ADOÇÃO DE PRÁTICAS DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO: UM ESTUDO COM GESTORES PÚBLICOS

ADOPTION OF SECURITY INFORMATION MANAGEMENT PRACTICES: A STUDY WITH PUBLIC MANAGERS

Anna Cláudia dos Santos Nobre
Governo do Estado do RN - Secretaria da Administração e dos Recursos Humanos (SEARH)

Mestre em Administração pela Universidade Federal do Rio Grande do Norte
Endereço: Rua Anibal Correia, 3260. Candelária - Natal/RN. CEP: 59064-340
Telefone: (84) 2010-2504 / 9116-1541.
E-mail: nobre@rn.gov.br / annacsnobre@gmail.com
Lattes: http://lattes.cnpq.br/4758823921043608

Anatália Saraiva Martins Ramos
Universidade Federal do Rio Grande do Norte

Doutora em Engenharia de Produção pela Universidade Federal do Rio de Janeiro
Endereço Avenida Afonso Pena, 1224. Tirol. CEP 59020-265 Natal-RN
Telefone: (84) 8807-3324 / (84) 3216-3536
E-mail: anatalia@ufrnet.br
Lattes: http://lattes.cnpq.br/1151025937054810

Thiago Cavalcante Nascimento
Universidade Federal do Paraná

Doutorando em Administração pela Universidade Federal do Paraná - UFPR
Endereço: Rua Urbano Lopes, 60. Cristo Rei. CEP: 80050-520 Curitiba – PR
Telefone: (41) 9878-2523
E-mail: thiagocn1@hotmail.com
Lattes: http://lattes.cnpq.br/9661555663056683

Data de submissão: 28 Mai. 2011. **Data de aprovação**: 30 Out. 2011. **Data da publicação**: 19 Dez. 2011. **Sistema de avaliação**: *Double blind review*. Centro Universitário UNA. Prof. Dr. Mário Teixeira Reis Neto, Profª. Dra. Wanyr Romero Ferreira

Resumo

O presente estudo tem por objetivo verificar os fatores que influenciam a adoção de práticas avançadas de gestão da segurança da informação por gestores públicos estaduais no Brasil. Argumenta que a informação possui, cada vez mais, papel de destaque nas organizações, sendo imprescindível a utilização de técnicas de gestão que deem maior segurança ao seu uso. O quadro teórico do estudo utilizou, como base, os postulados do *Technology Acceptance Model* - TAM de autoria de Davis, Bagozzi, Warshaw (1989) e os processos preconizados na Norma ISSO/IEC 27001. Metodologicamente, adotou-se uma abordagem quantitativa de análise por meio de técnicas descritivas e inferenciais, como medidas de tendência central, análise fatorial e regressões lineares. Os resultados evidenciam que a idade média dos gestores é de aproximadamente 43 anos e que 70% possuem algum tipo de pós-graduação concluída. Quanto aos resultados da análise inferencial, os construtos 'percepção de utilidade em adotar práticas de segurança', 'atitude frente às práticas de segurança' e 'intenção de utilização de práticas de segurança' confirmaram ser influentes na aceitação dos gestores estaduais do PNAGE, quanto a práticas mais avançadas de controle de acesso e de controle de recursos humanos para a

segurança da informação. Apenas o construto 'facilidade de uso' não foi um bom preditor do nível de concordância com as práticas preconizadas pela Norma ISO/IEC 27001. Espera-se que este estudo possa subsidiar futuras políticas de segurança de informação, especialmente, quando formulada para obter adesão de gestores das áreas foco desta pesquisa (planejamento e gestão).

Palavras-Chave: Segurança da Informação; Adoção de Tecnologias; Gestão Pública.

Abstract

This paper aims to identify which factors influence the adoption of management security information advanced practices by state public managers in Brazil. Argues that information has increasingly proeminent role in organizations, being imperative to use management techniques that give greater security to its use. The theoretical reference of the paper was based on the postulates of the Technology Acceptance Model - TAM authored by Davis, Bagozzi, Warshaw (1989) and the procedures recommended in accordance with ISO/IEC 27011. Methodologically, was adopted a quantitative aproach of analysis using descriptive and inferential techniques, like measures of central tendency, factor analysis and linear regression. The results show that the average age of managers is approximately 43 years and that 70% have some type of postgraduated course completed. About the results of inferential analysis, the constructs "perceived usefulness of adopting safety practices", "attitude toward the safety practices" and "intention to use safety practices" confirmed to be influential in the acceptance of PNAGE's state managers on the practice more advanced access control and control of human resources for information security. Only the construct 'ease of use' was not a good predictor of the level of agreement with the practices recommended by ISO / IEC 27001. It is hoped that this study can support future information security policies, especially when formulated for adhesion to the managers of this research focus areas (planning and management).

Keywords: Information Security; Technology Adoption; Public Management.

1. Introdução

A informação pode ser considerada um dos bens mais valiosos dentro de qualquer organização. Manter esse bem seguro, confiável e acessível a todos os que dela têm direito ao acesso passou a ser um fator fundamental, bem como um diferencial que poderá possibilitar sua sobrevivência no mercado. A segurança dos dados de uma empresa inclui desde a preservação da integridade dos equipamentos até as informações que estão armazenadas neles. Falhas nessa estrutura podem resultar em quebras da confidencialidade, através de acesso por pessoas não autorizadas; da integridade, através de alteração indevida de dados; e da disponibilidade, com a acessibilidade não permitida a quem é autorizado (MOREIRA, 2001, SÊMOLA, 2003; CAMPOS, 2006; LUCAS JR., 2006). Fatores como a alta conectividade, através do uso de redes de computadores e da *internet*, aumentaram a vulnerabilidade das empresas e sua preocupação com tais falhas.

Gerenciar adequadamente as informações, atendendo aos requisitos de segurança dos dados, é uma necessidade inadiável. Uma medida importante é a adoção de normas ou código de práticas. A ABNT (Associação Brasileira de Normas Técnicas), em sintonia com a Organização Internacional para Normalização (International Organization for Standartization – ISO), elaborou a versão brasileira da norma ISO 27001, relativa à segurança da informação (SI), que promove a adoção de uma abordagem de processo para estabelecer e implementar, operar, monitorar, analisar criticamente, manter e melhorar o Sistema de Gerenciamento da Segurança da Informação - SGSI de uma organização.

Nas últimas décadas, o debate sobre a questão da Segurança da Informação e da sua governança tem aumentado no meio empresarial, havendo reflexos na produção científica. No cenário acadêmico nacional, há relativamente poucos trabalhos em Gestão de Segurança da Informação. A literatura encontrada na área de Segurança da Informação é mais de cunho técnico que gerencial. Mesmo os gerenciais direcionam-se ao estudo de casos e setores específicos (RAMOS; FEIJÓ, 2004; LESSA, 2004; MENEZES, 2005; LIMA, 2006; BAUER, 2006; SILVA NETTO, 2007; SOUZA, 2007; LORENS, 2007; FRÓIO, 2008). Também são escassos os estudos brasileiros que levam em consideração os fatores comportamentais na adoção e difusão de códigos de práticas de segurança com base na norma ISO/IEC, podendo ser citados os trabalhos de Gabbay (2003), Oliva e Oliveira (2003) e Ramos e Cavalcante (2005). Portanto, do ponto de vista científico, esta é uma área do conhecimento que tem lacunas e necessita de mais estudos e pesquisas.

No que se refere aos estudos sobre adoção, aceitação e implantação de tecnologias e sistemas de informação nas organizações, existem diversos modelos de verificação de aceitação de tecnologia por parte dos usuários. Uma das abordagens teóricas mais conhecidas é a do modelo de aceitação de tecnologia (*Technology Acceptance Model* - TAM). Tanto o modelo TAM quanto suas adaptações e as teorias que lhe deram origem foram testadas em vários tipos de organizações e para as mais diversas áreas, como ERP, *E-learning*, Compras *online*, *Internet Banking*, caixas automáticos, voz sobre IP, dentre outras (VENKATESH; DAVIS, 1996; MORRIS; VENKATESH, 2000; CHAU; LAI, 2003; BUENO; ZWICKER; OLIVEIRA, 2004; SANTOS; AMARAL, 2004; ALMEIDA; SOBRAL, 2005; CARVALHO; FERREIRA, 2005; BROWN; VENKATESH; BALA, 2005; LÖBLER; VISENTINI; VIEIRA, 2006; RODRIGUES; COSTA, 2006; PIRES; YAMAMOTO; COSTA FILHO, 2006; SILVA; DIAS, 2006; OLIVEIRA JUNIOR, 2007; OLIVEIRA; RAMOS, 2008; SILVA; DIAS; SENA JUNIOR, 2008; SILVA, 2009).

