Fatores Organizacionais e sua Influência na Segurança da Informação em Universidades Públicas: Um Estudo Empírico

Carlos A. N. Machado[1], Lucídio A. F. Cabral[1], Jozemar P. Santos[1], Gustavo H. M. B, Motta[1]

[1]Programa de Pós-Graduação em Informática - Universidade Federal da Paraíba (UFPB)
58059-900 – João Pessoa, PB – Brasil

carlos@ccen.ufpb.br, lucidio@de.ufpb.br, jozemar@de.ufpb.br, gustavo@di.ufpb.br

Abstract. *An empirical study was carried out to analyze the influence of organizational factors on the perception of the effectiveness of information security in public universities. It was used the exploratory factorial analysis (EFA) technique to analyze data from a questionnaire answered by 75 IT professionals from 46 public universities from all Brazilian states. The results of EFA allowed us to conclude that any measure to improve information security aspects should occur in accordance and with top management support.*

Resumo. *Um estudo empírico foi realizado para analisar a influência de fatores organizacionais na percepção da efetividade da segurança da informação em universidades públicas. Empregou-se a técnica da análise fatorial exploratória (AFE) para analisar dados de um questionário respondido por 75 profissionais de TIC de 46 universidades públicas de todos os estados do Brasil. Os resultados da AFE permitiram concluir que medidas de melhoria dos aspectos de segurança da informação devem ocorrer em sintonia e com o apoio da administração superior dessas instituições.*

1. Introdução

Nas últimas décadas, o aumento do uso de avançadas tecnologias da informação e de comunicação (TIC), principalmente no apoio às ações de pesquisa e desenvolvimento (P&D), provocou a massificação do acesso aos bens e serviços de TIC em universidades públicas. Como conseqüência, houve um incremento na produção e na troca de informações utilizando recursos computacionais, assim como, um crescimento na quantidade de usuários e na diversificação em seu perfil.

A evolução de sistemas de processamento centralizado para sistemas abertos e distribuídos provocou grandes mudanças no ambiente computacional e no perfil dos usuários. Anteriormente, os ambientes se caracterizavam por terem uma quantidade restrita de usuários acessando de forma controlada, através de terminais, um computador central, com o acesso físico permitido apenas para administradores e operadores do sistema. Atualmente, professores e alunos passaram a usar computadores pessoais como uma ferramenta indispensável do processo de ensino-aprendizagem e também nas atividades de P&D. Utilizam a Internet para navegar via *web browsers*; para se comunicar via e-mail ou com ferramentas *peer-to-peer*. Por outro lado, aplicativos passaram para a plataforma da web, como os de matrícula, diário de classe, controle de processos administrativos e bibliotecas digitais para acesso a literatura científica. Ou seja, hoje as tecnologias da informação e de comunicação permeiam as atividades-fim da universidade pública nas áreas de ensino, pesquisa e extensão, tanto na graduação como na pós-graduação, bem como as atividades-meio administrativas.

A intensificação do uso de computadores em rede trouxe, além de inegáveis benefícios, os problemas decorrentes de uma comunicação permissiva. Além de obter in-

formações úteis ao ensino, à extensão e à pesquisa, a rede facilita a contaminação não intencional por programas maliciosos (e. g., vírus, cavalos de tróia) e permite que pessoas mal intencionadas obtenham conhecimento de como invadir computadores, promover ataques, dentre outras ações maléficas. Ademais, o perfil do usuário fica cada vez mais diversificado e com necessidades específicas. Os responsáveis pela TIC nas universidades têm, assim, uma dificuldade crescente em apoiar e educar o usuário para a utilização eficaz dos serviços oferecidos e para coibirem o seu uso indevido. Portanto, torna-se premente a existência de uma política de segurança bem definida e implementada com o devido apoio dos dirigentes e da comunidade universitária.

Uma política de segurança da informação estabelece direitos e responsabilidades às pessoas, definindo as suas atribuições em relação à segurança dos recursos computacionais com que trabalham. Seu desenvolvimento é o primeiro e o principal passo de estratégia de segurança das organizações. Define os aspectos envolvidos na proteção dos recursos existentes, com grande parte do trabalho dedicado a sua elaboração e ao seu planejamento. No entanto, as maiores dificuldades estão mais na sua implementação do que no seu planejamento e elaboração (Nakamura e Geus, 2004).

Uma conseqüência é que as medidas de segurança, que de fato são implementadas e que permanecem funcionando, definem uma política real de segurança, nem sempre correspondendo à política formal, institucionalmente estabelecida. Pode-se ainda considerar que, mesmo quando não há uma política formal, há sempre uma política real, em geral tácita, em vigor num dado momento. A política real existente é possivelmente influenciada por fatores organizacionais que podem contribuir, positiva ou negativamente, para a efetividade da segurança da informação. A segurança é efetiva quando atinge seu objetivo real, que é proteger a confidencialidade, a integridade e a disponibilidade das informações, mantidas ou em trânsito, na infra-estrutura de TIC da organização, segundo os seus interesses.

