect.com/science/article/pii/S1361372309700193

Gaunt, N. (1998) Installing an appropriate information security police. *International Journal of Medical Informatics***.** 49(1),131-134. Retrieved in June 15, 2014, from http://www.ijmijournal.com/article/S1386-5056(98)00022-7/abstract

Hair Jr, J. F.; Black, W. C.; Babin, B. J., Anderson; R. E.; Tatham, R. L. (2009) *Análise multivariada de dados***.** (6.ed). Porto Alegre: Artmed.

Herath, T.; Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*.47, 154-165, ed in April 09, 2013 from

http://www.sciencedirect.com/science/article/pii/S0167923609000530

Höne, K.; Eloff, J.H.P. Information security policy (2002) – what do international information security standards say? *Computers & Security*, 21 (5), 402-409. Retrieved in November 03, 2013, from http://www.sciencedirect.com/science/article/pii/S0167404802005047

IBGE (2013, dezembro). *Sala de imprensa: Acesso à internet e posse de telefone móvel celular para uso pessoal em 2011*. Recuperado em 14 fevereiro, 2014 de http://ftp.ibge.gov.br/Acesso_a_internet_e_posse_celular/2011/PNAD_Inter_2011.pdf

Loiola, R. (2009, outubro). Geração Y. *Revista Galileu***,** 219/comportamento. p. out 2009. Recuperado em 30 novembro, 2014, de http://revistagalileu.globo.com/Revista/Galileu/0,,EDG87165-7943-219,00-GERACAO+Y.html

Maciel, C. O.; Camargo, C. (2011). Comprometimento, satisfação e cooperação no trabalho: evidências da primazia dos aspectos morais e das normas de reciprocidade sobre o comportamento. *Revista de Administração Contemporânea*. 15(3), 433-453. Recuperado em 04 novembro, de Disponível em: http://www.anpad.org.br/periodicos/arq_pdf/a_1188.pdf

Mattord, H. J; Whitman, M. E (2004). Improving Information Security Through Policy Implementation" *SAIS 2004 Proceedings*. Paper 41. Retrieved in August 20, 2013 in: http://aisel.aisnet.org/sais2004/41

Marôco, J. (2007) *Análise estatística com utilização do SPSS*. (3ª ed.). Lisboa: Sílabo.

Meyer, J.P.; Allen, N. J. (1991) A three-component conceptualization of organizational commitment. *Human Resource Management Review*. 1(1),61-89. Retrivied in October 30, 2014 in http://cyb.ox.or.kr/lms_board/bbs_upload/%C1%B6%C1%F7%B8%F4%C0%D4-%B1%B9%BF%DC%B3%ED%B9%AE.pdf

Mendonça, H. (2015, fevereiro 23). Conheça a geração z: nativos digitais que impõem desafios às empresas. *El País Brasil*, carreira. Recuperado em 10 março, 2016, de http://brasil.elpais.com/brasil/2015/02/20/politica/1424439314_489517.html

Pahnila, S.; Siponen, M.; Mahmood, A. (2007, January). Employees' Behavior towards IS Security Policy Compliance. *Proceedings of the 40th Hawaii International Conference on System Sciences*, Waikoloa, Big Island, HI,3-6. Retrieved in November 4, 2013 in http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.106.7038&rep=rep1&type=pdf"type=pdf

Parasuraman, A.(2000) Technology Readiness Index (Tri): a multiple item scale to measure readiness to embrace new Technologies. *Journal of Service Research*. 2(4), 307-320. Retrieved in July 16, 2015, from http://jsr.sagepub.com/content/2/4/307.abstract

Pereira, F. A. M. (2013). A *satisfação e a intenção de continuidade de uso em serviços de e-learning: validação empírica de um modelo aplicado no serviço público*. Dissertação de mestrado, Universidade Federal do Rio Grande do Norte, Natal, RN, Brasil.

PWC. (2013). *Principais resultados da Pesquisa Global de Segurança da Informação 2013 – The Global State of Information Security Survey 2013*. Brasil. Recuperado em 5 novembro, 2014, em http://www.pwc.com.br/pt_BR/br/estudos-pesquisas/assets/pesquisa-seguranca-inforrmacao-13.pdf

PWC. (2014). *Principais resultados da Pesquisa Global de Segurança da Informação 2014 - The Global State of Information Security Survey 2014*. Brasil: 2014. Recuperado em 14 junho, 2015, em http://www.pwc.com.br/pt_BR/br/estudos-pesquisas/assets/pesquisa-seguranca-inforrmacao-14.pdf

Rodrigues, A.; Assmar, E. M. L.; Jablonski, B. (2012) *Psicologia social***.** (29ª ed). Petrópolis: Vozes.

Silva Netto, A.; Silveira, M. A. P. (2007). Gestão da segurança da informação: fatores que influenciam sua adoção em pequenas e médias empresas. *Journal of Information Systems and Technology Management (Online)*.4 (3), 375-397. Retrieved in November 28, 2013, from http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1807-17752007000300007&lng=en&nrm=iso.

Thomsom, K.; Nierkek, J. V. (2012) Combating information security apathy by encouraging prosocial organisational behaviour. *Information*

Management & Computer Security. 20 (1), 39-46. Retrieved in May 8, 2012, from www.emeraldinsight.com/0968-5227.htm.

Viapiana, L.T. (2006) *Economia do crime: uma explicação para a formação do criminoso*. Porto Alegre: AGE,

Von Solms, B. (2001) Corporate governance and information security. *Computers & Security*. 20(3), 215-218. Retrieved in May 15, 2013, from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.103.1168&rep=rep1&type=pdf.