Apesar de muito ricos, existem poucos estudos, utilizando o modelo de aceitação de tecnologia ou suas adaptações para a área de Gestão de Segurança da Informação em particular. Emanavin (2004), Appunn (2008), Shropshire (2008) e Jones (2009) foram referências encontradas na literatura que abordam a aceitação de tecnologia na perspectiva da gestão da segurança de informação, especificamente, com foco no comportamento das pessoas ou de usuários.

Os estudos pesquisados também evidenciaram uma lacuna de estudos específicos voltados para a ótica do setor público. Tendo em vista as especificidades legais e culturais que diferem o setor público do privado. Em organizações públicas, problemas relacionados à segurança de dados tomam proporções maiores por afetarem um número maior de pessoas, já que todos os cidadãos devem ter acesso e utilizar os serviços ofertados pelos órgãos de governo. Outra preocupação específica da área pública é a viabilidade de uma estrutura segura, mas ágil e que não sofra descontinuidade pelas dificuldades de contratação impostas pela legislação.

Diante da problemática exposta, verifica-se a importância de estudos que relacionem os gestores públicos com as práticas de Gestão de Segurança da Informação, uma vez que a adoção de práticas nas organizações públicas depende fortemente do apoio ou decisão de tais gestores. Dessa forma, este estudo teve por objetivo identificar quais fatores influenciam os gestores públicos estaduais em relação à aceitação de práticas avançadas de Gestão da Segurança da Informação.

2. Referencial teórico

Nesta seção, é feita uma breve exposição dos conceitos relacionados com a gestão da segurança da informação, os modelos de certificação em segurança da informação e a norma de segurança ISO/IEC 27001. Em seguida, os conceitos de Aceitação de tecnologia

e sistemas são revistos e, por fim, é apresentado o modelo de pesquisa desenvolvido a partir das relações estabelecidas entre os construtos investigados.

2.1 Segurança da informação e modelos de certificação

Os princípios da Segurança da Informação são os conceitos que norteiam todas as ações nessa área. Os mais citados são a confidencialidade, no qual a informação somente pode ser acessada por pessoas autorizadas; a disponibilidade, no qual a informação ou sistema de computador deve estar disponível a quem possa acessá-la no momento em que a mesma for necessária; e a integridade, que é a proteção dos dados ou informações contra modificações intencionais ou acidentais não-autorizadas.

Sêmola (2003) alerta a importância de estar atento aos princípios em todos os momentos do ciclo de vida da informação (manuseio, armazenamento, transporte e descarte). Com a adoção de políticas e estratégias de segurança eficientes, as organizações pretendem obter: maior padronização das informações e processos; alinhamento dos objetivos do órgão com as leis e obrigações contratuais; definição dos responsáveis pelos ativos do órgão; definição das penalidades pela não aderência à Política de Segurança; aumento da conscientização da empresa; aderência aos padrões internacionais de gestão de segurança; Segurança dos processos do negócio; retorno do investimento por meio de redução de acidentes; e consolidação da imagem de uma empresa segura (TURBAN; RAINER; POTTER, 2003). No entanto, segundo Ramos e Cavalcante (2005), adotar práticas mais avançadas de segurança de informação não é trivial, devido à complexidade, ao custo e ao tempo de implantação de tais políticas.

A informação é um recurso importante nas organizações e sua proteção de ataques externos e internos é o objetivo da segurança computacional. Devido ao crescimento da importância da informação como ativo de valor, as organizações vêm adotando diversas práticas (também denominadas técnicas, medidas, códigos ou métodos) para promover a política de Segurança da Informação. As práticas mais citadas são resumidas, a seguir, em ordem cronológica, conforme Solms (1999).

O mais antigo é o *Trusted Computer Security Evaluation Criteria* (TCSEC), que foca em critério de funcionalidade, efetividade e garantia (ou confiabilidade). Após a publicação do TCSEC, a Comissão das Comunidades Européias publicou o *Information Technology Security Evaluation Criteria* (ITSEC) em 1990. Após extensa revisão internacional, a versão 1.2 foi posteriormente publicada, em junho de 1991, pela Comissão das Comunidades Europeias, para a utilização operacional dentro de avaliação e de sistemas de certificação. Outro código de práticas que se destaca é o *Canadian Trusted Computer Products* (CTCPEC). Trata-se de uma norma de segurança da informação publicada em 1993 pela Instituição de Segurança das Comunicações do Canadá, para fornecer uma avaliação de critérios de produtos de TI.

Os padrões CTCPEC, ITSEC e TCSEC formam a base para a criação da norma *Common Criteria*, padrão que consiste de um *framework,* no qual os usuários podem especificar os requisitos de segurança e os laboratórios podem avaliar os produtos para determinar se eles realmente satisfazem as reivindicações. Os órgãos de certificação em cada país são responsáveis por atestar a adoção de critérios e normas estabelecidos pelos padrões de Segurança da Informação. No Brasil, o órgão responsável é a Associação Brasileira de Normas Técnicas (ABNT). A Norma ISO/IEC 27001:2005 é uma das mais recentes normas de Segurança da Informação e, por isso, foi adotada nesta pesquisa.

A ISO (*International Organization for Standartization*) é uma organização internacional que trata de normalização, cujo objetivo é criar normas e padrões universalmente aceitos sobre as mais diversas atividades comerciais, industriais, científicas e tecnológicas. Já o IEC (*International Engineering Consortium*) é uma organização internacional sem fins lucrativos que funciona basicamente através de parcerias entre as universidades e indústrias, promovendo o desenvolvimento de pesquisas inovadoras e programas de serviços em engenharia (IEC, 2008).

Na área de Segurança da Informação, a norma mais recente certificada pelas duas organizações (ISO e IEC) é a 27001. Publicada em 2005, é um código com as melhores práticas de segurança em TI. Ela resulta da revisão de sua antecessora, a Norma ISO/IEC 17799:2000, que, por sua vez, está ligada à norma Britânica BS 7799 de 1995. Em 2000, a Norma foi votada e aprovada pelo órgão, resultando na publicação da Norma ISO/IEC 17799:2000. Já a série ISO/IEC 27000 é mais recente e passou por ajustes. Ela pretende contemplar todos os aspectos da segurança da informação. O planejamento das ações relativas à norma deve atender a um conjunto de requisitos que fazem parte de seus capítulos, cada qual abordando um aspecto da segurança da informação. Essa norma alinha-se com as outras normas, como a ISO 9000 (gestão da qualidade) e a ISO 14000 (gestão ambiental).

Nesta pesquisa, foi adotada a norma ISO/IEC 27001 brasileira, que foi publicada em outubro de 2005, cujo objetivo é proporcionar um modelo para a criação, aplicação, funcionamento, acompanhamento, revisão, manutenção e melhoria do Sistema de Gestão da Segurança da Informação. A Norma ISO/IEC 27001:2005 define o seu "processo de abordagem", empregando o modelo PDCA (*Plan-Do-Check-Act*) para os processos, composta das seguintes seções: a) Gestão de Responsabilidade; b) Auditorias internas; c) Melhorias para SGSI; d) Anexo A - objetivos dos controles e controles; e) Anexo B - princípios da OCDE e norma internacional; f) Anexo C - correspondência entre ela e a ISO 9001 e ISO 14001.

Os objetivos de controle, também conhecidos como domínios da referida norma, são divididos nas seguintes áreas: Política de Segurança (A5); Organização da Segurança da Informação (A6); Gestão de Ativos (A7); Gestão de Recursos Humanos (A8); Segurança do Ambiente Físico (A9); Gerenciamento de Comunicação e Operação (A10); Controle de Acesso (A11); Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação (A12); Gestão de Incidentes (A13); Gestão de Continuidade do Negócio (A14) e Aderência (A15). Devido à restrição de espaço, não será caracterizado com detalhes o conteúdo dos controles de cada uma desses domínios da Norma.