Identificar fatores organizacionais, conhecer melhor a natureza de sua influência sobre a efetividade da segurança da informação, para saber os que são mais críticos, são atividades essenciais para que se possa formular e implementar políticas de segurança eficientes e eficazes. Deve-se também estabelecer o grau de importância de cada um dos fatores para que se possa agir de forma mais rápida e adequada na construção de uma política de segurança da informação efetiva. Foram encontrados poucos estudos empíricos sobre o tema, com destaque para os trabalhos de Chang e Ho (2006), Wold (2004) e de Knapp e colaboradores (2005, 2006), que investigaram fatores que influenciam a efetividade da segurança da informação em organizações empresariais.

Consideramos que as universidades públicas são organizações que têm características diferentes daquelas usualmente encontradas em organizações empresariais. Embora fatores organizacionais estudados nas organizações empresariais sejam também encontrados em universidades públicas, postulamos que as universidades possuem fatores organizacionais específicos, que merecem ser investigados em relação à sua influência na segurança da informação.

Com base no exposto e ainda considerando a importante escassez de estudos empíricos na área de segurança da informação (Kotulic e Clark, 2004), o objetivo deste trabalho foi realizar um estudo empírico sobre a influência de fatores organizacionais na percepção da efetividade da segurança da informação em universidades públicas.

O trabalho está assim organizado. A seção 2 traz a metodologia considerada para o estudo. A seção 3 apresenta os resultados obtidos e a seção 4 discute os resultados à luz dos trabalhos relacionados. Por fim, a seção 5 traz as conclusões do trabalho.

2. Metodologia

Uma metodologia qualitativa e quantitativa foi empregada para alcançar o objetivo deste trabalho. Segundo Kaplan & Duchon (1988), a combinação de pesquisas qualitativa e quantitativa provê uma rica base conceitual para a interpretação e a validação dos resultados. A pesquisa qualitativa visa suprir o estudo com subsídios que ajudem a identificar fatores organizacionais específicos, que potencialmente influenciem a segurança da informação em universidades públicas, em complemento àqueles encontrados na literatura (Wold, 2004; Knapp *et al.*, 2005, 2006, Chang e Ho,2006), focados em ambientes empresariais, visto que postulamos que as universidades públicas apresentam fatores organizacionais diferenciados.

A pesquisa quantitativa foi realizada utilizando a técnica multivariada da análise fatorial exploratória (AFE), que é classificada por Sharma (1996) como uma técnica paramétrica que trata da interdependência entre variáveis, visando compreender como e por que as variáveis estão correlacionadas. A análise fatorial resulta num conjunto de fatores, que são novas variáveis definidas por combinações lineares das variáveis em análise e que, em princípio, vão explicar como as variáveis iniciais estão correlacionadas (Hill e Hill, 2005). Em particular, a análise fatorial exploratória lida com a questão de responder quantos fatores são necessários para explicar as relações de um conjunto de indicadores (fatores organizacionais), juntamente com uma estimativa das cargas fatoriais (contribuição de cada fator) (Rennie, 1997). Geralmente é utilizada para investigar fenômenos pouco estudados, sobre os quais não existem teorias estabelecidas o suficiente para se realizar uma análise fatorial confirmatória, com interesse em testar hipóteses. Optou-se, portanto, pela AFE em virtude da ausência de estudos empíricos prévios sobre a influência de fatores organizacionais na segurança da informação em universidades públicas. Busca-se saber quais são esses fatores, suas relações e sua importância para segurança da informação e se há fatores relevantes distintos daqueles encontrados em organizações empresariais.

Para tanto, aplicaram-se dois questionários, um aberto, analisado de forma qualitativa, e um fechado, analisado pelo método quantitativo da AFE. Os casos (entidades que responderam os questionários) foram profissionais de TIC de universidades públicas no Brasil, atuando direta ou indiretamente em segurança da informação, nos anos de 2007 e 2008. Foram levantados 134 e-mails e telefones profissionais de Núcleos de Tecnologia da Informação ou similares de 53 universidades públicas. Para uma estimativa de cerca de 5 casos por universidade, têm-se uma população de aproximadamente 250 respondentes. As subseções seguintes apresentam detalhes da elaboração, aplicação e coleta dos dados nos dois questionários.

2.1. Elaboração e Aplicação do Questionário da Pesquisa Qualitativa

A meta do estudo qualitativo foi obter subsídios que ajudassem a identificar fatores organizacionais críticos para segurança da informação em universidades públicas, na percepção dos casos, em complemento àqueles encontrados na literatura para ambientes empresariais. Foi desenvolvido um questionário na Internet para coleta dos dados qualitativos e de informações básicas sobre os casos, como instituição, nome (opcional), formação, função administrativa. O questionário foi hospedado no site https://www.ccen.ufpb.br/li/consultPerguntaForm, onde também estavam esclarecidos os objetivos da pesquisa e afirmado o compromisso com a confidencialidade dos dados fornecidos. Os dados qualitativos foram obtidos pela resposta em texto livre a uma única pergunta aberta, enunciada a seguir:

> Em geral, o que você pensa ser o fator mais crítico para determinar a efetividade de uma política de segurança da informação numa organização com as características de uma universidade?