Para efeito desta pesquisa, foram escolhidas como práticas relevantes às relativas aos capítulos ou domínios da norma referentes à Controle de Acesso (A11) e Recursos Humanos (A8). O domínio de Controle de Acesso tem sete partes: normas de controle de acesso; gerenciamento dos usuários; responsabilidades dos usuários; controle de acesso em rede; controle de acesso em sistema operacional; controle de acesso em aplicativos e informação; computação móvel. Os objetivos de controle para Recursos Humanos são organizados em três partes: a primeira relata recomendações de atitudes a serem adotadas antes da contratação dos funcionários para a organização; a segunda trata dos funcionários contratados; e a terceira trata de funcionários que já deixaram a organização.

Tal escolha justifica-se com base no fato de que tais premissas são geralmente as primeiras trabalhadas na implementação de uma política de segurança e suas práticas são facilmente compreensíveis por público não especialista em TI, que é o que se pretende atingir com este trabalho. Assim, procurou-se eliminar o viés de grande número de respostas do tipo “desconheço” por parte dos respondentes que não são da área de TI.

2.2 Adoção e aceitação de tecnologia

Além dos conceitos de Segurança da Informação apresentados, o outro pilar teórico deste trabalho está relacionado com a questão da aceitação de tecnologia, tendo em vista que a pesquisa estuda os fatores que podem influenciar a adoção/**aceitação** de práticas relacionadas à tecnologia da informação.

Um dos modelos mais conhecidos e testados é o modelo TAM – *Technology Acceptance Model*, que há mais de vinte anos vem sendo utilizado em diversas áreas de atuação para verificar a aceitação de tecnologias e sistemas de informação e se seus construtos estão em constante avaliação e testes. Um pressuposto essencial do Modelo TAM baseia-se nos fundamentos da Teoria de Ação Racional (*TRA – Theory of Reasoned Action*), desenvolvida por Martin Fishbein e Icek Aizen entre 1975 e 1980. Essa teoria preconiza que parte

significativa do comportamento humano tem fundamento racional que o torna previsível pela intenção de agir (ALMEIDA; SOBRAL, 2005). Segundo o modelo TRA, um comportamento deriva de uma intenção, que, por sua vez, deriva de atitudes e normas subjetivas. Essas atitudes e normas subjetivas resultam em crenças e motivações para um determinado comportamento. Além da Psicologia, a base teórica do TAM inclui conceitos de outras áreas como Sociologia e Gestão Organizacional (SANTOS; AMARAL, 2004).

A proposta do modelo de aceitação de tecnologia é traçar o impacto de variáveis em crenças, atitudes e intenções, com base em construtos que interferem na aceitação de tecnologias, conforme FIG. 1.

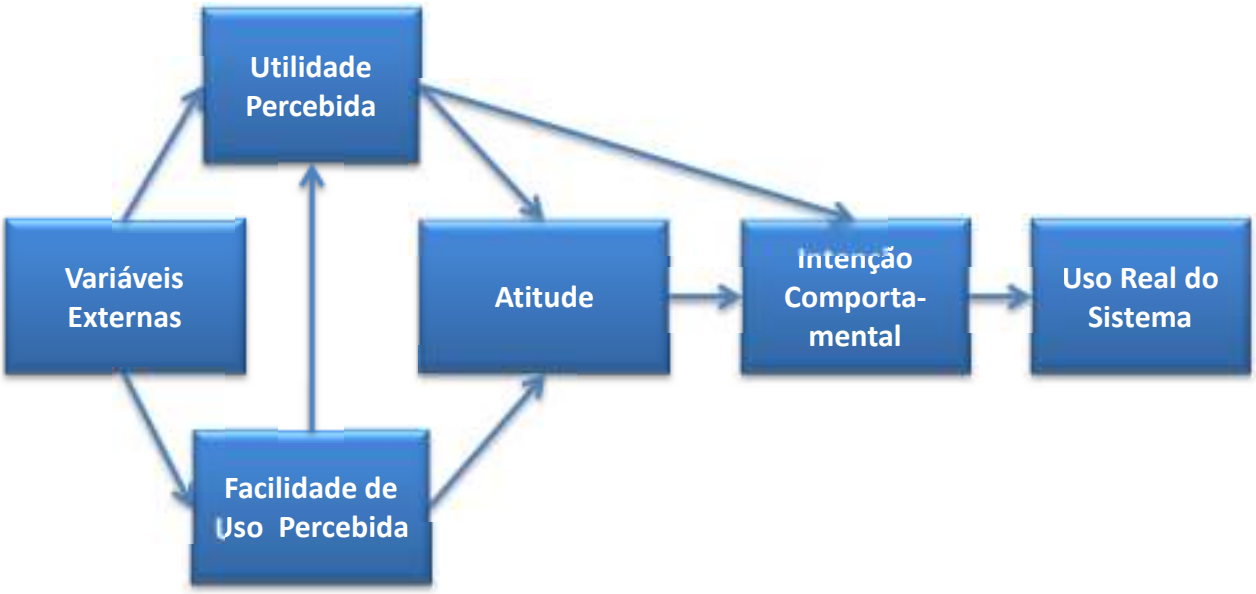

FIGURA 1. Relação dos construtos do modelo TAM
Fonte: Davis; Bagozzi,; Warshaw (1989)

O TAM sustenta-se em dois construtos baseados na crença, que são a facilidade de uso percebida e a utilidade percebida (DAVIS; BAGOZZI,; WARSHAW, 1989). A **facilidade de uso percebida** refere-se à expectativa do usuário de tecnologia na isenção de esforço físico ou mental com seu uso, enquanto a **utilidade percebida** pode ser definida como uma probabilidade verificada de que o desempenho do usuário de tecnologia melhore com sua utilização. Esse construto mede o grau de utilidade ou benefício gerado pelo novo sistema ou nova sistemática adotada.

O modelo TAM permite a análise da relação entre a facilidade de uso percebida e a utilidade percebida com outros construtos. O construto **atitude** é definido como um sentimento individual (positivo ou negativo) em relação a um comportamento que se tenha. Oliveira Junior (2007) destaca que não houve medição completa entre tal construto e os outros dois (facilidade de uso e utilidade percebida) e, portanto, não o destaca como tão relevante no modelo.

A **intenção comportamental** é entendida como o grau em que uma pessoa tem intenção de desempenhar determinado comportamento. Alguns estudos colocam-na como função direta da utilidade percebida, sem considerar o construto atitude.

Dias, Zwicker e Vicentin (2003) destacam, como limitações do Modelo TAM, a impossibilidade de analisar o contexto organizacional e avaliar apenas um sistema específico e não opções de sistemas distintas, mas suportam que tal modelo pode ser utilizado como importante ferramenta gerencial nas organizações. Já Rodrigues e Costa (2006) alertam que são os indivíduos que atuam e modificam as práticas, reforçando a importância de estudá-los juntamente com o modelo. Uma utilidade prática do modelo TAM

foi apresentada por Silva e Dias (2006), na qual gerentes utilizaram-se de tal modelo para ampliar um de seus construtos, a utilidade percebida.

O TAM combina-se com outros modelos ou amplia-se por diversos autores para testar hipóteses. Dessa forma, outros modelos têm sido propostos como adaptações do Modelo TAM, consistindo em detalhar algum construto ou incluir um novo, mas a base permanece a mesma, que é a verificação de fatores que interferem na adoção de tecnologias. Um exemplo é o estudo de Almeida e Sobral (2005), que é baseado no Modelo TAM e nas Teorias TRA e TPB. Eles propuseram o Modelo Organizacional de Atitudes perante a Tecnologia da Informação (MOATI), que inclui variáveis relacionadas ao processo estrutural da organização que influenciam na tomada de decisão, particularmente adaptado ao dirigente empresarial.

Venkatesh e Davis (2000) propuseram uma versão mais complexa do modelo original, o TAM2, que acrescenta outras variáveis aos modelos e possibilita análises mais detalhadas dos fatores que influenciam na aceitação e adoção de tecnologias. O modelo TAM2 testa outros relacionamentos. No caso da utilidade percebida, pode-se verificar sua influência por variáveis como: norma subjetiva, imagem, relevância do trabalho, qualidade do resultado e demonstrabilidade do resultado. A norma subjetiva oriunda do TRA é utilizada como impulsionador da intenção de uso, já presente no modelo TAM original, porém sofrendo influência da voluntariedade. Dessa relação, pode-se extrair que as normas subjetivas são relevantes em situação de uso obrigatório, mas não de uso voluntário.