No dia 01/02/2007 foram enviados 134 e-mails para os profissionais até então identificados. Nos primeiros 15 dias foram obtidas 10 respostas à chamada do e-mail. Devido ao baixo índice de respostas, fizemos contatos telefônicos usando o serviço fone@RNP (VoIP), que a Rede Nacional de Ensino e Pesquisa (RNP) implantou para as instituições usuárias da rede acadêmica nacional, solicitando o atendimento a nossa chamada e obtivemos uma resposta positiva. Um total de 23 indivíduos respondeu à pesquisa qualitativa. As respostas dadas à pergunta aberta foram analisadas e utilizadas para subsidiar a identificação dos fatores organizacionais presentes em universidades públicas, apresentados na subseção 3.1.

2.2. Elaboração e Aplicação do Questionário da Pesquisa Quantitativa

Neste estudo, postula-se que a variável latente (dependente) "percepção da segurança da informação" é definida por um conjunto de outras variáveis, designadas por variáveis componentes (independentes), porque, de certo modo, elas compõem a variável latente. Geralmente, as variáveis componentes são medidas a partir de respostas a afirmações em um questionário, denominadas de itens (Hill e Hill, 2005). Cada fator organizacional identificado com base na revisão da literatura e na pesquisa qualitativa (ver subseção 3.1) corresponde a uma variável componente medida pela coleta da opinião dos casos. Para reduzir as chances de uma questão mal formulada prejudicar os resultados da pesquisa, cada variável componente foi coletada por um conjunto com cinco itens (afirmações), que procuram ter um mesmo significado, embora formulado de forma distinta. Cada um dos itens foi medido numa escala ordinal (escala de Lickert) de cinco pontos, variando de "discordo fortemente", passando por "discordo", "neutro", "concordo", até "concordo fortemente". Ou seja, em vez de se fazer uma frase interrogativa, faz-se uma afirmação e solicita-se a opinião do caso na escala de Lickert.

Como foram identificados dez fatores organizacionais (ver subseção 3.1), foi elaborado um questionário com 50 itens, cinco para cada fator organizacional (variável componente). O questionário foi hospedado no site https://www.ccen.ufpb.br:8080/formulario2, onde também estavam esclarecidos os objetivos da pesquisa e afirmado o compromisso com a confidencialidade dos dados fornecidos. Também foram coletadas informações características dos casos, como instituição, nome (opcional), formação, função administrativa. Os dados coletados foram armazenados em um banco de dados MYSQL, com acesso restrito aos responsáveis pela pesquisa. Posteriormente, ao final da coleta, os dados foram migrados para plataforma do aplicativo SPSS (*Statistical Package for the Social Sciences*), para Windows, a fim de se realizar a análise estatística dos dados com a técnica da AFE.

O questionário foi aplicado preliminarmente, para verificar a adequação das questões e da escala de resposta, a uma pequena amostra de profissionais, que atuavam na área de TIC da UFPB e que lidavam com segurança da informação, assim como os respondentes da pesquisa qualitativa já realizada. Logo após o preenchimento, os respondentes foram convidados a falar sobre qualquer problema encontrado no preenchimento, como perguntas sensíveis ou ambíguas. Somente foram observados problemas menores, como erros de digitação, sendo todos os itens aproveitados, bem como as respostas coletadas na aplicação preliminar do questionário.

3. Resultados

Esta seção apresenta os resultados obtidos a partir da análise dos dados coletados com a aplicação dos questionários. A subseção 3.1 traz os fatores organizacionais identificados, enquanto a subseção 3.2 apresenta os resultados da análise fatorial exploratória dos dados obtidos com a aplicação do questionário da pesquisa quantitativa.

3.1. Fatores Organizacionais Identificados

Nos parágrafos a seguir estão listados os dez fatores organizacionais identificados, com o *rationale* de sua escolha como fator que possivelmente influencia a percepção da efetividade da segurança da informação em universidades públicas, tendo por base a literatura ou os dados coletados no questionário da pesquisa qualitativa. Os fatores 1, 3, 4, 5 e 10 são peculiares às universidades públicas.

1. **O ambiente liberal das universidades**. Verificou-se que 50% dos respondentes da pesquisa qualitativa mencionaram que o ambiente das universidades é liberal e que isso, de alguma forma, dificulta a implementação de medidas de segurança. A seguir têm-se trechos extraídos das respostas dadas à pergunta aberta da pesquisa qualitativa que corroboram a seleção deste fator:

- "Toda medida restritiva ou definidora de regras não é bem recebida pela comunidade universitária";
- "Num ambiente em que os usuários não estão acostumados a seguir regras, sobretudo regras organizacionais que os obriguem a utilizar os recursos institucionais de forma mais responsável, a política de segurança soa como um inimigo à vista";
- "O principal argumento é que por ser um órgão acadêmico tudo deve ser permitido";
- "eu penso que o fator determinante de sucesso é Regras e Limites Claros [...]";
- "A maior dificuldade é a necessidade de algumas aplicações de pesquisa que necessitam de portas abertas ou de outras especialidades que podem trazer vulnerabilidades para a rede e fica o ponto em que não podemos atrapalhar o projeto em si, mas o projeto também não pode trazer insegurança para a rede".

Pode-se concluir que há nas universidades públicas uma cultura de liberalidade, visto que a liberdade para realização de atividades acadêmicas é um valor inalienável conquistado pela comunidade universitária. Em geral, quaisquer medidas que visem impor limites são vistas com desconfiança, ainda que para elevar a segurança do uso dos recursos computacionais. Isto nos leva a pensar que um ambiente em que (quase) tudo é permitido contribui negativamente para a segurança da informação, pois a liberdade e a segurança, embora desejadas, são valores contraditórios entre si.

2. O apoio dos dirigentes universitários. Os resultados do estudo exploratório de Knapp *et al.* (2006) indicaram que o apoio da cúpula administrativa está positivamente relacionado à cultura de segurança e ao cumprimento da política de segurança. Num outro trabalho, Knapp *et al.* (2005) concluíram que o apoio da cúpula administrativa para treinamento de empregados, para criação de uma cultura de segurança e para a qualidade da gestão de segurança pode ter impactos significativos na efetividade da segurança da informação. Wold (2004) também chegou a conclusão semelhante, afirmando que o engajamento da gerência é um importante fator para se alcançar as condições apropriadas para tornar efetiva uma política de segurança. Uma das respostas dada na pesquisa qualitativa também apóia a seleção deste fator:

- "As administrações superiores das universidades não possuem conhecimento suficiente, na área de TI, para gerar a vontade de estabelecer políticas de segurança. É fato que, sem apoio da Reitoria, nada pode ser implantado, pois as IFES são as empresas com o maior número de donos e ao mesmo tempo não tem dono".

3. Elevada rotatividade de usuários. Observa-se que a maioria dos usuários de serviços de TIC nas universidades é formada por alunos que, sabidamente, permanecem vinculados à instituição por um tempo relativamente curto. A cada ano, aproximadamente ¼ dos estudantes são renovados. Possivelmente, esse curto período de tempo favorece a manutenção de laços frágeis dos alunos com a instituição, dificultando o comprometimento com os valores de segurança. Sennett (2005), discutindo a questão do compromisso e da lealdade em organizações empresariais contemporâneas, afirma que a inexistência de vínculos de longo prazo "é um princípio que corrói a confiança, a lealdade e o compromisso mútuo".

4. Os ambientes de TIC heterogênos. Observa-se nas universidades públicas uma grande variedade de plataformas de hardware e software, o que dificulta a implementação de medidas de segurança padronizadas e com grande repercussão. Por exemplo, a existência de plataformas de sistemas operacionais variadas (por exemplo, Linux e Windows), com diferentes versões instaladas e de distribuições diversificadas, dificulta manter os sistemas atualizados com os *patchs* de segurança mais recentes, bem como com um antivírus padrão atualizado. Também se torna difícil adotar padrões mínimos de segurança com o uso de *firewalls* e de sistemas para detecção de invasão. Por outro lado, os ambientes universitários são permissivos quanto à entrada de *notebooks*, mesmo sem estes atenderem aos requisitos de segurança que possam existir.

5. A autonomia administrativa das unidades organizacionais. Observa-se que os responsáveis por unidades organizacionais (centros, faculdades, departamentos, laboratórios de pesquisa, etc.), geralmente, decidem o que, como e quando fazer, mesmo em questões que afetem a segurança da informação. Em geral, o projeto, a implementação e a configuração da infra-estrutura e dos serviços de rede são realizados, nas unidades organizacionais, sem o conhecimento dos gestores ou responsáveis pela segurança no âmbito da organização. Torna-se difícil, portanto, impor às unidades organizacionais a implementação de boas práticas de segurança, dando seguimento a uma política de segurança. Trechos extraídos das respostas à pergunta aberta da pesquisa qualitativa, que corroboram a seleção deste fator, são mostrados a seguir:

- "A maior dificuldade de implantar uma política é a pluralidade e os conceitos de independência administrativas que ocorrem nos diversos departamentos, laboratórios dos ambientes universitários";
- "O fator mais crítico é o confrontamento entre a autoridade acadêmica e a autoridade do CSIRT, na ocorrência de um incidente de segurança.";
- "[...] as IFES são as empresas com o maior número de donos e ao mesmo tempo não têm dono algum. Cada Diretor, Chefe, Coordenador, Pró-Reitor e professor decide o que, como e quando fazer e se alguém tentar mudar ou sugerir algum controle, a resposta é sempre a mesma 'Este É MEU projeto (ou máquina, ou prédio, ou setor) e aqui quem decide sou EU' [...]";
- "[...] a rede [...] cresce desordenadamente com inclusão de equipamentos de baixa qualidade, cascateados de maneira inaceitável (já cheguei a encontrar 8 níveis), equipamentos estes colocados pelos donos dos locais".

Pode-se entender que a autonomia *de facto* das unidades organizacionais contribui negativamente para a efetividade da segurança da informação, pois dificulta a implementação de uma política de segurança institucional. Muitas vezes, esta autonomia não é aliada da responsabilidade pela própria segurança da unidade organizacional.