Dando sequência aos estudos nessa área, Venkatesh, Morris, Davis e Davis (2003) propuseram e testaram um modelo unificado que integra os elementos de oito modelos que abordam a aceitação da tecnologia, desenvolvendo, assim, a Teoria Unificada de Aceitação e Uso da Tecnologia (UTAUT). Os autores sugerem quatro construtos para explicar a aceitação individual de uma nova TI: a expectativa de performance, a expectativa de esforço, as condições facilitadas e a influência social.

Mais recentemente, estendendo os domínios teóricos do TAM, Venkatesh e Bala (2008) descrevem o TAM3, no qual acrescentam algumas variáveis como influenciadores da Facilidade de Uso Percebida, a saber: de fundamento ou base (ansiedade computacional, autoeficácia em ambiente tecnológico, percepção de controle e diversão em ambiente tecnológico) e os de sistematização (Usabilidade Objetiva e Prazer Percebido).

Há poucas pesquisas que aliam os dois assuntos desta pesquisa: Aceitação de Tecnologia e Segurança da Informação. Foram encontradas na literatura as referências de pesquisas de Emanavin (2004) e Appunn (2008), as quais testaram e validaram os construtos do modelo UTAUT, para verificar a intenção de adoção de práticas de Segurança da informação.

O modelo adotado nesta pesquisa baseia-se no modelo de aceitação de tecnologia clássico e sua representação é detalhada na FIG. 2.

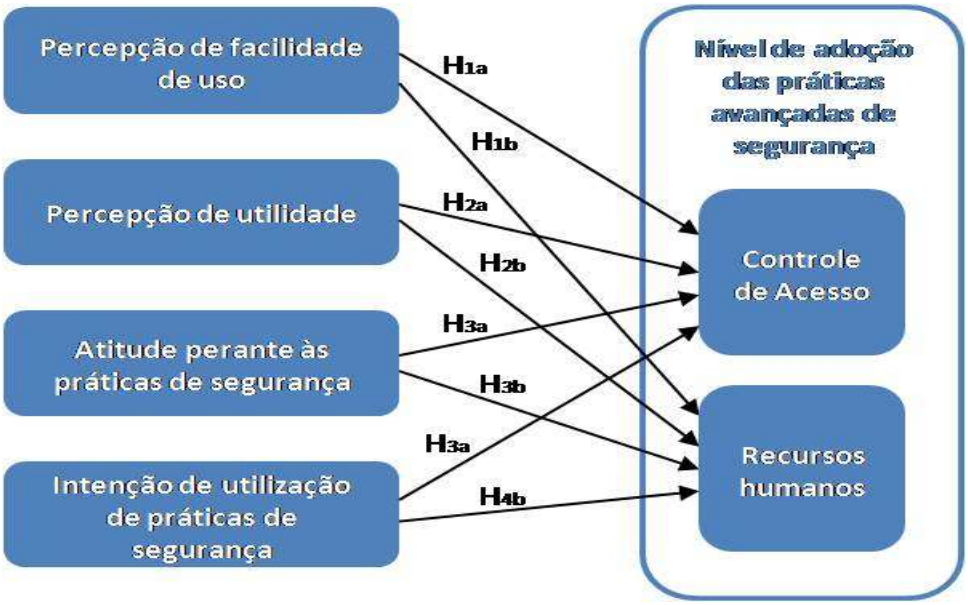

FIGURA 2 – Modelo Proposta da Pesquisa
Fonte: Elaboração própria

Na presente pesquisa, optou-se por não testar os relacionamentos em uma modelagem de equações estruturais e deu-se preferência pelo relacionamento entre duas variáveis, utilizando a análise de regressão linear. Também não foram testadas variáveis externas.

A proposta consiste em testar o relacionamento entre quatro variáveis independentes com a variável dependente que é representada pelo nível de concordância com serviços e controles de segurança, baseados na norma ISO/IEC 27001:2005. Essa variável dependente representa o nível de concordância sobre a adoção de práticas de SI que será gerado através de análise fatorial das assertivas da Norma, extraídas para as categorias *Controle de Acesso* e *Recursos Humanos*. Já as variáveis independentes são adaptadas de Davis, Bagozzi e Warshaw (1989).

3. Procedimentos metodológicos

Para a consecução do objetivo deste estudo de verificar os fatores que influenciam as percepções dos gestores públicos estatuais sobre a aceitação de práticas avançadas de gestão da segurança da informação, adotou-se uma postura metodológica hipotético-dedutiva. Do ponto de vista de seu objetivo, a pesquisa é descritiva; quanto à abordagem do problema, é de natureza quantitativa. Os dados da pesquisa foram obtidos através de pesquisa de campo do tipo levantamento de dados (*survey*).

Quanto ao universo da pesquisa, o estudo foi endereçado aos gestores públicos estaduais que coordenam, em seus respectivos estados, o Programa Nacional de Apoio à Modernização da Gestão e do Planejamento dos Estados e do Distrito Federal – PNAGE. Esses gestores públicos são responsáveis por ações transversais do governo como o planejamento e a gestão. Esse público é constituído de gestores que **não** são especialistas em TI. De uma população de 97 gestores cadastrados no PNAGE, houve resposta de 80 indivíduos, englobando uma amostra de gestores de todos os estados da Federação e do Distrito Federal, com exceção do estado de Goiás, conforme se verifica na TAB. 1.

TABELA 1 – Quantitativos da Amostra por estado e número de questionários respondidos

Centro-oeste	N	Nordeste	N	Norte	N	Sudeste	N	Sul	N
Distrito Federal	04	Alagoas	04	Acre	03	Esp. Santo	03	Paraná	03
Goiás	0	Bahia	04	Amazonas	04	Minas Gerais	04	RS	04
MS	01	Ceará	04	Amapá	04	RJ	04	SC	03
Mato Grosso	01	Maranhão	02	Rondônia	01	São Paulo	02		
		Paraíba	04	Roraima	03				
		Pernambuco	03	Tocantins	04				
		Piauí	02	Pará	02				
		RN	03						
		Sergipe	04						

Fonte: Resultados da Pesquisa (2010)

Essa amostra pode ser considerada não-probabilística, devido à seleção dos indivíduos ter ocorrido de acordo com o critério de acessibilidade. No entanto, a taxa de retorno representa uma amostra com menos de 5% de margem de erro para um nível de confiança de 95%. Os meios utilizados para devolução dos questionários respondidos deram-se da seguinte forma: 41 pessoalmente, 12 por fax, 27 por *e-mail*. A forma de entrega predominante foi pessoalmente (51,3%), porque a pesquisadora contatou os Coordenadores por ocasião da reunião trimestral do Colegiado Técnico Consultivo do PNAGE, realizado em Recife, no mês de setembro de 2008. Se um(a) determinado(a) coordenador(a) não estivesse presente no evento, era solicitado ao seu colega de estado que intermediasse a entrega do questionário, para que, posteriormente, o mesmo fosse devolvido por outros meios (*e-mail* ou *fax*).

Como instrumento de coleta de dados, foi aplicado um questionário estruturado, com todas as questões fechadas, contendo quatro partes. A primeira parte identificou dados organizacionais, como tipo e setor de atuação da organização, a unidade da federação, o parque de informática, o número estimado de usuários que acessam a rede de computadores, a ocorrência anterior de ataques à segurança e a vinculação do setor responsável pela segurança da informação. A segunda parte do questionário referiu-se aos dados demográficos, como idade, sexo, nível de escolaridade, conhecimento de informática, tipo de treinamento em segurança de informação, papel desempenhado na adoção de TI na organização, uso da rede para acessar contas pessoais e prática de realização de *backups*.

Compondo a terceira parte do questionário, encontravam-se as variáveis dependentes, as quais foram adaptadas do TAM. Tem como objetivo obter respostas com relação a crenças e percepções relacionadas com os construtos Facilidade de uso, Utilidade e Atitude perante as práticas de Segurança de práticas de Segurança. São dois itens para cada construto. As escalas desses seis itens são do tipo *Likert* em cinco níveis de gradação, desde o “discordo totalmente” até o “concordo totalmente”. Ainda, nessa parte, o respondente é indagado sobre sua intenção comportamental de utilização das práticas de Segurança da Informação. A escala dessas duas perguntas do questionário tem cinco níveis de gradação, desde o “altamente improvável” até o “altamente provável”.

Na última parte do questionário, foram dispostos 20 itens com assertivas que visavam a identificar o grau de concordância do gestor público quanto à adoção de práticas avançadas de segurança da informação, com foco nos controles de Acesso e de Recursos humanos. A escala é de cinco pontos, variando do 1 - discordo totalmente até o 5 - concordo totalmente.