6. O treinamento dos usuários. O estudo realizado por Knapp *et al.* (2005) detectou que há uma influência significativa entre o apoio da cúpula administrativa e a percepção da efetividade da segurança da informação mediada pelo treinamento do usuário. A análise qualitativa realizada por Knapp *et al.* (2005) também reforça a importância do treinamento do usuário: as pessoas precisam ter consciência das conseqüências de suas a-

ções, mas somente aqueles educados para a segurança conseguem sê-lo. Sem usuários adequadamente treinados, fica difícil obter a colaboração deles em favor da segurança, mesmo quando há boa vontade. Abaixo seguem trechos das respostas dadas à pergunta aberta da pesquisa qualitativa que apóiam a seleção deste fator:

- "Uma educação dos usuários da comunidade da [omitido] com relação à segurança do seu próprio computador bem como da própria rede";
- "Treinamento de usuários";
- "A conscientização dos usuários";
- "[...] institucionalização da política para racionalizar o uso dos recursos, atestar periodicamente o seu cumprimento e manter um canal de comunicação com laboratórios de pesquisa, usuários de laboratórios e gerentes de rede dos setores, com o intuito de informar toda a comunidade acadêmica sobre uma definição de requisitos e procedimentos mínimos de segurança a serem adotados para minimizar o impacto das ameaças mais recentes".

7. A relevância da política de segurança da informação. Knapp *et al.* (2005) observaram que há uma influência significativa entre o apoio da cúpula administrativa e a percepção da efetividade da segurança da informação mediada pela relevância concedida a políticas de segurança da informação. Desprezar, não dar importância à política de segurança, certamente contribui para que a segurança não seja efetiva. Isso é corroborado nos trechos abaixo, extraídos da pesquisa qualitativa realizada:

- "[...] o principal argumento é que por ser um órgão acadêmico tudo deve ser permitido (até pirataria? e pornografia?) já se teve até a idéia de liberar e difundir a utilização de P2P como se praticamente tudo que circula na rede P2P não fosse ilegal";
- "Comprometimento dos funcionários da instituição com a política";
- "Comprometimento";
- "A conscientização dos usuários".

8. O cumprimento da política de segurança da informação. Knapp *et al.* (2005) observaram que há um influência significativa entre o apoio da cúpula administrativa e a percepção da efetividade da segurança da informação mediada pelo cumprimento da política de segurança da informação. A existência de uma política que não é cumprida certamente é um fator que afeta negativamente a efetividade da segurança da informação. Isso é corroborado nos trechos abaixo, extraídos da pesquisa qualitativa:

- "Acredito que o principal obstáculo ainda seja a resistência dos usuários em trabalhar de forma segura, muitas vezes por preferir a praticidade de uso ou por não ter esta cultura ainda formada";
- "Num ambiente em que os usuários não estão acostumados a seguir regras, sobretudo regras organizacionais que os obriguem a utilizar os recursos institucionais de forma mais responsável, a política de segurança soa como um inimigo a vista".

9. A cultura de segurança da informação. Knapp *et al.* (2005) observaram que há uma influência significativa entre o apoio da cúpula administrativa e a percepção da segurança da informação mediada pela cultura de segurança. A cultura de segurança se amalgama ao tecido social da organização, favorecendo a propagação e o cumprimento dos seus valores de segurança. Ambientes em que se pratica certa cultura naturalmente tendem a inibir um comportamento divergente. Portanto, a existência de uma cultura de segurança numa organização reforça a segurança. De modo inverso, um ambiente permissivo quanto a atitudes perigosas tende a reforçar a insegurança. Romper esta dinâmica exige grandes esforços. Trechos abaixo extraídos da pesquisa qualitativa corroboram esses argumentos:

- "A questão cultural da universidade. Toda medida restritiva ou definidora de regras não é bem recebida pela comunidade universitária";
- "eu penso que o fator determinante de sucesso é Regras e Limites Claros assim como o envolvimento dos usuários (eles se sentirem [...] que ou são parte da solução ou do problema)";

- "Acredito que um dos motivos que mais tem influência na questão de adotar políticas de segurança da informação é a cultura dos usuários".

10. A rigidez imposta a gestão de recursos humanos. É sabida a limitada autonomia que os dirigentes de universidades públicas têm na gestão de recursos humanos, em particular, na área de TIC. Salários pouco competitivos com aqueles pagos na iniciativa privada dificultam a retenção de bons profissionais, com qualificações especializadas, como os da área de segurança. Tem-se então elevada rotatividade de profissionais de TIC, agravada pela utilização de mão-de-obra temporária, formada por estagiários e bolsistas. A conseqüência é que os responsáveis pela TIC têm de lidar com quadros técnicos insuficientes, com baixo nível de especialização, pois todos têm de fazer tudo. Isso certamente influencia negativamente a segurança dessas organizações. Os trechos abaixo da pesquisa qualitativa corroboram esse ponto de vista:

- "Um outro agravante são os quadros deficitários de RH ligados a TI na maioria dos NTIs das IFES, bem como a enorme defasagem salarial em relação ao mercado. Isso dificulta a criação de equipes específicas voltadas a segurança (normalmente, quando se tem RH, são todos 'fazem tudo')";
- "[...] outra dificuldade é o número reduzido de pessoas, pois em nossa Instituição, na maioria das vezes, quem planeja, implementa e executa";
- "[...] nos deparamos com o fato de não haver profissionais experientes e com capacitação específica que implementem recursos nas redes que administram e que permitam o cumprimento da política de segurança instituída na universidade";
- "Outro problema é a falta de pessoal que por sua vez é conseqüência dos baixos salários. Não é possível gerir uma rede com mais de 4000 equipamentos e 20000 usuários apenas com bolsistas 12 horas semanais, aliás, nesta área, bolsista chega a ser mais um problema que uma solução".