O procedimento de tabulação e análise dos dados ocorreu por meio do SPSS, versão 17.0. O processo de análise ocorreu por meio de procedimentos de estatística descritiva e inferencial, com destaque para a técnica de análise fatorial e regressão linear múltipla. A análise fatorial foi utilizada por meio do método dos componentes principais e o número de fatores foi determinado *a priori,* seguindo a estrutura dos modelos originais (HAIR *et al., 2005*). Essa postura de análise metodológica foi utilizada para a obtenção de novas variáveis que representam seus fatores, ou seja, o agrupamento das variáveis originais em um fator de elevada correlação comum entre as variáveis.

Em relação à análise de regressão, esta consiste em uma técnica de análise multivariada que, por meio de uma função matemática, determina uma relação causal entre variáveis independentes e uma variável dependente. De acordo com Hair *et al* (2005, p. 131), a análise de regressão é "a técnica de dependência mais amplamente usada e versátil, aplicável em cada faceta da tomada de decisões em negócios." O autor ainda complementa, dizendo que essa técnica consiste em "uma ferramenta analítica poderosa planejada para explorar todos os tipos de relações de dependência".

4. Apresentação e discussão dos resultados

A primeira parte do questionário buscou realizar uma sintética caracterização sobre as organizações em que os gestores estão inseridos. A variável "setor de atuação na organização" demonstrou que 46,8% dos respondentes estão lotados no setor de gestão, 31,6% são de planejamento, 15,2% no setor de Gestão e Planejamento e apenas uma pequena quantidade atua em uma área que se relaciona com Tecnologia de informação (6,4%). Tal resposta já era esperada, uma vez que os respondentes são coordenadores do PNAGE e tal projeto está intrinsecamente vinculado às Secretarias Estaduais de Planejamento e Gestão.

Constatou-se que 50,6% dos entrevistados não sabem se a organização, onde trabalha, já sofreu algum ataque aos arquivos do governo, 28,6% afirmam que já sofreram ataque à segurança e apenas 13% nunca sofreram ataques. Uma pequena parte preferiu não responder. O alto índice de desconhecimento sobre ataques pode demonstrar falta de interesse pelas questões de segurança da informação ou até mesmo pouca disseminação de tais assuntos na organização. Para 46,2% dos entrevistados, as questões de segurança são de responsabilidade direta dos gestores principais das organizações, enquanto que 35,9% indicaram que o segundo escalão era quem deveria ser responsabilizado. Os demais 18% responderam que não existe setor formal que se responsabilize ou desconheciam o fato.

Sobre a caracterização do perfil demográfico dos respondentes, a idade média é de pouco mais de quarenta e três anos, com variação de 25 a 60 anos. Quanto ao gênero dos gestores, 56,3% são homens e 43,7% são mulheres. No tocante ao nível de escolaridade, contatou-se que apenas 5% não têm formação superior completa. Há uma expressiva maioria com pós-graduação concluída, sendo 60% em nível de especialização e 10% mestrado ou doutorado. Tal resultado é corroborado pelo fato de que esses gestores atuam na definição de políticas públicas dos governos de seus estados e precisam constantemente articular-se com organismos de outras esferas de governos e até internacionais, o que demanda maior preparação em termos de educação formal superior.

O nível de conhecimento em informática foi outra variável pesquisada para descrever o perfil do respondente. Apenas 16,3% dos gestores possuem um nível avançado de conhecimento em TI. Quanto à realização de cursos de treinamento ou capacitação em segurança da informação, foi constatado que a maioria (49,4%) não participou de nenhuma atividade até o momento, seguida por 31,6% que disseram ter noções básicas. Apenas 19% afirmaram ter feito um treinamento intermediário ou avançado. Isso pode indicar que a maioria dos respondentes possui conhecimentos na área de TI apenas como autodidata e que as organizações, onde trabalham, não investem na capacitação em segurança da informação. Foi possível verificar que mais de dois terços dos respondentes são apenas usuários das tecnologias impostas pela organização (76,3%), sem exercer nenhuma interferência na escolha ou autorização de novas tecnologias.

Sobre a frequência de realização de *backups* de arquivos realizados pelos respondentes, 35,4% fazem cópia de segurança pelo menos mensalmente. No entanto, temerariamente, 43,1% responderam que fazem *backup* com intervalos de mais de um mês e uma parcela

considerável dos respondentes (21,5%) disse que nunca realiza operação de *backup*. A segurança da informação ainda não é uma prática cotidiana de ampla difusão.

Outro dado de destaque sobre o comportamento dos gestores, como usuários de sistemas de informação, mostrou que apenas 23,7% afirmaram nunca ter utilizado a rede da organização para acesso das suas contas pessoais, os demais informaram que a usam 'sempre' (25%) ou às vezes (51,3%) para fins pessoais.

A TAB. 2 apresenta uma relação de seis assertivas estruturadas, a partir do modelo TAM, cujo processo de mensuração ocorreu por meio de escala do tipo *likert* de cinco pontos, oscilando de discordância total até a concordância plena com as afirmações. Verifica-se que os indivíduos da amostra dividem suas opiniões sobre o fato da utilização de práticas de segurança da informação não requerer muito esforço mental. Nesse mesmo sentido, apenas 35% concordam ou concordam totalmente que têm muita facilidade para a utilização de tais práticas. Por outro lado, é possível verificar um elevado índice de concordância em relação à crença de que essas práticas podem tornar seu trabalho mais eficiente, mais interessante e que são importantes para a realização de seu trabalho.

TABELA 2 - Práticas Avançadas de Segurança da Informação

Indicadores	Construtos (TAM)	1*	2*	3*	4*	5*
A utilização de práticas de Segurança da Informação requer muito do meu esforço mental (*reversa*).	Facilidade de uso percebida	21,3%	31,3%	30%	15%	2,5%
Eu tenho muita facilidade em utilizar práticas avançadas de Segurança da Informação	Facilidade de uso percebida	11,3%	23,8%	30%	25%	10%
Adotar práticas de Segurança da Informação torna meu trabalho mais eficiente.	Utilidade percebida	5%	8,8%	10%	51,3%	25%
A utilização de práticas de Segurança da Informação é extremamente importante para a realização do meu trabalho.	Utilidade percebida	1,3%	10%	18,8%	46,3%	23,8%
Eu gosto de utilizar práticas avançadas de Segurança da Informação.	Atitude	3,8%	12,5%	38,8%	33,8%	11,3%
Utilizar práticas avançadas de Segurança da Informação torna meu trabalho mais interessante.	Atitude	3,8%	16,3%	38,8%	33,8%	7,5%

Nota: 1-Discordo Totalmente; 2-Discordo Parcialmente; 3-Neutro; 4-Concordo Parcialmente; 5-Concordo Totalmente
Fonte: Resultados da Pesquisa

Buscando verificar o quão provável seria a utilização das práticas de segurança de informação, dado o acesso às normas, foi possível verificar uma alta aceitabilidade por parte dos usuários, desde que tenham acessos aos manuais de instruções normativas (TAB. 3).

TABELA 3 – Intenção de Utilização de Práticas Avançadas de Segurança da Informação

Indicadores	Altamente Improvável	Improvável	Não sei	Provável	Altamente Provável
Se eu tiver acesso às normas das práticas avançadas de Segurança da Informação, pretendo usá-las.	0%	1,3%	10,1%	58,2%	30,4%
Dado que eu tenha acesso às normas avançadas de Segurança da Informação, prevejo que as usaria.	0%	2,5%	11,4%	54,4%	31,6%

Fonte: Resultados da Pesquisa

A TAB. 4 apresenta os resultados descritivos da disposição dos gestores públicos em concordar ou não com os serviços de segurança da informação contidos na norma 27001. As questões de maior nível de concordância são relativas à questão de senhas para controle de acesso, enquanto as que obtiveram menores médias foram sobre a necessidade de bloquear acesso nas férias e realizar investigação sobre o passado do usuário.