3.2. Análise Fatorial Exploratória

Um total de 75 participantes, atuantes na área de TIC e com envolvimento em segurança da informação, respondeu ao questionário da pesquisa quantitativa. Para se reduzir as chances de se utilizar itens mal formulados, que de fato tenham sido interpretados com significado divergente dos demais pelos casos, efetuou-se uma análise de confiabilidade interna. A análise é útil para excluir os itens menos confiáveis, mantendo-se aqueles que têm boa contribuição para confiabilidade interna do questionário. Foi aplicada uma técnica estatística oferecida pelo SPPS chamada *estimação de confiabilidade interna alfa* (α) *de Cronbach*. A técnica estima o coeficiente de confiabilidade interna α como o valor médio de todos os coeficientes possíveis do tipo "split-half", fornecendo um índice que varia entre zero e um (Hill e Hill, 2005). Quanto mais próximo de um, mais eficazes são as variáveis que estão sendo testadas.

No questionário quantitativo têm-se dez variáveis componentes, que são medidas cada uma por cinco itens, perfazendo um total de 50 variáveis indicadoras (itens). Como só se conseguiu uma massa de dados correspondente a 75 casos, ficou-se com um número de casos insuficiente em relação ao número de variáveis indicadoras para que fosse possível aplicar a AFE. Para diminuir o número de variáveis indicadoras, aplicou-se aos itens de cada variável componente a técnica α de Cronbach com a opção "scale if item deleted" no SPSS. Essa opção calcula cinco vezes o valor de α, cada vez excluindo um dos cinco itens que compõem cada uma das dez variáveis componentes. Para o conjunto de itens que apresentou um valor de α mais próximo de um, mostrando que tem confiabilidade interna adequada, escolheram-se apenas as duas variáveis indicadoras que possuíam os maiores valores de correlação entre si. No caso, o conjunto de variáveis indicadoras foi reduzido de 50 para 18 (e não 20), pois os itens correspondentes ao fator organizacional "ambiente liberal" foram rejeitados por terem um coeficiente α inferior a 0,6. Com isso, o número de variáveis indicadoras tornou-se compatível com

número de casos na pesquisa: 4,2 casos para cada variável indicadora.

A análise fatorial exploratória tem o objetivo de encontrar combinações de variáveis (fatores) que expliquem correlações paramétricas (do tipo Pearson) entre todos os pares de variáveis de um conjunto de variáveis. Um dos pressupostos é que as variáveis estejam correlacionadas umas com as outras, o que implica, por sua vez, que as variáveis tenham relações lineares entre si. A AFE foi realizada utilizando o método da máxima verossimilhança com rotação oblíqua porque esse método tem a vantagem de usar uma estatística de "goodness of fit", que indica se os fatores obtidos explicam bem as correlações entre as variáveis. Também se utilizou a opção "exclude cases listwise" da AFE no SPSS para garantir que os dados utilizados na pesquisa fossem totalmente genuínos em todas as análises.

A Tabela 1 apresenta o valor da medida de adequação da amostra KMO (Kaiser-Mayer-Olkin). Kaiser e Rice (1974) sugeriram que um valor de KMO inferior a 0,5 é inaceitável para realizar uma análise fatorial. A Tabela 1 traz um valor de KMO aceitável (0,673) para a amostra deste trabalho, sendo portanto, razoável efetuar a AFE. O teste de profundidade de Bartlett apresenta outro enfoque sobre o tema. Testa a hipótese nula de que a matriz de correlações seja uma matriz diagonal, isto é, uma matriz com as correlações entre as variáveis iguais a zero. Quando o valor da estatística do χ^2 é significativo, então as correlações entre as variáveis são adequadas para se fazer a AFE. Como o resultado da Tabela 1 indica uma significância de 0,000, então é legítimo efetuar a análise fatorial também por esse critério.

Das 18 variáveis indicadoras, apenas 16 se mostraram adequadas para realização da AFE. Isto porque a MSA ("Measures of Sampling Adequacy" ou medida de adequação de amostra), correspondente a medida da diagonal da matriz anti-imagem de correlação (não mostrada) foi inferior a 0,5 para as variáveis ROTAT3 (terceiro item do fator organizacional elevada rotatividade de usuários) e RIGI5 (quinto item do fator organizacional rigidez imposta à gestão de recursos humanos). A AFE foi realizada com as demais 16 variáveis indicadoras.

A Tabela 2 indica (nas três primeiras colunas da metade direita) que a análise fatorial encontrou cinco fatores para explicar as correlações entre as 16 variáveis e que estes fatores explicam respectivamente (12,895%, 19,788%, 9,510%, 9,048% e 6,234%) a variância total no conjunto das 16 variáveis analisadas. Nas colunas da metade esquerda, temos os resultados dos autovalores (*Eigenvalues*) maiores do que 1, indicando cinco fatores obtidos na análise fatorial pelo método da máxima verossimilhança (4,351, 2,266, 1,773, 1,470 e 1,307), com 69,794% das variáveis totais explicadas na extração dos fatores pelo método considerado.

A Tabela 3 mostra, em ordem de maior influência, os cinco fatores obtidos da análise fatorial exploratória. Cada um dos fatores é composto de variáveis indicadoras (itens) correspondentes aos fatores organizacionais, com respectivas cargas fatoriais para explicar a variável dependente percepção da efetividade da segurança da informação em universidades públicas. Os fatores da AFE foram nomeados de acordo com as de variáveis indicadoras presentes, conforme listado a seguir:

Fator 1. Apoio dos dirigentes universitários. Fator com maior influência composto das variáveis **APOIO5** (quinto item do fator organizacional apoio dos dirigentes universitários), contribuindo com a carga fatorial de 0,983, seguida por **APOIO4** (quarto item do fator organizacional apoio dos dirigentes universitários), contribuindo com carga fatorial de 0,653, seguida por **CUTU4** (quarto item do fator organizacional cultura de segurança da informação), contribuindo com a carga fatorial de 0,411.

Tabela 1. KMO – Medida de adequação da amostra e teste de profundidade de Bartlett's

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		,673
Bartlett's Test of Sphericity	Approx. Chi-Square	436,383
	df	120
	Sig.	,000

Tabela 2. Total da variância explorada pelo método da máxima verossimilhança, explicado para análise fatorial exploratória

	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation
Factor	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total
1	4,351	27,196	27,196	2,063	12,895	12,895	2,236
2	2,266	14,161	41,356	3,166	19,788	32,683	2,787
3	1,773	11,083	52,439	1,522	9,510	42,193	2,724
4	1,470	9,188	61,627	1,448	9,048	51,241	2,311
5	1,307	8,167	69,794	,997	6,234	57,475	1,370
6	,806	5,038	74,832				
7	,781	4,879	79,711				
8	,682	4,260	83,971				
9	,523	3,271	87,241				
10	,479	2,993	90,235				
11	,395	2,471	92,706				
12	,336	2,100	94,806				
13	,275	1,722	96,528				
14	,231	1,441	97,969				
15	,198	1,235	99,204				
16	,127	,796	100,000				

Extraction Method: Maximum Likelihood.

a. When factors are correlated, sums of squared loadings cannot be added to obtain a total variance.

Tabela 3. Matriz estrutura (solução da pesquisa)

	Factor				
	1	2	3	4	5
APOIO5	,983				
APOIO4	,656				
CUTU4	,411				
RELE4		,932			
RELE2		,829			
CUMP1		,720			
TREI4			-,901		
TREI3			-,725		
CUMP2			-,652		
CUTU5			-,560		
AMBIE1				,806	
AMBIE4				,795	
AUTO3				,587	
AUTO1				,414	
RIGI2					,552
ROTAT2					,524

Extraction Method: Maximum Likelihood.
Rotation Method: Oblimin with Kaiser Normalization.

Fator 2. Importância e execução da política de segurança da informação. Fator composto das variáveis **RELE4** (quarto item do fator organizacional relevância da política de segurança da informação), contribuindo com 0,932, seguida pela variável **RELE2** (segundo item do fator organizacional relevância da política de segurança da informação), contribuindo com carga fatorial de 0,829, seguida pela variável **CUMP1** (primeiro item do fator organizacional cumprimento da política de segurança da informação), contribuindo com carga fatorial de 0,720.

Fator 3. Treinamento dos usuários. Fator composto das variáveis **TREI4** (quarto item do fator organizacional treinamento dos usuários), contribuindo com carga fatorial de -0,901, seguida pela variável **TREI3** (terceiro item do fator organizacional treinamento dos usuários), contribuindo com carga fatorial de -0,725, seguida da variável **CUMP2** (segundo item do fator organizacional cumprimento da política de segurança

da informação), contribuindo com carga fatorial de -0,652, seguida da variável **CUTU5** (quinto item do fator organizacional cultura de segurança da informação), contribuindo com carga fatorial de -0,560.

Fator 4. Autonomia administrativa e ambientes heterogêneos. Fator composto das variáveis **AMBIE1** (primeiro item do fator organizacional ambientes de TIC heterogêneos), contribuindo com carga fatorial de 0,806, seguida da variável **AMBIE4** (quarto item do fator organizacional ambientes de TIC heterogêneos), contribuindo com carga fatorial de 0,795, seguida da variável **AUTO3** (terceiro item do fator organizacional autonomia administrativa das unidades organizacionais), contribuindo com carga fatorial de 0,587, seguida pela variável **AUTO1** (primeiro item do fator organizacional autonomia administrativa das unidades organizacionais), contribuindo com carga fatorial de 0,414.

Fator 5. Gestão de recursos humanos. Fator composto das variáveis **RIGI2** (segundo item do fator organizacional rigidez imposta à gestão de recursos humanos), contribuindo com carga fatorial de 0,552, seguida da variável **ROTAT2** (segundo item do fator organizacional elevada rotatividade de usuários), contribuindo com carga fatorial de 0,524.