TABELA 4 – Nível de concordância com as práticas avançadas de segurança da informação

Indicadores	Dimensão	Média	1	2	3	4	5
Identificador da rede ser única para usuário.	*CA	4,6	1	1	3	19	56
Remoção de acesso para usuários desligados.	*CA	4,5	0	2	4	25	48
Regras claras de responsabilização por má utilização.	**RH	4,4	0	0	2	42	36
Reativação de senha via identificação rigorosa.	*CA	4,3	1	1	6	34	37
Alerta de evitar senha registrada em papel.	*CA	4,3	1	2	9	27	41
Recebimento de treinamento.	**RH	4,3	1	0	4	43	32
Revisão regular de direitos de acesso.	*CA	4,3	0	0	8	42	30
Procedimento formal para criação de novo usuário.	*CA	4,3	1	0	9	37	33
Assinatura documento de responsabilidade p/ novos usuários	**RH	4,1	2	4	7	40	27
Cuidados especiais para uso de notebooks.	*CA	4,0	0	5	14	35	26
Existência de monitoramento ou gravação das instalações.	*CA	3,9	1	3	24	28	24
Comprometimento de sigilo, por escrito.	*CA	3,9	5	8	11	26	30
Limitação de três tentativas para *login.*	*CA	3,7	1	12	19	29	19
Alteração de senha regularmente.	*CA	3,6	6	15	11	25	23
Acesso físico por biometria.	*CA	3,5	1	6	37	25	10
Entrada de senha por teclado virtual.	*CA	3,5	1	6	36	29	8
Procedimentos disciplinares p/ usuários que cometem erros.	**RH	3,5	1	16	25	27	11
Proibição de reutilização de senhas.	*CA	3,3	6	11	28	25	9
Não aceitação de *login* nas férias.	*CA	3,2	9	23	12	14	22
Investigação do passado do usuário.	**RH	3,2	8	13	24	26	9

Nota: ***CA**- dimensão de controle de acesso da Norma; ****RH**- dimensão de recursos humanos
1-Discordo Totalmente; **2**-Discordo Parcialmente; **3**-Neutro; **4**-Concordo Parcialmente; **5**-Concordo Totalmente
Fonte: Resultados da Pesquisa

Após o processo de análise descritiva dos dados, deu-se início ao tratamento estatístico multivariado para verificação das hipóteses norteadoras do estudo. Inicialmente, utilizou-se o processo de análise fatorial para criação de novas variáveis que agrupassem as variáveis originais do instrumento de coleta de dados. Os testes de confiabilidade, de normalidade, de homoscedasticidade e de multicolinearidade foram feitos para identificar se havia violação dos pressupostos da análise fatorial, tendo obtido resultado satisfatório.

O procedimento teve início com a criação das variáveis dependentes do estudo que se basearam na norma ISO/IEC 27001, para identificar o nível de concordância com a adoção de práticas avançadas em Segurança da Informação. A análise foi feita através da segmentação em dois controles: Controle de Acesso e Recursos Humanos, a seguir descritos. Por meio da análise fatorial, obteve-se um fator relacionado ao Controle de

Acesso que contemplou 13 dos 15 indicadores presentes no instrumento de coleta de dados. O procedimento obteve um índice de adequacidade da amostra igual a 0,784, o que atende os pressupostos básicos indicados na literatura (HAIR *et al.*, 2005).

Em relação ao grupo de cinco indicadores referentes aos Recursos Humanos na norma ISO 27001, utilizou-se o mesmo procedimento de análise fatorial confirmatória, de forma a obter um fator no qual todas as cinco variáveis contempladas na norma foram agrupadas. O índice de adequacidade foi semelhante ao procedimento anterior e resultou em um KMO igual a 0,767. Dessa forma, foram obtidas as duas variáveis dependentes do estudo.

Foi necessário trabalhar com o procedimento de AF para a obtenção das variáveis relacionadas à percepção sobre facilidade de uso, percepção sobre utilidade, atitudes perante as práticas de segurança e intenção de utilização de práticas de segurança. Dessa forma foram obtidas as variáveis independentes para verificação das hipóteses H_1, H_2, H_3 e H_4, em cada uma das dimensões, segundo o modelo apresentado na FIG. 2.

Com a criação dessas novas variáveis métricas, deu-se início ao processo de verificação de hipóteses do estudo por meio do procedimento de análise de regressão. Essa técnica foi empregada com o intuito de se verificar a existência de uma relação significante entre as variáveis independentes e as variáveis dependentes do modelo.

Como pode ser observado na TAB. 5, a dimensão facilidade de uso não influencia o controle de acesso e os recursos humanos, logo as hipóteses H_{1a} e H_{1b} não podem ser aceitas. Esse resultado não é esperado, embora Jones (2009) também não tenha obtido relação significante entre as variáveis de facilidade de uso com a intenção de utilizar sistemas de segurança da informação. Estudos posteriores devem ser desenvolvidos a fim de testar esses construtos no âmbito da gestão de sistemas de segurança da informação.

TABELA 5 - Verificação da Hipótese H_1: Facilidade de uso das práticas de segurança x Adoção de práticas de segurança

Variável Dependente: Controle de Acesso							
Modelo	**Unstandardized Coefficients**		**Standardized Coefficients**	**t**	**Sig.**	**R**	**R^2**
	B	**Std. Error**	**Beta**				
Constante	0,005	0,113	-	0,048	0,962	0,178	0,032
Facilidade de Uso	0,178	0,114	0,178	1,567	0,121		
Variável Dependente: Recursos Humanos							
Modelo	**Unstandardized Coefficients**		**Standardized Coefficients**	**t**	**Sig.**	**R**	**R^2**
	B	**Std. Error**	**Beta**				
Constante	0,000	0,111	-	0,000	1,000	0,187	0,035
Facilidade de Uso	0,187	0,111	0,187	1,678	0,097		

Fonte: Resultados da Pesquisa

Na TAB. 6, apresenta-se os resultados da análise de regressão para a dimensão Utilidade Percebida. Nota-se que, para a variável dependente de controle de acesso, há uma influência estatisticamente significante, com um coeficiente beta de 0,54, significante para um valor $p < 0,05$, suportando a hipótese H_{2a}. No caso da dimensão recursos Humanos, também verifica-se que há condições de rejeitar a hipótese nula, ou seja, é possível inferir que os gestores que estão mais propensos a aderir às normas de SI são influenciados pela variável de percepção de utilidade.

Esse resultado corrobora várias outras pesquisas sobre TAM, nas quais a percepção de utilidade é um dos construtos com mais força nas explicações da aceitação de tecnologia.

TABELA 6 -Verificação da Hipótese H_2: Utilidade de uso percebida das práticas de segurança x Adoção de práticas de segurança

Variável Dependente: Controle de Acesso							
Modelo	**Unstandardized Coefficients**		**Standardized Coefficients**	**t**	**Sig.**	**R**	**R^2**
	B	**Std. Error**	**Beta**				
Constante	0,020	0,097	-	0,206	0,837	0,538	0,289
Utilidade Percebida	0,540	0,098	0,538	5,527	0,000		
Variável Dependente: Recursos Humanos							
Modelo	**Unstandardized Coefficients**		**Standardized Coefficients**	**t**	**Sig.**	**R**	**R^2**
	B	**Std. Error**	**Beta**				
Constante	0,000	0,103	-	0,000	1,000	0,396	0,157
Utilidade Percebida	0,396	0,104	0,396	3,806	0,000		

Fonte: Resultados da Pesquisa

A TAB. 7 apresenta os dados encontrados nos testes das hipóteses H_{3a} e H_{3b}. A pesquisa confirmou que uma atitude mais favorável à adoção de práticas de segurança influencia positivamente na visão de gestores a favor de mais controles prescritivos da Norma, tanto em relação ao controle de acesso como para os recursos humanos.

TABELA 7 - Verificação da Hipótese H_3: Atitude frente às práticas de segurança x Adoção de práticas de segurança

Variável Dependente: Controle de Acesso							
Modelo	**Unstandardized Coefficients**		**Standardized Coefficients**	**t**	**Sig.**	**R**	**R^2**
	B	**Std. Error**	**Beta**				
Constante	0,007	0,105	-	0,065	0,948	0,411	0,169
Atitude	0,409	0,105	0,411	3,902	0,000		
Variável Dependente: Recursos Humanos							
Modelo	**Unstandardized Coefficients**		**Standardized Coefficients**	**t**	**Sig.**	**R**	**R^2**
	B	**Std. Error**	**Beta**				
Constante	0,000	0,106	-	0,000	1,000	0,339	0,115
Atitude	0,339	0,107	0,339	3,187	0,002		

Fonte: Resultados da Pesquisa

Para concluir o conjunto de testes das proposições do modelo proposto, a TAB. 8 evidencia que a dimensão de Intenção de Uso é estatisticamente significante em relação ao controle de acesso e aos recursos humanos. Nesse caso as hipóteses H_{4a} e H_{4b} também podem ser confirmadas.

TABELA 8 - Verificação da Hipótese H_4: Intenção comportamental x Adoção de práticas de segurança

Variável Dependente: Controle de Acesso							
Modelo	**Unstandardized Coefficients**		**Standardized Coefficients**	**t**	**Sig.**	**R**	**R^2**
	B	**Std. Error**	**Beta**				
Constante	-0,006	0,105	-	-0,061	0,951	0,406	0,165
Intenção de Uso	0,404	0,105	0,406	3,851	0,000		
Variável Dependente: Recursos Humanos							
Modelo	**Unstandardized Coefficients**		**Standardized Coefficients**	**t**	**Sig.**	**R**	**R^2**
	B	**Std. Error**	**Beta**				
Constante	-0,010	0,103	-	-0,096	0,924	0,411	0,169
Intenção de Uso	0,412	0,104	0,411	3,957	0,000		

Fonte: Resultados da Pesquisa

Para efeito de síntese dos resultados, o QUADRO 1 retoma as hipóteses que tornearam o desenvolvimento do estudo e apresenta a situação dessas hipóteses para cada uma das variáveis dependentes.

QUADRO 1 – Síntese das hipóteses do modelo

Hipóteses	Fator	Situação
H_1) A percepção sobre a **facilidade de utilização** das práticas de Segurança exerce uma influência positiva significativa sobre a adoção de práticas avançadas de Segurança.	Controle de Acesso	Não Confirmada
	Recursos Humanos	Não Confirmada
H_2) A percepção sobre a **utilidade** de práticas de Segurança exerce uma influência positiva significativa sobre a adoção de práticas avançadas de Segurança.	Controle de Acesso	Confirmada
	Recursos Humanos	Confirmada
H_3) A percepção sobre a **atitude** perante as práticas de Segurança exerce uma influência positiva significativa sobre a adoção de práticas avançadas de Segurança.	Controle de Acesso	Confirmada
	Recursos Humanos	Confirmada
H_4) A **intenção** de utilização das práticas de Segurança exerce uma influência positiva significativa sobre a adoção de práticas avançadas de Segurança.	Controle de Acesso	Confirmada
	Recursos Humanos	Confirmada

Fonte: Elaboração Própria

Como é possível verificar, a percepção de utilidade, atitude e intenção de uso das práticas de segurança da informação são variáveis que exercem influência direta sobre os dois níveis de adoção de práticas de segurança de informação utilizados neste estudo (controle de acesso e recursos humanos).

5. Considerações finais

O Modelo de Aceitação de Tecnologia (TAM) e suas extensões, como o TAM2, TAM3 e o UTAUT, são abordagens teóricas que podem ajudar ao administrador a prever a aceitação por usuários, ou seja, ajudam a predizer as melhores escolhas a serem adotadas em processos de implantação de novas práticas e novos sistemas dentro das organizações. A pesquisa buscou testar as relações entre os construtos do TAM (facilidade de uso, utilidade

percebida, atitude e intenção de uso) e o nível de concordância com a adoção de práticas avançadas de Segurança da Informação.

O modelo proposto da pesquisa confirmou as hipóteses H_2, H_3 e H_4 em ambas as dimensões: controle de acesso e recursos humanos. No entanto, não foi possível confirmar a hipótese H_1, isso é, a facilidade de uso não foi uma boa preditora do nível de concordância com as práticas preconizadas pela Norma ISO/IEC 27001. Isso indica que mais estudos futuros serão necessários para entender com mais profundidade esse resultado.

A pesquisa possui algumas limitações. Como a população da pesquisa é constituída de gestores públicos que são das áreas administrativas e de planejamento, a generalização de seus resultados só deve ser considerada para tal público específico. O caráter transversal da pesquisa de campo também limita o presente estudo, visto que essa abordagem baseia-se na fotografia de um único momento, podendo vir a influenciar os resultados dos construtos e suas relações.

Outra limitação que pode ser apontada diz respeito à falta de clareza em duas questões referentes ao perfil organizacional (número de equipamentos do parque de informática e número de usuários que acessam a rede), não detectadas no pré-teste. Para tais questões, houve três tipos de resposta. Alguns responderam em relação ao setor de trabalho, outros de todo o Governo do Estado e apenas uma parte como se esperava, ou seja, da organização de trabalho (órgão, empresa). Além da falha de interpretação, tais perguntas tiveram um índice considerável de omissões, o que inviabilizou os testes que poderiam ter sido feitos. Como forma de correção para trabalhos futuros, sugere-se deixar a questão mais clara ou obter tais números através de dados secundários.

Como direcionamento de futuras pesquisas, podem ser desenvolvidos estudos com dirigentes e gestores do setor público de outras áreas, como: tributação, saúde, educação e segurança. Nesse caso, o modelo adotado e a metodologia poderão ser replicados. Também são sugeridos estudos comparativos entre gestores não especialistas em TI e gestores especialistas em TI.

Em termos de implicações gerenciais, o estudo poderá subsidiar futuras políticas que visem a obter certificações na área de segurança da informação, especialmente quando formulada para obter adesão de gestores das áreas foco desta pesquisa (planejamento e gestão). Espera-se que novas pesquisas sobre esse assunto sejam desenvolvidas por parte dos acadêmicos e dirigentes organizacionais, permitindo o avanço do conhecimento no campo da aceitação de práticas de segurança da informação.

Referências

ALMEIDA, F.J.R.; SOBRAL, F.J.B.A. Os condicionantes psicológicos e estruturais da informatização organizacional: um estudo sobre empresas portuguesas utilizando o modelo de equações estruturais. Reunião Anual da Associação Nacional de Programas de Pós-Graduação em Administração (ANPAD), 29., 2005, Brasília. *Anais...* Brasília: ANPAD, 2005.

APPUNN, F.D. *Computer user security*: A model facilitating measurement. Ph.D. dissertation, Capella University, Minnesota, United States, 2008.

BARNUM, G. Availability, access, authenticity, and persistence: creating the environment for permanent public access to electronic government information. Washington*: Government Information Quarterly*, n. 19, p. 37-43, 2002.

BAUER, C.A. *Política de segurança da informação para redes corporativas*. 2006. 71 f. Trabalho de Conclusão de Curso (Graduação em Ciências da Computação) – Instituto de Ciências Exatas e Tecnológicas, Centro Universitário FEEVALE, Novo Hamburgo. 2006.

BROWN, S. A.; VENKATESH, V; BALA, H. Household technology use: integrating household life cycle and the model of adoption of technology in holseholds. Minneapolis: *MIS Quartely,* v. 29, n. 3, p. 399-426, 2005.

BUENO, U.; ZWICKER, R.; OLIVEIRA, M.A. Um estudo comparativo do modelo de aceitação aplicado em sistemas de informação e comércio eletrônico. Congresso Internacional de Gestão de Tecnologia e Sistemas de Informação, 1., 2004, São Paulo. *Anais...* São Paulo: USP, 2004.

CAMPOS, A. N. *Sistema de segurança da informação*. Florianópolis: Visual Books, 2006.

CARVALHO, R.B.; FERREIRA, M.A.T. Avaliação da qualidade de intranets e portais corporativos: proposta de modelo e pesquisa exploratória em médias e grandes organizações. XXIX Reunião Anual da ANPAD, 29., 2005, Brasília. *Anais...* Brasília: ANPAD, 2005.

CHAU, P. Y. K; LAI, V. S. K. An Empirical Investigation of the Determinants of User Acceptance of Internet Banking. *Journal of Organizational Computing & Eletronic Commerce.* v. 13, n.2, p.123-145, 2003.

COSTA FILHO, B. A.; PIRES, P. J. Revisitando os caixas-automáticos: o modelo TAM (technology acceptancy model) aplicado aos ATM´S. XXVIII Reunião Anual da ANPAD, 28., 2004, Curitiba. *Anais...* Curitiba: ANPAD, 2004.

DAVIS, F. D.; BAGOZZI, R.; WARSHAW, P. R. User acceptance of computer technology: A comparison of two theoretical models, *Management Science*, v. 5, n.8, p.982-1003, 1989.

DIAS, M. C.; ZWICKER, R.; VICENTIN, I. C. Análise do modelo de aceitação de tecnologia de Davis. Curitiba: *Revista Spei*, v. 4, n. 2, 2003. p. 15-23.

EMANAVIN, C.C. *Testing lessing: Applying user acceptance theory to internet use and behavior for privacy and security applications*. Master of Art in Communication, Culture and Technology Thesis, Georgetown University, United States, 2004.