4. Discussão

O Fator 1 (apoio dos dirigentes universitários) foi revelado pela AFE como o fator de maior influência para explicar a efetividade de segurança da informação em universidades públicas, segundo a percepção dos profissionais de TIC das 46 instituições que participaram da pesquisa. Esse achado é compatível com aqueles de estudos empíricos similares realizados em organizações empresariais. Os resultados quantitativos da pesquisa realizada por Knapp *et al.* (2005) sugerem que o apoio da cúpula administrativa é essencial para efetividade da segurança da informação numa organização. Em outro estudo, Knapp *et al.* (2006) concluem que é incumbência da cúpula administrativa prover a liderança para quebrar barreiras culturais e organizacionais a fim de forçar a colaboração relativa à segurança. Chang e Ho (2006) acharam em seu estudo que a competência em TIC dos gerentes de negócio está positivamente associada à implementação da gestão de segurança da informação através de normas tácitas, liderança, crenças e comportamento. Em sua dissertação, Wold (2004) identificou o engajamento da gerência como um fator chave para implementação de políticas de segurança efetivas.

Os dois fatores seguintes (Fator 2 e Fator 3), em ordem de importância, também são compatíveis com os achados da literatura para organizações empresariais, que evidenciaram a influência do apoio da cúpula administrativa na percepção da efetividade da segurança da informação mediada pela relevância e cumprimento da política de segurança e pelo treinamento dos usuários (Knapp *et al.*, 2005, 2006).

Os fatores restantes (Fator 4 e Fator 5) identificados na AFE como influentes para explicar a percepção da efetividade da segurança da informação não são encontrados nos estudos empíricos similares realizados em ambientes empresariais. Postulamos que tais fatores são peculiares a universidades públicas. Em relação ao Fator 4, pode-se interpretar que há uma relação entre autonomia administrativa e ambientes heterogêneos porque, se numa unidade organizacional cada um age conforme deseja, então fica difícil impor ambientes de hardware e software mais homogêneos, ampliando a sensação de insegurança para os que têm a responsabilidade de manter a segurança nessas instituições. Em relação ao Fator 5, pode-se interpretar que a rigidez imposta à gestão de recursos humanos leva os responsáveis pela TIC nas universidades públicas a lidar com profissionais com vínculo precário, como bolsistas e estagiários, com qualificação insufici-

ente, resultando em elevada rotatividade. Isso possivelmente reduz a confiança entre os responsáveis pela TIC e seus subordinados, levando esse fator a influenciar na percepção da efetividade da segurança da informação.

5. Conclusão

Os fatores organizacionais identificados neste estudo como mais relevantes para explicar a percepção da efetividade da segurança da informação em universidades públicas são compatíveis com estudos empíricos similares realizados em empresas, apesar das universidades públicas terem um caráter específico de ensino, pesquisa e extensão. Os resultados obtidos permitem recomendar que qualquer medida de melhoria nos aspectos de segurança da informação no ambiente de uma universidade pública ocorra em sintonia com a administração superior, dado que a análise fatorial exploratória apresentou a variável apoio dos dirigentes universitários com maior carga fatorial, explicando sozinha 27,19% da variância observada. Sugerem, portanto, que uma boa política de segurança da informação (Fator 2) e o treinamento adequado de usuários (Fator 3) dependem do apoio dos dirigentes para melhorar a situação das TICs nas universidades públicas. Em menor grau de influência para explicar a efetividade da segurança da informação, encontramos fatores peculiares a universidades públicas, como autonomia administrativa, ambientes heterogêneos e rigidez imposta à gestão de recursos humanos.

Agradecimentos

Agradecemos aos profissionais da área de tecnologia da informação de 46 universidades públicas de todas as regiões do Brasil que participaram desta pesquisa.

Referências

Chang, S. E.; Ho, C. B. Organizational factors to the effectiveness of implementing information security management. Industrial Management & Data Systems, v. 106, n. 3, p. 345-361, 2006.

Hill, M. M.; Hill, A. Investigação por questionário. 2ª Ed. Silabo, Lisboa. 2005

Kaiser, H. F.; Rice, J. Little Jiffy Mark IV. Educational and Psychological Measurement, v. 34 (Spring), p. 111-117, 1974.

Kaplan, B.; Duchon, D. Combining qualitative and quantitative methods in information systems research: a case study. MIS Quartely, v. 12, n. 4, p. 571-587, 1988.

Knapp, K. J.; Marshall, T. E.; Rainer, R. K.; Ford, F. N. Information security: management's effect on culture and policy. Information Management & Computer Security, v. 14, n. 1, p. 24-36, 2006.

Knapp, K. J.; Marshall, T. E.; Rainer, R. K.; Ford, F. N. Managerial dimensions in information security: a theoretical model of organizational effectiveness. October 25, 2005. $(ISC)^2$ Inc., Palm Harbor, Florida and Auburn University, Auburn, Alabama.

Kotulic, A. G.; Clark J. G. Why there aren't more information security research studies. Information & Management, v. 41, n. 5, p. 597-607, 2004.

Nakamura, E. T.; Geus, P. L. Segurança de rede. 2ª Ed. Futura, São Paulo, 2004.

Rennie, K. M. Exploratory and Confirmatory Rotation Strategies in Exploratory Factor Analysis. In: Annual Meeting of the Southwest Educational Research Association, 1997. **Proceedings…** p. 1-26.

Sennett, R. A Corrosão do caráter: conseqüências pessoais do trabalho no novo capitalismo. 10ª Ed. Record, Rio de Janeiro. 2005.

Sharma, S. Applied Multivariate Techniques. Wiley, New York. 1996.

Wold, G. Key factors in making information segurity policies effective. Dissertação de Mestrado. NISlab Norwegian Information Security Laboratory, 2004.