FRÓIO, L.R. *Um modelo baseado de gestão de segurança da informação*. 2008. 145 f. Dissertação (Mestrado em Engenharia Elétrica) – Faculdade de Tecnologia, Universidade de Brasília, Brasília. 2008.

GABBAY, M. S. *Fatores influenciadores da implementação de ações de gestão de segurança da informação*: um estudo com executivos e gerentes de tecnologia da informação das empresas do Rio Grande do Norte. 2003. 169 f. Dissertação (Mestrado em Engenharia de Produção) – Universidade Federal do Rio Grande do Norte, Natal, 2003.

HAIR *et al. Análise Multivariada de Dados*. 5. ed. Porto Alegre: Bookman, 2005.

IEC. History. International Engineering Consortium. Disponível em: <http:\\www.iec.org/about/history.html> Acesso em: 01 maio 2008.

JONES, C.M. *Utilizing the Technology Acceptance Model to Assess Employee Adoption of Information Systems Security Measures*. Ph.D. Thesis. H. Wayne Huizenga School of Business and Enterpreneurship, Nova Southerastern University, United States, 2009.

LESSA, B.M. *Gestão estratégica da segurança da informação*. 2004. 56 f. Monografia (Especialização em Tecnologia da Informação) – Gerência de TI, Universidade FUMEC, Belo Horizonte. 2004.

LIMA, L.F.F.M. *Percepção de segurança em sistemas de informação e sua relação com a qualidade percebida de serviços, perfil de liderança e perfil dos seguidores, entre as diretorias do INMETRO*. 2006. Dissertação (Mestrado em Engenharia da Produção) – Universidade Federal Fluminense, Rio de Janeiro. 2006.

LÖBLER, M.L.; VISENTINI, M.S.; VIEIRA, K.M. A aceitação do comércio eletrônico explicado pelos modelos TAM e TIF combinados. XXX Reunião Anual da ANPAD, 30., 2006, Salvador. *Anais...* Salvador: ANPAD, 2006.

LORENS, E.M. *Aspectos normativos da segurança da informação*: um modelo de cadeia de regulamentação. 2007. 144 f. Dissertação (Mestrado em Ciência da Informação) – Departamento de Ciência da Informação e Documentação, Universidade de Brasília, Brasília, 2007.

LUCAS JUNIOR, H. C. *Tecnologia da informação***:** tomada de decisão estratégica para administradores. Rio de Janeiro: LTC, 2006.

MENEZES, J.C. *Gestão de segurança da informação*: análise em três organizações brasileiras. 2005. 103 f. Dissertação (Mestrado Profissional em Administração) – Escola de Administração, Universidade Federal da Bahia, Salvador. 2005.

MOREIRA, Nilton S. *Segurança Mínima*: uma visão corporativa da segurança de informações. Rio de Janeiro: Axcel Books, 2001.

MORRIS, M. G.; VENKATESH, V. Age differences in technology adoption decicions: implications for a changing work force. College Park: *Personnel Psychology*. v. 53, n. 2, p. 375-403, 2000.

OLIVA, R.P.; OLIVEIRA, M. Elaboração, Implantação e Manutenção de Política de Segurança por Empresas no Rio Grande do Sul em Relação às Recomendações da NBR/ISO17799. XXVII Reunião Anual da ANPAD, 27., 2005, Atibaia-SP. *Anais...* Brasília: ANPAD, 2003.

OLIVEIRA JUNIOR, R.S. Avaliação de aceitação de sistemas integrados de gestão. Encontro De Administração da Informação, 1., 2007, Florianópolis. *Anais...* Florianópolis: ANPAD, 2007.

OLIVEIRA, B.M.K.; RAMOS, A.S.M. Padrão de uso do *e-learning* a partir do modelo de aceitação de tecnologia: uma pesquisa com alunos do curso a distância de graduação em administração da UFRN. V Congresso Virtual Brasileiro de Administração., 5., 2008, Natal. *Anais...* São Paulo: COVINBRA, p. 18, 2008.

PIRES, P.J.; YAMAMOTO, C.S; COSTA FILHO, B.A. Avaliação e reespecificação de um modelo unificado de aceitação da tecnologia da informação (UTAUT) a partir de usuários de um sistema de voz sobre protocolo IP. XXX Reunião Anual da ANPAD, 30., 2006, Salvador. *Anais...* Salvador: ANPAD, 2006.

RAMOS, A. S. M.; FEIJO, D. F. B. Um estudo prospectivo sobre segurança da informação em uma empresa de telecomunicações segundo a NBR ISO/IEC 17799:2001. I Congresso Internacional de Gestão de Tecnologia e Sistemas de Informação (CONTECSI), *Anais..,* São Paulo: USP, 2004.

RAMOS, A.S.M; CAVALCANTE, S.M. Práticas de Conscientização e Treinamento em Segurança da Informação no Correio Eletrônico: Um Estudo de Caso, Congresso Anual de Tecnologia da Informação - CATI 2005, *Anais..,* FGV-EAESP, 2005.

RODRIGUES, E.T.; COSTA, I.S.A. Valores individuais: uma lente conceitual para o estudo do uso da tecnologia da informação nas organizações. XXX Reunião Anual da ANPAD, 30., 2006, Salvador. *Anais..* Salvador: ANPAD, 2006.

SANTOS, L.D.; AMARAL, L.A.M. Determinantes do sucesso de adoção e difusão de serviços de informação online. V Conferência da Associação Portuguesa de Sistemas de Informação, 5., 2004, Lisboa. *Atas..* Lisboa: APSI, 2004, 13 p.

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

SHROPSHIRE, J.D. *Predicting compliance with prescribed organizational information security protocols.* Ph.D. Thesis. Faculty of Mississipi State University. United States, 2008.

SILVA NETTO, A. *Gestão de segurança da informação: fatores que influenciam sua adoção em pequenas e médias empresas.* 2007. 106 f. Dissertação (Mestrado em Administração) – Universidade Municipal de São Caetano do Sul, São Caetano do Sul. 2007.

SILVA, A.L.M.R.; DIAS, D.S. Influência do treinamento de usuários na aceitação de sistemas ERP no Brasil. XXX Reunião Anual da ANPAD, 30., 2006, Salvador. *Anais...* Salvador: ANPAD, 2006.

SILVA, P. M. Modelo de aceitação de tecnologia (TAM) aplicado ao Sistema de Informação da Biblioteca Virtual em Saúde (BVS) nas Escolas de Medicina da Região Metropolitana do Recife*. Informação & Sociedade*. Estudos, v. 19, p. 117-117, 2009.

SILVA, P. M.; DIAS, G. A., SENA JUNIOR, M. R. A importância da cultura na adoção tecnológica: o caso do Technology Acceptance Model (TAM). Florianópolis: *Revista Eletrônica de Biblioteconomia e Ciência da Informação,* v. 13, n. 26, p 1-7, 2008.

SOLMS, R. von. Information security management: why standards are important. *Information Management & Computer Security*, v. 7, n.1, p. 50-57, 1999.

SOUZA, R.M. *Implantação de ferramentas e técnicas de segurança da informação em conformidade com as normas ISO 27001 e 17799*. 2007. 131 f. Dissertação (Mestrado em Gestão de Redes e Telecomunicações) – Centro de Ciências Exatas, Ambientais e de Tecnologias, Pontifícia Universidade Católica de Campinas, Campinas. 2007.

TURBAN, E.; RAINER, R. K.; POTTER, R. E. *Administração da tecnologia da informação:* teoria e prática. Rio de Janeiro: Campus, 2003.

VENKATESH, V.; MORRIS, M. G.; DAVIS, G. B.; DAVIS, F. D. *User acceptance of information technology: toward a unified view. Minneapolis:* MIS Quarterly, v. 27 n. 3, p. 425-478, 2003.

VENKATESH, V.; BALA, H. Technology acceptance model 3 and a research agenda on interventions. *Decision Sciences*, v. 39, n. 2, p.273-307, 2008.

VENKATESH, V.; DAVIS, F. D. A model of the antecedents of perceived ease of use: development and test. North St Paul: *Decision Sciences***,** v. 23, n. 2, p. 451-481, 1996.

VENKATESH, V.; DAVIS, F. D. A theoretical extension of the technology acceptance model: four longitudinal field studies. Philadelphia*: Management Science*, v. 46, n. 2, p. 186–204, 2000.